

Comenzado el lunes, 4 de noviembre de 2019, 21:12

Estado Finalizado

Finalizado en lunes, 4 de noviembre de 2019, 22:26

Tiempo empleado 1 hora 14 minutos

Puntos 5,00/5,00

Calificación 10,00 de 10,00 (100%)

Pregunta 1

Finalizado

Puntúa 1,00 sobre 1,00

Las funciones hash son una de las primitivas más utilizadas en criptografía. ¿Qué afirmaciones son ciertas sobre las funciones hash?

Seleccione una o más de una:

- ☐ a. Calcular el hash de un mensaje m es un problema computacionalmente difícil.
- ☐ b. La función hash MD5 se considera segura actualmente.
- ☒ c. Es difícil encontrar dos mensajes m y m' tales que $H(m) = H(m')$.
- ☒ d. Dado el valor de un hash h , es difícil encontrar un mensaje m tal que $H(m) = h$.

Pregunta 2

Finalizado

Puntúa 1,00 sobre 1,00

Utilizando la definición de función hash que encontrareis en el ejemplo de la página 14 del módulo de funciones hash, calculad el valor hash del mensaje 00100001. En este caso, debéis tomar como vector inicial de la función hash el valor 0101.

Respuesta:

Pregunta 3

Finalizado

Puntúa 1,00 sobre 1,00

Calculad el resultado de la función $\sigma_1(a)$, utilizada en el SHA256, sobre el valor $a=0\text{xff}0\text{f}0\text{f}$.

Expresad el resultado en hexadecimal en el mismo formato que se muestran los valores de entrada.

Respuesta:

Pregunta 4

Finalizado

Puntúa 1,00 sobre 1,00

Calculad el resultado de la función $\text{Ch}(a,b,c)$, utilizada en el SHA256, sobre los valores $a=0\text{xffff}0\text{ff}0\text{f}$, $b=0\text{xf}0\text{ff}0000$, $c=0\text{xff}0\text{ffff}0$.

Expresad el resultado en hexadecimal en el mismo formato que se muestran los valores de entrada.

Respuesta:

Pregunta 5

Finalizado

Puntúa 1,00 sobre
1,00

Suponed que utilizamos una función hash que devuelve valores decimales y su salida puede tomar 11436 como valor máximo. Estamos en un sistema que utiliza dicha función como mecanismo de prueba de trabajo y nuestro objetivo es el valor 0. Cual es la probabilidad que con el cálculo de un solo hash obtengamos la prueba de trabajo?.

Seleccione una:

- ☐ a. 0,25
- ☐ b. 0,5
- ☐ c. 1
- ☒ d. 1/11436

◀ PEC2

Ir a...



PEC4 ▶