Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale — temi e correzione

Mauro Brunato

Mercoledì 7 giugno 2017

Contenuti

- Testi dei temi d'esame
- Traccia della soluzione dei primi due esercizi del Tema 1
- Risposte corrette e commentate alle domande dell'ultimo esercizio
- Griglie di correzione dei temi

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato

Tema 1

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
4. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
5. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
6. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
8. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato

Tema 2

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
2. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Considera la chiave non valida.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
3. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
5. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) La suriettività.
   (c) L'iniettività.
6. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 3

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
3. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
5. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) La suriettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato

Tema 4

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 9$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
3. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
4. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
5. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) La suriettività.
   (c) L'iniettività.
6. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 5

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
4. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
5. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
7. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
8. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato

Tema 6

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
3. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
4. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
5. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
6. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
8. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Considera la chiave non valida.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato

Tema 7

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
5. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
6. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Considera la chiave non valida.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) La suriettività.
   (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 8

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
2. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
3. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta...
   (a) ...è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) ...è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) ...è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Considera la chiave non valida.
5. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
6. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) La suriettività.
   (c) L'iniettività.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 9

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
3. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine.
4. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
5. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Considera la chiave non valida.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
8. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 10

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
4. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
5. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
6. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 11

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
2. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
3. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
5. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) La suriettività.
   (c) L'iniettività.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
8. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 12

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 9$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
4. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
5. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
6. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
7. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 13

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
4. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
5. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
6. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
7. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 14

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
2. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
3. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
5. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
6. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 15

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
3. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
5. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
8. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 16

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
2. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
4. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
5. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
6. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 17

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
2. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
4. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
5. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Considera la chiave non valida.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
6. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
8. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 18

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Considera la chiave non valida.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
4. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
5. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
6. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
7. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.
8. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 19

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
2. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
4. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
7. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) La suriettività.
   (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 20

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
3. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
4. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
5. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
6. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 21

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Considera la chiave non valida.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
2. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
3. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
4. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
8. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 22

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
4. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
5. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
7. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 23

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
2. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) La suriettività.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
4. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
6. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
7. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
8. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 24

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
3. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
4. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
6. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 25

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
2. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
5. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta...
   (a) ...è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) ...è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) ...è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
6. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
7. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 26

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
3. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
4. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
6. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
8. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Considera la chiave non valida.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 27

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
2. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
3. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
5. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 28

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
2. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
3. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
6. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
8. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 29

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Considera la chiave non valida.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
3. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
4. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
6. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) La suriettività.
   (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 30

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
3. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
5. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
7. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 31

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
3. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
5. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
6. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) La suriettività.
7. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
8. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 32

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Considera la chiave non valida.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
5. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
6. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
7. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 33

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
2. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
6. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 34

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
3. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
5. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
6. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
7. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
8. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 35

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
2. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
3. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta...
   (a) ...è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) ...è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) ...è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
4. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
6. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
8. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 36

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 9$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
2. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Considera la chiave non valida.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
4. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
6. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
7. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 37

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
2. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
4. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
5. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
6. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
7. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 38

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
4. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
6. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
7. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
8. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 39

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
4. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
5. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
7. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 40

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
2. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
3. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta...
   (a) ...è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) ...è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) ...è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
5. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
6. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 41

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
4. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta...
   (a) ...è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) ...è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) ...è necessario che né Alice né Bob divulghino il proprio numero segreto.
5. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
6. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.
7. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Considera la chiave non valida.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
8. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 42

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
5. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
6. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
7. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 43

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
4. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
5. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
8. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 44

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
3. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
4. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
6. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 45

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
4. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
6. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
7. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 46

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
4. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
6. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
7. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) La suriettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 47

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
2. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
4. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
6. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 48

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
2. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
3. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
5. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta...
   (a) ...è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) ...è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) ...è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
6. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 49

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
4. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
5. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
6. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 50

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
2. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Considera la chiave non valida.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
6. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
8. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 51

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
5. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
7. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine.
8. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 52

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
3. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta...
   (a) ...è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) ...è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) ...è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
6. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) La suriettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 53

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
4. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
5. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
6. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
7. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 54

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 9$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
2. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
3. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
5. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
7. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
8. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 55

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 9$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
3. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta...
   (a) ...è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) ...è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) ...è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
5. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
6. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 56

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
2. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
3. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
5. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
6. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 57

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
2. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
3. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
4. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
7. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
8. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 58

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
2. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
3. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
5. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
6. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 59

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
4. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
5. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
7. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 60

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 9$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
3. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta...
   (a) ...è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) ...è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) ...è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
5. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
6. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
7. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
8. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 61

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
4. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) La suriettività.
5. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
8. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 62

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
2. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
3. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
5. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
8. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 63

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
3. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
5. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta...
   (a) ...è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) ...è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) ...è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
6. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
7. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 64

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
4. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
6. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
7. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) La suriettività.
   (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 65

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
2. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
3. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
5. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
6. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Considera la chiave non valida.
7. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 66

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
2. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
3. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
5. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
7. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
8. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 67

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
6. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) La suriettività.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
8. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 68

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Considera la chiave non valida.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
6. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
7. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) La suriettività.
   (c) L'iniettività.
8. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 69

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 9$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
3. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.
4. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
6. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
7. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
8. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 70

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
2. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
3. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
4. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) La suriettività.
   (c) L'iniettività.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 71

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 9$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
4. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
5. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine.
6. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 72

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) L'iniettività.
2. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
4. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta...
   (a) ...è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) ...è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) ...è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
6. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
7. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
8. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 73

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 7$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
2. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Considera la chiave non valida.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
7. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) La suriettività.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 74

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
3. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
4. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
5. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) La suriettività.
6. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 75

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
4. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) La determinazione dell'initialization vector.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
5. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
6. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
7. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 76

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
3. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (b) Considera la chiave non valida.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
4. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
5. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
6. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
7. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.
8. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 77

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 5$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
2. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine.
   (c) La suriettività.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
4. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Non deve fare nulla, il certificato può essere verificato comunque.
   (c) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
5. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
7. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
8. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 78

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
2. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La determinazione dell'initialization vector.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
4. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
6. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine.
   (b) L'iniettività.
   (c) La suriettività.
7. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La determinazione dell'initialization vector.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La fattorizzazione di un prodotto di grandi numeri primi.
8. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 79

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$.

1.1) Dimostrare che uno dei due interi $g_1 = 3$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 3$ e $b = 6$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Considera la chiave non valida.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Non deve fare nulla, il certificato può essere verificato comunque.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
3. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
   (c) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
4. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
5. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
6. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) La determinazione dell'initialization vector.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Mauro Brunato
Tema 80

Mercoledì 7 giugno 2017

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$.

1.1) Dimostrare che uno dei due interi $g_1 = 4$ e $g_2 = 2$ è un generatore primo per p, mentre l'altro no.
Alice e Bob scelgono, ovviamente, il generatore primo.

1.2) Supponiamo che i valori segreti generati da Alice e da Bob siano rispettivamente $a = 2$ e $b = 8$.
Quali valori pubblici A e B verranno comunicati?

1.3) Qual è la chiave K generata con questo protocollo?
Calcolarla dal punto di vista di Alice oppure da quello di Bob, a seconda di quale risulti più facile.

Esercizio 2

Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile.
Il server web di Alice applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit.
In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.
Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash richieda un miliardesimo di secondo.
La risposta alla domanda 2.1 cambia?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?
   (a) Non deve fare nulla, il certificato può essere verificato comunque.
   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.
   (c) Considera la chiave non valida.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
3. Qual è il problema, considerato difficile, alla base del cifrario RSA?
   (a) La determinazione dell'initialization vector.
   (b) La fattorizzazione di un prodotto di grandi numeri primi.
   (c) L'inversione dell'elevamento a potenza modulo un grande numero primo.
4. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?
   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.
   (b) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.
   (c) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.
5. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?
   (a) La fattorizzazione di un prodotto di grandi numeri primi.
   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.
   (c) La determinazione dell'initialization vector.
6. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…
   (a) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.
   (b) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.
   (c) …è necessario che né Alice né Bob divulghino il proprio numero segreto.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine.

Traccia della soluzione all'esercizio 1 (tema 1)

1.1 — Determinazione del generatore primo

Se proviamo le potenze successive di $g_1 = 4$ modulo $p = 13$, otteniamo $4^6 \equiv 1$, e da qui la sequenza si ripete. Invece, le potenze di $g_2 = 2$ generano tutti i valori da 1 a $p - 1 = 12$. Il generatore primo è dunque $g_2 = 2$.

1.2 — Calcolo dei valori pubblici di Alice e Bob

Applichiamo le formule, basandoci sulle potenze che abbiamo calcolato al punto 1:

$$A = g_2^a = 2^3 \equiv 8 \pmod{13};$$

$$B = g_2^b = 2^8 \equiv 9 \pmod{13}.$$

1.3 — Chiave condivisa

Possiamo calcolare K in due modi:

$$K \equiv A^b \equiv B^a \pmod{13}$$

Ad esempio,

$$K = B^a = 9^3 \equiv 1 \pmod{13}.$$

Osservazioni

Si noti che l'esercizio richiedeva espressamente di verificare entrambi i valori g_1 e g_2, non di procedere per esclusione una volta controllato il primo.
Anche la chiave K va calcolata modulo p.

Traccia della soluzione all'esercizio 2 (tema 1)

2.1 — Tempo per un attacco brute force

Charlie non ne sa nulla della funzione H, ovviamente non conosce h_{Bob}, e possiamo assumere che non conosca nemmeno la dimensione dell'hash generato. Tutto quello che può fare è generare password in sequenza e spedirle al server, sperando che una delle password P sia in collisione con quella di Bob:

$$H(P) = h_{\text{Bob}}.$$

Dato che i valori hash possibili sono 2^{32}, la probabilità di una collisione ad ogni tentativo è 2^{-32}, quindi saranno necessari mediamente 2^{32} tentativi. Si noti che Charlie può generare password sempre diverse, ma non può sperare che gli hash generati siano tutti diversi.

Potendo controllare 10^3 password al secondo, il tempo medio per arrivare a una collisione è

$$2^{32} \cdot 10^{-3} = 2^2 \cdot 2^{30} \cdot 10^{-3} \approx 4 \cdot 10^9 \cdot 10^{-3} = 4 \cdot 10^6 \text{s}.$$

Siccome in un giorno ci sono $86400 \approx 10^5$ secondi, Charlie impiegherà circa 40 giorni a trovare una collisione che gli permetta di assumere l'identità di Bob.

2.2 — Dipendenza dalla lunghezza della password

La risposta precedente non dipende dalla lunghezza della password di Bob, ma solo dal numero di bit dell'hash e dalla velocità con cui possono essere provati. Infatti, Charlie non ha bisogno di trovare la password di Bob, ma un valore che generi lo stesso hash.

2.3 — Conoscenza della funzione di hash

Anche se Charlie è ora in grado di calcolare 10^9 hash al secondo, non conoscendo h_{Bob} non può farsene molto. Il collo di bottiglia rimane sempre il tempo di avvio della sessione di login, quindi Charlie è vincolato a provare 1000 password al secondo.

In realtà, Charlie può utilizzare la propria capacità di calcolare a priori gli hash delle password prima di inviarle al server, escludendo quelle che collidono con password già provate. In questo modo, i 2^{32} hash possibili sono tentati senza ripetizione, e il numero medio di tentativi necessari si dimezza. Questa osservazione non era comunque necessaria per ottenere il punteggio pieno.

Osservazioni

Gil errori dovuti ad approssimazioni numeriche sono ovviamente stati perdonati, così pure eventuali dimezzamenti nella stima dei tempi dovuti a errate interpretazioni della probabilità.

Esercizio 3 — domande a risposta multipla

Nel seguito, la prima risposta è sempre quella corretta; nella prima domanda, le risposte a e b sono state considerate entrambe corrette.

1. Qual è il problema, considerato difficile, alla base del cifrario RSA?

   (a) La fattorizzazione di un prodotto di grandi numeri primi.

   (b) L'inversione dell'elevamento a potenza modulo un grande numero primo.

   (c) La determinazione dell'initialization vector.

   RSA consiste nell'elevamento a potenza modulo un grande numero (anche se non primo), e l'operazione è invertibile con facilità solo conoscendone i fattori. La risposta a è preferibile, ma la b è (quasi) corretta. Un initialization vector è tutt'altra cosa.

2. Alice e Bob avviano una sessione Diffie-Hellman; Charlie può solo ascoltare i loro messaggi; affinché la chiave condivisa resti segreta…

   (a) …è necessario che né Alice né Bob divulghino il proprio numero segreto.

   (b) …è sufficiente Alice, che ha iniziato il protocollo, non divulghi il proprio numero segreto.

   (c) …è sufficiente che Bob, che risponde ad Alice, non divulghi il proprio numero segreto.

   Come abbiamo visto nell'esercizio 1, è sufficiente conoscere uno dei due segreti per calcolare la chiave.

3. Bob deve verificare l'autenticità della chiave pubblica di Alice, corredata di certificato, ma non è in grado di contattare la certification authority che l'ha firmato. Cosa può fare?

   (a) Non deve fare nulla, il certificato può essere verificato comunque.

   (b) Si rivolge alla certification authority di livello superiore nella gerarchia, oppure a una root certification authority.

   (c) Considera la chiave non valida.

   Il meccanismo delle certificazioni e delle certification authorities è progettato al preciso scopo di rendere possibile la verifica dei certificati senza il bisogno di comunicare con terze parti: Bob procede alla verifica in proprio, senza il bisogno di contattare una certification authority. Le autorità di livello superiore non servono da backup.

4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?

   (a) La chiave privata del richiedente.

   (b) La chiave pubblica del richiedente.

   (c) Il common name del richiedente.

   Un certificato serve a garantire l'associazione tra un'identità e una chiave pubblica, quindi entrambe le informazioni devono essere presenti nella richiesta di firma. Al contrario, una chiave privata non deve mai, per messun motivo, essere trasmessa.

5. Qual è il problema, considerato difficile, alla base del protocollo Diffie-Hellman?

   (a) L'inversione dell'elevamento a potenza modulo un grande numero primo.

   (b) La fattorizzazione di un prodotto di grandi numeri primi.

   (c) La determinazione dell'initialization vector.

   La segretezza di Diffie-Hellman si basa sulla difficoltà di invertire l'elevamento a potenza.

6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?

   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.

(b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.

(c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.

I due termini si riferiscono all'eventuale concatenazione tra cifrature di blocchi successivi di uno stesso messaggio per evitare che blocchi uguali generino codici uguali. L'aggiunta del padding è considerata meno critica. Per quanto riguarda la decisione se utilizzare un one-time pad, non è applicabile, visto parliamo di cifrari a blocchi.

7. Quale delle seguenti affermazioni relative ai cifrari a flusso (stream cipher) **non** è vera?

   (a) Richiedono la generazione di sequenze (pseudo-) casuali, quindi non erano praticabili prima dell'avvento degli elaboratori elettronici.

   (b) Idealmente, la chiave dev'essere un flusso potenzialmente illimitato di simboli (per es. bit) casuali.

   (c) In molte applicazioni, una chiave di dimensioni limitate viene usata per inizializzare un generatore di numeri pseudocasuali.

   Esistono molti esempi di cifrari a flusso non basati su calcolatori elettronici: il cifrario di Vernam, Enigma, gli one-time pad cartacei... La seconda risposta è sostanzialmente la definizione di cifrario a flusso, e in molti casi i generatori pseudocasuali sono inizializzati con chiavi di dimensione limitata (gli "initialization vector").

8. Quale delle seguenti proprietà non è posseduta da nessuna funzione hash crittografica?

   (a) L'iniettività.

   (b) La suriettività.

   (c) La resistenza agli attacchi di preimmagine.

   Le funzioni hash hanno un dominio infinito e un codominio finito, quindi è impossibile che associno valori diversi a tutti gli input.

Griglie di soluzione

Sono elencati, per ogni tema:

- i valori pubblici A e B e la chiave K ottenuti con l'esercizio 1;
- il numero di tentativi N e il tempo richiesto T per l'esercizio 2;
- l'elenco delle risposte corrette alle domande dell'ultimo esercizio (salvo obiezioni ammissibili, vedi pagine precedenti).

```
1
 p = 13; g1 = 4; g2 = 2; a = 3; b = 8; A = 8; B = 9; K = 1
 bit = 32; N = 4294967296; T = 429496729.6
 1.a 2.ab 3.a 4.c 5.c 6.c 7.c 8.c
2
 p = 13; g1 = 3; g2 = 2; a = 3; b = 8; A = 8; B = 9; K = 1
 bit = 30; N = 1073741824; T = 107374182.4
 1.a 2.a 3.c 4.a 5.c 6.bc 7.c 8.b
3
 p = 11; g1 = 3; g2 = 2; a = 2; b = 6; A = 4; B = 9; K = 4
 bit = 26; N = 67108864; T = 6710886.4
 1.a 2.bc 3.a 4.a 5.c 6.b 7.b 8.a
4
 p = 13; g1 = 3; g2 = 2; a = 2; b = 9; A = 4; B = 5; K = 12
 bit = 26; N = 67108864; T = 6710886.4
 1.a 2.a 3.b 4.a 5.c 6.bc 7.b 8.b
5
 p = 11; g1 = 3; g2 = 2; a = 2; b = 6; A = 4; B = 9; K = 4
 bit = 28; N = 268435456; T = 26843545.6
 1.a 2.b 3.b 4.c 5.b 6.c 7.c 8.bc
6
 p = 11; g1 = 5; g2 = 2; a = 2; b = 7; A = 4; B = 7; K = 5
 bit = 24; N = 16777216; T = 1677721.6
 1.c 2.b 3.c 4.a 5.ac 6.c 7.b 8.b
7
 p = 13; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 12; K = 12
 bit = 24; N = 16777216; T = 1677721.6
 1.a 2.bc 3.b 4.a 5.c 6.a 7.a 8.c
8
 p = 13; g1 = 5; g2 = 2; a = 3; b = 8; A = 8; B = 9; K = 1
 bit = 32; N = 4294967296; T = 429496729.6
 1.b 2.b 3.b 4.b 5.ac 6.c 7.c 8.a
9
 p = 11; g1 = 4; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
 bit = 28; N = 268435456; T = 26843545.6
 1.a 2.b 3.b 4.bc 5.b 6.b 7.a 8.a
10
 p = 11; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
 bit = 30; N = 1073741824; T = 107374182.4
 1.bc 2.c 3.b 4.c 5.a 6.b 7.b 8.c
11
 p = 13; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 12; K = 12
 bit = 24; N = 16777216; T = 1677721.6
 1.a 2.a 3.b 4.a 5.c 6.a 7.a 8.ac
12
 p = 13; g1 = 4; g2 = 2; a = 2; b = 9; A = 4; B = 5; K = 12
 bit = 28; N = 268435456; T = 26843545.6
```

1.a 2.c 3.b 4.c 5.bc 6.a 7.a 8.b
13
p = 11; g1 = 4; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
bit = 24; N = 16777216; T = 1677721.6
1.a 2.b 3.a 4.b 5.a 6.bc 7.b 8.b
14
p = 11; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
bit = 32; N = 4294967296; T = 429496729.6
1.ac 2.a 3.c 4.a 5.c 6.b 7.c 8.c
15
p = 13; g1 = 3; g2 = 2; a = 2; b = 6; A = 4; B = 12; K = 1
bit = 28; N = 268435456; T = 26843545.6
1.b 2.bc 3.b 4.a 5.a 6.c 7.c 8.b
16
p = 11; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
bit = 26; N = 67108864; T = 6710886.4
1.a 2.c 3.c 4.c 5.ab 6.c 7.c 8.c
17
p = 13; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 12; K = 12
bit = 26; N = 67108864; T = 6710886.4
1.a 2.b 3.b 4.a 5.a 6.b 7.a 8.ab
18
p = 11; g1 = 3; g2 = 2; a = 2; b = 7; A = 4; B = 7; K = 5
bit = 24; N = 16777216; T = 1677721.6
1.a 2.c 3.a 4.b 5.b 6.bc 7.a 8.b
19
p = 11; g1 = 5; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
bit = 30; N = 1073741824; T = 107374182.4
1.a 2.a 3.a 4.ab 5.a 6.a 7.a 8.c
20
p = 11; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
bit = 32; N = 4294967296; T = 429496729.6
1.b 2.a 3.a 4.c 5.b 6.ab 7.b 8.c
21
p = 11; g1 = 4; g2 = 2; a = 2; b = 7; A = 4; B = 7; K = 5
bit = 28; N = 268435456; T = 26843545.6
1.a 2.c 3.a 4.ab 5.a 6.a 7.a 8.a
22
p = 11; g1 = 4; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
bit = 32; N = 4294967296; T = 429496729.6
1.a 2.c 3.a 4.b 5.bc 6.a 7.c 8.b
23
p = 11; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
bit = 30; N = 1073741824; T = 107374182.4
1.c 2.a 3.a 4.c 5.a 6.ac 7.c 8.b
24
p = 13; g1 = 5; g2 = 2; a = 2; b = 7; A = 4; B = 11; K = 4
bit = 32; N = 4294967296; T = 429496729.6
1.c 2.b 3.c 4.b 5.c 6.ac 7.b 8.b
25
p = 11; g1 = 4; g2 = 2; a = 2; b = 6; A = 4; B = 9; K = 4
bit = 26; N = 67108864; T = 6710886.4
1.a 2.c 3.c 4.b 5.a 6.b 7.ab 8.a
26
p = 13; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 12; K = 12
bit = 32; N = 4294967296; T = 429496729.6
1.b 2.a 3.bc 4.b 5.b 6.b 7.a 8.a

27
p = 13; g1 = 3; g2 = 2; a = 2; b = 8; A = 4; B = 9; K = 3
bit = 28; N = 268435456; T = 26843545.6
1.ab 2.b 3.b 4.c 5.c 6.c 7.a 8.c
28
p = 13; g1 = 5; g2 = 2; a = 2; b = 7; A = 4; B = 11; K = 4
bit = 24; N = 16777216; T = 1677721.6
1.b 2.c 3.c 4.c 5.a 6.bc 7.c 8.b
29
p = 11; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
bit = 24; N = 16777216; T = 1677721.6
1.a 2.a 3.c 4.ab 5.c 6.b 7.b 8.c
30
p = 13; g1 = 3; g2 = 2; a = 3; b = 8; A = 8; B = 9; K = 1
bit = 26; N = 67108864; T = 6710886.4
1.c 2.c 3.c 4.b 5.a 6.c 7.ab 8.c
31
p = 11; g1 = 3; g2 = 2; a = 2; b = 6; A = 4; B = 9; K = 4
bit = 26; N = 67108864; T = 6710886.4
1.a 2.a 3.c 4.b 5.b 6.a 7.a 8.bc
32
p = 13; g1 = 4; g2 = 2; a = 3; b = 6; A = 8; B = 12; K = 12
bit = 30; N = 1073741824; T = 107374182.4
1.a 2.ab 3.a 4.a 5.b 6.a 7.c 8.c
33
p = 13; g1 = 5; g2 = 2; a = 2; b = 8; A = 4; B = 9; K = 3
bit = 26; N = 67108864; T = 6710886.4
1.ac 2.c 3.a 4.c 5.a 6.b 7.a 8.a
34
p = 13; g1 = 3; g2 = 2; a = 3; b = 7; A = 8; B = 11; K = 5
bit = 30; N = 1073741824; T = 107374182.4
1.b 2.b 3.bc 4.b 5.a 6.b 7.b 8.b
35
p = 13; g1 = 4; g2 = 2; a = 3; b = 8; A = 8; B = 9; K = 1
bit = 28; N = 268435456; T = 26843545.6
1.b 2.b 3.b 4.c 5.c 6.c 7.a 8.ac
36
p = 13; g1 = 5; g2 = 2; a = 2; b = 9; A = 4; B = 5; K = 12
bit = 26; N = 67108864; T = 6710886.4
1.b 2.b 3.b 4.a 5.a 6.b 7.bc 8.c
37
p = 13; g1 = 4; g2 = 2; a = 2; b = 8; A = 4; B = 9; K = 3
bit = 26; N = 67108864; T = 6710886.4
1.a 2.b 3.c 4.a 5.a 6.b 7.bc 8.a
38
p = 11; g1 = 5; g2 = 2; a = 2; b = 7; A = 4; B = 7; K = 5
bit = 26; N = 67108864; T = 6710886.4
1.c 2.a 3.c 4.c 5.a 6.c 7.b 8.ac
39
p = 13; g1 = 3; g2 = 2; a = 3; b = 8; A = 8; B = 9; K = 1
bit = 24; N = 16777216; T = 1677721.6
1.a 2.c 3.b 4.a 5.b 6.c 7.bc 8.b
40
p = 13; g1 = 4; g2 = 2; a = 3; b = 6; A = 8; B = 12; K = 12
bit = 28; N = 268435456; T = 26843545.6
1.a 2.c 3.b 4.c 5.b 6.ab 7.c 8.c
41

p = 11; g1 = 5; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
bit = 26; N = 67108864; T = 6710886.4
1.bc 2.a 3.a 4.c 5.c 6.a 7.a 8.b
42
p = 13; g1 = 5; g2 = 2; a = 2; b = 8; A = 4; B = 9; K = 3
bit = 30; N = 1073741824; T = 107374182.4
1.b 2.c 3.b 4.c 5.c 6.c 7.ab 8.c
43
p = 13; g1 = 4; g2 = 2; a = 3; b = 6; A = 8; B = 12; K = 12
bit = 26; N = 67108864; T = 6710886.4
1.ac 2.a 3.b 4.c 5.b 6.c 7.a 8.a
44
p = 13; g1 = 5; g2 = 2; a = 3; b = 7; A = 8; B = 11; K = 5
bit = 28; N = 268435456; T = 26843545.6
1.ab 2.b 3.a 4.b 5.b 6.b 7.b 8.b
45
p = 13; g1 = 5; g2 = 2; a = 2; b = 6; A = 4; B = 12; K = 1
bit = 30; N = 1073741824; T = 107374182.4
1.a 2.c 3.a 4.a 5.c 6.c 7.ab 8.c
46
p = 13; g1 = 3; g2 = 2; a = 3; b = 7; A = 8; B = 11; K = 5
bit = 32; N = 4294967296; T = 429496729.6
1.c 2.c 3.b 4.a 5.c 6.c 7.ac 8.a
47
p = 11; g1 = 5; g2 = 2; a = 2; b = 6; A = 4; B = 9; K = 4
bit = 24; N = 16777216; T = 1677721.6
1.bc 2.c 3.b 4.b 5.b 6.c 7.b 8.a
48
p = 13; g1 = 4; g2 = 2; a = 3; b = 6; A = 8; B = 12; K = 12
bit = 26; N = 67108864; T = 6710886.4
1.c 2.c 3.c 4.a 5.b 6.ac 7.b 8.a
49
p = 13; g1 = 4; g2 = 2; a = 2; b = 8; A = 4; B = 9; K = 3
bit = 32; N = 4294967296; T = 429496729.6
1.b 2.ac 3.b 4.a 5.b 6.b 7.b 8.a
50
p = 11; g1 = 4; g2 = 2; a = 2; b = 6; A = 4; B = 9; K = 4
bit = 32; N = 4294967296; T = 429496729.6
1.a 2.b 3.c 4.a 5.c 6.a 7.c 8.ab
51
p = 11; g1 = 4; g2 = 2; a = 2; b = 6; A = 4; B = 9; K = 4
bit = 24; N = 16777216; T = 1677721.6
1.a 2.b 3.a 4.b 5.c 6.c 7.b 8.ab
52
p = 13; g1 = 4; g2 = 2; a = 3; b = 7; A = 8; B = 11; K = 5
bit = 24; N = 16777216; T = 1677721.6
1.a 2.bc 3.a 4.a 5.c 6.b 7.a 8.a
53
p = 13; g1 = 4; g2 = 2; a = 3; b = 7; A = 8; B = 11; K = 5
bit = 24; N = 16777216; T = 1677721.6
1.a 2.bc 3.b 4.b 5.b 6.c 7.b 8.c
54
p = 13; g1 = 5; g2 = 2; a = 2; b = 9; A = 4; B = 5; K = 12
bit = 26; N = 67108864; T = 6710886.4
1.b 2.c 3.a 4.b 5.b 6.c 7.bc 8.a
55
p = 13; g1 = 5; g2 = 2; a = 2; b = 9; A = 4; B = 5; K = 12

```
 bit = 28; N = 268435456; T = 26843545.6
 1.a 2.bc 3.a 4.b 5.c 6.b 7.c 8.a
56
 p = 11; g1 = 4; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
 bit = 24; N = 16777216; T = 1677721.6
 1.b 2.a 3.b 4.c 5.a 6.ac 7.a 8.c
57
 p = 13; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 12; K = 12
 bit = 30; N = 1073741824; T = 107374182.4
 1.a 2.c 3.c 4.c 5.c 6.b 7.a 8.bc
58
 p = 13; g1 = 3; g2 = 2; a = 2; b = 8; A = 4; B = 9; K = 3
 bit = 28; N = 268435456; T = 26843545.6
 1.b 2.b 3.bc 4.b 5.a 6.c 7.c 8.c
59
 p = 13; g1 = 3; g2 = 2; a = 3; b = 7; A = 8; B = 11; K = 5
 bit = 28; N = 268435456; T = 26843545.6
 1.a 2.c 3.c 4.ac 5.a 6.b 7.a 8.b
60
 p = 13; g1 = 5; g2 = 2; a = 2; b = 9; A = 4; B = 5; K = 12
 bit = 32; N = 4294967296; T = 429496729.6
 1.b 2.c 3.b 4.b 5.c 6.a 7.ac 8.c
61
 p = 11; g1 = 5; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
 bit = 28; N = 268435456; T = 26843545.6
 1.c 2.ac 3.a 4.a 5.c 6.c 7.a 8.c
62
 p = 11; g1 = 4; g2 = 2; a = 2; b = 6; A = 4; B = 9; K = 4
 bit = 26; N = 67108864; T = 6710886.4
 1.c 2.b 3.b 4.a 5.a 6.a 7.c 8.bc
63
 p = 11; g1 = 3; g2 = 2; a = 2; b = 6; A = 4; B = 9; K = 4
 bit = 28; N = 268435456; T = 26843545.6
 1.a 2.c 3.ab 4.c 5.a 6.a 7.a 8.a
64
 p = 13; g1 = 5; g2 = 2; a = 3; b = 8; A = 8; B = 9; K = 1
 bit = 32; N = 4294967296; T = 429496729.6
 1.c 2.b 3.a 4.ac 5.b 6.c 7.a 8.c
65
 p = 11; g1 = 5; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
 bit = 28; N = 268435456; T = 26843545.6
 1.c 2.b 3.bc 4.a 5.b 6.b 7.a 8.a
66
 p = 13; g1 = 5; g2 = 2; a = 2; b = 7; A = 4; B = 11; K = 4
 bit = 28; N = 268435456; T = 26843545.6
 1.a 2.c 3.a 4.c 5.a 6.c 7.bc 8.c
67
 p = 13; g1 = 5; g2 = 2; a = 2; b = 8; A = 4; B = 9; K = 3
 bit = 26; N = 67108864; T = 6710886.4
 1.c 2.ab 3.a 4.c 5.b 6.a 7.c 8.b
68
 p = 11; g1 = 3; g2 = 2; a = 2; b = 6; A = 4; B = 9; K = 4
 bit = 30; N = 1073741824; T = 107374182.4
 1.a 2.bc 3.a 4.b 5.a 6.b 7.c 8.c
69
 p = 13; g1 = 3; g2 = 2; a = 2; b = 9; A = 4; B = 5; K = 12
 bit = 26; N = 67108864; T = 6710886.4
```

1.c 2.b 3.a 4.ab 5.a 6.b 7.b 8.b
70
p = 11; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
bit = 24; N = 16777216; T = 1677721.6
1.ab 2.b 3.a 4.c 5.c 6.c 7.b 8.c
71
p = 13; g1 = 3; g2 = 2; a = 2; b = 9; A = 4; B = 5; K = 12
bit = 24; N = 16777216; T = 1677721.6
1.b 2.a 3.b 4.ab 5.b 6.c 7.c 8.a
72
p = 13; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 12; K = 12
bit = 24; N = 16777216; T = 1677721.6
1.c 2.b 3.c 4.b 5.c 6.a 7.c 8.ab
73
p = 11; g1 = 4; g2 = 2; a = 2; b = 7; A = 4; B = 7; K = 5
bit = 30; N = 1073741824; T = 107374182.4
1.ac 2.a 3.b 4.b 5.a 6.c 7.a 8.a
74
p = 13; g1 = 4; g2 = 2; a = 3; b = 8; A = 8; B = 9; K = 1
bit = 24; N = 16777216; T = 1677721.6
1.c 2.a 3.b 4.ac 5.a 6.c 7.b 8.b
75
p = 11; g1 = 4; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
bit = 32; N = 4294967296; T = 429496729.6
1.a 2.c 3.c 4.ac 5.c 6.a 7.a 8.b
76
p = 11; g1 = 3; g2 = 2; a = 2; b = 6; A = 4; B = 9; K = 4
bit = 28; N = 268435456; T = 26843545.6
1.c 2.c 3.c 4.b 5.c 6.ac 7.a 8.c
77
p = 13; g1 = 5; g2 = 2; a = 3; b = 6; A = 8; B = 12; K = 12
bit = 32; N = 4294967296; T = 429496729.6
1.a 2.a 3.c 4.b 5.b 6.a 7.bc 8.c
78
p = 13; g1 = 4; g2 = 2; a = 2; b = 8; A = 4; B = 9; K = 3
bit = 26; N = 67108864; T = 6710886.4
1.a 2.ac 3.c 4.b 5.c 6.b 7.b 8.a
79
p = 11; g1 = 3; g2 = 2; a = 3; b = 6; A = 8; B = 9; K = 3
bit = 28; N = 268435456; T = 26843545.6
1.c 2.a 3.c 4.ab 5.a 6.a 7.c 8.a
80
p = 13; g1 = 4; g2 = 2; a = 2; b = 8; A = 4; B = 9; K = 3
bit = 28; N = 268435456; T = 26843545.6
1.a 2.a 3.bc 4.a 5.b 6.c 7.c 8.b