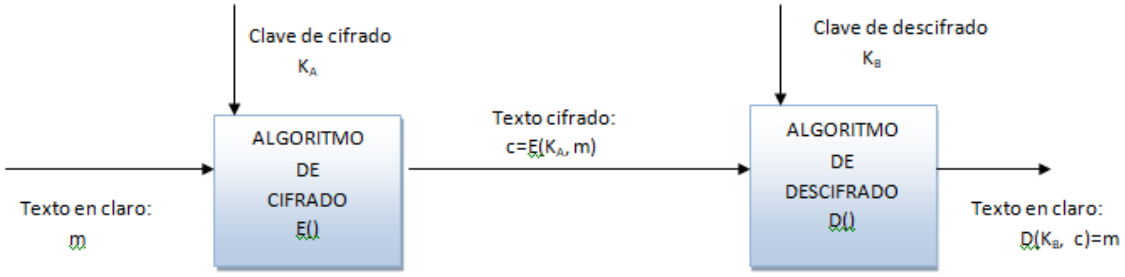
TEMA 079. ALGORITMOS DE CIFRADO SIMÉTRICOS Y ASIMÉTRICOS. LA FUNCIÓN HASH. EL NOTARIADO

Actualizado a 18/04/2023

1. INTRODUCCIÓN

Escenario de cifrado:



2. ALGORITMOS DE CIFRADO SIMÉTRICO

Los algoritmos de cifrado simétrico son aquellos en los cuales se emplea una única clave tanto para cifrar como para descifrar. Es decir, en el diagrama, K_A=K_B. Esta clave debe ser secreta y conocida únicamente por el emisor y el receptor.

2.1. CIFRADORES SIMÉTRICOS DE FLUJO

Combinan, dígito a dígito, el flujo de datos con un keystream. Este keystream es generado por el algoritmo pseudo-aleatoriamente a partir de la clave simétrica.
Existen dos perfiles dentro de los cifradores de flujo:

- Aplicaciones con requisitos estrictos de velocidad.
- Cifradores hardware con capacidad limitada de cómputo y almacenamiento.

Algoritmos existentes:

Algoritmo	Uso recomendado en la actualidad	
A5/1 y A5/2	No	Se usó en GSM
RC4	No	Se usó en WEP, WPA y SSL
E0	No	Se usó en Bluetooth
Rabbit	Sí	(Clave de 128 bits)
SNOW3G	Sí	Usado en UMTS (clave de 128 bits)

Otros: Mickey2.0, Trivium, Grain, Salsa.

2.2. CIFRADORES SIMÉTRICOS DE BLOQUE

El texto en claro se divide en bloques de tamaño fijo para su cifrado.

Modos de operación para el cifrado de varios bloques:

- **Modo *Electronic Code Book (ECB):*** se cifran los bloques de forma independiente.
- **Modo *Cipher Block Chaining (CBC):*** el cifrado de un bloque depende del bloque anterior.
- **Modo contador (CTR)**: se emplea el cifrador de bloque para obtener un keystream.
- ***Output Feedback (OFB).***
- ***Cipher Block Feedback (CBF).***

Algoritmo	Uso recomendado en la actualidad	
DES	No	Clave de 56 bits (más 8 de paridad) Basado en el cifrado Feistel
TripleDES	No	Clave de 112bits Aplica el cifrador DES en cascada
Kasumi	No	
Blowfish	No	Claves de entre 32 y 448 bits
AES	Sí	Claves de 128 bits, 192bits o 256bits Basado en el algortimo Rijndael
Camellia	Sí	

Otros: IDEA, RC6, TEA.

3. ALGORITMOS DE CIFRADO ASIMÉTRICO

Los algoritmos de cifrado asimétrico son aquellos que, para cifrar y para descifrar, emplean dos claves diferentes, K_A y K_B, aunque complementarias. De la pareja de claves, una es secreta y conocida únicamente por el propietario de la clave, mientras que la otra es pública.

Usos de la criptografía asimétrica:

- **Cifrado** (**confidencialidad**): el emisor cifra el mensaje con la clave pública del receptor (por lo que sólo el receptor podrá descifrarlo al ser el único que posee la clave privada complementaria).
- **Firma** (**integridad**, **autenticidad** y **no repudio**): el emisor cifra el mensaje con su clave privada (cualquiera puede descifrarlo con la clave privada, pero queda garantizado que el mensaje ha sido generado por ese emisor, ya que es único que posee la clave privada complementaria).

Debido al coste computacional de la criptografía, no se cifra todo el mensaje, sino que se aplican los esquemas híbridos explicados posteriormente.

Algoritmos:

- Basados en el problema de la factorización entera: RSA.
- Basados en el problema del logaritmo discreto: Diffie-Hellman, DSA, El Gamal.
- Basados en el problema del logaritmo discreto elíptico: ECDH, ECDSA.

3.1. FUNCIÓN HASH

Las funciones hash son funciones que presentan las siguientes características:

- **Compresión:** la salida es de longitud fija e independiente de la longitud del mensaje.
- **Difusión:** la salida es aleatoria y función de todos los bits de la entrada.
- **Resistencia a la preimagen:** dado un hash, no es posible obtener el mensaje que lo generó.
- **Resistencia débil a colisión**: dado un mensaje *m1* y su hash *h(m1),* no es posible encontrar otro mensaje *m2* tal que *h(m1)=h(m2).*
- **Resistencia fuerte a colisión**: no es posible encontrar dos mensajes *m1* y *m2* tales que *h(m1)=h(m2).*

Aplicaciones de las funciones hash:

- ***MDC (Message Detection Code):*** el cálculo del hash de un mensaje permite detectar si el mensaje ha sido modificado.
- ***MAC (Message Autentication Code):*** el cálculo del hash de un mensaje junto con una clave compartida permite detectar modificaciones en el mensaje, así como comprobar la autenticidad del origen. (No confundir con el identificador MAC de red).

Algoritmo	Uso recomendado en la actualidad	Longitud del hash
MD5	No	128bits
RIPMD-128	No	128bits
RIPMD-160	No	160bits
SHA1	No	160bits
SHA2	Sí	224, 256, 384 o 512bits
SHA3	Sí	Longitud configurable
Whirlpool	Sí	512bits

3.2. COMPARACIÓN

- Con funciones hash y cifrado simétrico se puede garantizar la **confidencialidad, integridad y autenticidad** de los mensajes, pero no el no repudio de los mismos. El cifrado asimétrico, sin embargo, sí permite garantizar el **no repudio** de los mensajes.
- Las claves asimétricas **tienen un tiempo de vida** mayor que las asimétricas.
- El **coste computacional** es mayor en los algoritmos asimétricos que en los simétricos.
- Para lograr un mismo nivel de seguridad, el cifrado asimétrico requiere **claves de mayor longitud.**

4. ESQUEMAS HÍBRIDOS

4.1. SOBRE DIGITAL

Emisor:

1. **Genera una clave aleatoria.**
2. **Cifra el mensaje** empleando un algoritmo de cifrado **simétrico** y la clave anteriormente generada.
3. **Cifra la clave aleatoria** generada empleando un algoritmo **asimétrico** y la **clave pública del receptor.**
4. Envía el mensaje cifrado y la clave cifrada.

Receptor:

1. Empleando su clave privada y el algoritmo asimétrico, **descifra la clave aleatoria.**
2. Empleando la clave aleatoria descifrada y el algoritmo simétrico, **descifra el mensaje.**

Resulta especialmente útil en envíos multidestino, al permitir cifrar el mensaje una única vez.

4.2. FIRMA DIGITAL

Emisor:

1. **Calcula el hash** del mensaje.
2. **Cifra el hash** del mensaje con un algoritmo **asimétrico** y con su clave privada.
3. Envía el mensaje y el hash cifrado.

Receptor

1. **Calcula el hash** del mensaje.
2. Empleando la clave pública del emisor, **descifra el hash.**
3. **Compara** el hash calculado con el hash descifrado.