

Iniziato	mercoledì, 20 gennaio 2021, 09:26
Stato	Completato
Terminato	mercoledì, 20 gennaio 2021, 10:03
Tempo impiegato	37 min. 23 secondi
Valutazione	13 su un massimo di 30 (43%)

Domanda 1


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. Il Record Protocol consente di ottenere la mutua autenticazione tra le parti.
- ☐ b. Il Record Protocol si occupa della segnalazione di situazioni anomale.
- ☐ c. I parametri negoziati tramite il Record Protocol sono utilizzati dall'Handshake Protocol.
- ☒ d. Nessuna delle altre tre scelte. 

Navigazione quiz

1 ✓	2 ✗	3 ✓	4 ✓	5 ✗
6 ✗	7 ✓	8 ✓	9 ✗	10 ✗
11 ✗	12 ✓	13 ✗	14 ✓	15 ✗
16 ✗	17 ✓	18 ✗	19 ✗	20 ✗

Risposta errata

Visualizza una pagina alla volta

Fine revisione

Domanda **2**

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 Time Stamping Authority (TSA) può essere parte di una PKI.
- ☐ b. Una Time Stamping Authority (TSA) è **✗** usata da una CA per verificare la scadenza di un certificato.
- ☐ c. Una Time Stamping Authority (TSA) è usata da un utente per verificare la scadenza di un certificato.
- ☐ d. Nessuna delle altre tre scelte.

Risposta errata.

La risposta corretta è: Una Time Stamping Authority (TSA) può essere parte di una PKI.

Domanda 3

Risposta
corretta

Punteggio
ottenuto 2 su 2



Contrassegna
domanda

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

Scegli un'alternativa:

- ☐ a. Le caratteristiche di un sistema biometrico sono: Universalità, Univocità, Permanenza e Catturabilità.
- ☐ b. Le caratteristiche di un sistema biometrico sono: Universalità, Unicità, Resilienza e Catturabilità.
- ☒ c. Le caratteristiche di un sistema biometrico sono: Universalità, Unicità, Permanenza e Catturabilità. ✓
- ☐ d. Nessuna delle altre tre scelte.

Risposta corretta.

La risposta corretta è: Le caratteristiche di un sistema biometrico sono: Universalità, Unicità, Permanenza e Catturabilità.

Domanda 4

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

Risposta corretta.

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

Domanda 5

Risposta errata

Punteggio
ottenuto 0 su 2



Contrassegna
domanda

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

Scegli un'alternativa:

- ☐ a. La generazione di bit pseudocasuali in OpenSSL avviene mediante un *Deterministic Random Bit Generator (DRBG)*.
- ☐ b. Per la generazione di bit pseudocasuali OpenSSL utilizza di default un CTR DRBG basato su AES a 256 bit.
- ☒ c. OpenSSL di default utilizza come seme i random bit forniti da */dev/urandom*. ❌
- ☐ d. Nessuna delle altre tre scelte.

Risposta errata.

La risposta corretta è: Nessuna delle altre tre scelte.

Domanda 6

Risposta errata

Punteggio
ottenuto 0 su 2



Contrassegna
domanda

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

Scegli un'alternativa:

- ☐ a. Una CRL contiene i numeri seriali di tutti i certificati che sono stati revocati.
- ☐ b. Una CRL è emessa periodicamente da una CA per rendere noti i certificati che sono stati revocati.
- ☒ c. Una CRL non contiene i numeri seriali di tutti i certificati che sono scaduti. ✖
- ☐ d. Nessuna delle altre tre scelte.

Risposta errata.

La risposta corretta è: Nessuna delle altre tre scelte.

Domanda 7

Risposta
corretta

Punteggio
ottenuto 2 su 2



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

Risposta corretta.

La risposta corretta è: 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 $g^{(xy)} \bmod p$.

Domanda 8

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. Il DES è stato abbandonato come standard a causa del suo *avalanche effect*. 
- ☐ b. Le S-box del DES furono progettate per resistere all'attacco noto poi come Crittoanalisi Differenziale.
- ☐ 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 9

Risposta errata

Punteggio
ottenuto 0 su 2



Contrassegna
domanda

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

Scegli un'alternativa:

- ☐ a. L'analisi dinamica consiste nell'esaminare un malware durante la sua esecuzione.
- ☒ b. L'analisi dinamica viene di solito effettuata dopo quella statica. ✖
- ☐ c. L'analisi dinamica può portare all'infezione del sistema su cui essa viene effettuata.
- ☐ d. Nessuna delle altre tre scelte.

Risposta errata.

La risposta corretta è: Nessuna delle altre tre scelte.

Domanda 10

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. Il cifrario one-time pad è impossibile da rompere.
- ☐ b. Le altre tre scelte sono tutte sbagliate. ✗
- ☐ c. È possibile rompere il cifrario one-time pad se la chiave non è lunga.
- ☐ d. Non si sa se esiste un algoritmo efficiente che rompe il cifrario one-time pad.

Risposta errata.

La risposta corretta è: Il cifrario one-time pad è impossibile da rompere.

Domanda 11

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. Assumendo che venga utilizzata la codifica in Base64, la stringa binaria 010011010110000101101110 può essere codificata mediante 8 caratteri stampabili.
- ☐ b. Assumendo che venga utilizzata la codifica in Base64, la stringa binaria 010011010110000101101110 può essere codificata mediante 3 caratteri stampabili.
- ☒ c. Assumendo che venga utilizzata la codifica in Base64, la stringa binaria 010011010110000101101110 può essere codificata mediante 4 caratteri stampabili.
- ☐ d. Nessuna delle altre tre scelte.



Risposta errata.

La risposta corretta è: Assumendo che venga utilizzata la codifica in Base64, la stringa binaria 010011010110000101101110 può essere codificata mediante 4 caratteri stampabili.

Domanda **12**

Risposta
corretta

Punteggio
ottenuto 1 su 1



Contrassegna
domanda

Indicare quale tra le seguenti affermazioni non contiene errori. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. Alcune modalità operative di cifratura sono: ECB, CBC, DSS, CTR, EFF.
- ☐ b. Alcune modalità operative di cifratura sono: ECB, CBC, PKCS, OFB, NIST.
- ☒ c. Alcune modalità operative di cifratura sono: ECB, CBC, CFB, OFB, CTR. ✓
- ☐ d. Alcune modalità operative di cifratura sono: CBC, MAC, OFB, CTR, HMAC.

Risposta corretta.

La risposta corretta è: Alcune modalità operative di cifratura sono: ECB, CBC, CFB, OFB, CTR.

Domanda **13**

Risposta errata

Punteggio
ottenuto 0 su 1



Contrassegna
domanda

Siano *rsaprivatekey.pem* ed *rsapublickey.pem* rispettivamente le chiavi private e pubbliche di Bob. Indicare quale tra i seguenti comandi consente ad Alice di cifrare un messaggio per Bob. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☒ a. `openssl rsautl -encrypt -pubin -inkey rsapublickey.pem -in testoInChiaro.txt -out testoCifrato.txt`
- ☐ b. `openssl rsautl -encrypt -inkey rsapublickey.pem -in testoInChiaro.txt -out testoCifrato.txt`
- ☐ c. `openssl rsautl -encrypt -inkey rsapublickey.pem -in testoInChiaro.txt -pubout -out testoCifrato.txt`
- ☐ d. Nessuna delle altre tre scelte ✗

Risposta errata.

La risposta corretta è: `openssl rsautl -encrypt -pubin -inkey rsapublickey.pem -in testoInChiaro.txt -out testoCifrato.txt`

Domanda 14

Risposta
corretta

Punteggio
ottenuto 1 su 1



Contrassegna
domanda

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

Scegli un'alternativa:

- ☐ a. La sicurezza della firma RSA e della firma DSS si basano entrambi sulla difficoltà di calcolare logaritmi discreti.
- ☐ b. Nessuna delle altre tre scelte.
- ☒ c. La sicurezza della firma RSA si basa sulla difficoltà di fattorizzare e la sicurezza del DSS sulla difficoltà di calcolare logaritmi discreti. ✓
- ☐ d. La sicurezza della firma RSA e della firma DSS si basano entrambi sulla difficoltà di fattorizzare.

Risposta corretta.

La risposta corretta è: La sicurezza della firma RSA si basa sulla difficoltà di fattorizzare e la sicurezza del DSS sulla difficoltà di calcolare logaritmi discreti.

Domanda 15

Risposta errata

Punteggio
ottenuto 0 su 2



Contrassegna
domanda

Indicare quale tra le seguenti affermazioni è corretta, per la cifratura a chiave pubblica RSA soprattutto quando il messaggio è di grandezza maggiore del modulo. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. La cifratura di un messaggio viene sempre fatta con una singola esponenziazione modulare. La grandezza di un messaggio non è un problema poiché l'operazione viene eseguita in aritmetica modulare.
- ☒ b. RSA viene usata per cifrare il messaggio purché sia ✗ meno grande del modulo, altrimenti si divide il messaggio in blocchi di grandezza opportuna e si cifra ogni singolo blocco con RSA.
- ☐ c. Il modulo di RSA viene scelto molto grande, proprio per cifrare messaggi molto grandi. Quindi RSA non può essere usata per messaggi di grandezza maggiore del modulo.
- ☐ d. RSA viene usata per cifrare una chiave scelta casualmente che poi verrà usata per cifrare il messaggio mediante un cifrario simmetrico.

Risposta errata.

La risposta corretta è: RSA viene usata per cifrare una chiave scelta casualmente che poi verrà usata per cifrare il messaggio mediante un cifrario simmetrico.

Domanda 16

Risposta errata

Punteggio
ottenuto 0 su 1



Contrassegna
domanda

Siano *rsaprivatekey.pem* ed *rsapublickey.pem* rispettivamente le chiavi private e pubbliche di Alice. Indicare quale tra i seguenti comandi consente ad Alice di calcolare una firma per l'hash SHA-256 per il file *testoInChiaro.txt*. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☒ a. `openssl sha256 -sign rsaprivatekey.pem -out rsasign.bin testoInChiaro.txt`
- ☐ b. `openssl sha256 -sign rsaprivatekey.pem -pubout -out rsasign.bin testoInChiaro.txt`
- ☐ c. `openssl sha256 -sign -pubin rsaprivatekey.pem -out rsasign.bin testoInChiaro.txt`
- ☐ d. Nessuna delle altre tre scelte



Risposta errata.

La risposta corretta è: `openssl sha256 -sign rsaprivatekey.pem -out rsasign.bin testoInChiaro.txt`

Domanda 17

Risposta
corretta

Punteggio
ottenuto 1 su 1



Contrassegna
domanda

Indicare quale tra le seguenti affermazioni è corretta, data una chiave pubblica RSA (n,e) con chiave privata (n,d) . È possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. La cifratura del messaggio M è data da $C = e^M \bmod n$ e la decifratura da $M = d^C \bmod n$
- ☐ b. La cifratura del messaggio M è data da $C = M^e \bmod n$ e la decifratura da $M = d^C \bmod n$
- ☐ c. La cifratura del messaggio M è data da $C = M^e \bmod n$ e la decifratura da $M = C^d \bmod \phi(n)$
- ☒ d. La cifratura del messaggio M è data da $C = M^e \bmod n$ e la decifratura da $M = C^d \bmod n$ ✓

Risposta corretta.

La risposta corretta è: La cifratura del messaggio M è data da $C = M^e \bmod n$ e la decifratura da $M = C^d \bmod n$

Domanda 18

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 ciphersuite definisce uno schema per l'accordo/scambio di chiavi, uno schema per l'autenticazione, uno schema per la cifratura simmetrica ed uno schema per l'autenticazione del messaggio.
- ☐ b. Una ciphersuite definisce uno schema per l'accordo/scambio di chiavi ed uno schema per la cifratura simmetrica.
- ☒ c. Una ciphersuite definisce uno schema per l'accordo/scambio di chiavi, uno schema per l'autenticazione, uno schema per la cifratura simmetrica, uno schema per l'autenticazione del messaggio, ed uno schema per la generazione di numeri pseudocasuali. ✗
- ☐ d. Una ciphersuite definisce uno schema per l'accordo/scambio di chiavi, uno schema per l'autenticazione, uno schema per la cifratura simmetrica, ma non uno schema per l'autenticazione del messaggio.

Risposta errata.

La risposta corretta è: Una ciphersuite definisce uno schema per l'accordo/scambio di chiavi, uno schema per l'autenticazione, uno schema per la cifratura simmetrica ed uno schema per l'autenticazione del messaggio.

Domanda 19

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. L'Handshake Protocol consente alle parti di negoziare le primitive crittografiche necessarie per la sicurezza della comunicazione.
- ☐ b. L'Handshake Protocol consente alle parti di negoziare i parametri necessari per la sicurezza della comunicazione.
- ☒ c. L'Handshake Protocol non consente alle parti di autenticarsi. ✓
- ☐ d. L'Handshake Protocol consente alle parti di negoziare la versione del protocollo SSL/TLS da utilizzare.

Risposta corretta.

La risposta corretta è: L'Handshake Protocol non consente alle parti di autenticarsi.

Domanda **20**

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'*Enrollment* è un processo iterativo.
- ☐ b. L'*Enrollment* è un processo ricorsivo.
- ☐ c. L'*Enrollment* è un processo in parte iterativo ed in parte ricorsivo.
- ☐ d. Nessuna delle altre tre scelte.



Risposta errata.

La risposta corretta è: L'*Enrollment* è un processo iterativo.