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

Seconda prova parziale — temi e correzione

Mauro Brunato

Lunedì 12 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

Lunedì 12 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 $p = 13$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 8$ e $B = 5$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 40 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari simmetrici sono tipicamente più veloci.
   (b) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (c) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
2. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
3. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (b) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (c) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
4. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (b) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (c) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
5. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (b) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
6. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Ricevono le chiavi da un server fidato.
   (b) Utilizzano solo chiavi pubbliche certificate.
   (c) Possono confrontare le fingerprint della chiave simmetrica che condividono.
7. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.
8. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La suriettività.
   (b) La biunivocità.
   (c) L'iniettività.

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

Seconda prova parziale

Mauro Brunato

Tema 2

Lunedì 12 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 $p = 13$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 8$ e $B = 5$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (b) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (c) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
2. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) L'iniettività.
   (b) La biunivocità.
   (c) La suriettività.
3. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (b) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (c) Perché i cifrari simmetrici sono tipicamente più veloci.
4. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (b) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (c) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
5. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
6. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.
7. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Ricevono le chiavi da un server fidato.
   (b) Utilizzano solo chiavi pubbliche certificate.
   (c) Possono confrontare le fingerprint della chiave simmetrica che condividono.
8. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).

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

Seconda prova parziale

Mauro Brunato

Tema 3

Lunedì 12 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 $p = 11$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 3$ e $B = 9$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 32 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari simmetrici sono tipicamente più veloci.
   (b) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (c) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
2. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.
3. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (b) Ricevono le chiavi da un server fidato.
   (c) Utilizzano solo chiavi pubbliche certificate.
4. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
5. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) La suriettività.
   (c) L'iniettività.
6. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (b) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (c) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
7. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (b) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (c) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
8. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (b) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.

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

Seconda prova parziale

Mauro Brunato

Tema 4

Lunedì 12 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 $p = 13$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 12$ e $B = 5$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 34 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari simmetrici sono tipicamente più veloci.
   (b) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (c) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
2. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
3. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) L'iniettività.
   (c) La suriettività.
4. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (b) Utilizzano solo chiavi pubbliche certificate.
   (c) Ricevono le chiavi da un server fidato.
5. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
6. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.
7. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (b) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (c) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
8. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (b) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (c) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.

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

Seconda prova parziale

Mauro Brunato

Tema 5

Lunedì 12 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 $p = 11$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 3$ e $B = 9$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (c) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
2. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
3. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (b) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (c) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
4. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Ricevono le chiavi da un server fidato.
   (c) Possono confrontare le fingerprint della chiave simmetrica che condividono.
5. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (b) Perché i cifrari simmetrici sono tipicamente più veloci.
   (c) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
6. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (b) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (c) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
7. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) La suriettività.
   (c) L'iniettività.
8. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).

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

Seconda prova parziale

Mauro Brunato

Tema 6

Lunedì 12 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 $p = 11$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 5$ e $B = 3$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 38 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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 proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) L'iniettività.
   (c) La suriettività.
2. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.
3. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari simmetrici sono tipicamente più veloci.
   (b) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (c) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
4. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (b) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (c) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
5. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
6. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (c) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
7. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (c) Ricevono le chiavi da un server fidato.
8. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (b) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (c) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.

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

Seconda prova parziale

Mauro Brunato

Tema 7

Lunedì 12 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 $p = 13$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 12$ e $B = 5$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (b) Perché i cifrari simmetrici sono tipicamente più veloci.
   (c) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
2. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (b) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (c) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
3. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (b) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (c) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
4. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
5. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (b) Ricevono le chiavi da un server fidato.
   (c) Utilizzano solo chiavi pubbliche certificate.
6. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
7. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
8. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La biunivocità.

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

Seconda prova parziale

Mauro Brunato

Tema 8

Lunedì 12 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 $p = 13$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 5$ e $B = 11$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 40 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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 proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) L'iniettività.
   (c) La suriettività.
2. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (b) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (c) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
3. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (b) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (c) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
4. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
5. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (b) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (c) Perché i cifrari simmetrici sono tipicamente più veloci.
6. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di bit di qualunque lunghezza.
7. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (b) Ricevono le chiavi da un server fidato.
   (c) Utilizzano solo chiavi pubbliche certificate.
8. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.

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

Seconda prova parziale

Mauro Brunato

Tema 9

Lunedì 12 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 $p = 13$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 12$ e $B = 5$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 40 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (c) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
2. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (c) Ricevono le chiavi da un server fidato.
3. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) L'iniettività.
   (c) La suriettività.
4. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (b) Perché i cifrari simmetrici sono tipicamente più veloci.
   (c) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
5. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (b) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (c) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
6. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (b) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (c) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
7. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
8. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.

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

Seconda prova parziale

Mauro Brunato

Tema 10

Lunedì 12 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 $p = 13$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 5$ e $B = 11$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Ricevono le chiavi da un server fidato.
   (c) Possono confrontare le fingerprint della chiave simmetrica che condividono.
2. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (b) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (c) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
3. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
4. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (b) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (c) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
5. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La suriettività.
   (b) La biunivocità.
   (c) L'iniettività.
6. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (b) Perché i cifrari simmetrici sono tipicamente più veloci.
   (c) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
7. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
8. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.

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

Seconda prova parziale

Mauro Brunato

Tema 11

Lunedì 12 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 $p = 13$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 5$ e $B = 11$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 30 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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 proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La biunivocità.
2. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (b) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (c) Perché i cifrari simmetrici sono tipicamente più veloci.
3. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (b) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (c) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
4. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di bit di qualunque lunghezza.
5. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (b) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
6. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (c) Ricevono le chiavi da un server fidato.
7. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
8. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (b) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (c) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.

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

Seconda prova parziale

Mauro Brunato

Tema 12

Lunedì 12 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 $p = 11$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 2$ e $B = 3$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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 dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.
2. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
3. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La biunivocità.
4. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (b) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (c) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
5. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (b) Perché i cifrari simmetrici sono tipicamente più veloci.
   (c) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
6. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (b) Ricevono le chiavi da un server fidato.
   (c) Utilizzano solo chiavi pubbliche certificate.
7. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (b) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (c) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
8. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).

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

Seconda prova parziale

Mauro Brunato

Tema 13

Lunedì 12 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 $p = 11$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 5$ e $B = 3$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 32 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
2. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (b) Utilizzano solo chiavi pubbliche certificate.
   (c) Ricevono le chiavi da un server fidato.
3. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.
4. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) L'iniettività.
   (c) La suriettività.
5. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (b) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (c) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
6. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (b) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (c) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
7. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
8. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (b) Perché i cifrari simmetrici sono tipicamente più veloci.
   (c) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.

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

Seconda prova parziale

Mauro Brunato

Tema 14

Lunedì 12 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 $p = 13$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 8$ e $B = 5$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 32 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (b) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (c) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
2. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
3. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.
4. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) La suriettività.
   (c) L'iniettività.
5. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (c) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
6. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Ricevono le chiavi da un server fidato.
   (c) Possono confrontare le fingerprint della chiave simmetrica che condividono.
7. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (b) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (c) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
8. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (b) Perché i cifrari simmetrici sono tipicamente più veloci.
   (c) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.

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

Seconda prova parziale

Mauro Brunato

Tema 15

Lunedì 12 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 $p = 11$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 2$ e $B = 10$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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 codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di bit di qualunque lunghezza.
2. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Ricevono le chiavi da un server fidato.
   (b) Utilizzano solo chiavi pubbliche certificate.
   (c) Possono confrontare le fingerprint della chiave simmetrica che condividono.
3. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La suriettività.
   (b) La biunivocità.
   (c) L'iniettività.
4. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (b) Perché i cifrari simmetrici sono tipicamente più veloci.
   (c) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
5. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (b) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (c) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
6. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (b) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (c) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
7. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (b) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
8. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).

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

Seconda prova parziale

Mauro Brunato

Tema 16

Lunedì 12 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 $p = 13$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 12$ e $B = 5$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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 codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
2. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (b) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (c) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
3. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Ricevono le chiavi da un server fidato.
   (c) Possono confrontare le fingerprint della chiave simmetrica che condividono.
4. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (b) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
5. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (b) Perché i cifrari simmetrici sono tipicamente più veloci.
   (c) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
6. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) L'iniettività.
   (c) La suriettività.
7. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
8. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (b) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (c) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.

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

Seconda prova parziale

Mauro Brunato

Tema 17

Lunedì 12 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 $p = 11$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 2$ e $B = 10$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 38 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (b) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
2. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
3. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (b) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (c) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
4. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari simmetrici sono tipicamente più veloci.
   (b) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (c) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
5. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
6. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) La suriettività.
   (c) L'iniettività.
7. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Ricevono le chiavi da un server fidato.
   (b) Utilizzano solo chiavi pubbliche certificate.
   (c) Possono confrontare le fingerprint della chiave simmetrica che condividono.
8. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (b) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (c) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.

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

Seconda prova parziale

Mauro Brunato

Tema 18

Lunedì 12 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 $p = 11$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 3$ e $B = 9$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (b) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (c) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
2. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (b) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (c) Perché i cifrari simmetrici sono tipicamente più veloci.
3. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (c) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
4. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (c) Ricevono le chiavi da un server fidato.
5. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di bit di qualunque lunghezza.
6. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
7. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La biunivocità.
8. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (b) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (c) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.

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

Seconda prova parziale

Mauro Brunato

Tema 19

Lunedì 12 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 $p = 13$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 10$ e $B = 11$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 40 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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 proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La biunivocità.
2. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari simmetrici sono tipicamente più veloci.
   (b) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (c) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
3. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
4. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Ricevono le chiavi da un server fidato.
   (b) Utilizzano solo chiavi pubbliche certificate.
   (c) Possono confrontare le fingerprint della chiave simmetrica che condividono.
5. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
6. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
7. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (b) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (c) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
8. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (b) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (c) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.

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

Seconda prova parziale

Mauro Brunato

Tema 20

Lunedì 12 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 $p = 13$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 5$ e $B = 11$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 38 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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 proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) L'iniettività.
   (c) La suriettività.
2. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
3. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (b) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
4. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (b) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (c) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
5. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (b) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (c) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
6. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
7. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari simmetrici sono tipicamente più veloci.
   (b) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (c) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
8. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Ricevono le chiavi da un server fidato.
   (c) Possono confrontare le fingerprint della chiave simmetrica che condividono.

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

Seconda prova parziale

Mauro Brunato

Tema 21

Lunedì 12 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 $p = 13$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 10$ e $B = 9$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari simmetrici sono tipicamente più veloci.
   (b) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (c) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
2. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) L'iniettività.
   (b) La biunivocità.
   (c) La suriettività.
3. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Ricevono le chiavi da un server fidato.
   (c) Possono confrontare le fingerprint della chiave simmetrica che condividono.
4. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
5. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (b) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (c) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
6. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.
7. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (b) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (c) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
8. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (c) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.

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

Seconda prova parziale

Mauro Brunato
Tema 22

Lunedì 12 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 $p = 13$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 10$ e $B = 9$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (b) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (c) Perché i cifrari simmetrici sono tipicamente più veloci.
2. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (b) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (c) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
3. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.
4. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (b) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (c) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
5. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
6. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) La suriettività.
   (c) L'iniettività.
7. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
8. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Ricevono le chiavi da un server fidato.
   (c) Possono confrontare le fingerprint della chiave simmetrica che condividono.

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

Seconda prova parziale

Mauro Brunato

Tema 23

Lunedì 12 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 $p = 11$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 2$ e $B = 10$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 40 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (b) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (c) Perché i cifrari simmetrici sono tipicamente più veloci.
2. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (c) Ricevono le chiavi da un server fidato.
3. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (b) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (c) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
4. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di bit di qualunque lunghezza.
5. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (b) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (c) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
6. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
7. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La biunivocità.
8. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (b) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.

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

Seconda prova parziale

Mauro Brunato

Tema 24

Lunedì 12 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 $p = 11$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 4$ e $B = 9$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 30 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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 codominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
2. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
3. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
4. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Ricevono le chiavi da un server fidato.
   (b) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (c) Utilizzano solo chiavi pubbliche certificate.
5. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (b) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (c) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
6. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (b) Perché i cifrari simmetrici sono tipicamente più veloci.
   (c) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
7. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (b) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (c) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
8. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La biunivocità.

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

Seconda prova parziale

Mauro Brunato
Tema 25

Lunedì 12 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 $p = 11$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 2$ e $B = 3$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 40 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (c) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
2. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La biunivocità.
3. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (b) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
   (c) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
4. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Ricevono le chiavi da un server fidato.
   (b) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (c) Utilizzano solo chiavi pubbliche certificate.
5. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
6. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (b) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (c) Perché i cifrari simmetrici sono tipicamente più veloci.
7. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
8. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (b) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (c) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.

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

Seconda prova parziale

Mauro Brunato

Tema 26

Lunedì 12 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 $p = 11$ e sul generatore $g = 7$.

1.1) Verificare se $g = 7$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 5$ e $B = 3$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (b) Perché i cifrari simmetrici sono tipicamente più veloci.
   (c) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
2. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (b) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (c) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
3. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
4. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
5. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (b) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (c) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
6. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di bit di qualunque lunghezza.
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
7. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (b) Utilizzano solo chiavi pubbliche certificate.
   (c) Ricevono le chiavi da un server fidato.
8. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La biunivocità.
   (b) L'iniettività.
   (c) La suriettività.

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

Seconda prova parziale

Mauro Brunato

Tema 27

Lunedì 12 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 $p = 13$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 12$ e $B = 5$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 32 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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 codominio tipico di una funzione hash crittografica?
   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di bit di qualunque lunghezza.
2. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La suriettività.
   (b) La biunivocità.
   (c) L'iniettività.
3. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (b) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (c) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
4. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
5. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (b) Ricevono le chiavi da un server fidato.
   (c) Utilizzano solo chiavi pubbliche certificate.
6. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (c) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
7. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
   (b) Perché i cifrari simmetrici sono tipicamente più veloci.
   (c) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
8. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
   (b) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (c) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.

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

Seconda prova parziale

Mauro Brunato
Tema 28

Lunedì 12 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 $p = 11$ e sul generatore $g = 5$.

1.1) Verificare se $g = 5$ è una radice prima modulo p; Alice e Bob convengono comunque sull'uso di questo valore.

1.2) Charlie intercetta le comunicazioni fra Alice e Bob, e viene a conoscenza dei rispettivi numeri pubblici $A = 3$ e $B = 9$, ovviamente scambiati in chiaro, oltre ai valori di p e g indicati prima.
Operare un attacco di forza bruta e ottenere la chiave segreta.

Esercizio 2

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 32 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

2.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

2.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

2.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 2.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare 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. In che cosa consiste la certificazione digitale di una chiave?
   (a) Un'autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.
   (b) Un'autorità considerata affidabile firma l'associazione fra una chiave privata e l'identità del possessore.
   (c) Un'autorità considerata affidabile firma l'associazione fra una chiave pubblica e l'identità del possessore.
2. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La biunivocità.
3. Qual è il dominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).
4. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?
   (a) Utilizzano solo chiavi pubbliche certificate.
   (b) Possono confrontare le fingerprint della chiave simmetrica che condividono.
   (c) Ricevono le chiavi da un server fidato.
5. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?
   (a) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.
   (b) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.
   (c) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.
6. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?
   (a) Perché i cifrari simmetrici sono tipicamente più veloci.
   (b) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.
   (c) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.
7. In che cosa consiste un attacco "Man-in-the-Middle"?
   (a) L'attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.
   (b) L'attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.
   (c) L'attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l'altro.
8. Qual è il codominio tipico di una funzione hash crittografica?
   (a) Stringhe di bit di qualunque lunghezza.
   (b) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).
   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).

Traccia della soluzione all'esercizio 1 (tema 1)

1.1 — Verifica del generatore primo

Se proviamo le potenze successive di $g = 5$ modulo $p = 13$, otteniamo $5^4 \equiv 1$, e da qui la sequenza si ripete. Quindi il valore proposto per g non è adeguato.

1.2 — Calcolo dei valori privati di Alice e Bob

Dalle potenze trovate nella verifica del punto precedente, abbiamo che $a = 3$, perché $5^3 = 8 \pmod{13}$, e $b = 1$. Di conseguenza, il modo più rapido per calcolare la chiave è senz'altro $K = A^b = 8^1 = 8 \pmod{13}$.

Traccia della soluzione all'esercizio 2 (tema 1)

1.1 — Verifica dell'integrità del pacchetto

Bob deve semplicemente calcolare l'hash $H(m)$ del pacchetto scaricato e confrontarlo con il valore pubblicato da Alice. Il tempo di verifica (al netto dello scaricamento del pacchetto e del valore di confronto) consiste nel milionesimo di secondo necessario a calcolare il valore hash.

1.2 — Generazione di un pacchetto fraudolento

Charlie deve generare una serie di pacchetti alternativi $m_1, m_2, \ldots, m_i, \ldots$ finché uno di questi non ha lo stesso valore hash del pacchetto originale: $H(m_i) = H(m)$. La probabilità di collisione è pari a 2^{-40} per ogni nuovo pacchetto.

Di conseguenza, Charlie dovrà generare in media $2^{40} \approx 10^{12}$ pacchetti, impiegando un tempo pari a $10^{12-6} = 10^6$ secondi (10–15 giorni).

1.3 — Proof of effort

La probabilità che un nonce azzeri i primi 20 bit della funzione hash è 2^{-20}, quindi il numero atteso di tentativi da parte di Alice è $2^{20} = 10^6$, e il tempo atteso è un secondo.

Indipendentemente dal numero di bit pari a zero, Charlie è ancora alla ricerca di un preciso valore hash, quindi il suo tempo atteso non cambia.

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. Perché in TLS, dopo l'handshake iniziale, si passa a un cifrario a chiave simmetrica?

   (a) Perché i cifrari simmetrici sono tipicamente più veloci.

   (b) Perché non tutti i client sono in grado di utilizzare cifrari a chiave pubblica.

   (c) Perché i cifrari a chiave pubblica non permettono lo scambio di più pacchetti tipico di un protocollo interattivo.

   Se i client non fossero in grado di utilizzare cifrari a chiave pubblica, allora non potrebbero usare TLS tout court, e ovviamente i cifrari a chiave pubblica permettono lo scambio di tutta l'informazione che si desidera.

2. Quale proprietà è essenziale in una funzione di cifratura $f_K(\cdot)$?

   (a) L'iniettività.

   (b) La suriettività.

   (c) La biunivocità.

   È necessario che due messaggi diversi diano luogo a due codici diversi (non collidano mai), perché la cifratura dev'essere invertibile. Non è invece necessario che la codifica sia suriettiva, anche se spesso lo si preferisce per evitare sprechi di bit.

3. Qual è il dominio tipico di una funzione hash crittografica?

   (a) Stringhe di bit di qualunque lunghezza.

   (b) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).

   (c) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).

   Le funzioni hash debbono essere applicabili a stringhe di qualsiasi lunghezza.

4. Qual è il codominio tipico di una funzione hash crittografica?

   (a) Stringhe di qualche centinaio di bit (da 128 a 512 a seconda dell'algoritmo).

   (b) Stringhe di bit di qualunque lunghezza.

   (c) Stringhe di qualche migliaio di bit (da 1024, meglio 2048 o più).

   Una funzione hash genererà una stringa di lunghezza prefissata.

5. In che modo gli utenti di WhatsApp e Telegram possono assicurarsi di non essere soggetti a un attacco Man-in-the-Middle nella creazione di chiavi Diffie-Hellman?

   (a) Possono confrontare le fingerprint della chiave simmetrica che condividono.

   (b) Utilizzano solo chiavi pubbliche certificate.

   (c) Ricevono le chiavi da un server fidato.

   La domanda parla espressamente del protocollo D-H, quindi non si usano solo chiavi precedentemente certificate; la ricezione delle chiavi da un server è esattamente quello che si vuole evitare (altrimenti il server è il MitM).

6. Come si utilizza una funzione hash crittografica nel contesto di una proof-of-work?

   (a) Si cerca un nonce che, appeso all'informazione da certificare, genera un riassunto hash di valore inferiore a una soglia data.

   (b) Si firma il riassunto hash dell'informazione con la chiave privata del mittente.

   (c) Si aggiunge una marca temporale all'informazione prima di calcolarne il riassunto hash.

7. In che cosa consiste un attacco “Man-in-the-Middle”?

   (a) L’attaccante si intromette in una comunicazione, e con ciascuno dei due interlocutori finge di essere l’altro.

   (b) L’attaccante ascolta la linea di comunicazione e può leggere tutti i messaggi scambiati fra i due interlocutori.

   (c) L’attaccante carpisce la fiducia di uno dei due interlocutori e ottiene la chiave segreta per decifrare le comunicazioni.

   Si parla di MitM quando l’attaccante assume un ruolo più attivo rispetto al solo ascolto.

8. In che cosa consiste la certificazione digitale di una chiave?

   (a) Un’autorità considerata affidabile firma l’associazione fra una chiave pubblica e l’identità del possessore.

   (b) Un’autorità considerata affidabile firma l’associazione fra una chiave privata e l’identità del possessore.

   (c) Un’autorità considerata affidabile fornisce su richiesta informazioni sul possessore di una chiave.

   Una CA non può firmare una chiave privata (che il possessore non deve mai affidare a terzi), e il certificato è pensato in modo che non sia necessario l’intervento della CA in fase di verifica.

Griglie di soluzione

Sono elencati, per ogni tema:

- i valori privati a e b e la chiave K ottenuti con l'esercizio 1 (NB: altri valori sono possibili per a e b);
- il numero di tentativi N e il tempo richiesto T per l'esercizio 2;
- l'elenco delle risposte corrette alle domande dell'ultimo esercizio.

```
1
 p = 13; g = 5; A = 8; B = 5; a = 3; b = 5; K = 8
 bit = 40; Nhash = 1.1e+12; Tcharlie = 1.1e+6
 1.a 2.a 3.a 4.c 5.c 6.c 7.c 8.c
2
 p = 13; g = 5; A = 8; B = 5; a = 3; b = 5; K = 8
 bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
 1.a 2.a 3.c 4.a 5.c 6.b 7.c 8.b
3
 p = 11; g = 5; A = 3; B = 9; a = 2; b = 4; K = 4
 bit = 32; Nhash = 4.3e+9; Tcharlie = 4.3e+3
 1.a 2.b 3.a 4.a 5.c 6.b 7.b 8.a
4
 p = 13; g = 5; A = 12; B = 5; a = 2; b = 5; K = 12
 bit = 34; Nhash = 1.7e+10; Tcharlie = 1.7e+4
 1.a 2.a 3.b 4.a 5.c 6.b 7.b 8.b
5
 p = 11; g = 5; A = 3; B = 9; a = 2; b = 4; K = 4
 bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
 1.a 2.b 3.b 4.c 5.b 6.c 7.c 8.c
6
 p = 11; g = 7; A = 5; B = 3; a = 2; b = 4; K = 9
 bit = 38; Nhash = 2.7e+11; Tcharlie = 2.7e+5
 1.b 2.c 3.a 4.a 5.c 6.b 7.b 8.b
7
 p = 13; g = 5; A = 12; B = 5; a = 2; b = 5; K = 12
 bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
 1.b 2.b 3.a 4.c 5.a 6.a 7.c 8.a
8
 p = 13; g = 7; A = 5; B = 11; a = 3; b = 5; K = 5
 bit = 40; Nhash = 1.1e+12; Tcharlie = 1.1e+6
 1.b 2.b 3.b 4.c 5.c 6.c 7.a 8.c
9
 p = 13; g = 5; A = 12; B = 5; a = 2; b = 5; K = 12
 bit = 40; Nhash = 1.1e+12; Tcharlie = 1.1e+6
 1.b 2.b 3.b 4.b 5.b 6.a 7.a 8.b
10
 p = 13; g = 7; A = 5; B = 11; a = 3; b = 5; K = 5
 bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
 1.c 2.a 3.b 4.b 5.c 6.b 7.b 8.c
11
 p = 13; g = 7; A = 5; B = 11; a = 3; b = 5; K = 5
 bit = 30; Nhash = 1.1e+9; Tcharlie = 1.1e+3
 1.a 2.c 3.a 4.a 5.c 6.b 7.a 8.b
12
 p = 11; g = 7; A = 2; B = 3; a = 3; b = 4; K = 5
 bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
 1.c 2.c 3.a 4.a 5.b 6.a 7.b 8.c
```

13
p = 11; g = 7; A = 5; B = 3; a = 2; b = 4; K = 9
bit = 32; Nhash = 4.3e+9; Tcharlie = 4.3e+3
1.b 2.a 3.b 4.b 5.b 6.c 7.a 8.b
14
p = 13; g = 5; A = 8; B = 5; a = 3; b = 5; K = 8
bit = 32; Nhash = 4.3e+9; Tcharlie = 4.3e+3
1.c 2.b 3.c 4.c 5.b 6.c 7.a 8.b
15
p = 11; g = 7; A = 2; B = 10; a = 3; b = 5; K = 10
bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
1.a 2.c 3.c 4.b 5.b 6.b 7.a 8.a
16
p = 13; g = 5; A = 12; B = 5; a = 2; b = 5; K = 12
bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
1.a 2.c 3.c 4.c 5.b 6.b 7.b 8.c
17
p = 11; g = 7; A = 2; B = 10; a = 3; b = 5; K = 10
bit = 38; Nhash = 2.7e+11; Tcharlie = 2.7e+5
1.a 2.b 3.a 4.a 5.c 6.c 7.c 8.a
18
p = 11; g = 5; A = 3; B = 9; a = 2; b = 4; K = 4
bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
1.b 2.c 3.a 4.b 5.a 6.a 7.a 8.c
19
p = 13; g = 7; A = 10; B = 11; a = 2; b = 5; K = 4
bit = 40; Nhash = 1.1e+12; Tcharlie = 1.1e+6
1.a 2.a 3.a 4.c 5.b 6.a 7.a 8.a
20
p = 13; g = 7; A = 5; B = 11; a = 3; b = 5; K = 5
bit = 38; Nhash = 2.7e+11; Tcharlie = 2.7e+5
1.b 2.c 3.c 4.c 5.a 6.b 7.a 8.c
21
p = 13; g = 7; A = 10; B = 9; a = 2; b = 4; K = 3
bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
1.a 2.a 3.c 4.b 5.a 6.c 7.a 8.b
22
p = 13; g = 7; A = 10; B = 9; a = 2; b = 4; K = 3
bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
1.c 2.b 3.b 4.a 5.a 6.c 7.b 8.c
23
p = 11; g = 7; A = 2; B = 10; a = 3; b = 5; K = 10
bit = 40; Nhash = 1.1e+12; Tcharlie = 1.1e+6
1.c 2.b 3.a 4.b 5.b 6.a 7.a 8.c
24
p = 11; g = 5; A = 4; B = 9; a = 3; b = 4; K = 3
bit = 30; Nhash = 1.1e+9; Tcharlie = 1.1e+3
1.b 2.b 3.b 4.b 5.c 6.b 7.c 8.a
25
p = 11; g = 7; A = 2; B = 3; a = 3; b = 4; K = 5
bit = 40; Nhash = 1.1e+12; Tcharlie = 1.1e+6
1.b 2.b 3.b 4.b 5.c 6.c 7.b 8.a
26
p = 11; g = 7; A = 5; B = 3; a = 2; b = 4; K = 9
bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
1.b 2.c 3.b 4.b 5.c 6.b 7.a 8.b
27

p = 13; g = 5; A = 12; B = 5; a = 2; b = 5; K = 12
bit = 32; Nhash = 4.3e+9; Tcharlie = 4.3e+3
1.a 2.c 3.c 4.a 5.a 6.a 7.b 8.c
28
p = 11; g = 5; A = 3; B = 9; a = 2; b = 4; K = 4
bit = 32; Nhash = 4.3e+9; Tcharlie = 4.3e+3
1.c 2.b 3.a 4.b 5.a 6.a 7.c 8.b