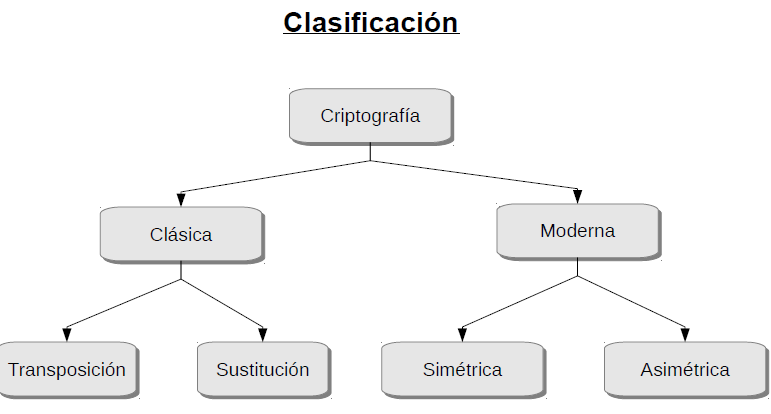
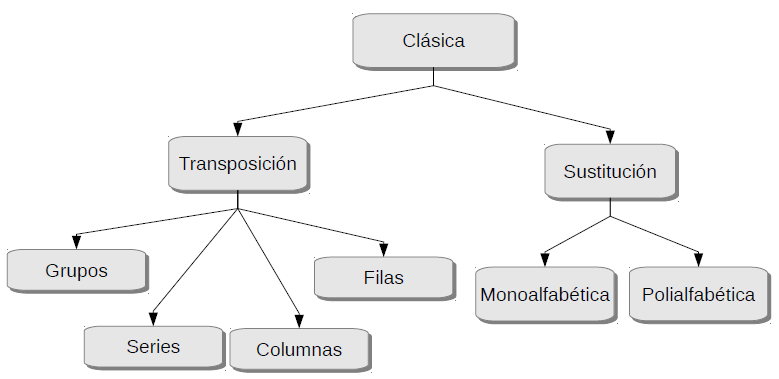
HASTA PAGINA 31



# CLASICA



TRANSPOSICION:

Consiste en PERMUTAR los caracteres por Grupo, Serie, Columna o Fila. Mediante un algoritmo especifico. Tomar todas las columnas por ejemplo y cambiarle el orden f(m, 5,3,1,2,4).

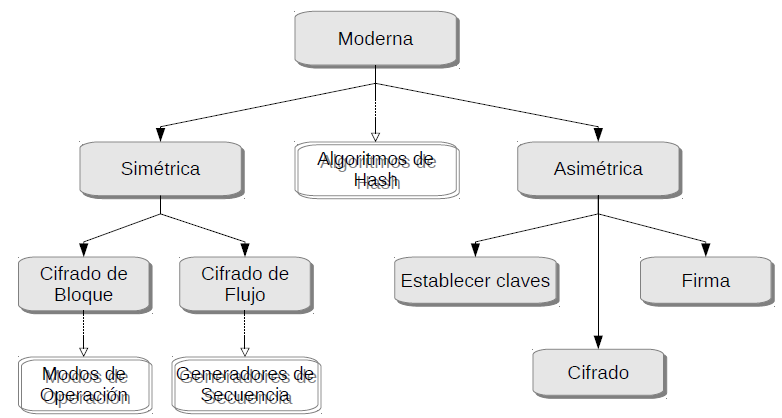
SUSTITUCION:

Consiste en MODIFICAR los caracteres de un texto claro por otro carácter de un alfabeto cifrado.

Monoalfabeticos: Cuando ambos alfabetos son los mismos. Ej: Cifrado de Cesar, mismo alfabeto solo que el receptor toma 3 posiciones mas.

Polialfabeticos: Utilizan diferentes caracteres para el reemplazo de un mismo carácter de origen. Ej: Cifrado de Vigenere, matriz cuyos filas y columnas son alfabetos en orden.

## MODERNA



ALGORITMOS SIMETRICOS:

Cifrado donde se usa la misma clave para Cifrar y Descifrar. Emisor y Receptor deben ponerse de acuerdo con que clave usar.

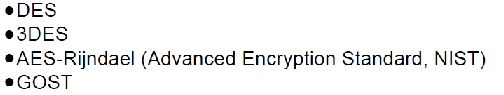
Ventajas:

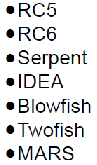
* Sencillez de implementación
* Robustez
* Velocidad de cifrado
* Longitud de mensaje

Desventajas:

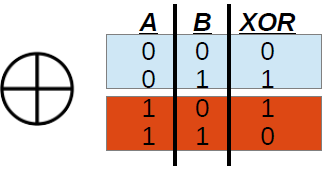
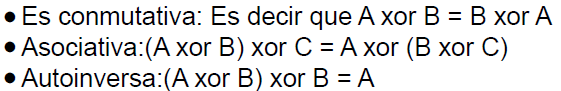
* La clave debe ser compartida previamente con seguridad
* La comunicación entre ambos actores requiere numerosas claves

Ejemplos:



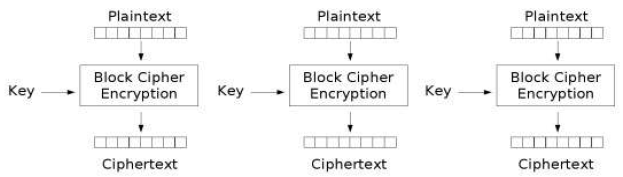


## REFERENCIA MATEMATICA – XOR



## MODOS DE CIFRADO EN BLOQUE

ECB (Electronic codebook): El mensaje se fracciona en partes y cada parte es cifrada de manera independiente.

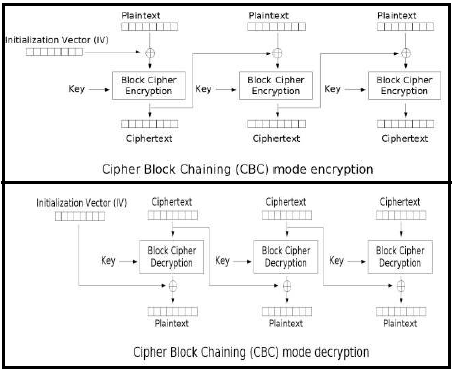


PADDING O ESQUEMA DE RELLENO

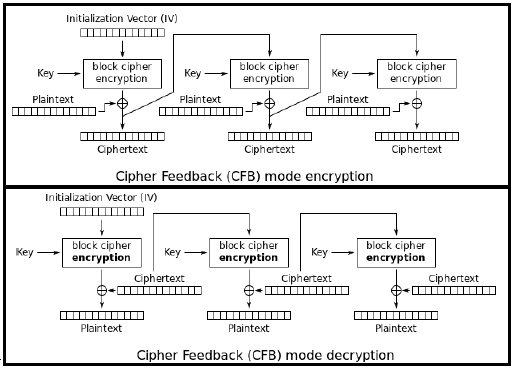
Como los algoritmos simétricos de bloque requieren que los bloques sean iguales, cuando el último bloque es menor se recurre a los métodos Padding para resolver este problema.

* Bit Padding: Opera a nivel Bit, adiciona 1 y todos 0 hasta completar.
* ISO/IEC 7816-4: Opera a nivel Bit, adiciona 80 y todos 0 hasta completar.
* PKCS7 (RFC5652); Opera a nivel Byte, adiciona bytes idénticos cuyo valor es la cantidad de bytes agregados.
* ISO 10126: Opera a nivel Byte, adiciona bytes aleatorios excepto el último que es la cantidad de bytes agregados.
* ANSI X.923: Opera a nivel Byte, adiciona todos 0 excepto el último que es la cantidad de bytes agregados.

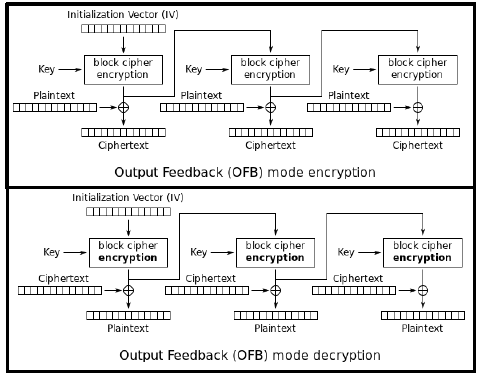
CBC (Cipher block chaining): El mensaje se fracciona en partes, y se realiza un XOR con el bloque previo antes de cifrar cada parte.



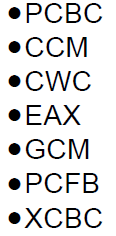
CFB (Cipher Feedback): El mensaje se fracciona en partes , se cifra el vector de inicialización y al resultado se le realiza un XOR con el bloque del mensaje. Los bloques posteriores utilizan como entrada el texto cifrado para reemplazar el vector de inicialización.



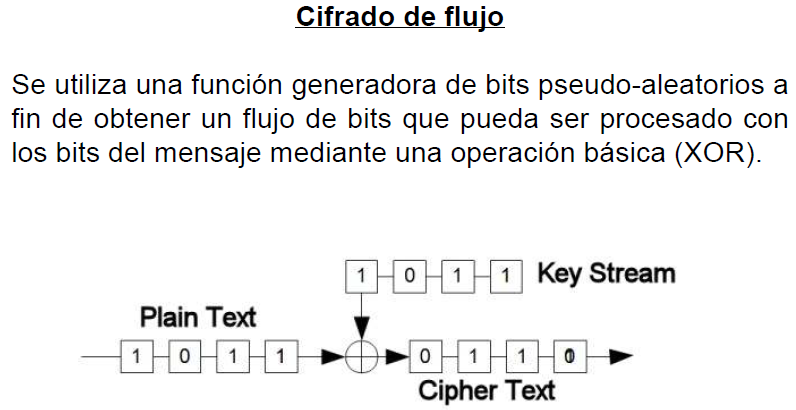
OFB (Output Feedback): Similar a CFB con la diferencia que el bloque a ser utilizado como entrada del siguiente proceso es tomado de la salida del algoritmo justo antes de realizar el XOR.

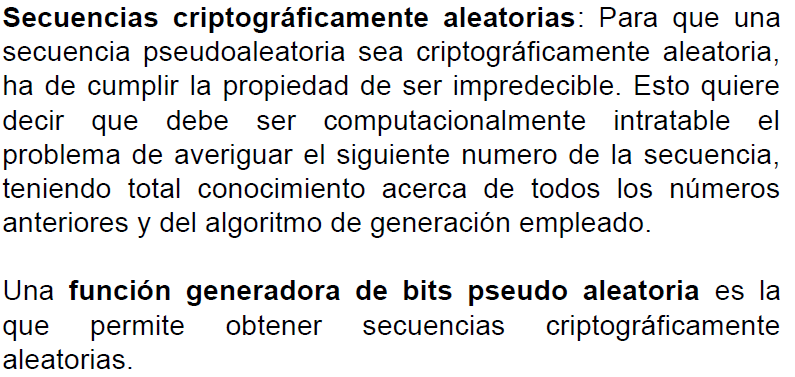


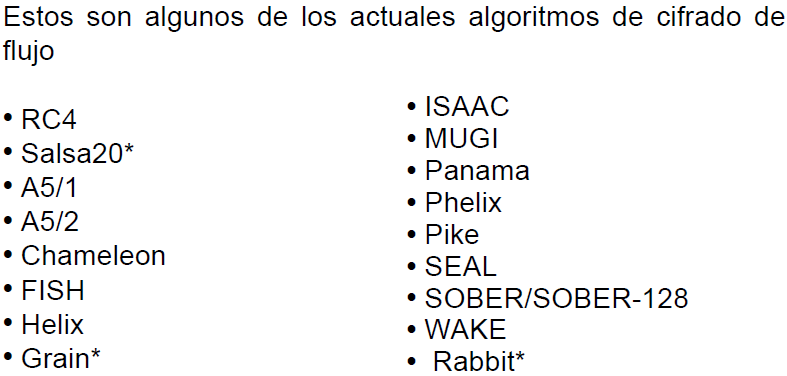
OTROS METODOS DE CIFRADO POR BLOQUE



CIFRADO DE FLUJO







## FUNCIONES DE HASH

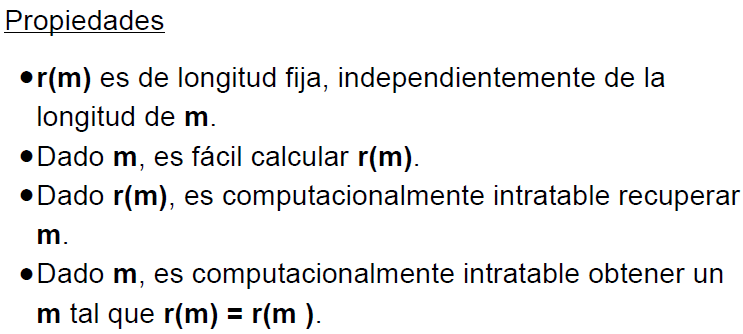
Funcion o método no reversible para generar un valor que represente de manera casi univoca un dato.

Principales usos

- Soporte para criptografia asimetrica

- Tablas de Hash

- Verificacion de integridad



HASTA PAGINA 31