VÍDEO intypedia014es

LECCIÓN 14: FUNCIONES UNIDIRECCIONALES Y HASH

EJERCICIOS

AUTOR: Hugo Krawzcyk

IBM Estados Unidos

EJERCICIO 1

Gracias a la propiedad de difusión de la función hash MD5, cuando se modifica 1 bit del mensaje:

a) Debería modificarse como máximo un 30% de los bits de resumen.
b) Debería modificarse aproximadamente un 50% de los bits del resumen.
c) Debería modificarse el 100% de los bits del resumen.
d) El algoritmo funcionará más rápido.

EJERCICIO 2

La principal vulnerabilidad de las funciones hash son los ataques basados en:

a) El cifrado cíclico.
b) Los bits de relleno por bloques.
c) La paradoja del cumpleaños.
d) La fuerza bruta.

EJERCICIO 3

Se dice que el hash h(M) de un mensaje M cumple la propiedad de unidireccionalidad:

a) Si conocido un resumen h(M), debe ser computacionalmente imposible encontrar el mensaje M que lo genera.
b) Si a partir de un mensaje M de cualquier longitud, el resumen h(M) debe tener una longitud fija.
c) Si es computacionalmente difícil que, conocido M, se encuentre un M' tal que h(M) = h(M').
d) Si h(M) es una función compleja de todos los bits del mensaje M.

EJERCICIO 4

Una función hash segura debe tener la siguiente característica:

a) Poseer una clave de al menos 128 bits.
b) Ser resistente a ataques por estadísticas del lenguaje.
c) Ser resistente a colisiones.
d) Realizar todos los cálculos con palabras de 32 bits.

EJERCICIO 5

Se dice que el hash h(M) de un mensaje M tiene una resistencia simple a colisiones o a preimagen:

a) Si es computacionalmente difícil que, conocido M, se encuentre un M' tal que h(M) = h(M').
b) Si conocido un resumen h(M), debe ser computacionalmente imposible encontrar el mensaje M a partir de dicho resumen.
c) Si es computacionalmente difícil encontrar un par al azar (M, M') de forma que h(M) = h(M').
d) Si h(M) es una función compleja de todos los bits del mensaje M.

RESPUESTAS

1. b
2. c
3. a
4. c
5. a

Madrid, España, mayo de 2012

http://www.intypedia.com

http://twitter.com/intypedia