

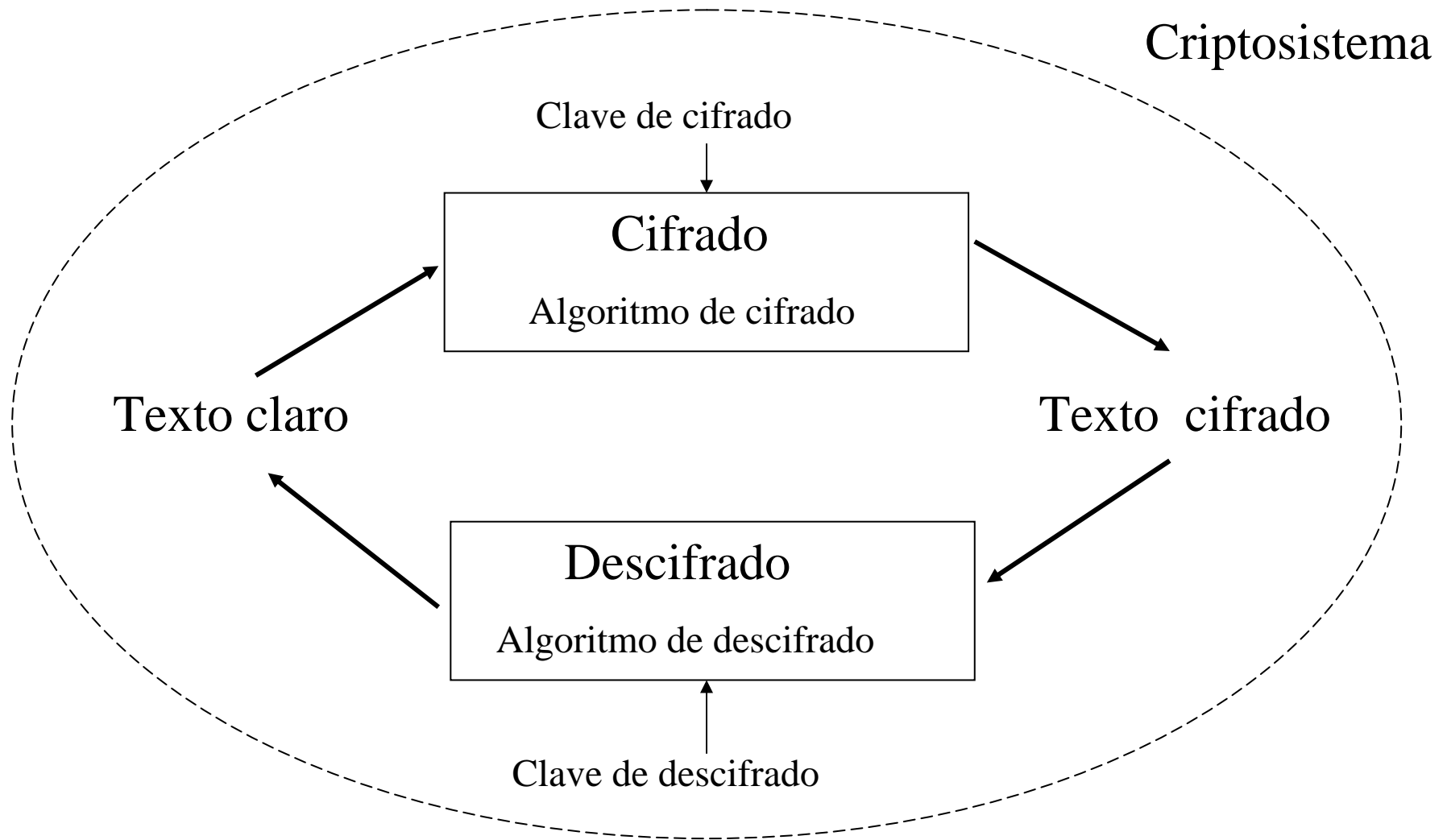
Criptología

Protección de la Información

Índice

- Conceptos
- Criptología clásica
- Criptología convencional
- Criptología de clave pública
- Aplicaciones

Conceptos básicos



Terminología básica

- **Criptografía**

- DRAE: Arte de escribir con clave secreta o de un modo enigmático
- Arte y ciencia de mantener los mensajes escritos en secreto
- Estudio de los principios y técnicas mediante los que se puede escribir ocultando la información

Cifrado
y
descifrado

- **Criptoanálisis**

- DRAE: Arte de descifrar criptogramas
- Arte y ciencia de recrear información cifrada

No se tiene
información para
descifrado

- **Criptología**

- Criptografía + criptoanálisis
- Arte y ciencia de la información segura

Criptografía. Características

- Lo que es **conocido**
 - Diseño **cerrado**: secreto **todo** lo posible
 - Algoritmos restringidos (a grupo)
 - Salida de miembro de grupo, supone cambio
 - Estandarización no posible
 - Diseño **abierto**: secreta sólo **clave**
 - 1 clave (o una a partir de la otra): Criptografía **simétrica**
 - Emisor y receptor comparten clave secreta
 - 2 claves (y no una a partir de la otra): Criptografía **asimétrica**
 - Una clave pública: conocida por todos
 - Una clave privada: secreta, conocida por dueño
 - Una para cifrar y otra para descifrar
 - Estandarización

Criptografía. Características (cont.)

- Tipo de **operaciones** usadas:
 - **Sustitución:**
 - Cada símbolo es reemplazado por otro
 - **Transposición:**
 - Cada símbolo reorganizado en el todo
 - **Producto:**
 - Combinación de sustitución y transposición
- Modo de **procesamiento** del texto claro
 - De **flujo:**
 - bit (byte) a bit
 - De **bloque:**
 - grupo de bits a grupo de bits
 - Modos de uso permiten convertirlos en cifradores de flujo

Un buen algoritmo

Criptografía

| Tipo de ataque | Conocido por atacante | Objetivo de atacante |
|-----------------------|---|---|
| Sólo texto cifrado | <ul style="list-style-type: none">• Algoritmo de cifrado• Texto cifrado | <ul style="list-style-type: none">• Texto claro• Clave• Algoritmo equivalente |
| Texto claro conocido | <ul style="list-style-type: none">• Algoritmo de cifrado• Texto cifrado• Pares texto claro – texto cifrado | <ul style="list-style-type: none">• Clave• Algoritmo equivalente |
| Texto claro elegido | <ul style="list-style-type: none">• Algoritmo de cifrado• Texto cifrado• Texto claro elegido y su texto cifrado | <ul style="list-style-type: none">• Clave• Algoritmo equivalente |
| Texto cifrado elegido | <ul style="list-style-type: none">• Algoritmo de cifrado• Texto cifrado• Texto cifrado elegido y su texto claro | <ul style="list-style-type: none">• Clave• Algoritmo equivalente |
| Directo a persona | (Ingeniería social y métodos delictivos: engaño, amenaza, chantaje, tortura, etc.) | <ul style="list-style-type: none">• Clave |

Texto elegido

adaptativo

Criptoanálisis (cont.)

- Mecanismos:

- Fuerza bruta

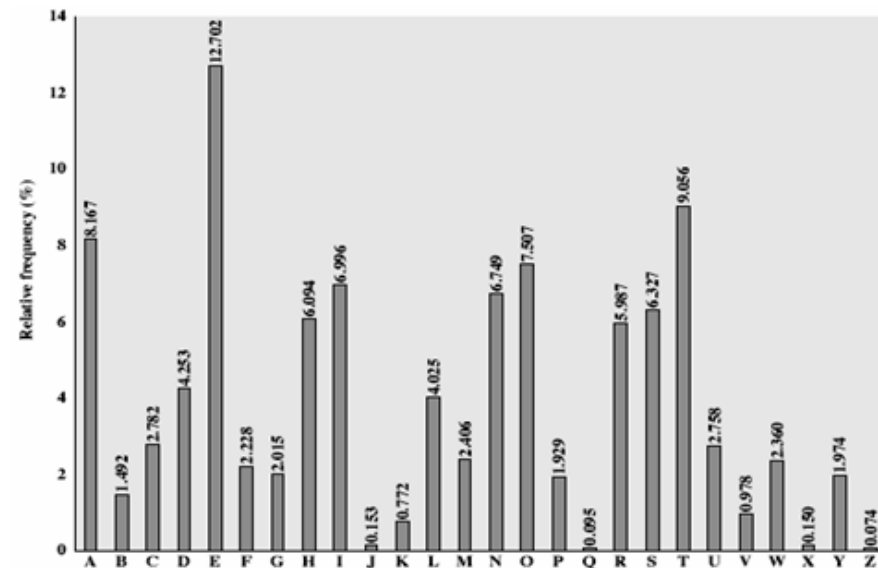
| Key Size (bits) | Number of Alternative Keys | Time required at 1 encryption/ μ s | Time required at 10^6 encryptions/ μ s |
|-----------------------------|--------------------------------|---|--|
| 32 | $2^{32} = 4.3 \times 10^9$ | $2^{31} \mu\text{s} = 35.8$ minutes | 2.15 milliseconds |
| 56 | $2^{56} = 7.2 \times 10^{16}$ | $2^{55} \mu\text{s} = 1142$ years | 10.01 hours |
| 128 | $2^{128} = 3.4 \times 10^{38}$ | $2^{127} \mu\text{s} = 5.4 \times 10^{24}$ years | 5.4×10^{18} years |
| 168 | $2^{168} = 3.7 \times 10^{50}$ | $2^{167} \mu\text{s} = 5.9 \times 10^{36}$ years | 5.9×10^{30} years |
| 26 characters (permutation) | $26! = 4 \times 10^{26}$ | $2 \times 10^{26} \mu\text{s} = 6.4 \times 10^{12}$ years | 6.4×10^6 years |

- Análisis basado en

- Conocimiento de **lengua**:

- Estudio de **patrones** en texto cifrado (estadística)

- Conocimiento de **algoritmo** (matemáticas)



Más definiciones

- Seguridad **incondicional**
 - No importa cuánto
 - texto cifrado, tiempo y capacidad computacionaleses imposible recuperar el texto claro
 - porque el texto cifrado no da información sobre el claro
 - Sólo *one-time pad* lo es
- Seguridad **computacional**
 - Dados
 - tiempo y capacidad computacional disponibleses imposible recuperar el texto claro, o
 - coste de ruptura > valor de información cifrada, o
 - tiempo de ruptura > tiempo útil de información cifrada

Criptografía clásica

Previa a computadora

Sustitución monoalfabética

- Sustitución: Remplazar una unidad básica por otra

- **Monoalfabética**

- Cesar: desplazamiento cíclico de 3 posiciones:

a b c d e f g h i j k l m n ñ o p q r s t u v w x y z
D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A B C

- Desplazamiento cíclico de k posiciones:

- Si asignamos un número a cada letra,

a b c d e f g h i j k l m ...
0 1 2 3 4 5 6 7 8 9 10 11 12 ...

podemos generalizar:

$$C_i = (p_i + k) \bmod |A|$$

$$p_i = (c_i - k) \bmod |A|$$



Español: $|A| = 27$


- Criptoanálisis:

- $|A|$ claves \rightarrow Fuerza bruta fácil

Sustitución monoalfabética (cont.)

- Permutación aleatoria del alfabeto: $|A|!$ claves

a b c d e f g h I j k l m n ñ o p q r s t u v w x y z
D K V Q F I B J W P E Ñ S C X H T M Y A U O L R G Z N

- Criptoanálisis: Análisis de frecuencias (letra, dos letras, tres letras, ...) 
- Otros:
 - Homofónica:
 - Cada letra con conjunto de símbolos (generalmente n^{os}) únicos
 - Cada vez se usa uno del conjunto → rompe frecuencias
 - Poligráfica:
 - Cifra grupos de símbolos: Playfair (2 letras), Hill (m letras)
 - Uso de matriz de sustitución

Sustitución polialfabética

- Varias sustituciones monoalfabéticas
 - Cifrado de símbolo depende de su posición
- **Vigenère**

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

- Generalizando con n^{os} :

$$C_i = (p_i + k_i) \bmod |A|$$

$$p_i = (c_i - k_i) \bmod |A|$$

clave: deceptivedeceptivedeceptive
 texto: wearediscoveredsaveyourself

→ ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Sustitución polialfabética

- **Vigenère** (cont.)

- Periodo: n° de letras tras el que se repite la clave

- **Mejora** (autoclave):

clave: `deceptivewearediscoveredsav`

texto: `wearediscoveredsaveyourself`



ZICVTWQNG...

- **Criptoanálisis:**

Determinar n° de alfabetos y

hacer criptoanálisis monoalfabético: Método de Kasiski

Sustitución polialfabética (cont.)

- **Vernam**

- **Clave:** Cinta (lista) de letras aleatorias
- Si se trata texto como datos binarios: $c_i = p_i \oplus k_i$
texto claro: 01100101
clave: 00110101
texto cifrado: 01010000
- Posible repetición para texto muy largo



↓ Mejora de Mauborgne:

One-time pad

- **Clave:** infinita y sin repeticiones
 - unidades generadas aleatoriamente
 - tan larga como texto
 - no reutilizable

Seguro
incondicionalmente

¿Distribución de clave?

Transposición



- Reorganizar el **orden** de las unidades básicas: **Permutación**
 - Usa bloques: con n° fijo de filas o n° fijo de columnas
 - Necesario todo el texto

- **Barrera de tren:** escritura en diagonal y lectura en filas

m e m a t r h t g p r y
e t e f e t e o a a t → M E M A T R H T G P R Y E T E F E T E O A A T

- Escritura en filas y **transposición de columnas**

Clave: 3 4 2 1 5 6 7

Texto: a t t a c k p

o s t p o n e
d u n t i l t
w o a m **x y z** ↗ Relleno

- Lectura por columnas

A P T M T T N A A O D W T S U O C O I X K N L Y P E T Z

- Lectura por filas


A T A T C K P P T O S O N E T N D U I L T M A W O X Y Z

- **Doble** transposición

- **Criptoanálisis**

- No ocultan propiedades del mensaje claro, solo las dispersan

Producto

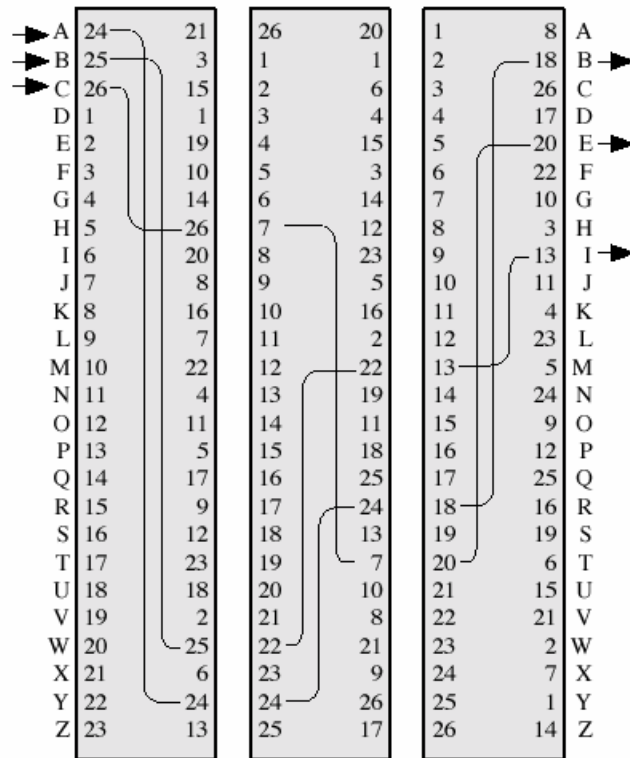
- Sustitución y transposición
amenazadas por características de lenguas
- **Producto:** Varias etapas de sustitución o transposición, o ambas 
- Shannon (1949): Características de un buen cifrado
 - **Confusión:**
Cambio en texto produce efecto no predecible en texto cifrado
 - Oculta relación entre texto claro y cifrado, mediante sustitución
 - **Difusión:**
Cambio en texto debe influir en muchas partes de texto cifrado
 - Disipa estructura estadística de texto claro por todo texto cifrado, mediante permutación
- Redes de **sustitución-permutación** (puestas en práctica por Feistel)

Nacimiento de la criptografía moderna

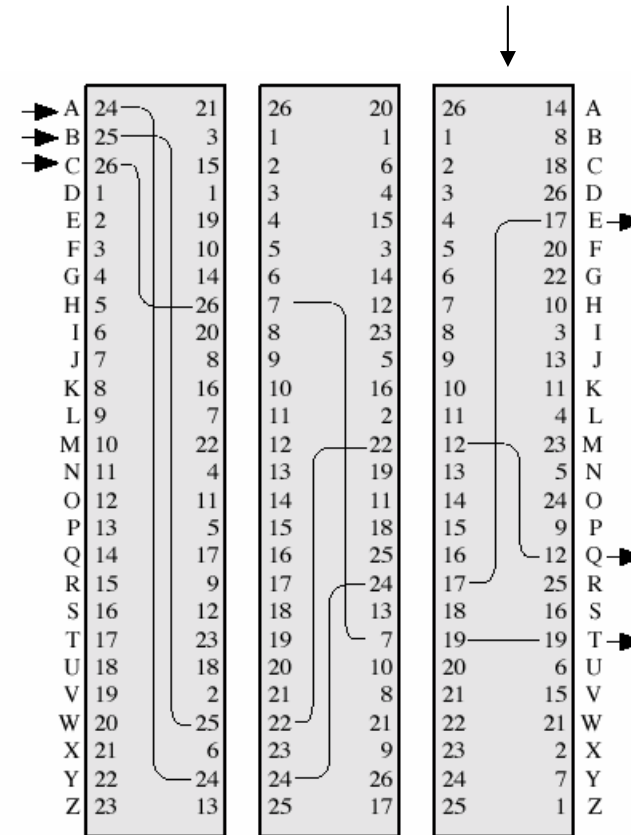
¿Preguntas?

Producto. Rotor

- Varias etapas de sustitución



Situación inicial

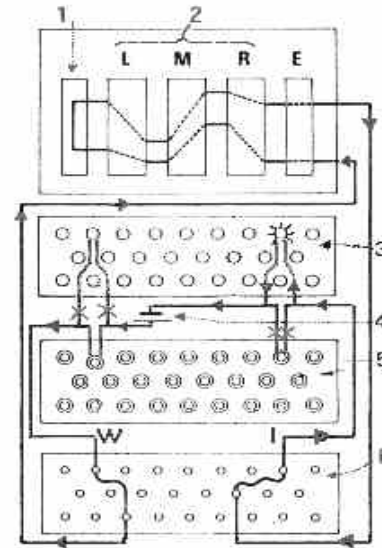


Situación tras cifrar un símbolo

- Cada **rotor** = alfabeto de **sustitución**
- Cifrado depende de estado inicial

3 cilindros: $26^3=17576$ alfabetos

Ejemplo de rotor



Enigma



Producto. Cifrador ADFGVX

- Usado en 1ª Guerra Mundial

bilateral substitution array

| | | | | | | |
|---|---|---|---|---|---|---|
| | A | D | F | G | V | X |
| A | C | O | 8 | X | F | 4 |
| D | M | K | 3 | A | Z | 9 |
| F | N | W | L | 0 | J | D |
| G | 5 | S | I | Y | H | U |
| V | P | 1 | V | B | 6 | R |
| X | E | Q | 7 | T | 2 | G |

intermediate ciphertext:

```
W E   A R E   D I S C O V E R E D
FD XA  DG VX XA  FX GF GD AA AD VF XA VXXA FX

S A V E   Y O U R S E L F
GD DG VF XA  GG AD GX VX GD XA FF AV
```

transposition matrix

| | | | | | |
|---|---|---|---|---|---|
| A | U | T | H | O | R |
| 1 | 6 | 5 | 2 | 3 | 4 |
| F | D | X | A | D | G |
| V | X | X | A | F | X |
| G | F | G | D | A | A |
| A | D | V | F | X | A |
| V | X | X | A | F | X |
| G | D | D | G | V | F |
| X | A | G | G | A | D |
| G | X | V | X | G | D |
| X | A | F | F | A | V |

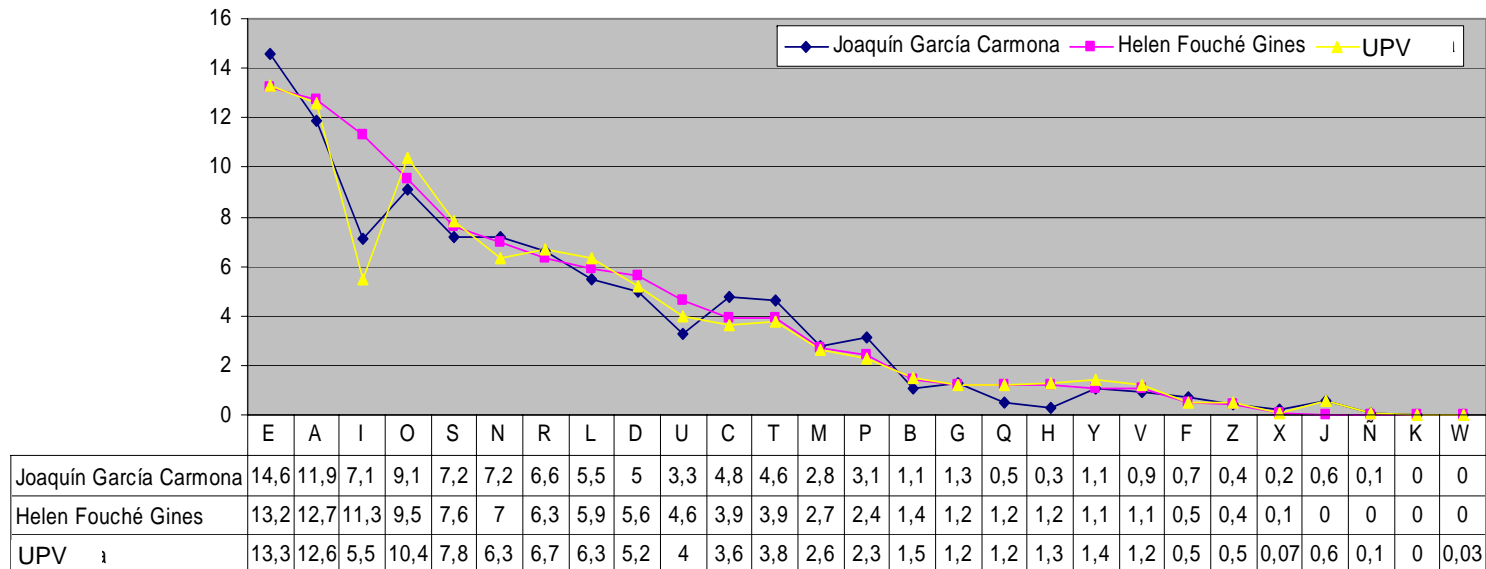
ciphertext:

```
FVGA V  GXGXA  ADFAG  GXFDF
AXFVA  GAGXA  AXFDD  VXXGV
XDGVF  DXFDX  DAXA
```

©1994 Encyclopaedia Britannica, Inc.



Frecuencias de las letras en español (cont.)



- 10 primeros bigramas:
 - OS, ES, EL, EN, DE, LA, AS, AN, ER, UE
- 10 primeros trigramas:
 - QUE, LOS, DEL, ENT, ELA, NTE, ODE, CON, SDE, IEN

Frecuencias de palabras en español

Palabras más frecuentes

| Palabra | Frec (por 10000) |
|----------------|-----------------------------|
| DE | 778 |
| LA | 460 |
| EL | 339 |
| EN | 302 |
| QUE | 289 |
| Y | 226 |
| A | 213 |
| LOS | 196 |
| DEL | 156 |
| SE | 119 |
| LAS | 114 |

Palabras de dos letras

| Palabra | Frec (por 10000) |
|----------------|-----------------------------|
| DE | 778 |
| LA | 460 |
| EL | 339 |
| EN | 302 |
| SE | 119 |
| UN | 98 |
| NO | 74 |
| SU | 64 |
| AL | 63 |
| ES | 47 |

Palabras de tres letras

| Palabra | Frec (por 10000) |
|----------------|-----------------------------|
| QUE | 289 |
| LOS | 196 |
| DEL | 156 |
| LAS | 114 |
| POR | 110 |
| CON | 82 |
| UNA | 78 |
| MAS | 36 |
| SUS | 27 |
| HAN | 19 |

Palabras de cuatro letras

| Palabra | Frec (por 10000) |
|----------------|-----------------------------|
| PARA | 67 |
| COMO | 36 |
| AYER(*) | 25 |
| ESTE | 23 |
| PERO | 18 |
| ESTA | 17 |
| AÑOS(*) | 14 |
| TODO | 11 |
| SIDO | 11 |
| SOLO | 10 |

