

Página Principal ► Mis cursos ► 192_75_601_01 : Criptografía aula 1 ►
Pruebas de Evaluación Continuada (PECs) ► PEC3

Comenzado el	martes, 31 de marzo de 2020, 21:05
Estado	Finalizado
Finalizado en	martes, 31 de marzo de 2020, 21:31
Tiempo empleado	25 minutos 45 segundos
Puntos	4,00/5,00
Calificación	8,00 de 10,00 (80%)

Pregunta 1

Correcta

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. Dado el valor de un mensaje m , es difícil encontrar el valor del hash h tal que $H(m) = h$.
- ☐ b. La entrada de la función tiene una longitud constante.
- ☒ c. La salida de la función tiene una longitud constante. ✓
- ☒ d. Dado el valor de un hash h , es difícil encontrar un mensaje m tal que $H(m) = h$.



Las respuestas correctas son: Dado el valor de un hash h , es difícil encontrar un mensaje m tal que $H(m) = h$, La salida de la función tiene una longitud constante.

Pregunta 2

Correcta

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:



La respuesta correcta es: 0000

Pregunta 3

Incorrecta

Puntúa 0,00 sobre 1,00

Calculad el resultado de la función $\sigma_1(a)$, utilizada en el SHA256, sobre el valor $a=0xff0ff00f$.

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

Respuesta:



La respuesta correcta es: 0x0639c39a

Pregunta 4

Correcta

Puntúa 1,00 sobre 1,00

Calculad el resultado de la función Ch(a,b,c), utilizada en el SHA256, sobre los valores a=0xf000ff00, b=0xff000fff, c=0xffff0fff.

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

Respuesta: 0xffff0fff



La respuesta correcta es: 0xffff0fff

Pregunta 5

Correcta

Puntúa 1,00 sobre 1,00

Suponed que utilizamos una función hash que devuelve valores decimales y su salida puede tomar 16072 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. 1/16072 ✓
- ☐ d. 1

La respuesta correcta es: 1/16072

◀ PEC2

Ir a...

PEC4 ▶