CRIPTOGRAFÍA SIMÉTRICA

AGENDA

- Definiciones (Criptografía, Criptoanálisis y Criptosistema).
- Clasificación de los sistemas criptográficos.
- Clasificación según cantidad de claves.
- Clasificación según tipos de operación.
- Clasificación según formas de procesar el texto.

CRIPTOGRAFÍA

"la escritura secreta"

- Conjunto de métodos y técnicas con el objetivo principal de proteger un mensaje por medio de un algoritmo, usando una o más **claves**.

Objetivos:

- Confidencialidad: Mantener el contenido de la información para aquellos autorizados a tenerla.
- Integridad: Asegurar la no alteración de los datos.
- Autentificación: Permitir la comprobación del origen de los datos. "Remitente es quien dice ser".
- No repudio: Una vez enviado el mensaje, no se puede negar ser parte de la comunicación (Origen y Destino).

CRIPTOANÁLISIS

"el enemigo conoce el sistema" (Shannon)

- Disciplina complementaria a la criptografía que intenta comprometer la seguridad de un criptosistema.

Clasificación:

- Fuerza bruta: Se prueban todas las claves posibles.
- Texto plano escogido:Se eligen varios textos planos y se obtienen sus criptogramas.
- Texto plano: Se tienen algunos textos planos y sus correspondientes criptogramas.

Análisis de frecuencias: Se estudian las frecuencias de aparición de los símbolos en el lenguaje y en criptograma.

CRIPTOSISTEMA

- Se define como la quíntupla (M,C,K,E,D), donde:

M	Mensajes que pueden ser enviados.
K	Claves que se pueden emplear.
C	Posibles mensajes cifrados.
E	Transformaciones de cifrado.
D	Transformaciones de descifrado.

Clada clave k determina las transformaciones Ek y Dk:

$Ek(m)=c \quad Dk(c)=m \Rightarrow \mathbf{Dk(Ek(m))=m}$

Clasificaciones de sistemas criptográficos

- Cantidad de claves
  - Simétricos
  - Asimétricos
- Tipo de operación de cifrado
  - Sustitución
  - Transposición
- Formas de procesar el texto
  - Por bloques
  - Por flujo

Clasificación según cantidad de claves

- **Sistemas simétricos**: Emplean una misma clave para encriptar y para desencriptar.
  - Desventaja: No puede ser utilizada en canales de comunicación → cómo enviamos la clave?

- **Sistemas asimétricos**: Emplean doble clave, una privada y una pública. Su seguridad radica en la dificultad de conocer la clave privada a partir de la pública.
  - Desventaja: muy costosa computacionalmente.

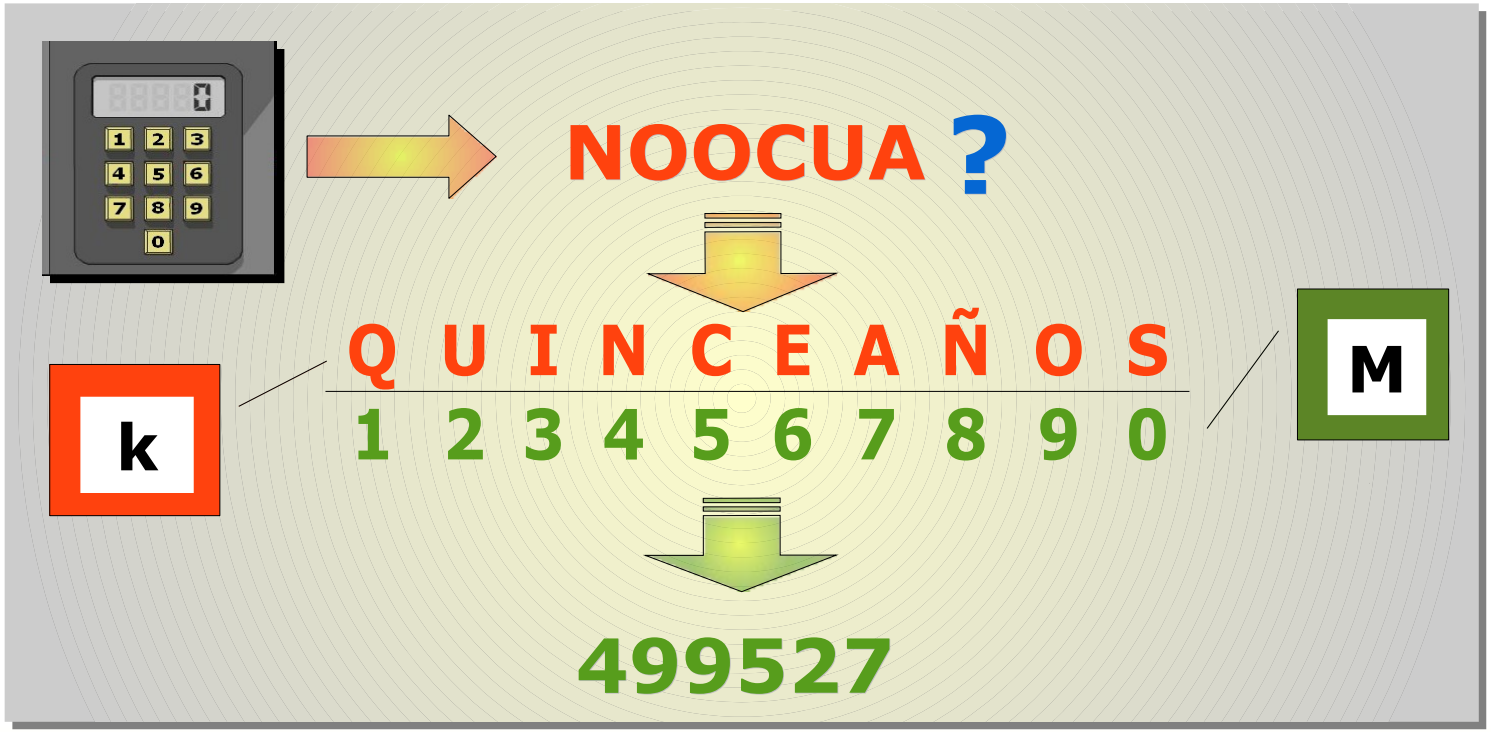
- Actualmente se encripta el mensaje con un algoritmo simétrico y la clave de encripción con uno antisimétrico (la clave tiene longitud más corta).

CRIPTOGRAFÍA SIMÉTRICA

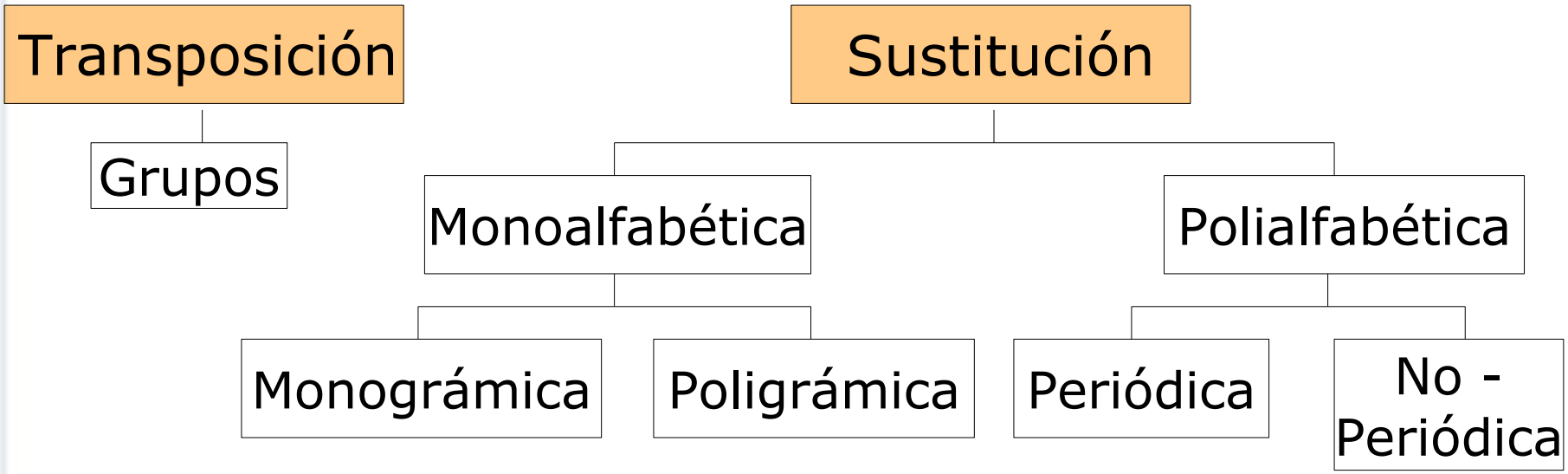
- Esquema general:

f(MENSAJE, **PASSWORD**) = CÓDIGO

f^{-1}(CÓDIGO, **PASSWORD**) = MENSAJE



Clasificación según tipo de operación



- Cifrado N-grámico: Se cifra por conjuntos de N caracteres.
- Cifrado N-alfabético: Cada carácter del texto plano puede cifrarse en N de texto encriptado, dependiendo de su posición en el mensaje.

Cifrados por transposición

- Transposición simple

- No sustituye símbolos por otros sino que cambia su orden.
- Rompe las cadenas características del lenguaje.
- Se divide el texto en bloques de tamaño **n**.
- El conjunto de claves posibles K se compone de las n! permutaciones de la sucesión **{1,2,..,n}**

Para cada k ∈ K se definen las funciones:

$$E_e(m) = (m_{e(1)} m_{e(2)} \ldots m_{e(n)})$$

$$D_d(c) = (c_{d(1)} c_{d(2)} \ldots c_{d(n)})$$

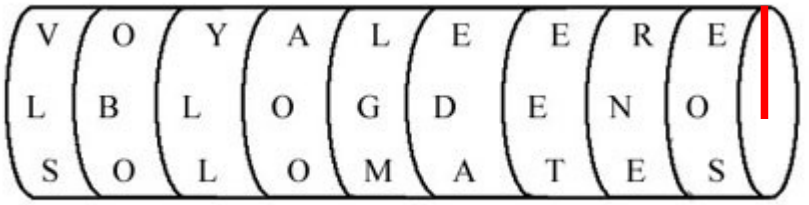
$$d = e^{-1}$$

Cifrados por transposición

- Escítala

- Usada en el siglo V a.d.C. por el pueblo griego de los lacedemonios.
- Bastón en el que se enrollaba una cinta de cuero y luego se escribía en ella el mensaje de forma longitudinal.

k → diámetro del bastón



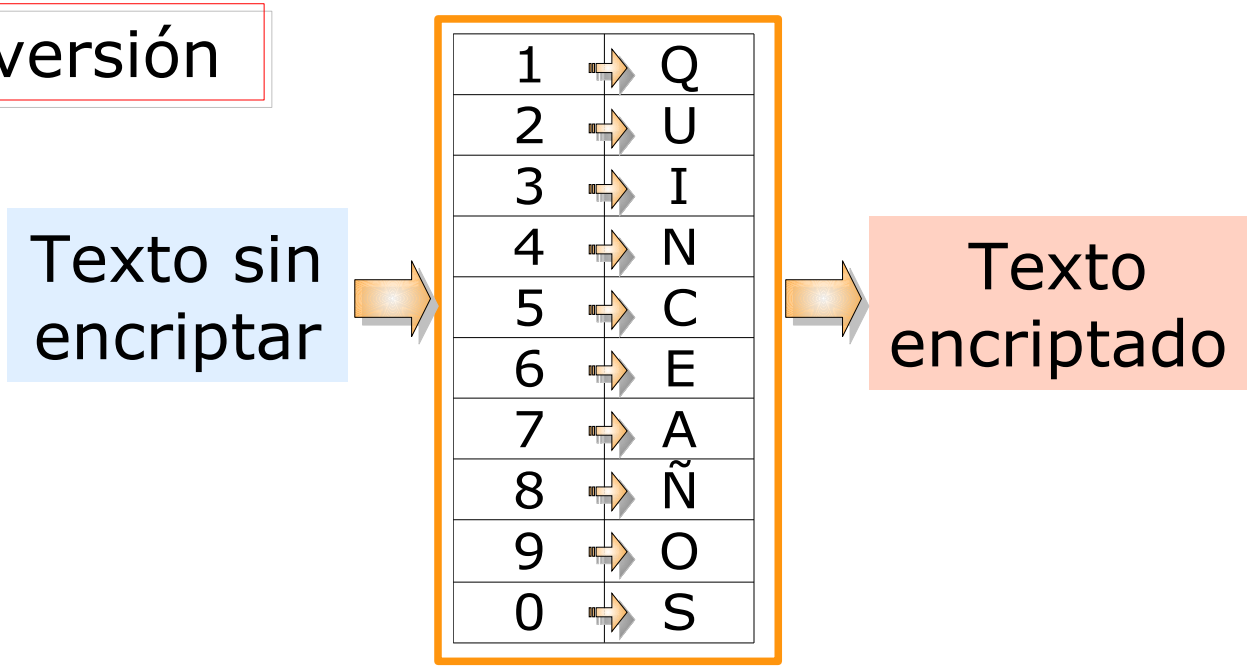
- Para desencriptar se debía enrollar dicha cinta en un bastón con el mismo diámetro que el usado en el extremo emisor y leer el mensaje de forma longitudinal.

Cifrados por sustitución

- Caso general

Se trata de una sustitución arbitraria de caracteres.

k → Tabla de conversión



Clasificación: Cifrado monoalfabético monográmico

Cifrados por sustitución

- Sustitución afín

- Se determinan dos enteros: *a* y *b*, con los cuales se define la siguiente transformación de cifrado:

k → a y b

$$E(a,b)=(aM+b)\,mod\,(N)$$

Con : $a \geq b$
$b \leq 25$

Caso particular:

- Algoritmo de César : $E(a,b)=(M+3)\,mod\,(N)$ k → a=1, b=3

Clasificación: Cifrado monoalfabético monográmico

Cifrados por sustitución

- Playfair

- Se distibuyen las letras del abecedario en una matriz de 5x5 (se suelen omitir la J y la W).
- La distribución en la matriz puede ser arbitraria o siguiendo una palabra secreta.

k → palabra clave o matriz arbitraria

k=CLAVE

C	L	A	V	E
B	D	F	G	H
I	K	M	N	O
P	Q	R	S	T
U	W	X	Y	Z

Clasificación: Cifrado monoalfabético poligrámico (orden 2)

Cifrados por sustitución

- Cifrado de Hill

- Se define una matriz M de NxN elementos.

$$\begin{matrix} c_{11} \\ c_{21} \\ \dots \\ c_{N1} \end{matrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} & \dots & k_{1N} \\ k_{21} & k_{22} & k_{23} & \dots & k_{2N} \\ \dots & \dots & \dots & \dots & \dots \\ k_{N1} & k_{N2} & k_{N3} & & k_{NN} \end{bmatrix} \begin{matrix} M_{11} \\ M_{21} \\ \dots \\ M_{N1} \end{matrix}$$

$k \rightarrow$ matriz

$D:\{0,1,..,25\}$

$k_{ij} \in D$

La matriz debe ser inversible utilizando aritmética módulo 26.

Clasificación: Cifrado monoalfabético N-grámico

Cifrados por sustitución

- Sustitución homofónica

- Asigna a cada caracter una cantidad X de símbolos en forma arbitraria.
- X es proporcional a la frecuencia del carácter en el lenguaje.

Intenta suavizar la distribución de frecuencias.

k → tabla de sustitución

Ai	H(Ai)
a	12 29 25 43 71 80 89 95
b	5 92
c	19 37 36

Clasificación: Cifrado polialfabético monográmico

Cifrados por sustitución

- Vigènere

- Utiliza un desplazamiento distinto para cada carácter según una clave.

$$E(m_i) = (m_i + k_i) \bmod (N)$$

k ➡ palabra secreta

T E X T O A C I F R A R
C L A V E C L A V E C L

➡ La clave se escribe periódicamente

Clasificación: Cifrado polialfabético monográmico periódico

Clasificación según formas de procesar el texto

- **Cifrado de bloques**: Toma un bloque de tamaño fijo del texto claro y produce otro de tamaño fijo del texto cifrado. Usualmente tienen la misma longitud.

- **Cifrado de flujo**: Emplea una secuencia aleatoria de símbolos de la misma longitud del texto claro (clave demasiado larga, poco práctico).

Cifrado de flujo

- One Time Pad

- Se combinan una secuencia aleatoria de símbolos con el texto plano mediante una función simple y reversible.
- La clave se utiliza una única vez.

k → secuencia aleatoria

Ejemplo:

Mensaje	*XOR*	01100011
S. Aleatoria		01011010
Criptograma		00111001

Caso particular: • Cifrado de *Vernam*

Clasificación: Cifrado de flujo

Cifrado de bloques

- Cifrado de producto

- Combina las técnicas de cifrado por sustitución y transposición brondando un grado más alto de seguridad.
- Se divide el mensaje en bloques y se aplica una sucesión de transformaciones de cifrado a cada uno de ellos.

IMPORTANTE : El cifrado no debe poseer *estructura de grupo*

Caso particular: • DES (Data Encryption Standar)

Referencias

• Criptografía y Seguridad en Computadores, tercera edición. Manuel José Lucena Lopez. Dpto. de Informática Universidad de Jaén. Edición virtual - 2003.
(http://www.loba.es/flossic/Contenidos/Manuales/Criptografia.pdf)

• Aplicaciones Criptográficas, segunda edición. Departamento de Publicaciones de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, España.
(http://www.criptored.upm.es/descarga/CriptoClasicapdf.zip)

• Una introducción a la criptografía. Eugenio García, Miguel Ángel López, Jesús Ortega. Dpto. De Matemáticas Universidad de Castilla. (http://www.criptored.upm.es/descarga/UnaIntroduccionCriptografia.zip)