

Indicare quale tra le seguenti affermazioni descrive una corretta generazione dei parametri per la firma digitale RSA. È possibile effettuare una sola scelta:

Scegli un'alternativa:

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

Risposta errata.

La risposta corretta è: Input L. Generare 2 numeri primi p, q di lunghezza L/2. Calcolare $n=pq$. Scegliere un e tale che $\text{gcd}(e, (p-1)(q-1))=1$. 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) .

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

Scegli un'alternativa:

- a. La sicurezza dei messaggi cifrati passati non dipende dalla compromissione futura della chiave privata. ✓
- b. La sicurezza dei messaggi cifrati vale anche per il futuro, poiché resistenti a tutti gli attacchi.
- c. Fornisce una maggiore sicurezza poiché garantisce anche l'anonimato del mittente.
- d. La confidenzialità dei messaggi cifrati permane anche inoltrandoli ad altri.

Risposta corretta

La risposta corretta è: La sicurezza dei messaggi cifrati passati non dipende dalla compromissione futura della chiave privata.

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

Scegli un'alternativa:

- a. La codifica in Base64 non consente di processare dati il cui numero di bit non sia multiplo di 24. ✓
- b. La codifica in Base64 consente di memorizzare o trasferire flussi arbitrari di bit mediante caratteri stampabili.
- c. La codifica in Base64 processa i dati in blocchi da 24 bit.
- d. La codifica in Base64 opera su blocchi di dati da 6 bit.

Risposta corretta.

La risposta corretta è: La codifica in Base64 non consente di processare dati il cui numero di bit non sia multiplo di 24.

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

Scegli un'alternativa:

- a. I cifrari a sostituzione monoalfabetica sono stati facilmente decifrati usando principalmente una analisi delle frequenze delle lettere. ✓
- b. I cifrari a sostituzione monoalfabetica sono stati facilmente decifrati usando le raccomandazioni del NIST.
- c. Nessuna delle altre tre scelte.
- d. I cifrari a sostituzione monoalfabetica sono stati facilmente decifrati usando semplicemente una ricerca esaustiva nello spazio delle chiavi.

Risposta corretta.

La risposta corretta è: I cifrari a sostituzione monoalfabetica sono stati facilmente decifrati usando principalmente una analisi delle frequenze delle lettere.

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

Scegli un'alternativa:

- a. Il certificato che lega l'identità di Alice alla propria chiave pubblica ed emesso da una CA è firmato usando la chiave pubblica della CA. X
- b. Il certificato che lega l'identità di Alice alla propria chiave pubblica ed emesso da una CA è firmato usando la chiave pubblica di Alice.
- c. Il certificato che lega l'identità di Alice alla propria chiave pubblica ed emesso da una CA è firmato usando la chiave privata della CA.
- d. Il certificato che lega l'identità di Alice alla propria chiave pubblica ed emesso da una CA è firmato usando la chiave privata di Alice.

Risposta errata.

La risposta corretta è: Il certificato che lega l'identità di Alice alla propria chiave pubblica ed emesso da una CA è firmato usando la chiave privata della CA.

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

Scegli un'alternativa:

- a. Il comando `dgst` ed il comando `cmp` possono essere usati per verificare se due file portano ad una collisione.
- b. Il comando `dgst` può essere usato per calcolare lo SHA256 di un file.
- c. Il comando `dgst` può essere usato in alternativa al comando `hmac` per calcolare l'HMAC di un file. ✓
- d. Il comando `dgst` può essere usato per calcolare l'MD5 di più file.

Risposta corretta.

La risposta corretta è: Il comando `dgst` può essere usato in alternativa al comando `hmac` per calcolare l'HMAC di un file.

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

Scegli un'alternativa:

- a. Il Record Protocol si occupa di garantire la compressione, la confidenzialità e l'integrità dei dati.
- b. Il Record Protocol utilizza gli algoritmi ed i parametri crittografici negoziati attraverso l'Handshake Protocol.
- c. Il Record Protocol si occupa di garantire l'autenticazione, la compressione, la confidenzialità e l'integrità dei dati. ✓
- d. Nessuna delle altre tre scelte.

Risposta corretta.

La risposta corretta è: Il Record Protocol si occupa di garantire l'autenticazione, la compressione, la confidenzialità e l'integrità dei dati.

Si assuma che `dhparams1.pem` contenga i parametri pubblici Diffie-Hellman p_1 e g_1 . Si assuma inoltre che `dhparams2.pem` contenga i parametri pubblici Diffie-Hellman p_2 e g_2 . Siano Utente₁ e Utente₂ due utenti. Indicare quale tra le seguenti affermazioni è sbagliata. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. Sia Utente₁ che Utente₂ devono usare `dhparams1.pem`, per generare ciascuno la propria coppia di chiavi.
- b. Sia Utente₁ che Utente₂ devono usare `dhparams2.pem`, per generare ciascuno la propria coppia di chiavi.
- c. Per derivare la propria coppia di chiavi, Utente₂ deve usare `dhparams2.pem`, mentre Utente₁ deve usare `dhparams1.pem`, rispettivamente. ✓
- d. Nessuna delle altre tre scelte.

Risposta corretta.

La risposta corretta è: Per derivare la propria coppia di chiavi, Utente₂ deve usare `dhparams2.pem`, mentre Utente₁ deve usare `dhparams1.pem`, rispettivamente.

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

Scegli un'alternativa:

- a. Di solito la firma digitale è concatenata all'hash di un file.
- b. Di solito la firma digitale è apposta sull'hash di un file.
- c. Di solito la firma digitale è ricavata a partire dall'hash di un file.
- d. Nessuna delle altre tre scelte. ✗

Risposta errata.

La risposta corretta è: Di solito la firma digitale è apposta sull'hash di un file.

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

Scegli un'alternativa:

- a. Senza l'utilizzo di una CRL l'unica entità a conoscenza della revoca di un determinato certificato è la CA che ha effettuato la revoca.
- b. Senza l'utilizzo di una CRL le uniche entità a conoscenza della revoca di un determinato certificato sono gli utenti i cui certificati sono stati rilasciati dalla stessa CA che ha effettuato la revoca.
- c. Senza l'utilizzo di una CRL l'unica entità a conoscenza della revoca di un determinato certificato è la CA di livello superiore rispetto a quella che ha effettuato la revoca. ✗
- d. Nessuna delle altre tre scelte.

Risposta errata.

La risposta corretta è: Senza l'utilizzo di una CRL l'unica entità a conoscenza della revoca di un determinato certificato è la CA che ha effettuato la revoca.

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

Scegli un'alternativa:

- a. L'autenticazione a due fattori richiede necessariamente la presenza di un cellulare per ricevere messaggi.
- b. L'autenticazione a due fattori richiede necessariamente la presenza di due diverse autenticazioni.
- c. L'autenticazione a due fattori richiede necessariamente la presenza di autenticazioni scelte tra fattori diversi (qualcosa che si sa, qualcosa che si possiede, caratteristiche biometriche). ✓
- d. L'autenticazione a due fattori richiede necessariamente la presenza di una device con one-time password.

Risposta corretta.

La risposta corretta è: L'autenticazione a due fattori richiede necessariamente la presenza di autenticazioni scelte tra fattori diversi (qualcosa che si sa, qualcosa che si possiede, caratteristiche biometriche).

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

Scegli un'alternativa:

- a. Il comando `rand` non può essere usato per generare stringhe di caratteri stampabili. ✓
- b. Il comando `rand` può utilizzare come seme un file arbitrario.
- c. Il comando `rand` utilizza di default come seme i `random` bit forniti da `/dev/urandom`.
- d. Il seme utilizzato dal comando `rand` può essere anche non specificato.

Risposta corretta

La risposta corretta è: Il comando `rand` non può essere usato per generare stringhe di caratteri stampabili.

Si assuma che Alice abbia generato una coppia di chiavi RSA (memorizzata in `rsaprivatekey.pem`), e voglia mandare a Bob la propria chiave pubblica. Indicare quale tra i seguenti comandi consente ad Alice di estrarre la propria chiave pubblica, a partire dalla coppia di chiavi generata in precedenza. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. `openssl rsa -pubin -in rsaprivatekey.pem -pubout -out rsapublickey.pem`
- b. `openssl rsa -in rsaprivatekey.pem -pubout -out rsapublickey.pem`
- c. `openssl rsa -in rsaprivatekey.pem -out rsapublickey.pem`
- d. Nessuna delle altre tre scelte

Risposta corretta.

La risposta corretta è: `openssl rsa -in rsaprivatekey.pem -pubout -out rsapublickey.pem`

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

Scegli un'alternativa:

- a. La caratteristica di permanenza stabilisce che una biometria non cambia nel tempo.
- b. La caratteristica di permanenza stabilisce il grado di permanenza di una determinata biometria.
- c. La caratteristica di permanenza può determinare la stabilità a breve o a lungo termine di un sistema biometrico.
- d. La caratteristica di permanenza caratterizza il tempo di permanenza necessario all'acquisizione di una determinata biometria.

Risposta corretta.

La risposta corretta è: La caratteristica di permanenza caratterizza il tempo di permanenza necessario all'acquisizione di una determinata biometria.

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

Scegli un'alternativa:

- a. L'analisi dinamica può portare alla diffusione del malware su altri sistemi mediante la rete.
- b. L'analisi dinamica è tipicamente effettuata utilizzando una modalità di rete chiamata "air-gapped".
- c. L'analisi dinamica è sempre indipendente dall'analisi statica. ✓
- d. L'analisi dinamica può portare all'infezione del sistema su cui il malware viene eseguito, oltre che dei dati in esso contenuti.

Risposta corretta.

La risposta corretta è: L'analisi dinamica è sempre indipendente dall'analisi statica.

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

Scegli un'alternativa:

- a. I cifrari a chiave pubblica sono utili perché rendono necessari i certificati digitali ed evitano l'anonymia.
- b. I cifrari a chiave pubblica sono utili perché si basano su problemi computazionali impossibili da risolvere efficientemente.
- c. I cifrari a chiave pubblica sono utili perché hanno una sicurezza maggiore rispetto ad AES, avendo chiavi di lunghezza maggiore di 256 bit.
- d. I cifrari a chiave pubblica sono utili perché risolvono il problema della condivisione di chiavi simmetriche. ✓

Risposta corretta.

La risposta corretta è: I cifrari a chiave pubblica sono utili perché risolvono il problema della condivisione di chiavi simmetriche.

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

Scegli un'alternativa:

- a. SHA1 è la più diffusa tra le funzione hash e non sono noti problemi di sicurezza ad oggi.
- b. Le funzioni hash SHA-256, SHA-392, SHA-512, raccomandate dal NIST, si basano sull'intrattabilità della fattorizzazione.
- c. L'output delle funzioni hash SHA-256, SHA-384, SHA-512 sono 256 bit, 384 bit e 512 bit, rispettivamente. ✓
- d. Le funzioni hash SHA-256, SHA-392, SHA-512, raccomandate dal NIST, si basano sull'intrattabilità del logaritmo discreto.

Risposta corretta.

La risposta corretta è: L'output delle funzioni hash SHA-256, SHA-384, SHA-512 sono 256 bit, 384 bit e 512 bit, rispettivamente.

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

Scegli un'alternativa:

- a. L'AES non è un cifrario di Feistel.
- b. Tutte le operazioni usate dall'AES sono facilmente ed efficientemente implementabili sia su architetture ad 8 bit che a 32 bit.
- c. Non sono chiari i criteri costruttivi delle S-box per l'AES.
- d. È possibile utilizzare chiavi di 128, 192, o 256 per l'AES e la lunghezza del blocco è 128 bit. ✗

Risposta errata.

La risposta corretta è: Non sono chiari i criteri costruttivi delle S-box per l'AES.

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

L'i-esima iterazione nel DES è data da

Scegli un'alternativa:

- a. $L_i = R_{(i-1)}$ ed $R_i = R_{(i-1)} \text{ XOR } f(L_{(i-1)}, K_i)$.
- b. $L_i = R_{(i-1)}$ ed $R_i = f(L_{(i-1)}) \text{ XOR } R_{(i-1)}, K_i$.
- c. $L_i = R_{(i-1)}$ ed $R_i = L_{(i-1)} \text{ XOR } f(R_{(i-1)}, K_i)$.
- d. $L_i = L_{(i-1)}$ ed $R_i = R_{(i-1)} \text{ XOR } f(L_{(i-1)}, K_i)$. X

Risposta errata.

La risposta corretta è: $L_i = R_{(i-1)}$ ed $R_i = L_{(i-1)} \text{ XOR } f(R_{(i-1)}, K_i)$.

Indicare quale tra i seguenti metodi è preferibile come generatore pseudocasuale (dal cui output ottenere dopo chiavi, challenge, ...). È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. Utilizzare la stringa ipod oppure ipad (usate nell'HMAC) come chiave per cifrare il seme, poi cifrare seme+1, poi cifrare seme+2, ... X
- b. Utilizzare la stringa concatenando $X(1), X(2), X(3), \dots$ dove $X(0)=\text{seme}$ e $X(i)=A*X(i-1)+B \bmod C$, ed A, B, C sono costanti.
- c. Utilizzare il seme come chiave per AES in counter mode.
- d. Utilizzare la stringa ottenuta concatenando seme, seme+1, seme+2, seme+3, ...

Risposta errata.

La risposta corretta è: Utilizzare il seme come chiave per AES in counter mode.