

### Domanda 1

Risposta  
corretta

Punteggio  
ottenuto 3 su 3



Contrassegna  
domanda

Indicare quale tra le seguenti descrizioni è corretta relativamente all'accordo su chiavi Diffie-Hellman, dato un numero primo  $p$  ed un generatore  $g$ . È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. Alice genera a caso  $x$  ed invia  $g^x \bmod p$ . Bob genera a caso  $y$  ed invia  $(g^y)(g^x) \bmod p$ . La chiave condivisa è  $g^y \bmod p$ .
- ☐ b. Alice genera a caso  $x$  ed invia  $g^x \bmod p$ . Bob genera a caso  $y$  ed invia  $(g^x)^y \bmod p$ . La chiave condivisa è  $g^{(xy)} \bmod p$ .
- ☒ c. Alice genera a caso  $x$  ed invia  $g^x \bmod p$ . Bob genera a caso  $y$  ed invia  $g^y \bmod p$ . La chiave condivisa è  $g^{(xy)} \bmod p$ . ✓
- ☐ d. Alice genera a caso  $x$  ed invia  $g^{\text{SHA}(x)} \bmod p$ . Bob genera a caso  $y$  ed invia  $g^{\text{SHA}(y)} \bmod p$ . La chiave condivisa è  $g^{(\text{SHA}(xy))} \bmod p$ .

Risposta corretta.

La risposta corretta è: Alice genera a

		✓	✓
9	10	11	12
✓		✓	
13	14	15	16
✓	✓		✓
17	18	19	20
✓	✓	✓	✓

Visualizza una pagina  
alla volta

Fine revisione

Domanda 2

Risposta  
corretta

Punteggio  
ottenuto 3 su 3



Contrassegna  
domanda

Indicare quale dei seguenti metodi è preferibile per memorizzare le password in forma cifrata usando l'AES rispetto agli altri 3 metodi:

Scegli un'alternativa:

- ☐ a. Usando l'account concatenato ad un nonce (che sarà poi memorizzato accanto al testo cifrato) come chiave AES e la password come testo in chiaro.
- ☐ b. Usando l'account concatenato ad un nonce (che sarà poi memorizzato accanto al testo cifrato) come chiave AES e la password concatenata allo stesso nonce come testo in chiaro.
- ☐ c. Usando l'account come chiave AES e la password come testo in chiaro.
- ☒ d. Usando la password come chiave AES e l'account come testo in chiaro. ✓

Risposta corretta.

La risposta corretta è: Usando la password come chiave AES e l'account come testo in chiaro.

**Domanda 3**

Risposta  
corretta

Punteggio  
ottenuto 1 su 1



Contrassegna  
domanda

Indicare quale tra le seguenti affermazioni è sbagliata. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. I sistemi biometrici consentono l'identificazione e l'autenticazione di un utente.
- ☐ b. I sistemi biometrici possono essere basati su caratteristiche fisiologiche o comportamentali.
- ☐ c. I sistemi biometrici sono tipicamente utilizzati per il controllo degli accessi in sedi governative.
- ☒ d. Nessuna delle altre tre scelte. ✓

Risposta corretta.

La risposta corretta è: Nessuna delle altre tre scelte.

Domanda 4

Risposta  
corretta

Punteggio  
ottenuto 2 su  
2



Contrassegna  
domanda

Indicare quale tra le seguenti affermazioni descrive una corretta generazione dei parametri per il cifrario a chiave pubblica RSA. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. Input L. Generare 2 numeri primi  $p, q$  la cui somma delle lunghezze è L. Calcolare  $n=pq$ . Scegliere  $e = 2^{16} - 1$ . Scegliere  $d$  come inverso moltiplicativo di  $e$  mod  $(p-1)(q-1)$ . La chiave pubblica è  $(n,e)$  e la chiave privata è  $(n,d)$ .
- ☐ b. Input L. Generare 2 numeri primi  $p, q$  di lunghezza  $L/2$ . Calcolare  $n=pq$ . Scegliere  $e = 2^{16} - 1$ . Scegliere  $d$  come inverso moltiplicativo di  $e$  mod  $n$ . La chiave pubblica è  $(n,e)$  e la chiave privata è  $(n,d)$ .
- ☒ c. Input L. Generare 2 numeri primi  $p, q$  di lunghezza  $L/2$ . Calcolare  $n=pq$ . Scegliere un  $e$  tale che  $\gcd(e, (p-1)(q-1))=1$ . Scegliere  $d$  come inverso moltiplicativo di  $e$  mod  $(p-1)(q-1)$ . La chiave pubblica è  $(n,e)$  e la chiave privata è  $(n,d)$ . ✓
- ☐ d. Input L. Generare 2 numeri primi  $p, q$  la cui somma delle lunghezze è L. Calcolare  $n=pq$ . Scegliere un  $e$  tale che  $\gcd(e, (p-1)(q-1))=1$ . Scegliere  $d$  come inverso moltiplicativo di  $e$  mod  $n$ . La chiave pubblica è  $(n,e)$  e la chiave privata è  $(n,d)$ .

Risposta corretta.

La risposta corretta è: Input L. Generare 2 numeri primi  $p, q$  di lunghezza  $L/2$ . Calcolare  $n=pq$ . Scegliere un  $e$  tale che  $\gcd(e, (p-1)(q-1))=1$ . Scegliere  $d$  come inverso moltiplicativo di  $e$  mod  $(p-1)(q-1)$ . La chiave pubblica è  $(n,e)$  e la chiave privata è  $(n,d)$ .

Domanda 5

Risposta errata

Punteggio  
ottenuto 0 su  
2



Contrassegna  
domanda

Indicare quale tra i seguenti comandi non consente ad Alice di generare una coppia di chiavi RSA. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☒ a. openssl genrsa -pubout -out rsaprivatekey.pem -passout pass:P1pp0B4ud0 -aes128 1024
- ☐ b. openssl genrsa -out rsaprivatekey.pem -passout pass:P1pp0B4ud0 -aes128 1024 ✖
- ☐ c. openssl genrsa -out rsaprivatekey.pem -aes128 1024
- ☐ d. openssl genrsa -out rsaprivatekey.pem -aes128

Risposta errata.

La risposta corretta è: openssl genrsa -pubout -out rsaprivatekey.pem -passout pass:P1pp0B4ud0 -aes128 1024



Domanda 6

Risposta errata

Punteggio  
ottenuto 0 su  
2



Contrassegna  
domanda

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☒ a. Enigma usava 3 rotori ed un disco per l'involuzione.
- ☐ b. Le macchine a rotori sono state inventate da Alan Turing per rompere Enigma.
- ☐ c. Le altre tre scelte sono tutte sbagliate.
- ☐ d. Ogni rotore di Enigma realizza una sostituzione polialfabetica. ✖

Risposta errata.

La risposta corretta è: Enigma usava 3 rotori ed un disco per l'involuzione.

Domanda 7

Risposta  
corretta

Punteggio  
ottenuto 1 su 1



Contrassegna  
domanda

Indicare quale tra le seguenti motivazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☒ a. La Certificate Revocation List (CRL) contiene il numero seriale di tutti i certificati revocati. ✓
- ☐ b. La Certificate Revocation List (CRL) contiene tutti i certificati con lunghezza della chiave non conforme alle raccomandazioni NIST.
- ☐ c. La Certificate Revocation List (CRL) contiene tutti i certificati revocati e scaduti.
- ☐ d. La Certificate Revocation List (CRL) contiene chiave pubblica e numero seriale di tutti i certificati revocati e scaduti.

Risposta corretta.

La risposta corretta è: La Certificate Revocation List (CRL) contiene il numero seriale di tutti i certificati revocati.

**Domanda 8**

Risposta  
corretta

Punteggio  
ottenuto 2 su  
2



Contrassegna  
domanda

Indicare quale tra le seguenti motivazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. I certificati sono importanti nel Code Signing per garantire i diritti di autore.
- ☐ b. I certificati sono importanti nel Code Signing per garantire la mancanza di codice malevolo.
- ☒ c. I certificati sono importanti nel Code Signing per garantire integrità e provenienza del codice. ✓
- ☐ d. I certificati sono importanti nel Code Signing per garantire la qualità del codice e la versione dell'aggiornamento.

Risposta corretta.

La risposta corretta è: I certificati sono importanti nel Code Signing per garantire integrità e provenienza del codice.



**Domanda 9**

Risposta  
corretta

Punteggio  
ottenuto 1 su 1



Contrassegna  
domanda

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. Due certificati emessi dalla stessa CA possono avere numeri di serie differenti.
- ☒ b. Due certificati emessi dalla stessa CA devono sempre avere numeri di serie differenti. ✓
- ☐ c. Due certificati emessi dalla stessa CA devono sempre avere numeri di serie uguali.
- ☐ d. Nessuna delle altre tre scelte.

Risposta corretta.

La risposta corretta è: Due certificati emessi dalla stessa CA devono sempre avere numeri di serie differenti.

Domanda 10

Risposta errata

Punteggio  
ottenuto 0 su  
2



Contrassegna  
domanda

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. L'algoritmo di decifratura del DES è uguale a quello di cifratura, incluso l'ordine delle sottochiavi.
- ☒ b. L'algoritmo di decifratura del DES è uguale a quello di cifratura, ma l'ordine delle sottochiavi deve essere invertito e bisogna in aggiunta scambiare la metà destra finale con la metà sinistra. ✖
- ☐ c. L'algoritmo di decifratura del DES è uguale a quello di cifratura, incluso l'ordine delle sottochiavi, ma bisogna in aggiunta scambiare la metà destra finale con la metà sinistra.
- ☒ d. L'algoritmo di decifratura del DES è uguale a quello di cifratura, ma l'ordine delle sottochiavi deve essere invertito.

Risposta errata.

La risposta corretta è: L'algoritmo di decifratura del DES è uguale a quello di cifratura, ma l'ordine delle sottochiavi deve essere invertito.

Domanda 11

Risposta  
corretta

Punteggio  
ottenuto 2 su  
2



Contrassegna  
domanda

Indicare quale tra le seguenti affermazioni è sbagliata. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. Le S-box del DES furono progettate per resistere all'attacco noto poi come Crittoanalisi Differenziale.
- ☒ b.  
Il DES è stato abbandonato come standard a causa del suo *avalanche effect*. ✓
- ☐ c. Il DES è stato abbandonato come standard perché la chiave è troppo corta.
- ☐ d. Il DES può essere rotto in meno di una settimana con poche migliaia di euro o anche meno di un giorno.

Risposta corretta.

La risposta corretta è:

Il DES è stato abbandonato come standard a causa del suo *avalanche effect*.

Domanda 12

Risposta errata

Punteggio  
ottenuto 0 su 1



Contrassegna  
domanda

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. Una Key Derivation Function (KDF) consente di derivare la componente pubblica da una coppia di chiavi asimmetriche.
- ☒ b. Una Key Derivation Function (KDF) consente di derivare una chiave pseudocasuale a partire da eventi che avvengono nel sistema. ✖

☒ c.

Una Key Derivation Function (KDF) consente di derivare una chiave di cifratura a partire da una Passphrase.

☐ d. Nessuna delle altre tre scelte.

Risposta errata.

La risposta corretta è:

Una Key Derivation Function (KDF) consente di derivare una chiave di cifratura a partire da una Passphrase.

**Domanda 13**

Risposta  
corretta

Punteggio  
ottenuto 2 su  
2



Contrassegna  
domanda

Sia *dhparams.pem* il file contenente i parametri pubblici Diffie-Hellman  $p$  e  $g$ . Sia *dhkey1.pem* la chiave privata di Alice e sia *dhpublish2.pem* la chiave pubblica di Bob. Indicare quale tra i seguenti comandi consente ad Alice di ottenere una chiave condivisa, a partire dalle informazioni ricevute da Bob. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. `openssl pkeyutl -derive -inkey dhparams.pem -peerkey dhpublish2.pem -out segreto1.bin`
- ☒ b. `openssl pkeyutl -derive -inkey dhkey1.pem -peerkey dhpublish2.pem -out segreto1.bin` ✓
- ☐ c. `openssl pkeyutl -derive -inkey dhpublish2.pem -peerkey dhkey1.pem -out segreto1.bin`
- ☐ d. Nessuna delle altre tre scelte

Risposta corretta.

La risposta corretta è: `openssl pkeyutl -derive -inkey dhkey1.pem -peerkey dhpublish2.pem -out segreto1.bin`



**Domanda 14**

Risposta  
corretta

Punteggio  
ottenuto 2 su  
2



Contrassegna  
domanda

Indicare quale tra le seguenti motivazioni è corretta. E' possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. La firma grafometrica, essendo un caso particolare della firma digitale, ha la medesima efficacia probatoria della scrittura privata.
- ☐ b. La firma grafometrica è essenzialmente un'immagine della firma autografa, senza altri rilevanti dati per la non falsificabilità.
- ☒ c. La firma grafometrica, al pari della firma digitale, ha la medesima efficacia probatoria della scrittura privata. ✓
- ☐ d.  
La firma grafometrica, essendo facilmente falsificabile, non ha la medesima efficacia probatoria della scrittura privata.

Risposta corretta.

La risposta corretta è: La firma grafometrica, al pari della firma digitale, ha la medesima efficacia probatoria della scrittura privata.

Domanda 15

Risposta errata

Punteggio  
ottenuto 0 su  
2



Contrassegna  
domanda

Siano *rsaprivatekey.pem* ed *rsapublickey.pem* rispettivamente le chiavi pubbliche e private di Alice. Indicare quale tra i seguenti comandi consente ad Alice di calcolare una firma per il file *testoInChiaro.txt*. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☒ a. `openssl rsautl -sign -pubin -inkey rsapublickey.pem -in testoInChiaro.txt -out rsasign.bin` ✖
- ☐ b. `openssl rsautl -sign -pubin -inkey rsaprivatekey.pem -in testoInChiaro.txt -out rsasign.bin`
- ☐ c. `openssl rsautl -sign -inkey rsapublickey.pem -in testoInChiaro.txt -pubout -out rsasign.bin`
- ☒ d. Nessuna delle altre tre scelte

Risposta errata.

La risposta corretta è: Nessuna delle altre tre scelte

Domanda **17**

Risposta  
corretta

Punteggio  
ottenuto 1 su 1



Contrassegna  
domanda

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. Se al comando *dgst* viene passato più di un file, viene calcolato l'hash della concatenazione dei file.
- ☐ b. Se al comando *dgst* viene passato più di un file, viene restituita in output la concatenazione dell'hash dei file.
- ☐ c. Se al comando *dgst* viene passato più di un file, viene restituito in output un messaggio di errore.
- ☒ d. Se al comando *dgst* viene passato più di un file, viene calcolato un hash separato per ciascun file. ✓

Risposta corretta.

La risposta corretta è: Se al comando *dgst* viene passato più di un file, viene calcolato un hash separato per ciascun file.

Domanda **18**

Risposta  
corretta

Punteggio  
ottenuto 1 su 1



Contrassegna  
domanda

Indicare quale tra le seguenti affermazioni è sbagliata. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☒ a. L'analisi statica viene di solito effettuata dopo quella dinamica. ✓
- ☐ b. L'analisi statica consente di effettuare l'analisi del codice e della struttura di un malware.
- ☐ c. Durante l'analisi statica il malware non viene eseguito.
- ☐ d. Nessuna delle altre tre scelte.

Risposta corretta.

La risposta corretta è: L'analisi statica viene di solito effettuata dopo quella dinamica.

**Domanda 19**

Risposta  
corretta

Punteggio  
ottenuto 2 su  
2



Contrassegna  
domanda

Indicare quale tra i seguenti comandi consente di generare una stringa pseudocasuale la cui lunghezza non sia multipla di 4. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. openssl rand -base64 12
- ☐ b. openssl rand -base64 32
- ☐ c. openssl rand -base64 19
- ☒ d. Nessuna delle altre tre scelte ✓

Risposta corretta.

La risposta corretta è: Nessuna delle altre tre scelte



Domanda **20**

Risposta  
corretta

Punteggio  
ottenuto 2 su  
2



Contrassegna  
domanda

Indicare quale tra le seguenti affermazioni è sbagliata. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. SSL/TLS consentono di ottenere i requisiti di autenticazione, confidenzialità ed integrità.
- ☐ b. SSL/TLS consentono alle parti di negoziare le primitive crittografiche da utilizzare per la sicurezza dell'informazione.
- ☐ c. SSL/TLS consente al Client di autenticare il Server, ed eventualmente anche al Server di autenticare il Client.
- ☒ d. Nessuna delle altre tre scelte. ✓

Risposta corretta.

La risposta corretta è: Nessuna delle altre tre scelte.