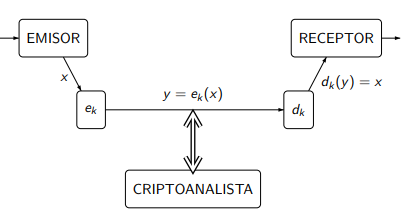
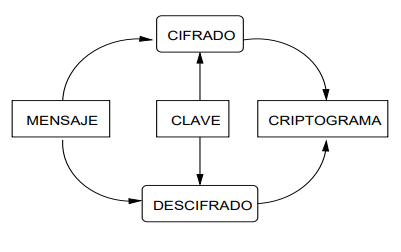
Criptografía

# Tema 1



Tiene 5 objetivos:

* Confidencialidad: ocultar el contenido de la información salvo para aquellos autorizados.
* Accesibilidad: asegurar quien y en qué momento, puede acceder a una información.
* Autenticidad: el receptor de un mensaje debe poseer la certeza de su origen.
* Integridad: seguridad, para el receptor, de que el mensaje no ha sido modificado, así como posibilidad de detectar su posible manipulación.
* No repudio: imposibilidad por parte del emisor de negar la autoría de un mensaje.

Tiene 3 características básicas:

* Cifrado y descifrado eficiente independientemente de la clave escogida.
* Sistema fácilmente utilizable.
* La seguridad del sistema debe depender únicamente del secreto de las claves utilizadas y no del secreto de los algoritmos de cifrado y descifrado.

Hay 4 tipos de ataque:

* Texto cifrado.
* Mensaje conocido.
* Mensaje escogido.
* Criptograma escogido.

Aproximaciones:

* Uso de códigos
* Sistemas monoalfabéticos
* Sistemas polialfabéticos
* Sistemas poligráficos
* Cifrado por permutación
* Transformaciones variables en el tiempo
* Cifrado por bloques

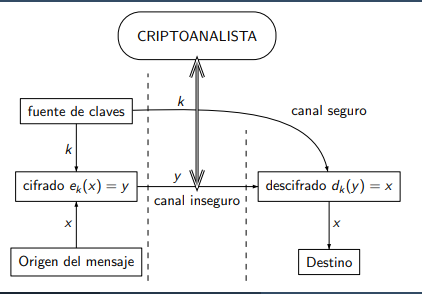
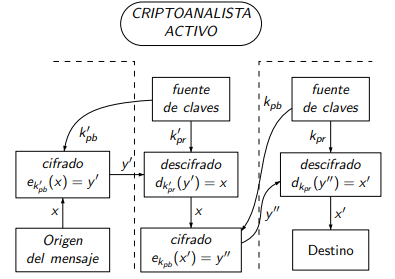
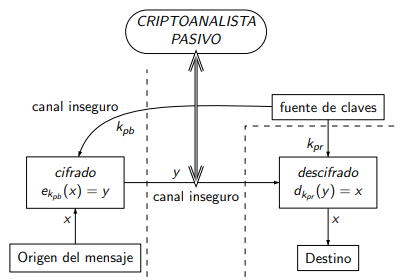
## Seguridad

Incondicional: el sistema siempre es seguro

Computacional: el coste de obtener el mensaje es superior al valor de este o el tiempo necesario para obtener el mensaje supera la vida útil del mensaje.

## Protocolos

### Envío de mensajes cifrados

* Clave simétrica: 
* Clave asimétrica: 
* Sistema híbrido: Pasar una clave privada mediante una clave pública y luego usar la clave privada para descifrar el resto de los mensajes.

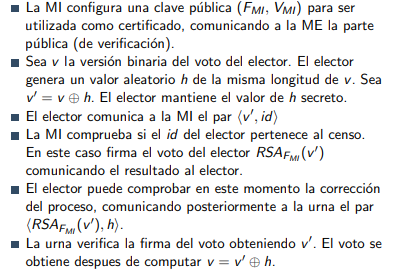
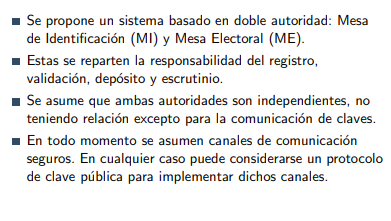
### Firma digital

* Clave simétrica: Emisor y receptor comparten clave de cifrado.
* Clave pública: se cifra con la clave privada y se comprueba la firma con la clave pública. No funciona bien para firmar textos largos, por eso se suele firmar el resumen del mensaje.

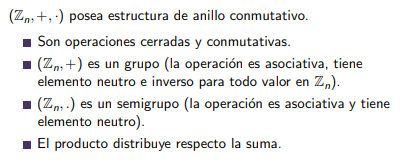
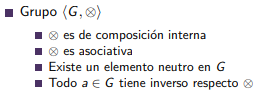
### Voto electrónico

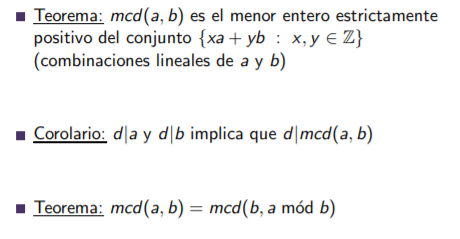
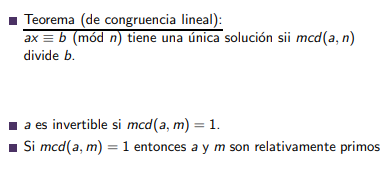
Propiedades:

* Democracia: Solo los inscritos en el censo pueden participar
* Privacidad: No puede relacionarse voto y elector.
* Seguridad: No se debe poder suplantar a un elector que decide no votar.
* Justicia: Nadie puede conocer el resultado antes de que finalice.
* Resistencia coercitiva: Ningún elector puede mostrar su voto
* Completitud: El resultado debe ser preciso
* Precisión: Un voto no puede ser alterado, los votos nulos no pueden contabilizarse de otro modo y el elector debe saber que su voto se ha considerado.
* Verificabilidad: Los electores pueden verificar que su voto ha sido considerado como se emitió.



# Tema 2





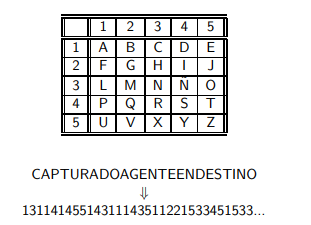


Para solucionar factorizar el número

# Tema 3

## Sistemas monoalfabéticos

Polibio



### Caesar:

Se cifra el mensaje desplazando los caracteres del mensaje

e(x) = x + k mod 27 e: encriptación

d(y) = y - k mod 27 d: desencriptación

Espacio de claves: desplazamientos posibles.  
Número de claves: talla del alfabeto.

## Sustitución simple:

Se sustituye una letra por otra 

Espacio de claves: Permutaciones del alfabeto.  
Número de claves: (Talla del alfabeto)!

### Afín:

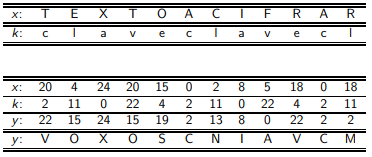
e(x) = ax + b mod 27

d(y) = a -1 (y – b) mod 27

## Sistemas polialfabeticos

### Vigenèrè

ek(xi) = xi + ki mod m mod 27

dk(yi) = yi - ki mod m mod 27clave: clave, en la parte de abajo salen las posiciones de las letras 

#### Criptoanálisis

Kasiski: un fragmento de mensaje que aparezca k veces será cifrado de k/n formas, donde n es el número de alfabetos. Dado ese fragmento las distancias entre las posiciones de ese fragmento será MCD del tamaño de la clave.

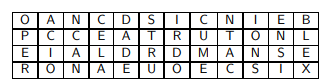
Índice de coincidencia: analiza la variación de la frecuencia relativa de cada letra respecto a una distribución uniforme, en español su valor es 0,072.

## Códigos

Se cifran las palabras mediante un código.

Ataque: se busca identificar sílabas, los números suelen ser patrones.

## Sistemas por transposición

Leer por columnas

## Sistemas poligráficos

### Playfair

## 

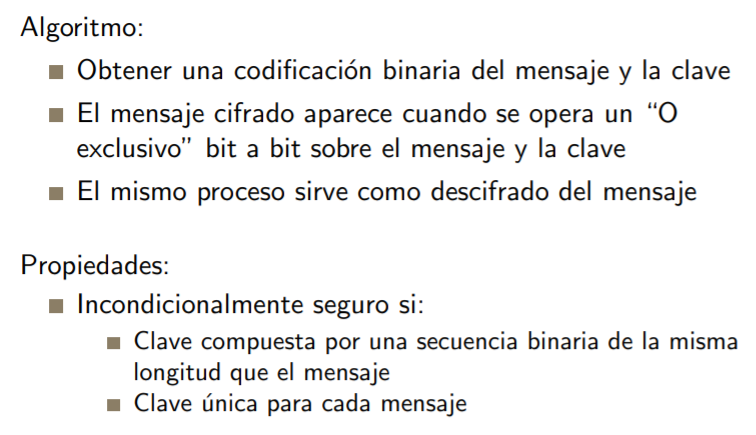
### Hill

## 

# Tema 4

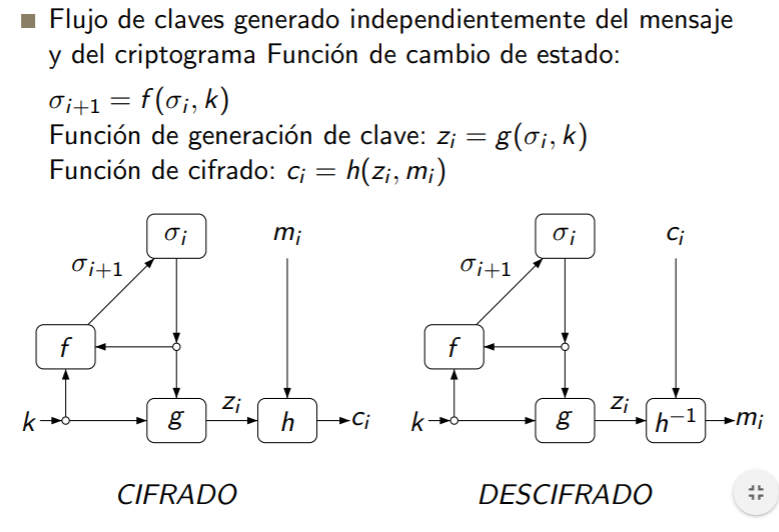
## Cifrado en flujo

Los símbolos individuales se cifran mediante una transformación que varía en el tiempo, se implementan mediante hardware, basados en generadores de clave pseudoaleatorias.



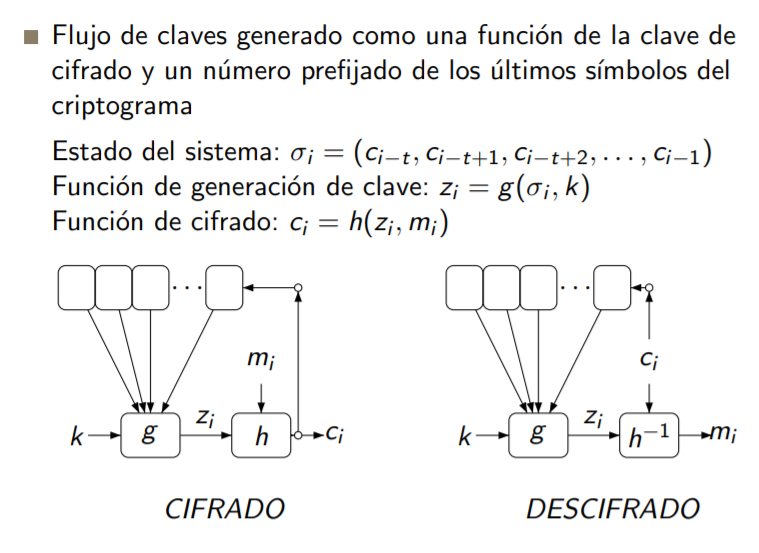
### Sistemas

#### Flujo síncrono

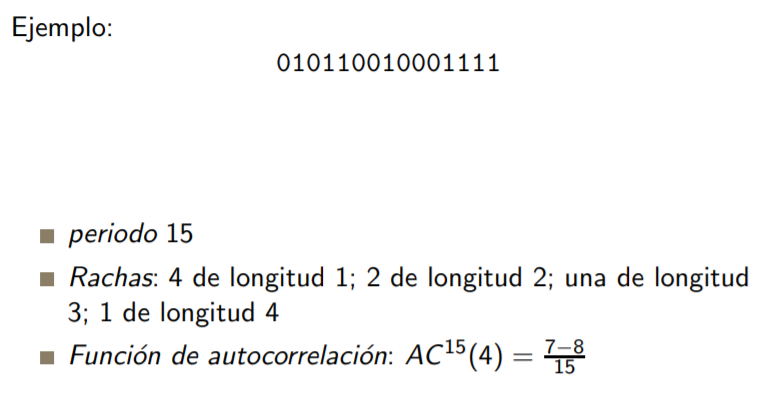
Necesita sincronización entre emisor y receptor, usa marcas a intervalos regulares para reiniciar la sincronización, gracias a eso no es sensible a errores de transmisión.

Es sensible a ataque activos, inserción, borrado, repetición de símbolos

#### Flujo autosíncrono

Depende de los últimos símbolos del criptograma, la pérdida de sincronización se resuelve sola, Los errores se propagan de forma limitada, es menos sensible a los ataques activos y a los basados en redundancias (ya que se desvirtúan las propiedades estadísticas).

## Secuencias binarias pseudoaleatorias

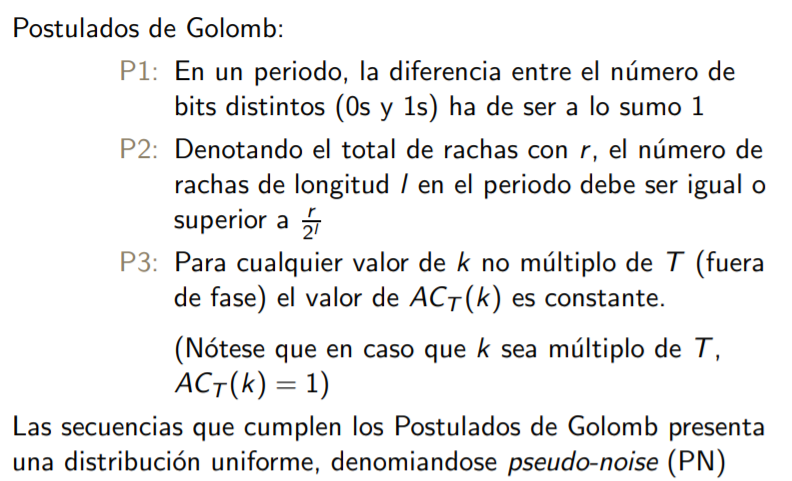


Periodo: número de caracteres hasta que se repita una cadena

Racha: secuencias de bits igua.

Función de autocorrelación: medida de similitud entre una secuencia de periodo T y la secuencia resultante de desplazar esa secuencia d posiciones.

ACT(k) = (Coincidencias – fallos) / Periodo



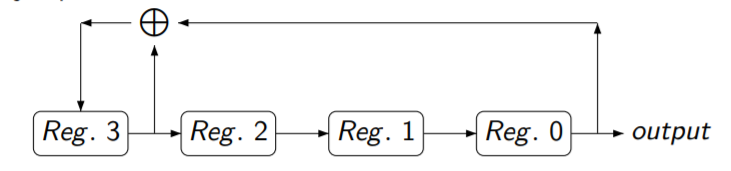
## Generadores pseudoaleatorios

### Generadores de congruencia lineal

Xi+1= axi + b (mod n) a, b, n son la clave secreta

x0 es la semilla, se usa el valor anterior de la secuencia en el resto de valores.  
Se pueden obtener los parámetros del generador teniendo en cuenta un fragmento de la secuencia generada, no se considera de utilidad criptográficas.

### LFSR



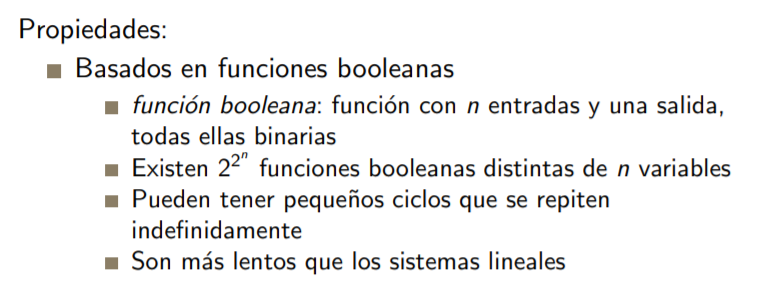
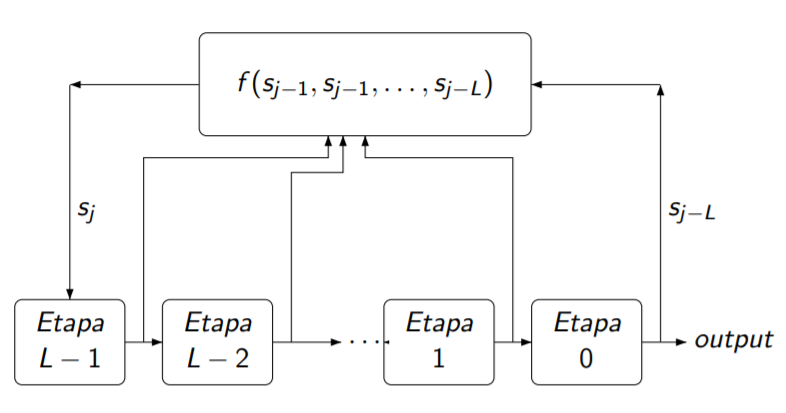
Cadenas de gran periodo, buenas propiedades estadísticas, fácil implementación hardware, se caracteriza por un polinomio módulo 2.

#### Tipos:

* Factorizables: pueden ser descompuestos, el T depende del estado inicial, varía entre n>= T >= 2n-1, puede haber periodos de longitud divisor del principal.
* Irreducibles: T es un factor de 2n-1.
* Primitivos: el polinomio es irreducible y genera el conjunto de configuraciones, T = 2n-1, hay 2n-1 polinomios de este tipo.

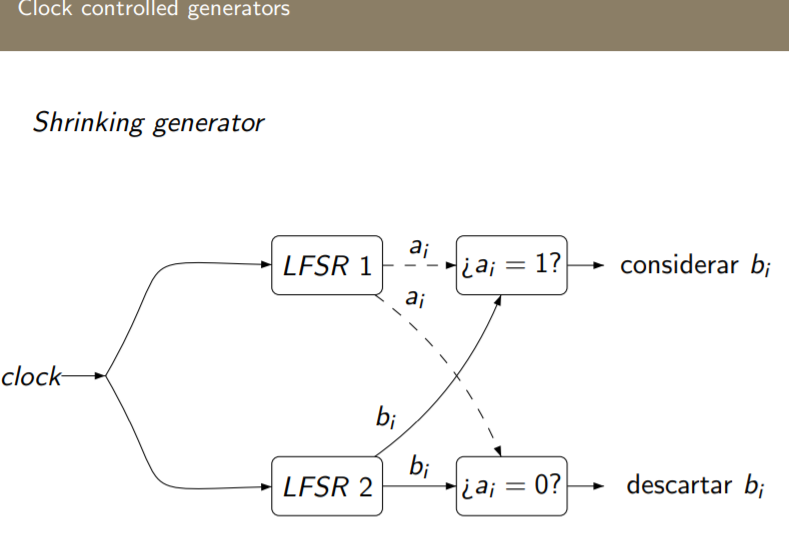
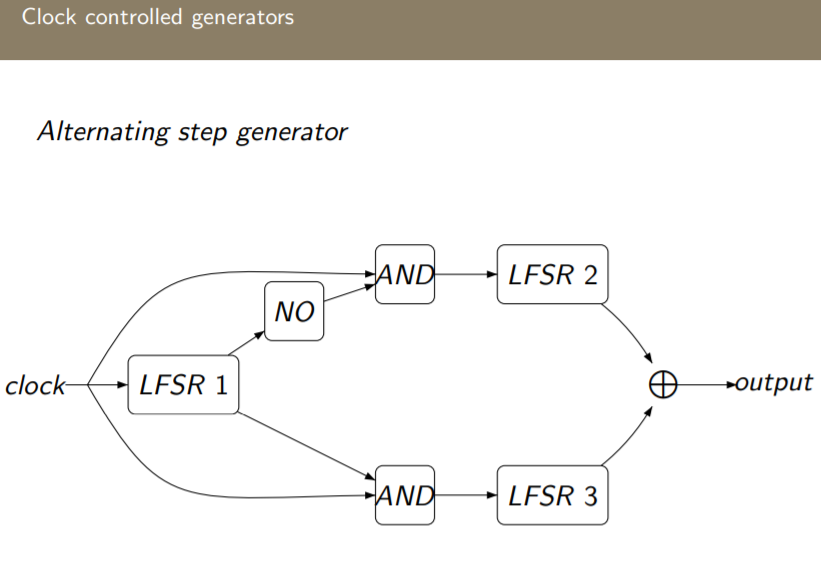
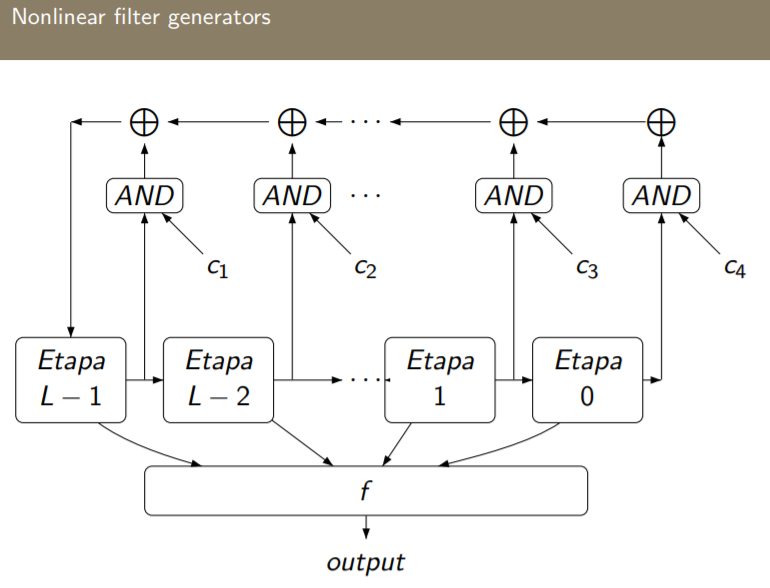
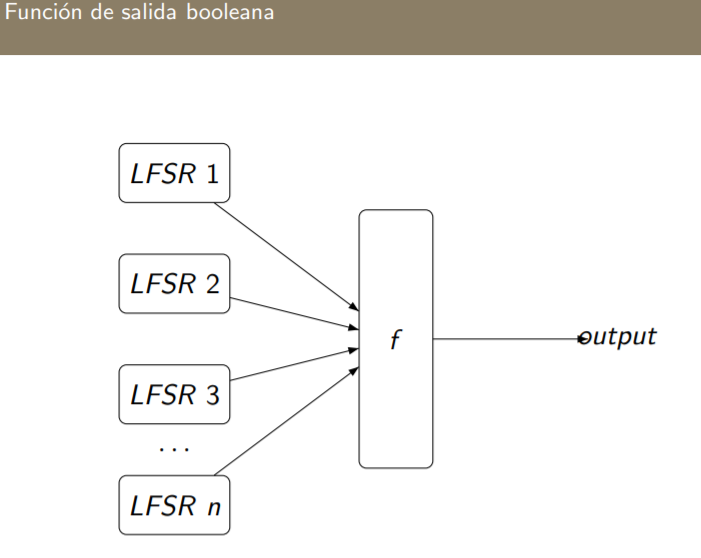
n es el número de etapas, se pueden romper con un segmento de 2n valores de la secuencia generada.

### FSR



### Combinaciones LFSR

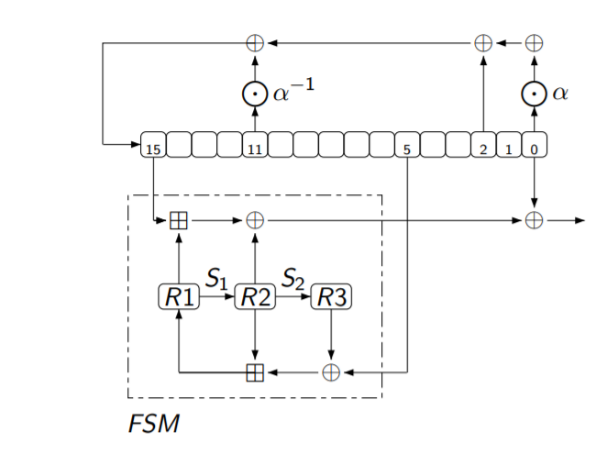
Las secuencias LFSR son predecibles, en la realidad se plantean 3 aproximaciones



### Cifrado A5

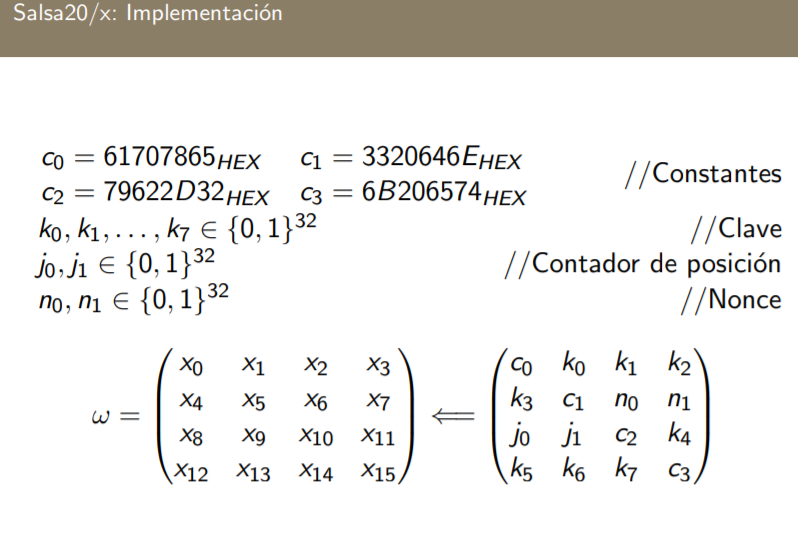
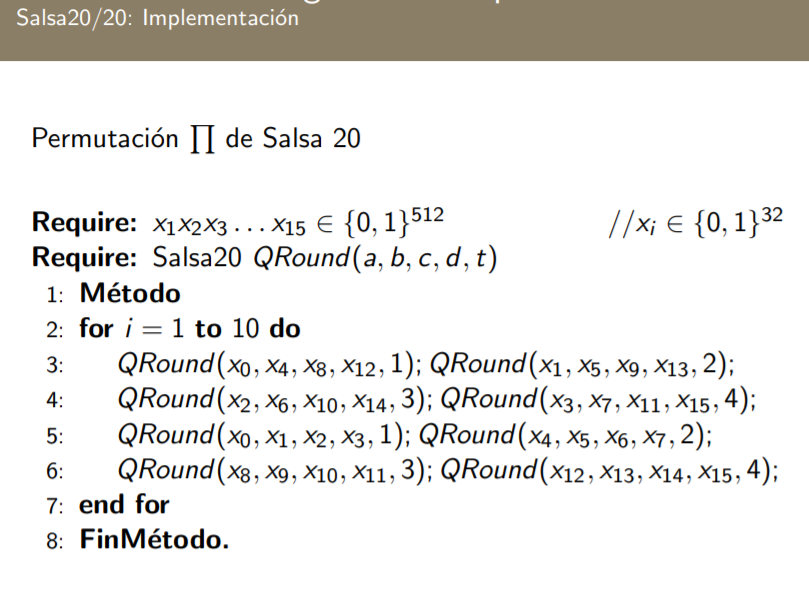
Los grises son para mirara que LFS se tienen que mover, aquellos que tengan el dígito mayoritario

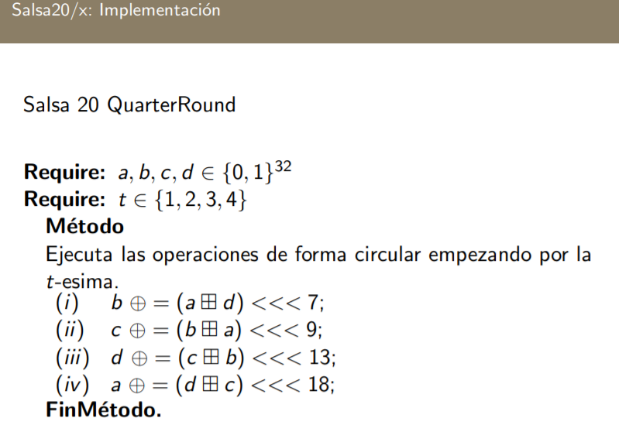
### Cifrado 4G

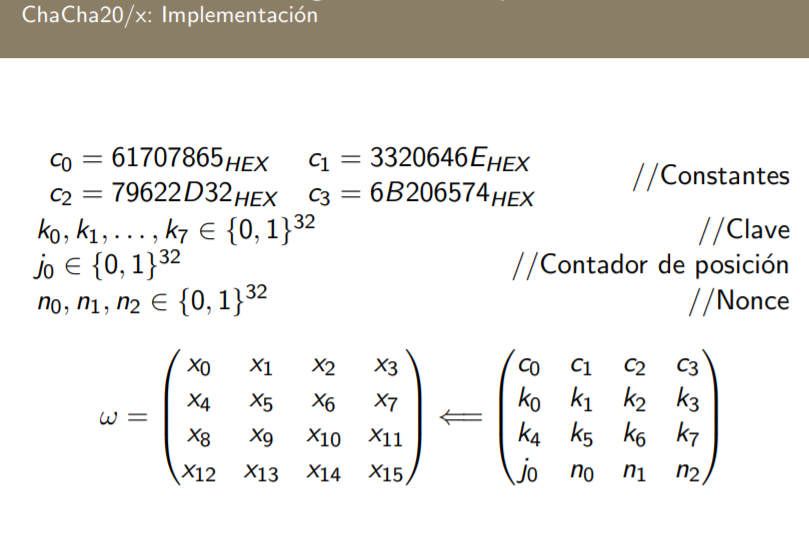
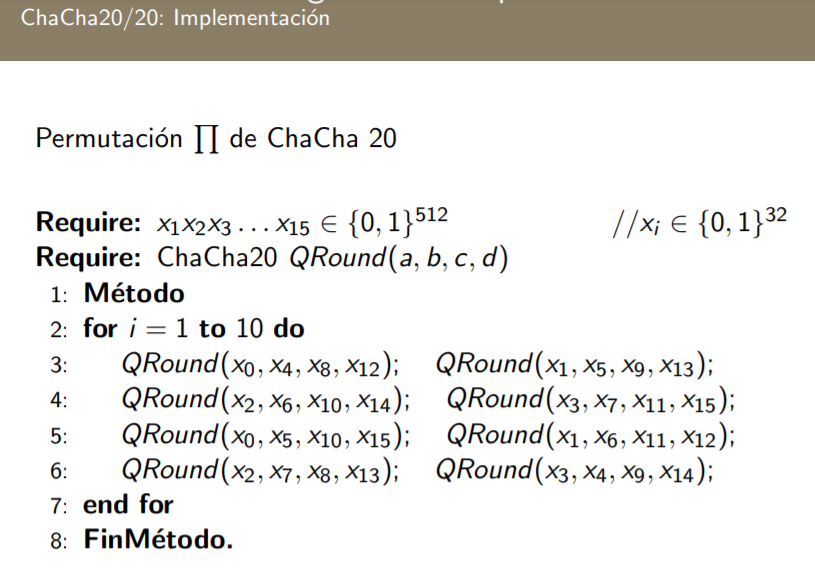
La FSM modifica dos de los 3 registros usando S-boxes

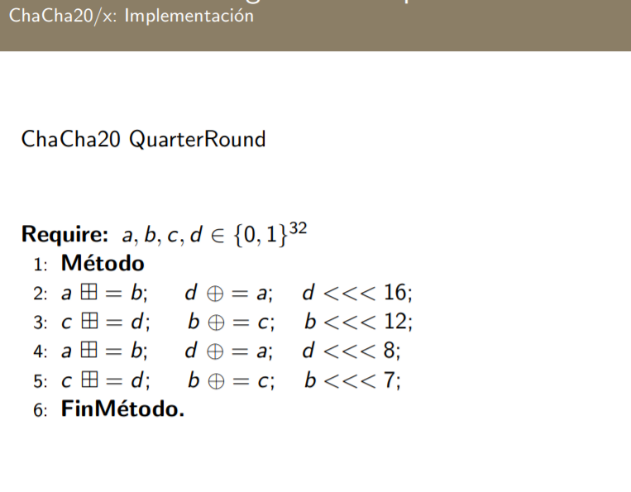
## Cifrados basados en generadores pseudoaleatorios

Una secuencia aleatoria hace de clave para combinar con el mensaje mediante una función.

Cada bloque viene de un hash de la clave (256 b) un nonce (único mensaje de 64 b) y un contador de posiciones (64 b)  
La función resumen se basa en una permutación fija de 512b. Se sugiere Salsa20/12

Mantiene arquitectura de Salsa20  
Cada bloque viene de un hash de la clave (256 b), un nonce (mensaje único de 96 b) y un contador de 32 b

# Tema 5

## Hashing

### Propiedades deseables de las funciones hash:

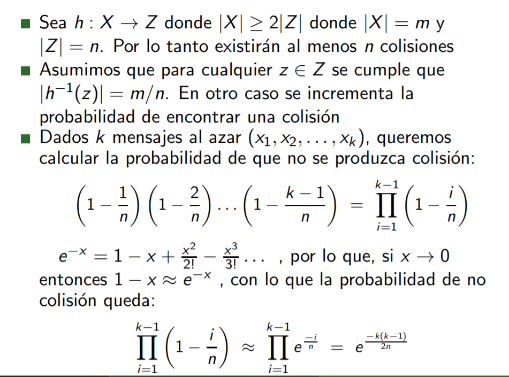
* Funciones hash unidireccionales (OWHF):
  + Resistentes 1º preimagen (one way hashing): dado un hash y no es computacionalmente posible encontrar una x | h(x) = y.
  + Resistentes a la 2º preimagen (weak colisión resistance): dado un mensaje x no se puede conseguir un mensaje x’ | h(x) = h(x’).
* Funciones hash resistentes a colisiones (CRHF):
  + Resistencia a las colisiones (strong colisión resistance): encontrar dos mensajes, x, x’ |h(x)=h(x’) es intratable.

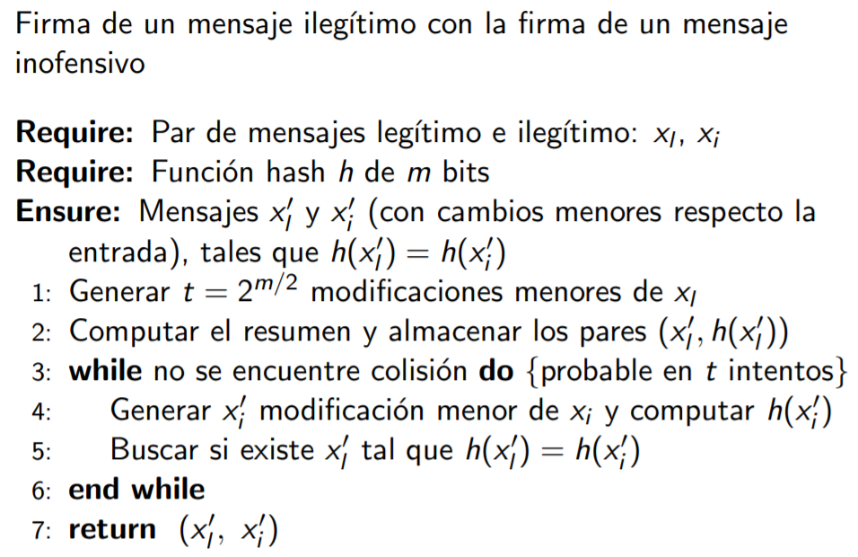
### Relación entre propiedades:

* Resistencia a la 1º preimagen no implica resistencia a la 2º preimagen ni a la inversa.
* CRHF implica resistencia a la 2º preimagen, pero no a la primera.

## Seguridad

### Ataque de cumpleaños

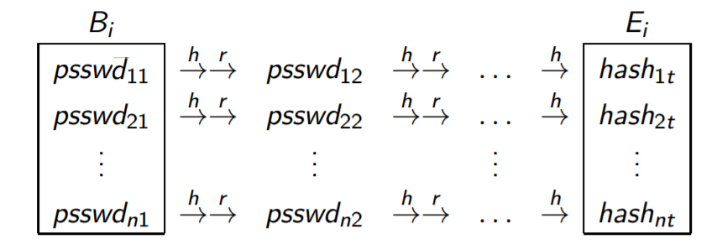
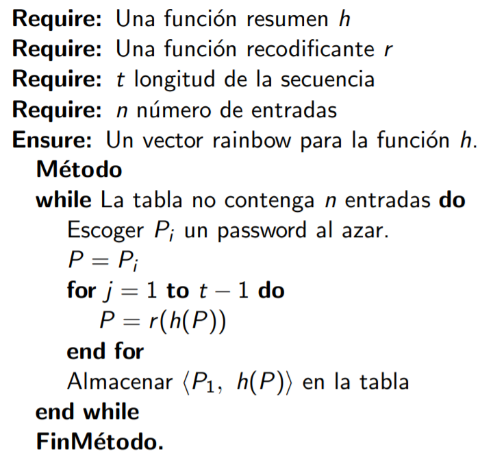
Algoritmo de Yuval:

Ensure = garantizas

El ataque acota inferiormente la talla  
del resumen, con 40 bitss se obtiene   
una colisión con probabilidad 0.5 con  
220 mensajes al azar.  
Para OWHF se necesita exploración   
exhaustiva. Una CRHF de n bits es   
sensible al algoritmo de Yuval.

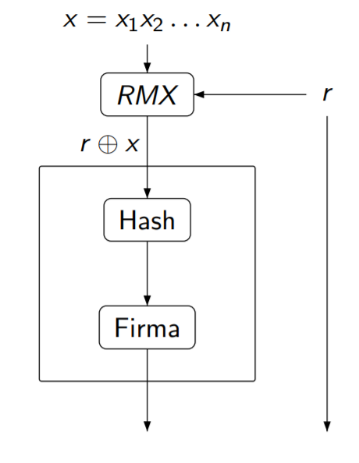
### Ataque arcoiris

Diseñado para encontrar colisiones en contraseñas, sensible a la función de resumen utilizada, usa una aproximación time-memory trade-off, TMTO.

  El inconveniente es obtener colisiones para la tabla, mediante salting se puede prevenir el uso de las técnicas.

### Randomized Hashing RMX

Complementa el proceso de firma contra ataques por colisión de las funciones resumen

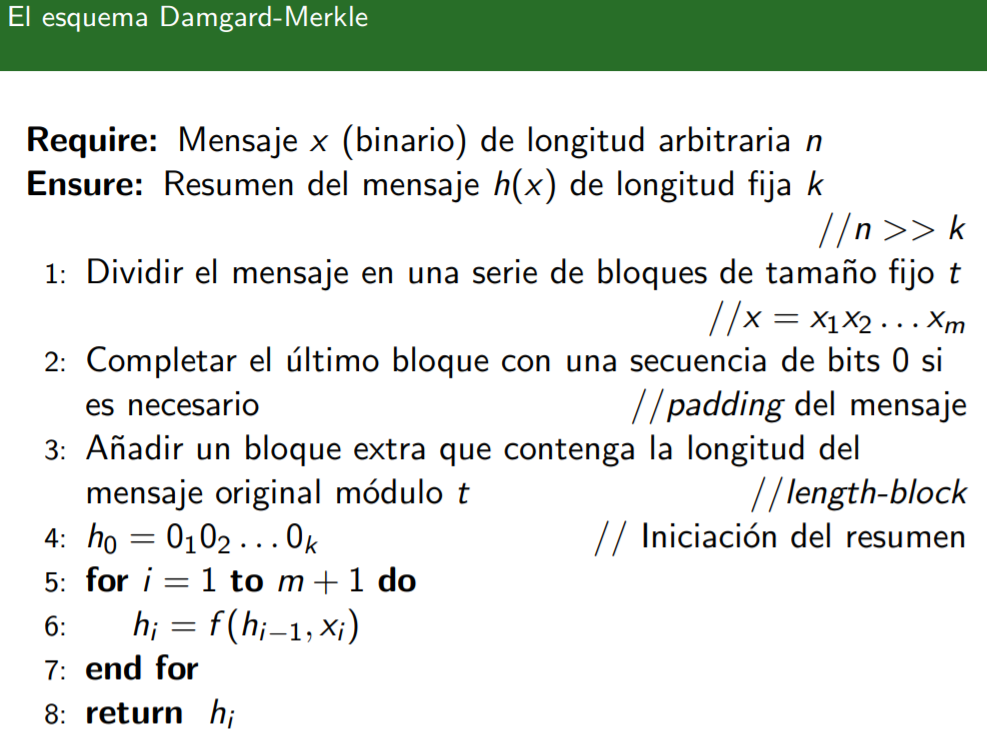
r es una secuencia binaria aleatoria que se genera para cada mensaje firmado.

La secuencia modifica el mensaje, mediante XOR, antes del cálculo del resumen y su firma.

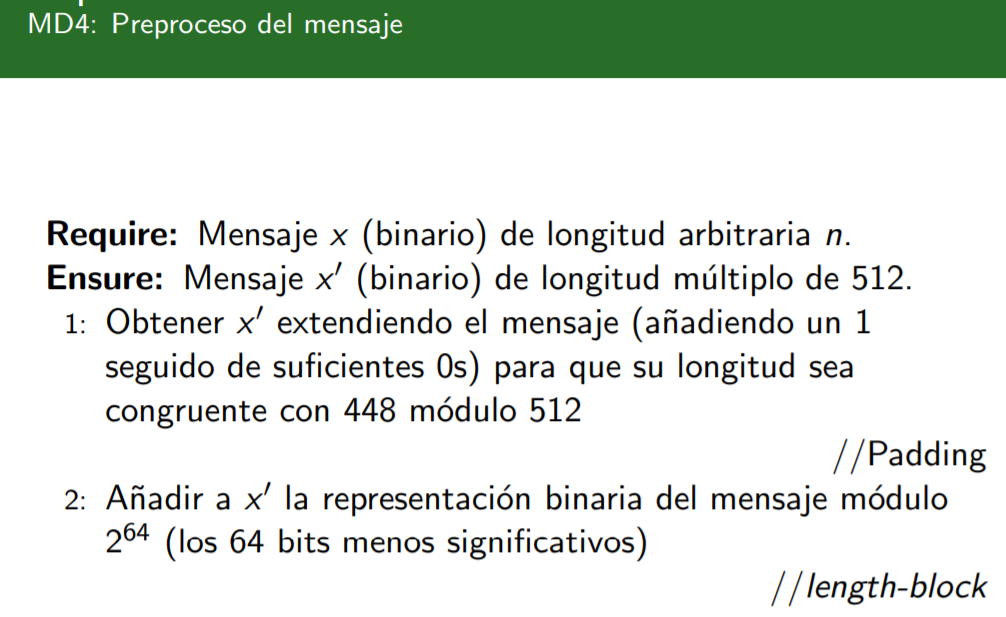
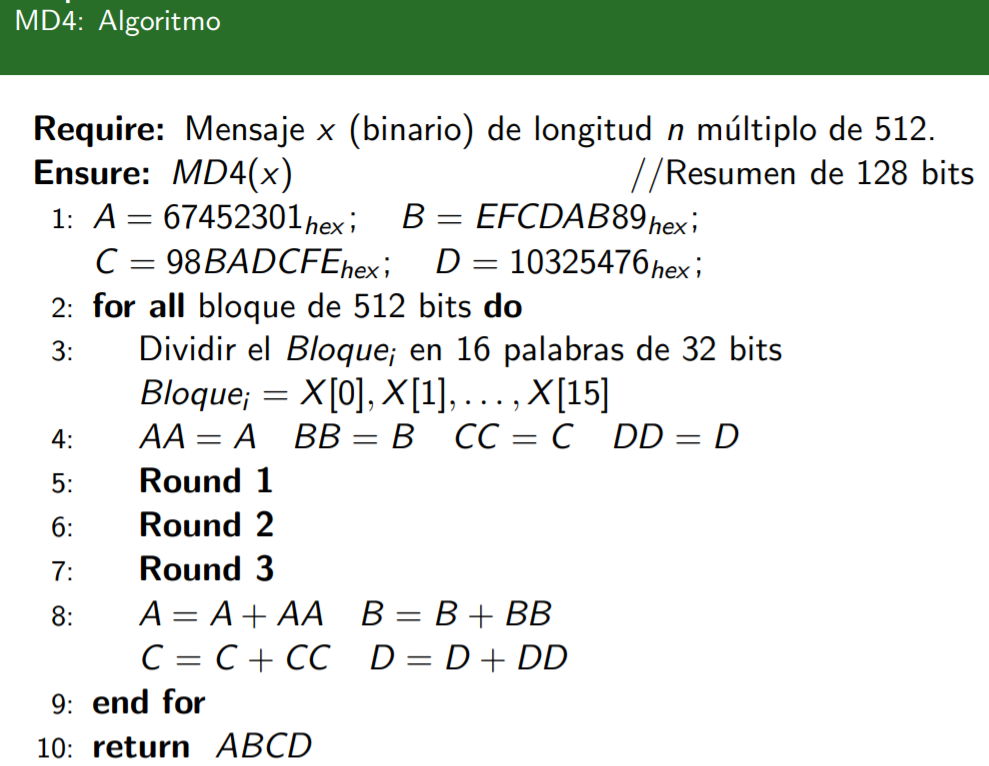
El ataque es equivalente a encontrar una 1º preimagen.

## Implementación funciones hash

Se computa el resumen considerando un *estado* que se modifica iterativamente



### Familia MDx

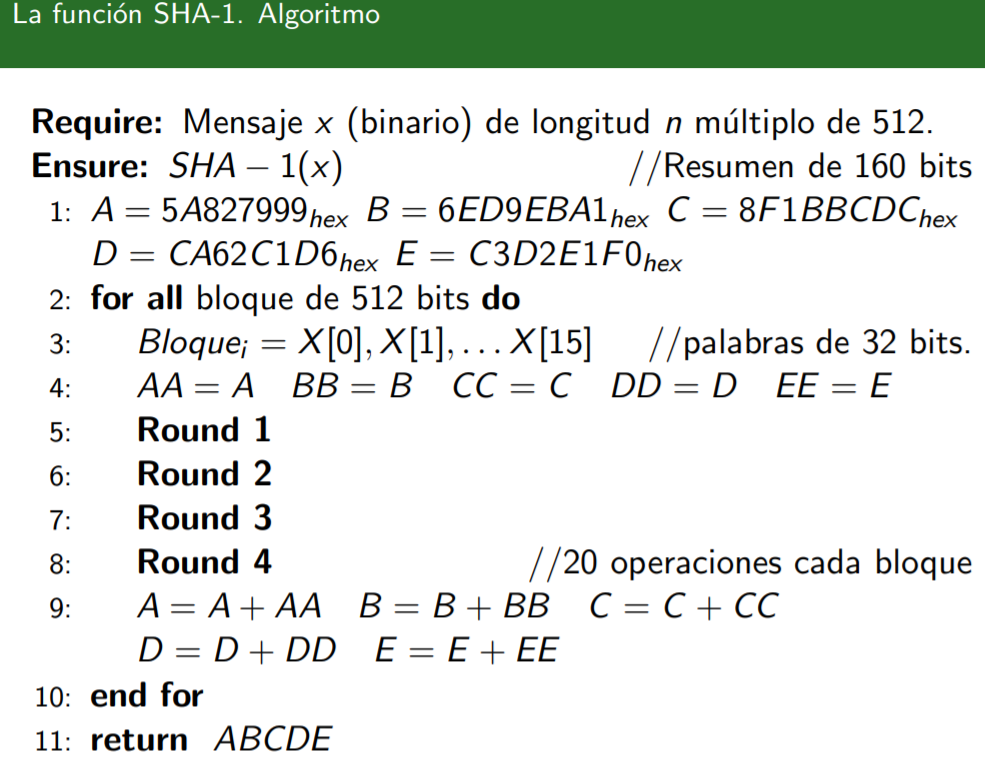
 

MD5 mismo esquema con un 4º round.

DNI electrónico utiliza SHA-1/RSA.  
No se recomienda firmar hashes MD5

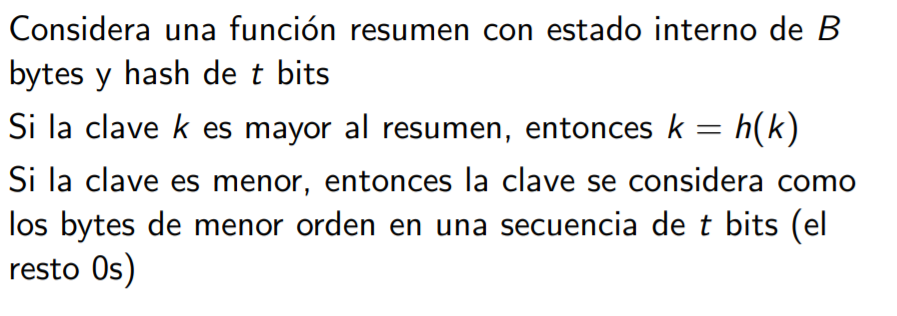
### Familia SHA

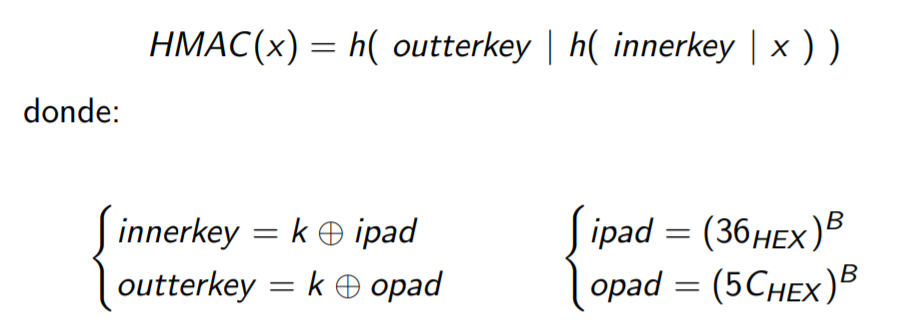
Mismo preproceso que MD4, excepto en que añade la longitud del mensaje (2 bloques de 32 bits, el más significativo primero) en lugar de los 64 bits menos significativos.



## Keyed hash

Modificación del proceso que considera una clave privada





# Tema 7

## Seguridad incondicional

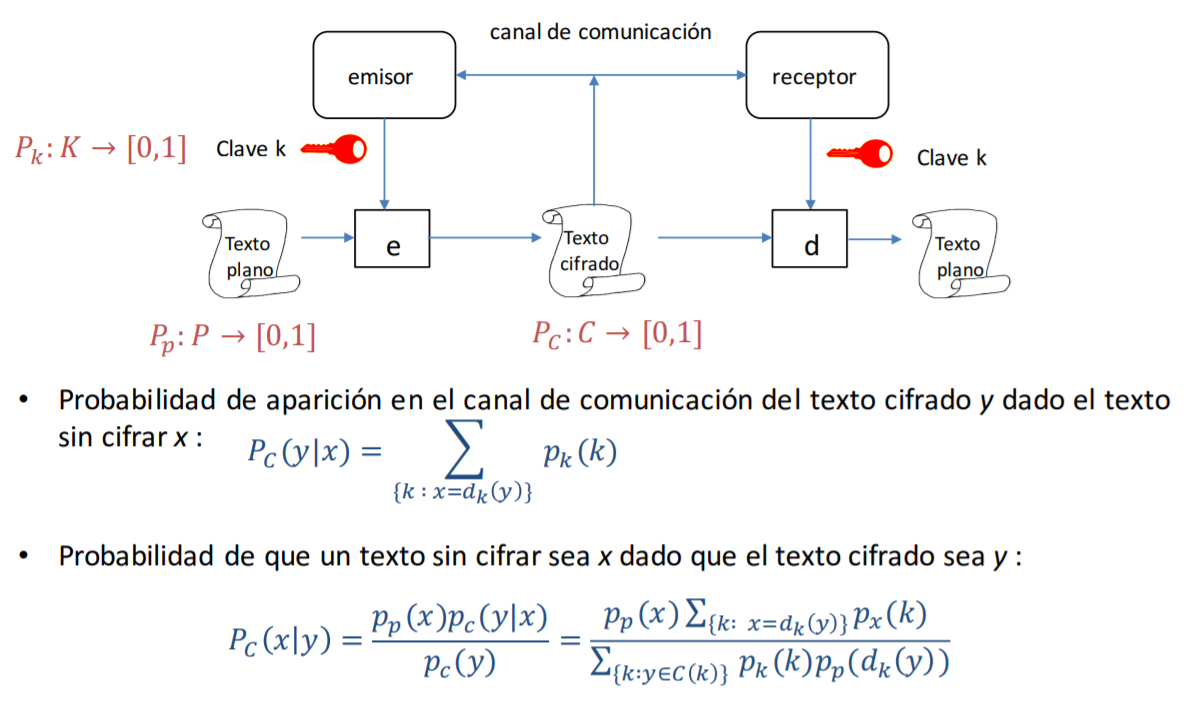
Asunción: los textos X y las claves K son variables independientes.

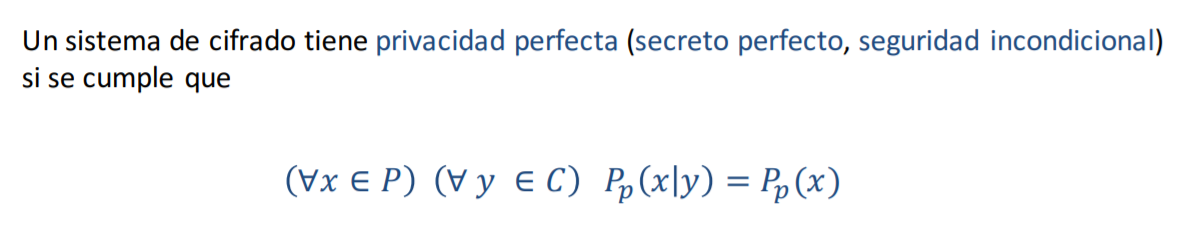
p(x,k) = p(x)p(k)

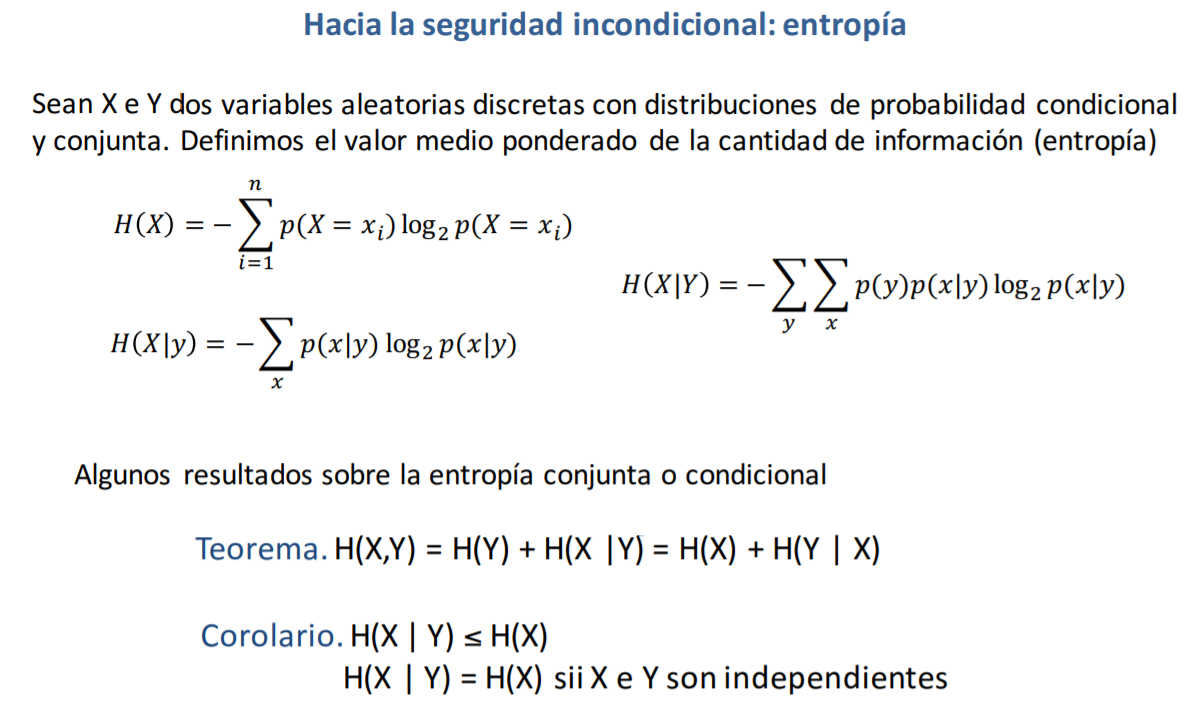
Prob condicional y conjunta: p(x,y) = p(x|y)p(y)

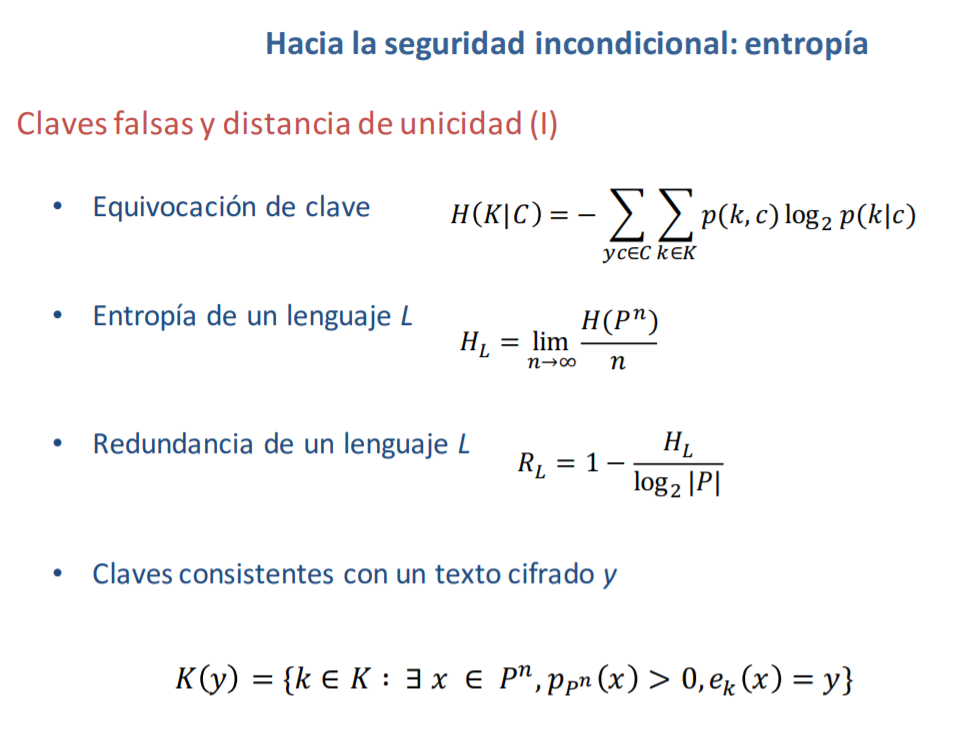
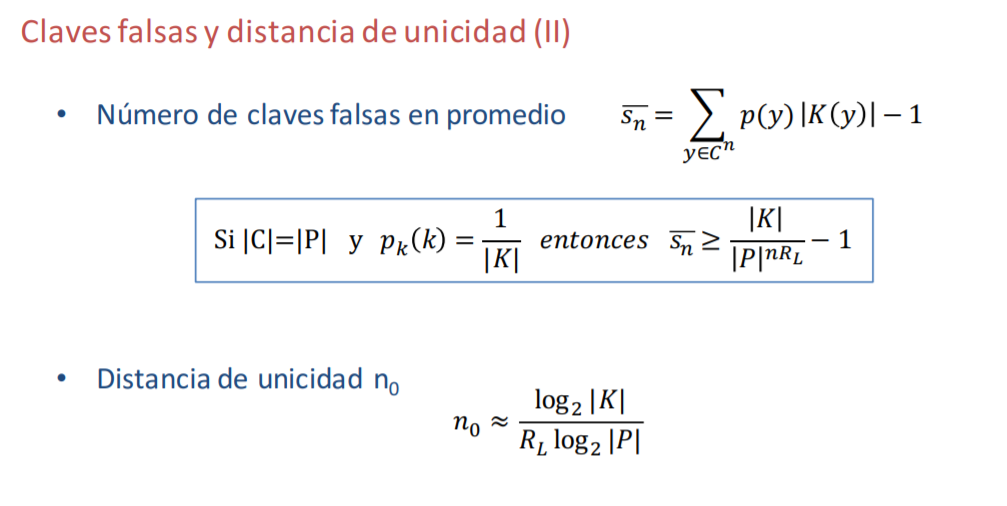
p(x,y) = p(y|x)p(x)

Regla de Bayes p(x|y) = p(y|x)p(x)/p(y)







## Seguridad computacional

