SIC - Quiz 02- Crypto Tools

Domanda 1

Domanda 1 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Il messaggio o i dati originali che vengono forniti in input all'algoritmo sono chiamati _____.

Scegli un'alternativa:

- a. Testo in chiaro
- b. Chiave segreta
- c. Algoritmo di cifratura
- d. Algoritmo di decifratura

[OK] A: Testo in chiaro

Domanda 2

Domanda 2 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

_ _ _ _ _ _ _ _ _ _ è l'algoritmo di cifratura eseguito al contrario.

Scegli un'alternativa:

- a. L'algoritmo di cifratura
- b. Il testo in chiaro
- c. Algoritmo di decifratura
- d. Il testo cifrato

[OK] C: Algoritmo di decifratura

Domanda 3

Domanda 3 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

_ _ _ _ _ _ _ _ _ _ è il messaggio cifrato prodotto come output.

Scegli un'alternativa:

- a. Testo cifrato
- b. Testo in chiaro
- c. Crittoanalisi
- d. Chiave segreta

[OK] A: Testo cifrato

Domanda 4

Domanda 4 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

In media, _____ di tutte le chiavi possibili devono essere provate per ottenere successo con un attacco a forza bruta.

Scegli un'alternativa:

- a. Due terzi
- b. Tre quarti
- c. Un quarto
- d. Metà

[ERROR]: Due terzi? ⇒ Metà

Domanda 5

Domanda 5 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Gli algoritmi simmetrici più importanti, tutti cifrari a blocchi, sono il DES, il triple DES e _____.

Scegli un'alternativa:

- a. SHA
- b. RSA
- c. AES
- d. DSS

[OK] C: AES

Domanda 6

Domanda 6 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Se l'unica forma di attacco che può essere effettuata su un algoritmo di cifratura è la forza bruta, allora il modo per contrastare tali attacchi sarebbe _____.

Scegli un'alternativa:

- a. Usare chiavi più lunghe
- b. Usare due chiavi
- c. Usare chiavi più corte
- d. Usare meno chiavi

[OK] A: Usare chiavi piu' lunghe

Domanda 7

Domanda 7 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

_ _ _ _ _ _ _ _ _ _ è una procedura che consente alle parti comunicanti di verificare che i messaggi ricevuti o memorizzati siano autentici.

Scegli un'alternativa:

- a. Resistenza alle collisioni
- b. Autenticazione del messaggio
- c. Decifratura
- d. Crittoanalisi

[OK] B: Autenticazione del messaggio

Domanda 8

Domanda 8 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Lo scopo di un/una _ _ _ _ _ _ _ _ _ _ è produrre un'"impronta digitale" di un file, messaggio o altro blocco di dati.

Scegli un'alternativa:

- a. Flusso di chiavi
- b. Firma digitale
- c. Funzione hash
- d. Chiave segreta

[ERRORE] B: Firma digitale ⇒ [OK] Funzione hash

Domanda 9

Domanda 9 Risposta non ancora data Punteggio max.: 1,00 Rimuovi contrassegno

_ _ _ _ _ _ _ _ _ _ è un cifrario a blocchi in cui il testo in chiaro e il testo cifrato sono interi compresi tra 0 e n-1 per un certo n.

Scegli un'alternativa:

- a. AES
- b. DSS
- c. RSA
- d. SHA

[ERRORE]: ⇒ [OK] RSA

Domanda 10

Domanda 10 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un/Una _ _ _ _ _ _ _ _ _ _ è creata utilizzando una funzione hash sicura per generare un valore hash per un messaggio e poi cifrando il codice hash con una chiave privata.

Scegli un'alternativa:

- a. Funzione hash unidirezionale
- b. Firma digitale
- c. Flusso di chiavi
- d. Chiave segreta

[OK] Firma digitale

Domanda 11

Domanda 11 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

I dati trasmessi memorizzati localmente sono chiamati _ _ _ _ _ _ _ _ _ _.

Scegli un'alternativa:

- a. Testo cifrato
- b. Dati a riposo
- c. ECC
- d. DES

[OK] Dati a riposo

Domanda 12

Domanda 12 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Le firme digitali e la gestione delle chiavi sono le due applicazioni più importanti della cifratura a _____.

Scegli un'alternativa:

- a. Avanzata
- b. Preimmagine resistente
- c. Chiave privata
- d. Chiave pubblica

[OK] Chiave pubblica

Domanda 13

Domanda 13 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un/Una _____ consiste nel provare ogni possibile chiave su un pezzo di testo cifrato finché non si ottiene una traduzione intelligibile in testo in chiaro.

Scegli un'alternativa:

- a. Crittoanalisi
- b. Modo di operazione
- c. Funzione hash
- d. Attacco a forza bruta

[OK] Attacco a forza bruta

Domanda 14

Domanda 14 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Chiamata anche cifratura a chiave singola, la tecnica universale per fornire riservatezza ai dati trasmessi o memorizzati è la _____.

Scegli un'alternativa:

- a. Cifratura asimmetrica
- b. Funzione hash
- c. Cifratura a chiave pubblica
- d. Cifratura simmetrica

[OK] Cifratura simmetrica

Domanda 15

Domanda 15 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Esistono due approcci generali per attaccare uno schema di cifratura simmetrica: attacchi crittoanalitici e attacchi a _____.

Scegli un'alternativa:

- a. Forza bruta
- b. Man-in-the-middle
- c. Collisione hash
- d. Replay

[ERRORE]: Replay ⇒ [OK] Forza bruta

Domanda 16

Domanda 16 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

L'algoritmo di _____ prende il testo cifrato e la chiave segreta e produce il testo in chiaro originale.

Scegli un'alternativa:

- a. Hash
- b. Cifratura
- c. Decifratura
- d. Firma digitale

[OK] Decifratura

Domanda 17

Domanda 17 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un attacco _____ sfrutta le caratteristiche dell'algoritmo per tentare di dedurre un testo in chiaro specifico o per dedurre la chiave utilizzata.

Scegli un'alternativa:

- a. Di crittoanalisi
- b. Man-in-the-middle
- c. A forza bruta
- d. Replay

[OK] Di crittoanalisi

Domanda 18

Domanda 18 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un _____ elabora l'input di testo in chiaro in blocchi di dimensione fissa e produce un blocco di testo cifrato di uguale dimensione per ogni blocco di testo in chiaro.

Scegli un'alternativa:

- a. Cifrario a flusso
- b. Firma digitale
- c. Funzione hash
- d. Cifrario a blocchi

[OK] Cifrario a blocchi

Domanda 19

Domanda 19 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un _ _ _ _ _ _ _ _ _ _ elabora gli elementi di input in modo continuo, producendo in output un elemento alla volta.

Scegli un'alternativa:

- a. Codice di autenticazione del messaggio
- b. Cifrario a blocchi
- c. Funzione hash
- d. Cifrario a flusso

[OK] Cifrario a flusso

Domanda 20

Domanda 20 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

La cifratura a chiave pubblica fu proposta pubblicamente per la prima volta da _ _ _ _ _ _ _ _ _ _ nel 1976.

Scegli un'alternativa:

- a. Merkle e Hellman
- b. Diffie e Hellman
- c. Turing
- d. El Gamal
- e. Rivest, Shamir e Adleman

[OK] Diffie e Hellman

Domanda 21

Domanda 21 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

I due criteri utilizzati per validare che una sequenza di numeri sia casuale sono l'indipendenza e la _____.

Scegli un'alternativa:

- a. Robustezza crittografica
- b. Prevedibilità
- c. Distribuzione normale
- d. Distribuzione uniforme

[OK] Distribuzione uniforme

Domanda 22

Domanda 22 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

L'approccio più semplice alla cifratura multipla a blocchi è noto come modalità _____, in cui il testo in chiaro è gestito n bit alla volta e ogni blocco di testo in chiaro è cifrato utilizzando la stessa chiave.

Scegli un'alternativa:

- a. Counter (CTR)
- b. Output feedback (OFB)
- c. Cipher block chaining (CBC)
- d. Electronic codebook (ECB)

[OK] Electronic codebook

Domanda 23

Domanda 23 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un flusso _____ è uno che è imprevedibile senza la conoscenza della chiave di input e che ha una sequenza apparentemente casuale.

Scegli un'alternativa:

- a. Deterministico
- b. Caotico
- c. Pseudocasuale
- d. Casuale

[ERRORE]: Casuale ⇒ [OK] Pseudo-casuale

Domanda 24

Domanda 24 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Le _ _ _ _ _ _ _ _ _ _ sono una coppia di chiavi che sono state selezionate in modo che se una è usata per la cifratura, l'altra è usata per la decifratura.

Scegli un'alternativa:

- a. Chiavi master
- b. Chiavi pubblica e privata
- c. Chiavi simmetriche
- d. Chiavi di sessione

[OK] Chiavi pubblica e privata

Domanda 25

Domanda 25 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Lo scopo dell'algoritmo _____ è consentire a due utenti di raggiungere in modo sicuro un accordo su un segreto condiviso che può essere utilizzato come chiave segreta per la successiva cifratura simmetrica dei messaggi.

Scegli un'alternativa:

- a. Advanced Encryption Standard (AES)
- b. RSA
- c. Diffie-Hellman Key Agreement
- d. Digital Signature Standard (DSS)

[OK] Diffie-Hellman Key Agreement.

Domanda 26

Domanda 26 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

La cifratura simmetrica è utilizzata principalmente per fornire riservatezza.

Scegli un'alternativa:

- a. Vero
- b. Falso

[OK] Vero

Domanda 27

Domanda 27 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Due delle più importanti applicazioni della cifratura a chiave pubblica sono le firme digitali e la gestione delle chiavi.

Scegli un'alternativa:

- a. Falso
- b. Vero

[OK] Vero

Domanda 28

Domanda 28 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Gli attacchi crittoanalitici provano ogni possibile chiave su un pezzo di testo cifrato finché non si ottiene una traduzione intelligibile in testo in chiaro.

Scegli un'alternativa:

- a. Vero
- b. Falso

[OK] Falso

Domanda 29

Domanda 29 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

La chiave segreta è fornita in input all'algoritmo di cifratura.

Scegli un'alternativa:

- a. Vero
- b. Falso

[OK] Vero

Domanda 30

Domanda 30 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Triple DES prende un blocco di testo in chiaro di 64 bit e una chiave di 56 bit per produrre un blocco di testo cifrato di 64 bit.

Scegli un'alternativa:

- a. Falso
- b. Vero

[ERRORE]: " ⇒ [OK] Falso

Domanda 31

Domanda 31 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

I modi di operazione sono le tecniche alternative che sono state sviluppate per aumentare la sicurezza della cifratura a blocchi simmetrica per grandi sequenze di dati.

Scegli un'alternativa:

- a. Falso
- b. Vero

[ERRORE]: " ⇒ [OK] Vero

Domanda 32

Domanda 32 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Il vantaggio di un cifrario a flusso è che si possono riutilizzare le chiavi.

Scegli un'alternativa:

- a. Falso
- b. Vero

[ERRORE]: " ⇒ [OK] Vero

Domanda 33

Domanda 33 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un codice di autenticazione del messaggio è un piccolo blocco di dati generato da una chiave segreta e aggiunto a un messaggio.

Scegli un'alternativa:

- a. Vero
- b. Falso

[OK] Vero

Domanda 34

Domanda 34 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Come il MAC, anche una funzione hash prende in input una chiave segreta.

Scegli un'alternativa:

- a. Falso
- b. Vero

[OK] Vero

Domanda 35

Domanda 35 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

La robustezza di una funzione hash contro gli attacchi a forza bruta dipende dalla lunghezza del codice hash prodotto dall'algoritmo.

Scegli un'alternativa:

- a. Falso
- b. Vero

[OK] Vero

Domanda 36

Domanda 36 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

La crittografia a chiave pubblica è asimmetrica.

Scegli un'alternativa:

- a. Falso
- b. Vero

[OK] Vero

Domanda 37

Domanda 37 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Gli algoritmi a chiave pubblica sono basati su operazioni semplici su pattern di bit.

Scegli un'alternativa:

- a. Falso
- b. Vero

[OK] Falso

Domanda 38

Domanda 38 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Lo scopo dell'algoritmo DSS è consentire a due utenti di raggiungere in modo sicuro un accordo su un segreto condiviso che può essere utilizzato come chiave segreta per la successiva cifratura simmetrica dei messaggi.

Scegli un'alternativa:

- a. Vero
- b. Falso

[OK] Falso

Domanda 39

Domanda 39 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un elemento importante in molti servizi e applicazioni di sicurezza informatica è l'uso di algoritmi crittografici.

Scegli un'alternativa:

- a. Falso
- b. Vero

[OK] Vero

Domanda 40

Domanda 40 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

È necessaria una qualche forma di protocollo per la distribuzione delle chiavi pubbliche.

Scegli un'alternativa:

- a. Vero
- b. Falso

[OK] Vero