Principio del formulario

Domanda 1

Risposta corretta

Punteggio ottenuto 1 su 1

Contrassegna domanda

Testo della domanda

Quale attacco può essere facilmente tentato verso un cifrario monoalfabetico?



a.

Crittoanalisi differenziale



b.

Statistica tau



c.

Attacchi temporizzati



d.

Analisi delle frequenze

Feedback

La risposta corretta è: Analisi delle frequenze

Domanda 2

Risposta corretta

Punteggio ottenuto 1 su 1

Contrassegna domanda

Testo della domanda

In quale fase del round di AES si utilizza una S-Box?



a.

Add round key



b.

Substitute bytes



c.

Shift rows



d.

Mix columns

Feedback

La risposta corretta è: Substitute bytes

Domanda 3

Risposta corretta

Punteggio ottenuto 1 su 1

Contrassegna domanda

Testo della domanda

La steganografia è una tecnica che consiste nel



a.

Proteggere il messaggio con l'hashing



b.

Proteggere il messaggio occultandolo



c.

Proteggere il messaggio usando la dattilografia



d.

Proteggere il messaggio con la crittografia

Feedback

La risposta corretta è: Proteggere il messaggio occultandolo

Domanda 4

Risposta errata

Punteggio ottenuto 0 su 1

Contrassegna domanda

Testo della domanda

Chi firma la chiave pubblica di una Root Certificate Authority?



a.

Una registration authority



b.

Lo Stato in cui risiedono i server della Root CA



c.

La Root CA tramite un certificato self-signed



d.

Una Key Certificate Authority

Feedback

La risposta corretta è: La Root CA tramite un certificato self-signed

Domanda 5

Risposta corretta

Punteggio ottenuto 1 su 1

Contrassegna domanda

Testo della domanda

Quale affermazione sull'hashing è FALSA?



a.

La funzione di hashing potrebbe produrre delle collisioni.



b.

La funzione di hashing è invertibile.



c.

La funzione di hashing prende un input di lunghezza variabile.



d.

La funzione di hashing produce un output di lunghezza fissa.

Feedback

La risposta corretta è: La funzione di hashing è invertibile.

Domanda 6

Risposta corretta

Punteggio ottenuto 1 su 1

Contrassegna domanda

Testo della domanda

Tralasciando la capacità computazionale odierna, il principale difetto del cifrario di Vigenère, che ne ha consentito una decrittografia anche manuale, è dovuto a



a.

la ripetizione della chiave porta con buona probabilità a sequenze ripetute dove è possibile effettuare attacchi statistici.



b.

una macchina inventata da Alan Turing durante la Seconda Guerra Mondiale, conosciuta come "The Bomb".



c.

l'attacco conosciuto come meet-in-the-middle.



d.

lo spazio delle chiavi è talmente piccolo che può essere ricercato a mano.

Feedback

La risposta corretta è: la ripetizione della chiave porta con buona probabilità a sequenze ripetute dove è possibile effettuare attacchi statistici.

Domanda 7

Risposta corretta

Punteggio ottenuto 1 su 1

Contrassegna domanda

Testo della domanda

Quale tra i seguenti NON è un campo contenuto in un certificato digitale X.509



a.

Validità temporale



b.

Chiave pubblica



c.

Firma digitale



d.

Chiave privata

Feedback

La risposta corretta è: Chiave privata

Domanda 8

Risposta errata

Punteggio ottenuto 0 su 1

Contrassegna domanda

Testo della domanda

L'algoritmo DES è un cifrario che lavora su



a.

Numeri binari



b.

Stringhe di testo



c.

Numeri decimali

Feedback

La risposta corretta è: Numeri binari

Domanda 9

Risposta errata

Punteggio ottenuto 0 su 1

Contrassegna domanda

Testo della domanda

L'algoritmo DES è deprecato.



a.

Falso: DES è usato ancora oggi



b.

Falso: DES è un cifrario perfetto ma inutilizzabile nella pratica



c.

Vero: lo spazio delle chiavi è troppo piccolo per la capacità computazionale odierna



d.

Vero: è stato decrittato con il test di Kasiski

Feedback

La risposta corretta è: Vero: lo spazio delle chiavi è troppo piccolo per la capacità computazionale odierna

Domanda 10

Risposta errata

Punteggio ottenuto 0 su 1

Contrassegna domanda

Testo della domanda

Se Eve controllando il canale di comunicazione intercetta le chiavi pubbliche di Alice e Bob, può falsificarle e mettersi in mezzo alla comunicazione?



a.

No, le chiavi pubbliche non possono essere intercettate



b.

Sì, può farlo



c.

Può farlo solo se le chiavi pubbliche non sono certificate



d.

No, anche se vengono intercettate non possono essere falsificate

Feedback

La risposta corretta è: Può farlo solo se le chiavi pubbliche non sono certificate

Domanda 11

Risposta corretta

Punteggio ottenuto 1 su 1

Contrassegna domanda

Testo della domanda

Bob imposta un certificato digitale X.509 sul proprio client di posta elettronica e scrive ad Alice usando la firma digitale. Quale affermazione è FALSA?



a.

Alice non può essere sicura che il messaggio provenga davvero da Bob.



b.

Se Alice cancella il certificato digitale non può più leggere la posta crittografata.



c.

Bob non può crittografare le email finché Alice non gli invia un messaggio che contiene il suo certificato.



d.

Bob deve revocare il certificato digitale se la sicurezza del suo dispositivo è compromessa.

Feedback

La risposta corretta è: Alice non può essere sicura che il messaggio provenga davvero da Bob.

Domanda 12

Risposta corretta

Punteggio ottenuto 1 su 1

Contrassegna domanda

Testo della domanda

Il cifrario AES è



a.

un algoritmo a chiave privata.



b.

un algoritmo a chiave pubblica.



c.

un algoritmo a chiave simmetrica.



d.

un algoritmo di scambio delle chiavi crittografiche.

Feedback

La risposta corretta è: un algoritmo a chiave simmetrica.

Domanda 13

Risposta errata

Punteggio ottenuto 0 su 1

Contrassegna domanda

Testo della domanda

AES può gestire chiavi crittografiche di quanti bit?



a.

256, 512 e 1024 bit



b.

128 bit



c.

Variabile, a discrezione di chi lo utilizza



d.

128, 192 e 256 bit

Feedback

La risposta corretta è: 128, 192 e 256 bit

Domanda 14

Risposta corretta

Punteggio ottenuto 1 su 1

Contrassegna domanda

Testo della domanda

L'hashing è:



a.

un algoritmo di crittografia simmetrica.



b.

un algoritmo di crittografia asimmetrica.



c.

un algoritmo di autenticazione del messaggio basato su una chiave crittografica.



d.

un algoritmo che produce un digest dell'input.

Feedback

La risposta corretta è: un algoritmo che produce un digest dell'input.

Domanda 15

Risposta errata

Punteggio ottenuto 0 su 1

Contrassegna domanda

Testo della domanda

L'analisi iniziale dei pattern nel test di Kasiski cosa permette di dedurre?



a.

La prima lettera della chiave.



b.

La frequenza delle vocali.



c.

La lunghezza del messaggio.



d.

La probabile lunghezza della chiave.

Feedback

La risposta corretta è: La probabile lunghezza della chiave.

Final del formulario

[Fine revisione](https://fad.its-ictpiemonte.it/mod/quiz/view.php?id=23567)