Principio del formulario

Domanda 1

Completo

Punteggio ottenuto 6 su 10

Contrassegna domanda

Testo della domanda

Che cos'è un algoritmo di hashing? Cosa sono la resistenza debole e forte alle collisioni?

Testo della risposta

La funzione di hash produce una sequenza di bit, detta digest, strettamente correlata con i dati in ingresso la sua lunghezza puo variare secondo la funzione

funzione che mappa una stringa di lunghezza arbitriARIA in una stringa di lunghezza predefinita

*collisione* hash *è* una situazione che avviene quando due diversi input producono lo stesso output tramite una funzione hash

Commenti

Commento:

Domanda 2

Completo

Punteggio ottenuto 6 su 10

Contrassegna domanda

Testo della domanda

Descrivere il principio di funzionamento della crittografia simmetrica. Scegliere inoltre un algoritmo tra DES e AES da approfondire.

Testo della risposta

la crittografia simmetrica consiste in un tipo di crittografia semplice nella quale per decrittarla serve avere una chiave la quale devono possederla entrambi comunicatori

un esempio di chiavi simmetriche potrebbe essere

Si avvale di un cifrario a blocchi, il quale riceve in ingresso una stringa di testo di lunghezza fissa e la trasforma, mediante una serie di operazioni complesse, in un'altra stringa della stessa lunghezza, però cifrata.

Commenti

Commento:

Domanda 3

Completo

Punteggio ottenuto 6 su 10

Contrassegna domanda

Testo della domanda

Descrivere e dettagliare ciò che riguarda la sicurezza delle password.

Testo della risposta

In quanto alla sicurezza delle password bisogna pensare che deva essere completamente casuale, e deva essere in ogni modo casuale e senza nessun riferimento al utente che scrive la password bisogna pensare alla ripetibilità e devono essere presenti delle maiuscole e numeri con l'intenzione di aumentare la casualità della password

una password può essere infranta mediante tecniche di infrazione come il Pishing la quale facendosi passare come una azienda conosciuta può iniziare a chiedere dati personali come la password.  
Inoltre la password può essere la piu casuale del mondo ma se viene utilizzata in diverse account non appena decifrata tutti gli account verranno infranti.

oggi ormai esistono anche nuovi metodi per proteggere il tuo account mediante metodi di autenticazione con i quali anche se la password viene infranta viene vietato l'accesso al intruso se non è in possesso dei metodi di autenticazione

inoltre è anche consigliabile cambiare ogni tanto la password

Commenti

Commento:

Final del formulario

[Fine revisione](https://fad.its-ictpiemonte.it/mod/quiz/view.php?id=23568)

[◄ Parte 2](https://fad.its-ictpiemonte.it/mod/quiz/view.php?id=23567&forceview=1)

Principio del formulario