Domanda 3

Risposta corretta

Punteggio max.: 2

Contrassegna domanda

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

Per lo scambio di chiavi Diffie-Hellman, una scelta corretta (tralasciando considerazioni sulla lunghezza) per il primo p ed il generatore g è:

a. p = 7 e g = 2.

b. p = 5 e g = 3. ✔

c. p = 5 e g = 1.

d. p = 13 e g = 3.

Domanda 4

Risposta errata

Punteggio max.: 1

Contrassegna domanda

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

a. L'AES è un cifrario a blocchi con una chiave di lunghezza 128, 192 oppure 256 bit. Se la chiave fosse di 128 bit potrebbe essere rotto nella pratica in pochi giorni da una macchina parallela. Tale attacco non è possibile se la chiave fosse di 256 bit.

b. L'AES con una chiave di lunghezza 128 bit potrebbe essere rotto nella pratica in pochi giorni da una macchina altamente parallela. Se la chiave fosse di 256 bit, tale attacco richiederebbe qualche anno. ✖

c. L'AES con una chiave di 128 bit ha una sicurezza poco più del doppio del cifrario DES.

d. Tutte le altre risposte sono errate.

Iniziato mercoledì, 28 giugno 2023, 09:33
Stato Completato
Terminato mercoledì, 28 giugno 2023, 10:33
Tempo impiegato 1 ora

Domanda 1
Risposta corretta
Punteggio max.: 1
Contrassegna domanda

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

a. Le macchine a rotori implementano cifrari a sostituzione monoalfabetica.

b. Le macchine a rotori implementano cifrari a sostituzione polialfabetica. ✓

c. Le altre tre scelte sono tutte sbagliate.

d. Le macchine a rotori implementano il cifrario di Vigenère.

Domanda 2
Risposta corretta
Punteggio max.: 1
Contrassegna domanda

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

a. La verifica del timestamp relativo ad un file può essere effettuata da chiunque. ✓

b. La verifica del timestamp relativo ad un file si basa esclusivamente sul calcolo di funzioni hash.

c. Nessuna delle altre tre scelte.

d. La verifica del timestamp relativo ad un file può essere effettuata solo da chi ha emesso il Timestamp Request.

nanda 18
posta errata
nteggio max.:
ntrassegna
manda

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

- a. Le altre tre scelte sono tutte sbagliate. ✖
- b. L'Electronic codebook chaining (ECB) è complesso da implementare.
- c. L'Electronic codebook chaining (ECB) non è parallelizzabile.
- d. L'Electronic codebook chaining (ECB) ha problemi di sicurezza per messaggi lunghi.

Domanda 19
Risposta corretta
Punteggio max.: 2
Contrassegna domanda

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

- a. Una CRL contiene per ciascun certificato revocato la relativa data di revoca.
- b. Una CRL contiene i numeri di serie di tutti i certificati che sono scaduti. ✔
- c. Una CRL contiene i numeri di serie dei certificati che sono stati revocati.
- d. Una CRL è emessa periodicamente da una CA per pubblicare i certificati che sono stati revocati.

Domanda 20
Risposta errata

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

Domanda 17
Risposta errata
Punteggio max.: 2
Contrassegna domanda

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

a. In un sistema biometrico multimodale con progettazione in serie le acquisizioni delle biometrie sono combinate mediante tecniche di fusione. ✖

b. In un sistema biometrico multimodale con progettazione in serie devono essere per forza soddisfatte tutte le biometrie del sistema.

c. Un sistema biometrico multimodale con progettazione in serie può avere un tempo di elaborazione ridotto rispetto ad un sistema biometrico multimodale con progettazione in parallelo.

d. In un sistema biometrico multimodale con progettazione in serie devono essere per forza utilizzate tutte le biometrie del sistema.

Domanda 18
Risposta errata
Punteggio max.: 1
Contrassegna domanda

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

a. Le altre tre scelte sono tutte sbagliate. ✖

b. L'Electronic codebook chaining (ECB) è complesso da implementare.

c. L'Electronic codebook chaining (ECB) non è parallelizzabile.

d. L'Electronic codebook chaining (ECB) ha problemi di

d. E l'hash di un MAC.

Domanda 15

Risposta corretta

Punteggio max.: 2

Contrassegna domanda

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

Il numero di possibili chiavi in un cifrario di Vigenère con alfabeto di 27 caratteri e lunghezza della chiave t è uguale a

a. 26^t. ✓

b. 26! t.

c. 26 t!.

d. 26^t!.

Domanda 16

Risposta corretta

Punteggio max.: 2

Contrassegna domanda

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

Supponiamo che n=pq, dove p=5 e q=11 (Si tralascino considerazioni sulla lunghezza). Gli esponenti pubblico e privato per RSA potrebbero essere

a. e=9 e d=9. ✓

b. e=11 e d=7.

c. e=9 e d=5.

d. e=3 e d=13.

Domanda 17

d. L'*Autenticazione* avviene su soggetti non cooperativi.

14
errata
o max.:
egna
a

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

a. È una funzione hash che utilizza un MAC. ✗

b. È un MAC che utlizza due volte una funzione hash.

c. È un MAC che può essere utilizzato anche come funzione hash.

d. È l'hash di un MAC.

da 15
ta
a
ggio max.:
assegna
nda

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

Il numero di possibili chiavi in un cifrario di Vigenère con alfabeto di 27 caratteri e lunghezza della chiave t è uguale a ✓

a. 26^t.

b. 26! t.

c. 26 t!.

d. 26^t!.

nanda 16
posta
retta

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

anda 12

osta
etta

teggio max.:

ntrassegna
manda

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

a. Nel Cipher Block Chaining (CBC) se decifriamo con un IV errato, solo il primo blocco è decifrato in modo errato. ✔

b. Nel Cipher Block Chaining (CBC) non vengono utilizzati IV.

c. Il Cipher Block Chaining (CBC) consente una cifratura ed una decifrtura parallelizzabili.

d. Le altre tre scelte sono tutte sbagliate.

Domanda 13

Risposta errata

Punteggio max.: 1

Contrassegna domanda

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

a. L'*Identificazione* avviene prima del processo di *Enrollment*.

b. L'*Autenticazione* si basa su un processo iterativo.

c. Nessuna delle altre tre scelte. ✖

d. L'*Autenticazione* avviene su soggetti non cooperativi.

Domanda 14

Risposta errata

Punteggio max.: 1

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

a. È una funzione hash che utilizza un MAC. ✖

10

o max.:

segna
a

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

a. L'analisi dinamica white box rappresenta un approccio meno dispendioso rispetto a quello black box.

b. L'analisi dinamica white box può essere usata in alternativa all'analisi statica.

c. L'analisi dinamica white box non può essere usata per ottenere informazioni dettagliate.

d. L'analisi dinamica white box richiede la conoscenza di dettagli sulle caratteristiche e sul codice del malware in esame. ✔

nda 11

sta errata

ggio max.:

assegna
nda

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

a. La richiesta e l'emissione di un certificato per una TSA richiede l'utilizzo di particolari estensioni.

b. Un certificato per una TSA non può essere emesso da una CA.

c. Nessuna delle altre tre scelte. ✖

d. Un certificato per una TSA può essere solo di tipo *self-signed*.

2^56.

d. Le altre tre scelte sono tutte sbagliate. ✗

Domanda 8

Risposta corretta

Punteggio max.: 1

Contrassegna domanda

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

a. Una Time Stamping Authority (TSA) è usata da un utente per verificare la scadenza di un certificato.

b. Nessuna delle altre tre scelte. ✓

c. Una Time Stamping Authority (TSA) è usata da una CA per verificare la scadenza di un certificato.

d. Una Time Stamping Authority (TSA) non può essere parte di una PKI.

Domanda 9

Risposta errata

Punteggio max.: 2

Contrassegna domanda

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

Supponiamo che n=pq,

a. p è circa n^(1/3) , cioè p=O(n^(1/3)).

b. Le altre tre scelte sono tutte sbagliate. ✗

c. p e q sono circa log n, cioè p=O(log n) e q=O(log n).

d. p è circa n^0,5, cioè p=O(n^0,5).

10

1080

acer

ASPIRE

per aggiornare la versione di TLS in uso.

anda 6
sta errata
eggio max.:
rassegna
anda

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

- a. In fase di analisi possono essere estratte generalmente poche stringhe a partire dai programmi legittimi (non malevoli). ✗
- b. Se in seguito all'analisi di un programma vengono individuate molte stringhe, probabilmente il programma è stato offuscato.
- c. Da un malware compresso (meccanismo di packing) o offuscato possono essere estratte moltissime stringhe.
- d. Nessuna delle altre tre scelte.

manda 7
posta errata
nteggio max.:
ntrassegna
manda

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

- a. Il numero delle possibili chiavi nel DES doppio è 2^128.
- b. Il numero delle possibili chiavi nel DES doppio è 2^112.
- c. Il numero delle possibili chiavi nel DES doppio è 2^56 + 2^56.
- d. Le altre tre scelte sono tutte sbagliate. ✗

omanda 8

Indicare quale tra le seguenti affermazioni è corretta. È

manda 4

sposta errata

unteggio max.:

Contrassegna domanda

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

a. L'AES è un cifrario a blocchi con una chiave di lunghezza 128, 192 oppure 256 bit. Se la chiave fosse di 128 bit potrebbe essere rotto nella pratica in pochi giorni da una macchina parallela. Tale attacco non è possibile se la chiave fosse di 256 bit.

b. L'AES con una chiave di lunghezza 128 bit potrebbe essere rotto nella pratica in pochi giorni da una macchina altamente parallela. Se la chiave fosse di 256 bit, tale attacco richiederebbe qualche anno. ✗

c. L'AES con una chiave di 128 bit ha una sicurezza poco più del doppio del cifrario DES.

d. Tutte le altre risposte sono errate.

Domanda 5

Risposta corretta

Punteggio max.: 1

Contrassegna domanda

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

a. Il Change Cipher Spec Protocol è caratterizzato dallo scambio di tre messaggi.

b. Il Change Cipher Spec Protocol è eseguito dalle parti alla cifratura di ogni messaggio.

c. Il Change Cipher Spec Protocol è utilizzato dalla parti per aggiornare la ciphersuite in uso. ✓

d. Il Change Cipher Spec Protocol è utilizzato dalle parti per aggiornare la versione di TLS in uso.

etta
nteggio max.:
ntrassegna
manda

a. Una CRL contiene per ciascun certificato revocato la relativa data di revoca.

b. Una CRL contiene i numeri di serie di tutti i certificati che sono scaduti. ✔

c. Una CRL contiene i numeri di serie dei certificati che sono stati revocati.

d. Una CRL è emessa periodicamente da una CA per pubblicare i certificati che sono stati revocati.

Domanda 20
Risposta errata
Punteggio max.:
2
Contrassegna domanda

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

a. Il messaggio *Certificate* è utilizzato per inviare al Client il certificato del Server.

b. Nessuna delle altre tre scelte. ✖

c. Il messaggio *Certificate* da parte del Server verso il Client è utilizzato per richiedere il Certificato del Client.

d. L'invio dei messaggi *Certificate* e *ServerKeyExchange* da parte del Server verso il Client è mutuamente esclusivo.

Fine revisione