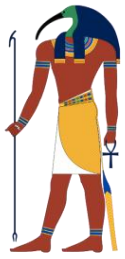
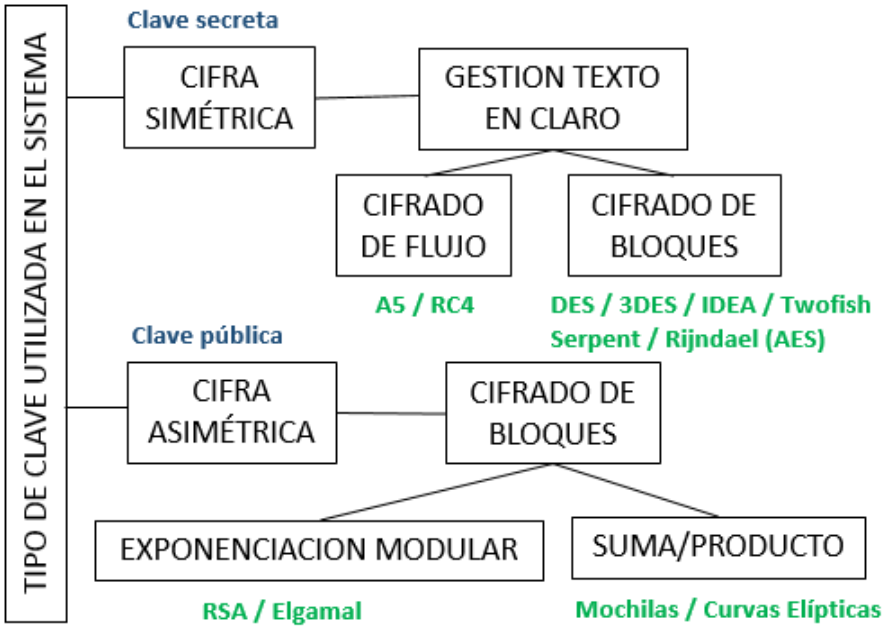


Píldora nº 26: ¿Cómo se clasifican los sistemas de cifra moderna?

Escena 1: Aquí nos importa la clave y el texto en claro

Según cómo sea el tipo de clave que utilizamos, vamos a dividir los sistemas de cifra moderna en algoritmos simétricos y algoritmos asimétricos. Dependiendo ahora de la manera en que tratemos el texto en claro a cifrar, se hablará de cifrado en flujo y de cifrado en bloque. Esto se recoge en al siguiente figura.



Entre los algoritmos más representativos de la criptografía moderna se encuentran A5, RC4, DES, 3DES, IDEA, AES (Rijndael), Serpent, Twofish, RSA, Elgamal, mochilas y curvas elípticas.

Escena 2: Cifra simétrica y cifra asimétrica

Se denomina cifra simétrica a aquella en la que se usa una misma clave secreta compartida en ambos extremos, emisor y receptor. Los algoritmos de cifra son los mismos pero actúan de forma inversa, de manera que en recepción se descifra lo que se ha cifrado en emisión.

En el caso de los sistemas de cifra asimétricos, cada usuario tendrá dos claves. Una clave pública, conocida por todos, y una clave privada (o secreta) que sólo él o ella conoce. Se denomina asimétrico porque lo que se cifra en el extremo emisor con una clave, por ejemplo la clave pública del receptor, en recepción deberá descifrarse con la clave inversa, en este caso la clave privada de ese receptor. No se usa la misma clave para cifrar y descifrar.

Escena 3: Cifra de flujo y cifra de bloques

Si la cifra se realiza bit a bit, esto es bit del texto en claro con bit de la clave, o bien byte a byte, se habla de cifrado de flujo. Es el caso por ejemplo del antiguo algoritmo telefonía móvil A5 (bits) o del algoritmo RC4 (bytes), muy común en plataformas seguras de Internet SSL/TLS.

Los demás cifradores simétricos utilizan bloques. Esto es, la información a cifrar se divide en bloques por lo general de 64 bits (8 bytes) como en el caso de DES, 3DES e IDEA, o bien 128 bits (16 bytes) en AES (Rijndael), Serpent y Twofish.

Escena 4: ¿Por qué la cifra asimétrica es por bloques?

Como se verá en una próxima píldora, la criptografía asimétrica se usará preferentemente para cifrar números de unas pocas centenas de bits, por ejemplo para intercambiar claves de cifra simétrica de una sesión o para firmar digitalmente el hash de un documento.

Si bien no se forman bloques para cifrar dicho número sino que el mismo se cifra en una sola operación, la cifra asimétrica se considera como una cifra por bloques aunque éste sea único.

Madrid, enero de 2015

Autor del guion: Jorge Ramió Aguirre

Dirección Proyecto Thoth: Jorge Ramió Aguirre, Alfonso Muñoz Muñoz