FUNCIONES HASH

El cifrado con confidencialidad protege de los ataques pasivos.

Función hash: función que asocia a cualquier documento electrónico M, un resumen h(M) suyo de longitud fija. La longitud depende del algoritmo utilizado. (128 bits en MD5 y 160 bits en SHA-1)

Propiedades

Facilidad de cálculo: debe ser fácil calcular h(M) a partir de M.

Unidireccionalidad: debe ser computacionalmente imposible encontrar M a partir del resumen h(M)

Compresión: a partir de un msj M de cualquier longitud, el resumen h(M) debe tener una longitud fija y lo normal es que sea menor que la de M.

Difusión: h(M) debe ser una función compleja de todos los bits del msj M. Si se modifica M, se modifica h(M).

Resistencia simple a colisiones: será computacionalmente difícil que, conocido M, se encuentre un M' tal que $h(M)=h(M')$

Resistencia fuerte a colisiones: será computacionalmente difícil encontrar un par al azar (M, M') de forma que $h(M)=h(M')$

Paradoja del cumpleaños: para tener una probabilidad mayor o igual que 50% en encontrar dos msjs distintos con el mismo resumen h(M) hay que buscar en el espacio $2^{n/2}$

MD5

- Obsoleta desde 2005
- Procesa msj en bloques de 512 bits y produce salida de 128 bits
- Expande el msj 64 bits menos que un múltiplo de 512 b. Añadiendo 1 y luego tantos 0 como sea necesario. Reserva los últimos 64b para representar el tamaño de M.

  448b (Msj + relleno) + 64b (long.)

- Cuatro vectores iniciales ABCD de 32 bits, con valor no secreto.
- Se aplican 64 operaciones de 32 b no lineales, a estos vectores y al primer bloque.
- Los 4 nuevos vectores serán la entrada al siguiente bloque de 512 bits y repite la operaciones con todos los bloques. El último bloque dará el resumen h(M).

SHA-1

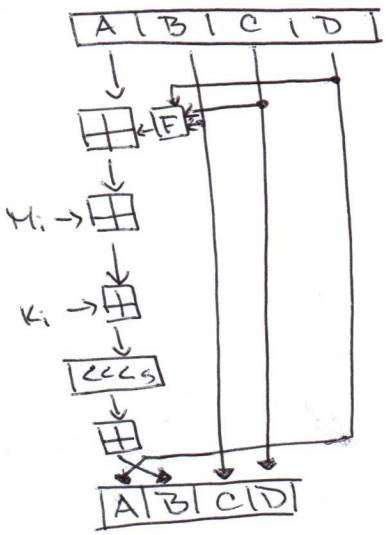
- Trata bloques de 512 bits, genera un resumen de 160 bits.
- Se realizan 80 operaciones con palabras de 32 bits, organizadas en 4 rondas; de 1-20 a 61-80 (4ª ronda)
- Como son 160 bits utiliza 5 vectores no secretos de 32 bits.
- Es el algoritmo actual en navegadores, banca, etc.

VULNERABILIDADES.

MD5, como su resumen es de 128 bits, existen 2^{128} resúmenes distintos; un ataque por paradoja del cumpleaños necesitaría unos 2^{64} intentos para que prosperase.

SHA-1, como su resumen es de 160, existen 2^{160} resúmenes distintos, por tanto un ataque por paradoja del cumpleaños necesitaría 2^{80} intentos.

SHA-1 es más seguro porque el posible hash es mayor.

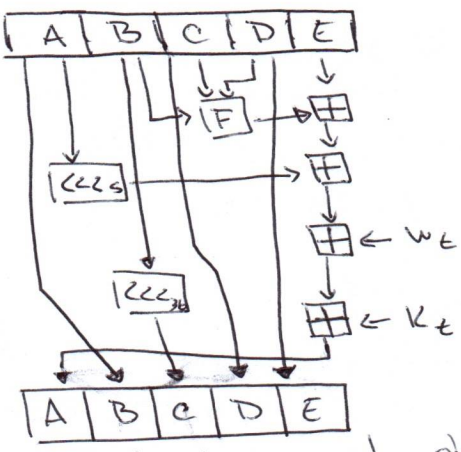


s: desplazamiento en c/ronda.
Viene en tabla

F = (B AND C) OR (NOT B AND D) 1º R
G = (B AND D) OR (C AND NOT D) 2º R
H = (B XOR C XOR D) 3º R
I = (C XOR (B OR NOT D)) 4º R

Mi: 16 palabras de 32 bits
Ki: cte 32 bits.
Viene en tablas.

We: 80 palabras de 32 bits
Ke: cte. de 32 bits.
1 para cada ronda



s: desplazamiento de 5 bits sobre A y 30 bits sobre B.

A, B, C, D, E.

F = (B AND C) OR (NOT B AND D) 1º R.
G = (B XOR C XOR D) 2º R
H = (B AND C) OR (B AND D) OR (C AND 3º
I = (B XOR C XOR D) 4º R