Universidad Salesiana de Bolivia
Ingeniería de Sistemas
Redes y Comunicaciones

LABORATORIO 4

Analizaremos la técnica de encriptación HASH.

MD5, Message Digest 5, resume un documento a 128 bits representativos del mismo.

MD5 selecciona bloques de 512 bits del texto en claro que hace pasar por una función en la que como clave se usan cuatro vectores de 32 bits cada uno (128 bits) y cuya salida también de 128 bits se convierte en la clave o vector para el próximo bloque de texto de 512 bits.

Al encadenar estas operaciones, el resumen del último bloque de texto corresponde a la función hash de todo el documento.

Parte 1: Operaciones de hash con teclado
a) Introduce por teclado los siguientes mensajes y calcula su función hash.
M1 = ABC.
M2 = Esta es una prueba de la función hash MD5.
M3 = ESTA ES UNA PRUEBA DE LA FUNCION HASH MD5.
b) Haz un seguimiento de este último mensaje M3 a nivel de bloques. Guarda el resultado en un archivo de nombre practmd5bloque.txt.

Parte 2: Propiedades de la función hash
a) Introduce por teclado el texto el siguiente texto y calcula su función hash:
M1 = NO BEBA COCA COLA.
Con la ayuda del portapapeles, guárdalo en un archivo de nombre hashCOCA.txt.
A continuación introduce el texto siguiente y vuelve a calcular su función hash:
M2 = NO BEBA CACA COLA.
Con la ayuda del portapapeles, guárdalo en un archivo de nombre hashCACA.txt.
b) Usando ahora calculadora científica de Windows compara la salida en binario de los dos hash y comprueba el cambio (la letra A por la O).

Parte 3: Operaciones de hash con ficheros
a) Calcula la función hash del fichero seguridad.txt
b) Calcula la función hash del fichero seguridad.doc
c) Comprueba que si bien los textos son iguales, la función hash de estos dos ficheros será distinta.

Universidad Salesiana de Bolivia
Ingeniería de Sistemas
Redes y Comunicaciones

LABORATORIO 4

PREGUNTAS PARA EL INFORME

1. ¿Por qué no son iguales las funciones resumen de M2 y M3 del apartado 1 a) si el texto es el mismo?
2.
    a. Calcula, comprueba y justifica el número de bloques de texto a tratar en este mensaje de 56 bytes:

    M = VEAMOS SI AHORA EL ALGORITMO PROCESARA UNO O DOS BLOQUES

    b. Calcula, comprueba y justifica el número de bloques de texto a tratar en este mensaje de 64 bytes:

    M = ESTA VA A SER LA SEGUNDA PRUEBA PARA VER EL TAMAÑO DE ESE BLOQUE
3. ¿Por qué son distintos los hash de los archivos seguridad.doc y seguridad.txt