Criptografía

Profesor: Melvin Fernández Ch.

Video 11

fidélitas

Virtual

fidélitas Virtual

Funciones de Hash y protocolos de seguridad

Módulo: 4

Secure Hash Algorithm (SHA)

- En 1993, NIST publica Secure Hash Standard, basado en el algoritmo MD4 de Ron Rivest.

- En 1995, publica SHA-1 con un ligero cambio debido a un fallo significativo no revelado.

- En 2001, publica SHA-2 revisado en 2008 y 2010.

Secure Hash Algorithm (SHA)

- En 2005, se identifican fallos de seguridad en SHA-1, que comenzó a reemplazarse por SHA-2.

- En 2012, una competición del NIST selecciona una nueva función SHA-3, el cual no se basa en SHA-2 y no pretende reemplazarlo, sino que NIST percibe la necesidad de una alternativa diferente.

Algoritmo Message Digest 5 (MD5)

- MD5 fue creado por Ronald Rivest en 1991 y presenta algunas mejoras con respecto a MD2 y MD4 del mismo autor (1990).

- Esta función ya está obsoleta desde mediados de 2005. No obstante, se sigue utilizando en diferentes aplicaciones locales, aunque no en Internet. Es interesante su estudio dada la sencillez del algoritmo, su rapidez y su generalidad.

Algoritmo Message Digest 5 (MD5)

- Procesa bloques de 512 bits con una salida de 128 bits.

- Expande el mensaje hasta una longitud 64 bits inferior a un múltiplo de 512 bits. Para el relleno, añade un 1 seguido de tantos 0 como sean necesarios y reserva los últimos 64 bits para añadir información sobre la longitud del mensaje.

Algoritmo Message Digest 5 (MD5)

- El algoritmo comienza con cuatro vectores iniciales (IV) ABCD de 32 bits cada uno, cuyo valor inicial no es secreto. A estos vectores y al primer bloque de 512 bits de M se le aplican 64 operaciones de 32 bits con puertas lógicas, cuyo carácter es no lineal.

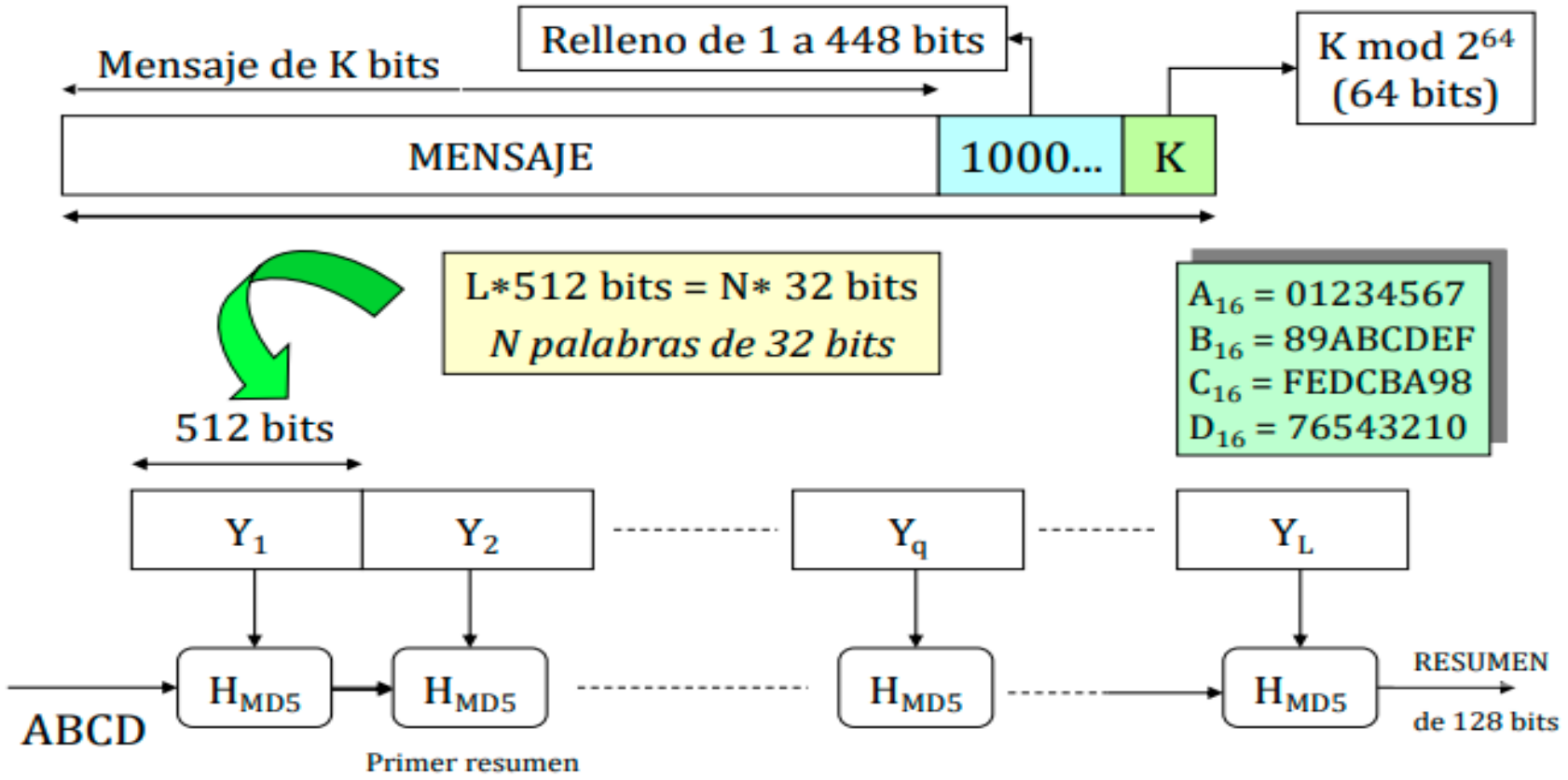
Algoritmo Message Digest 5 (MD5)

- Las 64 operaciones se engloban en 4 vueltas o rondas.

- Como resultado de estas operaciones, se obtienen cuatro nuevos vectores A'B'C'D' que serán la entrada IV' para el segundo bloque de 512 bits, repitiéndose esto con los restantes bloques de M.

- La última salida de IV corresponde al resumen final H = h(M).

Algoritmo Message Digest 5 (MD5)



Algoritmo Message Digest 5 (MD5)

fidélitas Virtual

- MD5 usa la construcción de Merkle-Damgård de compresión.

- Por lo tanto, divide el mensaje en bloques de 512 bits, incluyendo siempre un relleno de ceros que comienza por 0x 80 y dejando los últimos 64 bits para indicar el tamaño de texto.

- Trabaja con 4 vectores iniciales ABCD de 32 bits cada uno que se mezclan con el bloque de 512 bits del mensaje M en 64 vueltas o rondas con las funciones F, G, H e I, con 16 vueltas en cada una.

Algoritmo Message Digest 5 (MD5)

fidélitas Virtual

- En cada vuelta, se tomarán 16 palabras diferentes Mj de 32 bits del mensaje M, desde M0 hasta M15, además de 16 constantes tj diferentes y unos desplazamientos sj determinados en unas tablas.

- MD5 entrega un resumen de 128 bits y hoy no es recomendable su uso.

Gracias

fidélitas Virtual