Casos prácticos

Funciones Hash

Telefónica EDUCACIÓN DIGITAL

Casos prácticos

Software: CriptoRES: http://www.criptored.upm.es/software/sw_m001h.htm

http://www.mobilefish.com/services/big_number_bitwise_calculation/big_number_bitwise_calculation.php

1 | Hash MD5 1 y dispersión de bits (0,4 puntos)

Escribe los 2 primeros bytes del MD5 de estos dos textos. Texto 1: Cola. Texto 2: Bola. ¿Cuántos bits diferentes tienen los textos 1 y 2? ¿Cuántos bits diferentes tienen sus Funciones Hash MD5? ¿Por qué?

2 | Seguimiento hash MD5 (0,4 puntos)

Realiza un seguimiento a nivel de pasos del hash MD5 del mensaje 1234HOLA1234CHAO1234 (20 bytes y un solo bloque). ¿Qué relleno se usa y como se indica? ¿Qué tamaño tiene el archivo y cómo se indica? ¿Cómo se distribuyen los 512 bits del único bloque de entrada? Haz la suma correspondiente.

3 | Ataque por paradoja del cumpleaños a RSA (0,3 puntos)

Se conoce el módulo RSA de una clave de 60 bits es 975.489.807.177.105.347, con e = 65.537. Realiza un ataque por paradoja del cumpleaños y encuentra la clave privada d = 785.786.010.365.481.473. ¿Cuánto tarda el ataque? Comprueba con Fortaleza de Cifrados que es la clave correcta cifrando el número 1.234 con la clave pública y luego descifrando el criptograma con la clave privada.

Telefónica EDUCACIÓN DIGITAL