

Terminato venerdì, 4 settembre 2020, 16:19

Tempo impiegato 35 min. 46 secondi

Valutazione 25 su un massimo di 30 (83%)

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. Nel ciclo di vita di un malware le fasi seguono il seguente ordine: Infezione, Quiescenza, Replicazione e Propagazione, Azioni Malevole. 
- ☐ b. Nel ciclo di vita di un malware le fasi seguono il seguente ordine: Quiescenza, Infezione, Azioni Malevole, Replicazione e Propagazione.
- ☐ c. Nel ciclo di vita di un malware le fasi seguono il seguente ordine: Infezione, Replicazione e Propagazione, Azioni Malevole, Quiescenza.
- ☐ d. Nel ciclo di vita di un malware le fasi seguono il seguente ordine: Infezione, Azioni Malevole, Quiescenza, Replicazione e Propagazione.

Risposta corretta.

La risposta corretta è: Nel ciclo di vita di un malware le fasi seguono il seguente ordine: Infezione, Quiescenza, Replicazione e Propagazione, Azioni Malevole.

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

Visualizza una pagina alla volta

Fine revisione

Domanda 3

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. Il calcolo della Timestamp Request è basato sull'utilizzo di funzioni hash.
- ☐ b. Il calcolo della Timestamp Response è basato sull'utilizzo di funzioni hash e firme digitali.
- ☐ c. Il Timestamp Response include un timestamp.
- ☒ 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 motivazioni è corretta. E' possibile effettuare una sola scelta:

Scegli un'alternativa:

- ☐ a. La firma grafometrica è essenzialmente un'immagine della firma autografa, senza altri rilevanti dati per la non falsificabilità.
- ☐ b. La firma grafometrica, essendo un caso particolare della firma digitale, ha la medesima efficacia probatoria della scrittura privata.
- ☒ 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 5

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. I cifrari a chiave pubblica sono utili perché risolvono il problema della condivisione di chiavi simmetriche. 
- ☐ 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 rendono necessari i certificati digitali ed evitano l'anonimia.

Risposta corretta.

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

Domanda 6

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

Risposta corretta.

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

Domanda 7

Risposta
corretta

Punteggio
ottenuto 2 su 2

Contrassegna
domanda

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

Risposta corretta.

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

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. L'Handshake Protocol garantisce alle parti l'interoperabilità tra le diverse implementazioni del protocollo SSL/TLS.
- ☒ b. L'Handshake Protocol è utilizzato per imporre alle parti l'esecuzione di un nuovo handshake. ✓
- ☐ c. L'Handshake Protocol consente alle parti di negoziare una ciphersuite.
- ☐ d. L'Handshake Protocol consente al Server di autenticare il Client.

Risposta corretta.

La risposta corretta è: L'Handshake Protocol è utilizzato per imporre alle parti l'esecuzione di un nuovo handshake.

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

Risposta corretta.

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

Domanda 10

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'identificazione basata su sistemi biometrici si occupa di effettuare matching "uno a molti" e matching "uno a pochi".
- ☐ b. L'identificazione basata su sistemi biometrici può operare sia su soggetti cooperativi che su soggetti non cooperativi.
- ☐ c. L'identificazione basata su sistemi biometrici cerca una corrispondenza all'interno di un database di modelli.
- ☒ d. Nessuna delle altre tre scelte. 

Risposta corretta.

La risposta corretta è: Nessuna delle altre tre scelte.

Domanda 11

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 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.

Domanda 12

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. È possibile effettuare il "resume" di una sessione a patto che Client e Server abbiano memorizzato i parametri di sessione.
- ☐ b. È possibile effettuare il "resume" di una sessione mediante lo scambio di opportune chiavi.
- ☒ c. È possibile effettuare il "resume" di una sessione mediante generatori pseudo-casuali. ✖
- ☐ d. Nessuna delle altre tre scelte.

Risposta errata.

La risposta corretta è: È possibile effettuare il "resume" di una sessione a patto che Client e Server abbiano memorizzato i parametri di sessione.

Domanda 13

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 fase di replicazione e propagazione è tipica della maggior parte dei software malevoli.
- ☒ b. Tutti i software malevoli presentano obiettivi di replicazione e propagazione.
- ☐ c. La fase di replicazione e propagazione è tipicamente condotta dal malware al verificarsi di determinati eventi o condizioni.
- ☐ d. Nessuna delle altre tre scelte.



Risposta errata.

La risposta corretta è: Tutti i software malevoli presentano obiettivi di replicazione e propagazione.

Domanda 14

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 $g^x \bmod p$. 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 $g^y \bmod p$. 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 $(g^x)^y \bmod p$. 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 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 15

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'*Identificazione/Autenticazione* è un processo iterativo.
- ☐ b. Il processo di *Identificazione/Autenticazione* avviene dopo il processo di *Enrollment*.
- ☒ c. Il processo di *Identificazione/Autenticazione* avviene prima del processo di *Enrollment*. ✓
- ☐ d. Il processo di *Identificazione/Autenticazione* si basa su un template matcher.

Risposta corretta.

La risposta corretta è: Il processo di *Identificazione/Autenticazione* avviene prima del processo di *Enrollment*.

Domanda 16

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 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) . ✓
- ☐ b. 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) .
- ☐ c. 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) .
- ☐ 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

Domanda 17

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. A partire da una chiave pubblica RSA a 1024 bit è facile recuperare la relativa chiave privata. ✖
- ☒ b. A partire da una chiave pubblica RSA a 1024 bit è molto difficile recuperare la relativa chiave privata.
- ☐ c. A partire da una chiave pubblica RSA a 1024 bit è impossibile recuperare la relativa chiave privata.
- ☐ d. Nessuna delle altre tre scelte.

Risposta errata.

La risposta corretta è: A partire da una chiave pubblica RSA a 1024 bit è molto difficile recuperare la relativa chiave privata.

Domanda **18**

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. Il paradosso del compleanno è utile perché per la sicurezza di tutti è necessario evitare assembramenti e feste nel periodo emergenziale.
- ☐ b. Il paradosso del compleanno è utile per analizzare il tempo necessario per trovare la chiave privata per il DES.
- ☐ c. Il paradosso del compleanno è utile per analizzare la difficoltà di invertire le funzioni hash.
- ☒ d. Il paradosso del compleanno è utile per analizzare la probabilità di successo di trovare collisioni nelle funzioni hash. ✓

Risposta corretta.

La risposta corretta è: Il paradosso del compleanno è utile per analizzare la probabilità di successo di trovare collisioni nelle funzioni hash.

Domanda 19

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. 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.
- ☒ b. 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. ✓
- ☐ c. 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.
- ☐ 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 corretta.

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.

Domanda 20

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 perché la chiave è troppo corta.
- ☒ b. Il DES è stato abbandonato come standard a causa del suo *avalanche effect*. ✓
- ☐ c. Le S-box del DES furono progettate per resistere all'attacco noto poi come Crittoanalisi Differenziale.
- ☐ 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*.