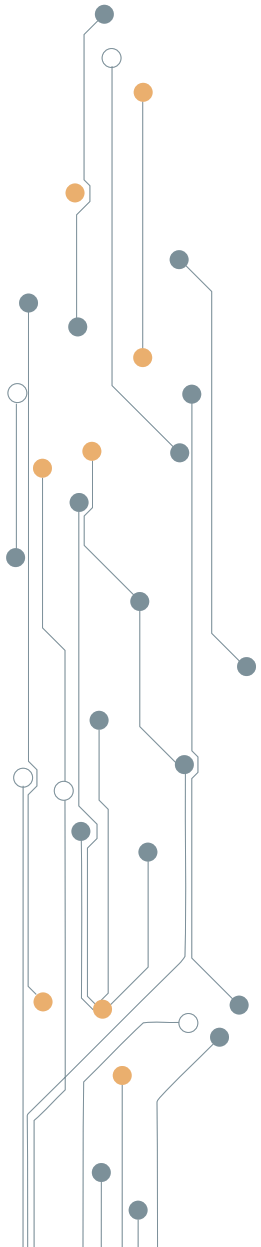
La cifra moderna

Telefónica EDUCACIÓN DIGITAL

Índice



1. Hitos en la historia de la criptografía

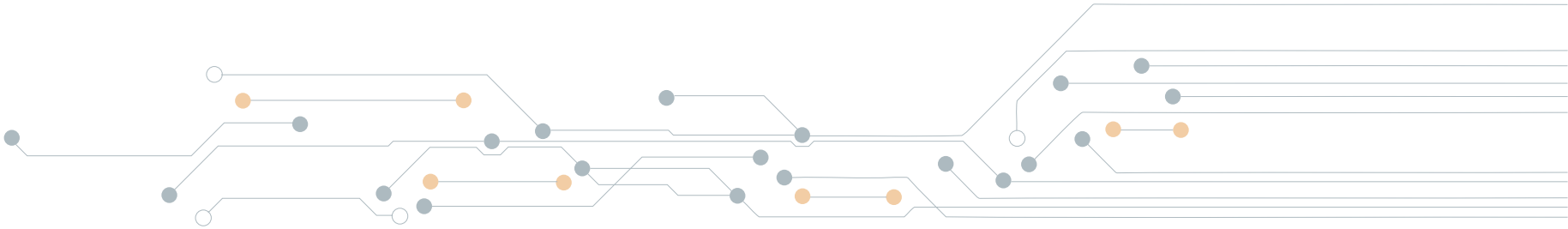
Hay tres hechos significativos que permiten hacer una división entre los sistemas de cifra clásica y los sistemas de cifra moderna, o actuales. Como todos ellos ocurren a partir aproximadamente de la mitad del siglo XX, a grandes rasgos podríamos decir que la criptografía clásica data desde el siglo V antes de Cristo hasta esa fecha y, obviamente, la criptografía moderna abarca desde esa época, hasta nuestros días.

El primer hecho lo encontramos en los trabajos desarrollados por el matemático norteamericano Claude Shannon sobre el estudio de la teoría de la información y los sistemas con secreto, entre los años 1948 y 1949. Esto permitió darle un soporte matemático formal a la criptografía y otros temas relacionados con ella, por lo que ésta deja de ser un arte y pasa a ser una ciencia.

El segundo hecho es la publicación como estándar en 1976 del algoritmo DES, Data Encryption Standard, por parte del NIST. Se trata del primer algoritmo de cifra simétrica para equipos informáticos de uso no militar, y cuyo código fuente era público. Este algoritmo se usa hasta finales de la década de los 90, ya en aquellos años en comunicaciones seguras en Internet a través de SSL.

Y, por último, uno de los acontecimientos más trascendentales de la criptografía moderna. El invento en 1976 por parte de dos investigadores de la Universidad de Stanford, Whitfield Diffie and Martin Hellman, de la denominada criptografía asimétrica o de clave pública. Esto permitirá realizar un intercambio de clave computacionalmente seguro y, posteriormente ya con otros algoritmos, también una firma digital. Una especie de piedra filosofal buscada durante siglos por la criptografía.

Los algoritmos de cifra moderna usan por lo general una operación algebraica en Zn, un cuerpo finito, sin que este módulo deba corresponder con el número de elementos del alfabeto o código utilizado, como sí sucedía en la cifra clásica. De hecho, siempre es mayor el módulo de cifra que el alfabeto usado, en este caso el ASCII extendido de 256 bytes.



2. Clasificación de la cifra moderna

La cifra moderna puede clasificarse de acuerdo a cómo se trata a la información antes de cifrarla, distinguiendo entre cifra en flujo y cifra en bloque. Una segunda clasificación, aplicada en este caso a la cifra en bloque, tiene que ver con el tipo de clave utilizada, diferenciando ahora entre la criptografía simétrica o de clave secreta y la criptografía asimétrica o de clave pública.

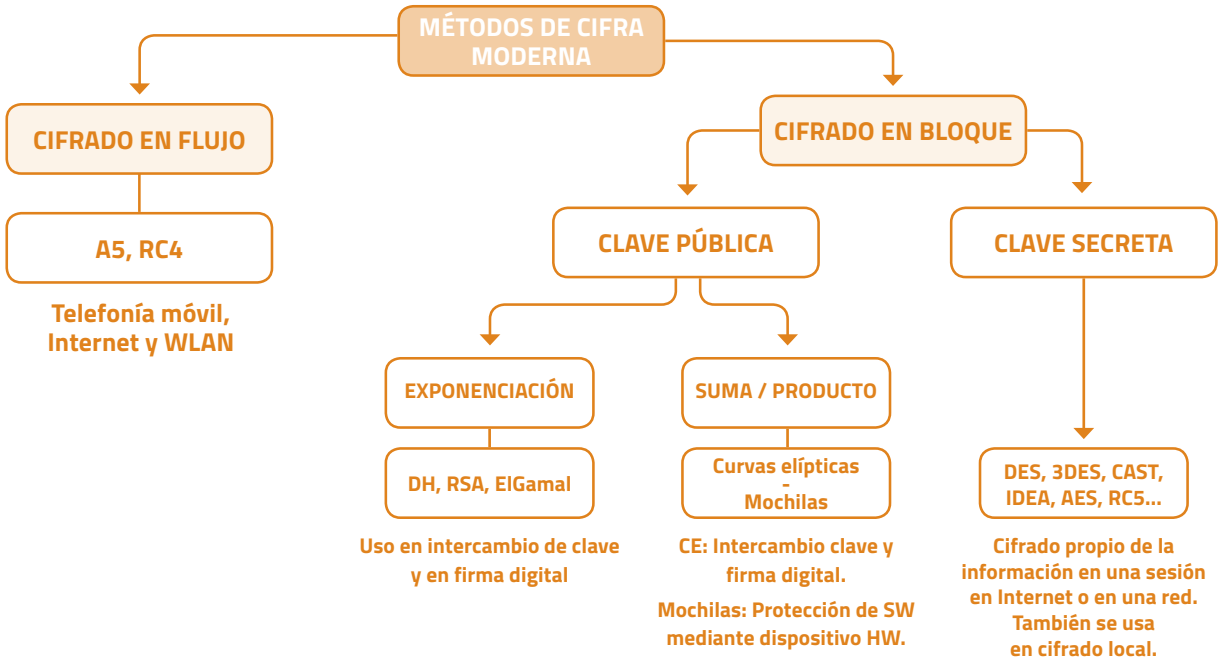


Figura 4.1. Clasificación de los sistemas de cifra moderna.

3. Cifrado en flujo y cifrado en bloque

Cifrado en flujo

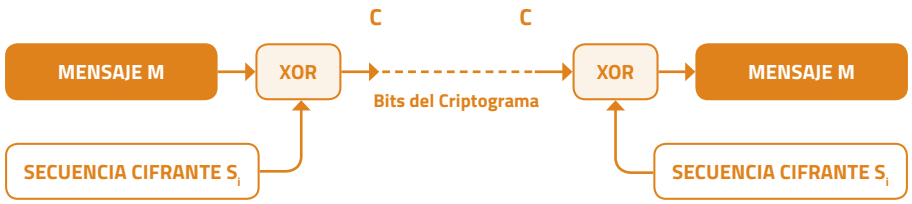


Figura 3.3. Clasificación de los sistemas de cifra clásica.

En el cifrado en flujo, emisor y receptor intercambian previamente una clave conocida como semilla, de sólo unas centenas de bits. A continuación, mediante un algoritmo determinista; por ejemplo, un LFSR *Linear Feedback Shift Register* o Registro de Desplazamiento Realimentado Linealmente, ambos generan una misma secuencia cifrante Si (si la semilla tiene 100 bits un periodo igual a 2^{100}) cuyos bits se cifrarán or exclusivo (xor) con los bits del texto en claro Mi.

El sistema de cifra es muy rápido y sencillo. Además, como la función xor es involutiva, para descifrar el criptograma y recuperar M_i, se hará la misma operación xor, pero ahora entre los bits C_i del criptograma con los bits de la misma secuencia de clave S_i.

Cifrado en bloque

En este caso el mensaje se agrupa en bloques, por lo general de 8 ó 16 bytes (64 ó 128 bits) antes de aplicar el algoritmo de cifra a cada bloque de forma independiente con la misma clave. Esto dará lugar a diferentes modos de cifra como veremos más adelante.

Si el bloque fuese muy pequeño, por ejemplo de uno o de dos bytes, esto facilitaría un ataque por estadísticas del lenguaje. Y si el bloque fuese muy grande, por ejemplo miles de bytes, el sistema no tendría un buen rendimiento. Los valores indicados de 64 y 128 bits son un término medio adecuado.

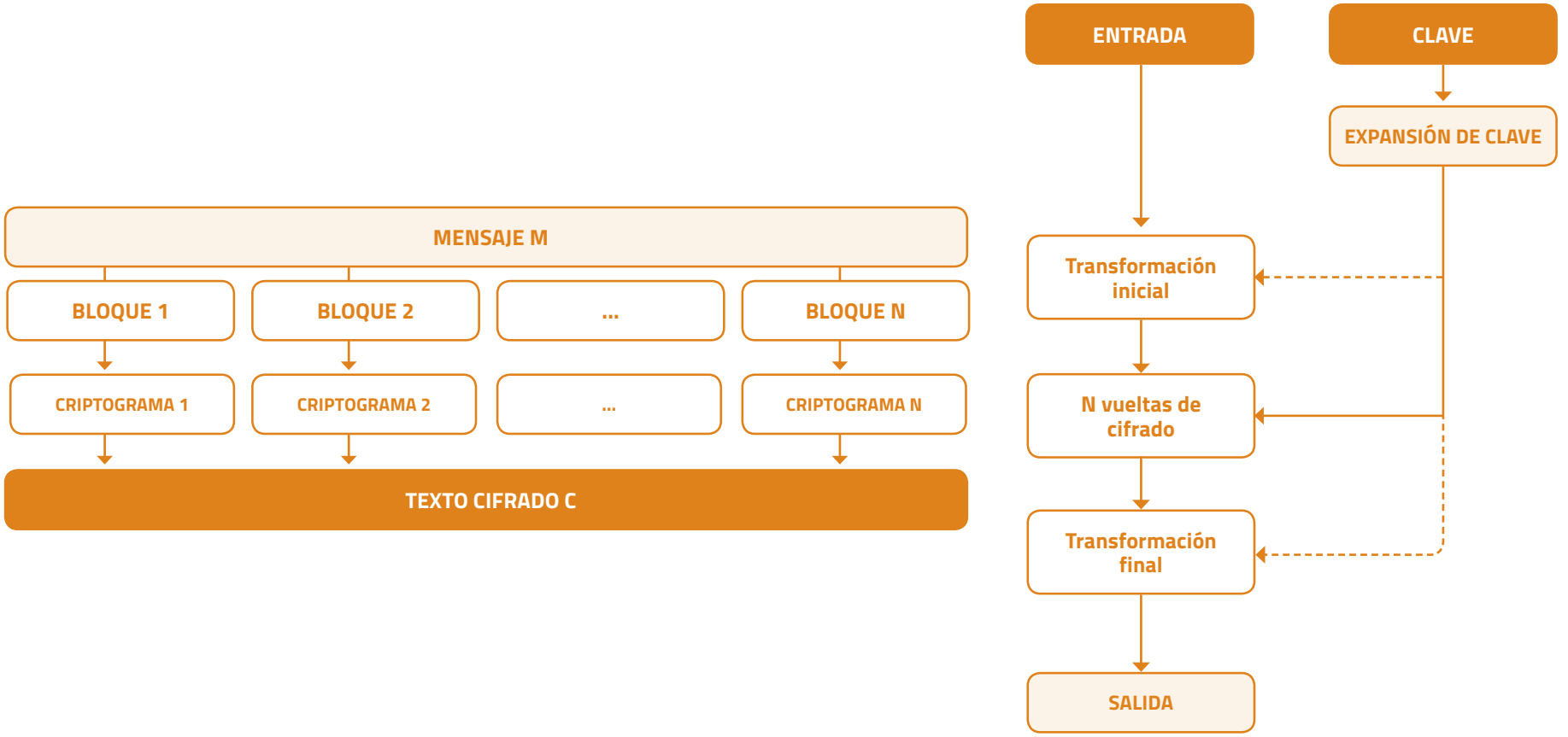


Figura 4.3. Esquema de la cifra en bloque.

De la misma manera que sucedía con la cifra clásica, al formar bloques de texto en claro, lo más común es que el último bloque no sea congruente con dicho tamaño, por lo que habrá que incluir un relleno (padding). En este caso el relleno será un conjunto de bits, de forma que el último bloque del mensaje a cifrar tenga igual tamaño que todos los demás.

La manera en que se tratan esos bloques durante la cifra, dará paso a diferentes modos de cifra.

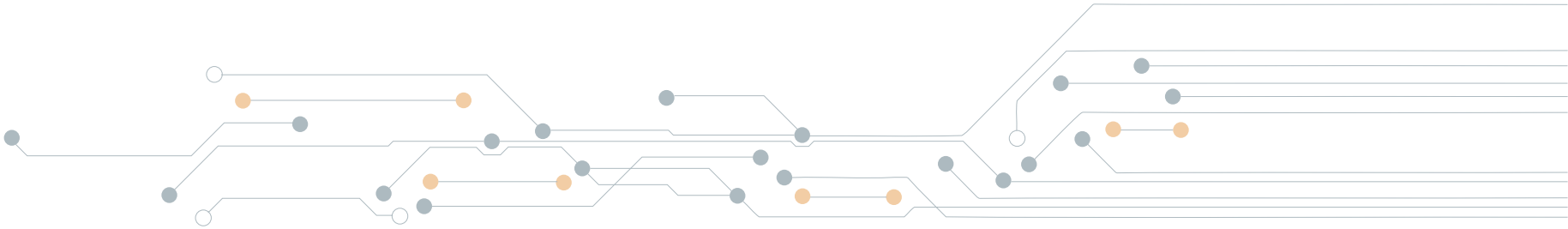
Si se cifran bloques independientes, el modo de cifra se conoce como ECB, Electronic Codebook o Libro Electrónico de Códigos. Este modo está prohibido pues permite ataques por repetición de bloques conocidos y ataques por inicios y finales repetidos.

Aunque existen varios modos de cifra para los sistemas por bloques, los más conocidos son el modo CBC, Cipher Block Chaining o Encadenamiento de Bloques Cifrantes, y el modo CTR, Counter o Contador.

En el modo CBC se usa una segunda clave, conocida como vector inicial IV, que se suma xor al primer bloque del texto en claro. El criptograma resultante de este primer bloque cifrado se usa en el segundo bloque de texto en claro a modo de nuevo IV, acción que se va repitiendo hasta el final del mensaje.

Para el descifrado, el receptor autorizado recibe tanto la clave de cifra K como el vector IV y puede por tanto ir recuperando bloque a bloque el texto en claro.

El modo CTR es similar al CBC, pero soluciona el problema del no paralelismo que tiene CBC ya que en este último al ir encadenada la cifra era obligatorio tener descifrado el bloque anterior para descifrar el próximo. Además, a diferencia del modo ECB, en CBC un error de transmisión afectará a todos los bloques siguientes. CTR usa ese mismo vector inicial IV pero en modo contador y no sumándolo xor al texto en claro, sino como entrada al algoritmo de cifra, de forma que para el primer bloque su valor es IV, para el segundo bloque es IV+1, etc., lo que permite solucionar los dos problemas del modo CBC antes mencionados. La salida de esa cifra se suma or exclusivo con el bloque de texto en claro a cifrar. Observa que, al introducir el vector inicial como entrada a cifrar en modo contador en el algoritmo, la salida de cada bloque del cifrador será distinta. Por lo tanto, el algoritmo de cifra de bloque se convierte en un sistema de cifra en flujo porque la clave (salida del algoritmo) con la cual se hace el xor con cada uno de los bloques texto en claro es distinta; se trata entonces de una secuencia de clave Si como en los sistemas de flujo.



4. Criptografía simétrica y criptografía asimétrica

Se denomina criptografía simétrica o de clave secreta, a aquella forma de cifra en que la clave que se utiliza en el extremo emisor para cifrar es la misma que se utilizará en el extremo receptor para descifrar. Se denomina simétrica por ser la clave igual en ambos extremos. En el extremo receptor, el algoritmo se usa en sentido inverso para poder recuperar el texto en claro, o bien las claves o funciones internas del algoritmo son inversas.

Por el contrario, se denomina criptografía asimétrica o de clave pública, a aquella forma de cifra en que la clave que se utiliza en el extremo emisor para cifrar y la clave que se utiliza en el extremo receptor para descifrar son distintas, básicamente son inversas entre sí dentro de un cuerpo finito. En este caso, son las claves inversas las que permiten descifrar el criptograma y no el algoritmo o sus funciones internas como en el caso anterior.

Los sistemas de cifra simétrica tienen las siguientes características:

1. No tienen una gestión de claves eficientes. El número de claves es n(n-1)/2.

2. No tienen intercambio de clave ni firma digital.

3. El espacio de sus claves está entre 128 y 256 bits (año 2016).

4. La duración de la clave de sesión (Internet) es corta (segundos, minutos).

5. Tienen una tasa de cifra de centenas de MegaBytes por segundos (muy rápidos).

Los sistemas de cifra asimétrica tienen las siguientes características:

1. Tienen una gestión eficiente de claves. Sólo se gestiona la clave privada.

2. Poseen intercambio de clave y firma digital.

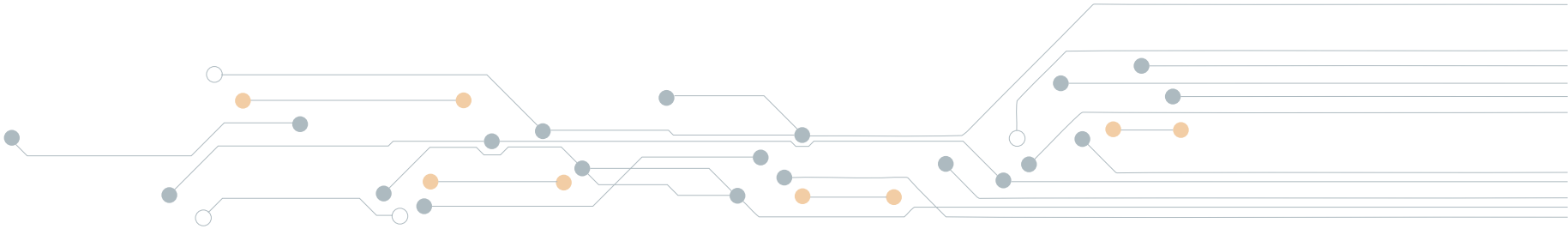
3. El espacio de sus claves está entre 2.048 y 4.096 bits (año 2016).

4. La duración de la clave en un certificado digital es larga (entre 1 y 2 años).

5. Tienen una tasa de cifra de centenas de KiloBytes por segundos (muy lentos).

5. Comparativa entre cifra simétrica y cifra asimétrica

La cifra asimétrica o de clave pública, tiene como fortalezas una eficiente gestión de claves, permite el intercambio de claves y posee firma digital, aspectos estos de los que adolece la cifra simétrica o de clave secreta. Pero los sistemas de cifra asimétricos tienen un talón de Aquiles y este es su velocidad; la tasa de cifra es unas mil veces más lenta que la de los simétricos. Por este motivo, en la práctica su hace uso de la denominada cifra híbrida; esto es, para las operaciones de intercambio de clave y de firma digital, que serán por lo general números de sólo algunas centenas de bits, se usarán los sistemas asimétricos, pero para el cifrado de grandes volúmenes de información se hará uso de los sistemas simétricos.



Telefónica EDUCACIÓN DIGITAL