



# Introducción a la criptografía

# Elementos de la Seguridad Informática

- Confidencialidad:

- El acceso a la información se permite únicamente a entidades autorizadas

mantener el mensaje secreto

- Disponibilidad:

- La información ha de estar siempre accesible para entidades autorizadas

mantener el servicio funcional

- Integridad:

- La información puede ser creada o modificada únicamente por entidades autorizadas

mantener el mensaje intacto

- Autenticidad:

- No hay duda del origen de la información

evitar la suplantación de identidad

# Criptosistema Clásicos

# Escítal espartana

- Descrita por Plutarco (Grecia, siglos I-II d. C.)
- Consiste en dos varas idénticas: una para el emisor y otra para el receptor
- Para escribir el mensaje, se enrollaba alrededor de la vara una tira larga y se escribía de arriba abajo y de derecha a izquierda
- Para descifrar el mensaje, se enrolla el papiro sobre una vara idéntica
- El primer ejemplo de escritura secreta del que se tiene constancia es del siglo V a. C. (Guerra entre Atenas y Esparta)
- Cifrado por transposición

# Escítal espartana



# Cifrado d Polybios

- Del siglo II a. C., es el cifrador por sustitución más antiguo que se conoce.

- El texto cifrado duplica en tamaño al texto en claro:  
no es un buen sistema

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

$M_1 = \text{QUE BUENA IDEA}$

$C_1 = \text{DA DE AE AB DE AE}$   
 $\text{CC AA BD AD AE EA}$

|   | 1 | 2 | 3 | 4  | 5 |
|---|---|---|---|----|---|
| 1 | A | B | C | D  | E |
| 2 | F | G | H | IJ | K |
| 3 | L | M | N | O  | P |
| 4 | Q | R | S | T  | U |
| 5 | V | W | X | Y  | Z |

$M_2 = \text{LA DEL GRIEGO}$

$C_2 = \text{31 11 14 15 31 22}$   
 $\text{42 24 15 22 34}$

# Cifrado de Julio César

- El historiador romano Suetonio, contemporáneo de Plutarco, nos describe un sistema de **cifrado** utilizado por **Julio César** (siglo I a.C.):
  - “...Para quienes deseen saber más diré que sustituía la primera letra del alfabeto, A, por D y así sucesivamente con todas las demás...”.
- También el emperador Augusto parece que utilizaba un sistema muy similar:
  - “...cada vez que escribía en código, ponía una B en lugar de A, C en lugar de B y así sucesivamente con todas las letras restantes...”.
- El sistema de cifrado de César o de Augusto se basa en la sustitución de letras.

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | K | L | M | N | O | P | Q | R | S | T | V | X |
| D | E | F | G | H | I | K | L | M | N | O | P | Q | R | S | T | V | X | A | B | C |

# Cifrado de Julio César

- La frase que pronunció en una expedición militar cuando tras bajarse de una barca cayó de bruces

TENEO TE AFRICA

en lenguaje cifrado se escribe como:

AHQHR AH DIVMFD

- Para descifrar un mensaje en clave bastaba con girar, para cada letra, el círculo cifrario tres posiciones en el sentido contrario al de las agujas del reloj. Así

BOHM BMGM BMFM

significa

VENI VIDI VICI

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | K | L | M | N | O | P | Q | R | S | T | V | X |
| D | E | F | G | H | I | K | L | M | N | O | P | Q | R | S | T | V | X | A | B | C |



# Cifrado de Julio César

- Es un cifrador por sustitución en el que las operaciones se realizan módulo  $n$ , con  $n$  siendo el número de elementos del alfabeto.

$m = \text{EL PATIO DE MI CASA ES PARTICULAR}$   
          ↓                                 ↓                                 ↓  
 $c = \text{HÑ SDWLR DH OL FDVD HV SDUWLFXÑDU}$

*Cada letra se cifrará siempre igual: es una debilidad*

|       |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|-------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $m_i$ | 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 |
| $c_i$ | 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 |

# Atbas hebreo

- Se escriben las letras del alfabeto en 2 líneas
- La primera mitad en la primera línea de izquierda a derecha
- La segunda mitad en la segunda línea de derecha a izquierda
- Cada letra se sustituye por la situada en la otra línea:

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

# La cifra de Felipe II

- En España, como en el resto de Europa, el uso de información cifrada era generalizado en el ámbito diplomático y militar.
- Merece especial mención la cifra, utilizada por Felipe II (siglo XVI) en la correspondencia con el Duque de Alba en las importantes misiones exteriores de éste.
- Se compone de seis tablas divididas en cuatro grupos de casillas en los que aparecen las letras del alfabeto, las parejas y los tríos de letras más comunes y las palabras que se supone se van a utilizar con más frecuencia.
- A cada casilla corresponde uno o más signos no convencionales formados por letras, números o trazos especiales.

# La cifra de Felipe II

INTRODUCCION E HISTORIA

|    |    |    |    |    |   |   |    |    |    |    |    |
|----|----|----|----|----|---|---|----|----|----|----|----|
| a  | b  | c  | d  | e  | f | g | h  | i  | l  | m  | n  |
| o  | p  | q  | r  | s  | t | u | x  | y  | z  |    |    |
| ba | be | bi | bo | bu |   |   | ca | ce | ci | co | cu |
| da | de | di | do | du |   |   | fa | fe | fi | fo | fu |
| ga | ge | gi | go | gu |   |   | ha | he | hi | ho | hu |
| ja | je | ji | jo | ju |   |   | la | le | li | lo | lu |

CIFRA USADA POR FELIPE II (S. XVI) (1/6)

INTRODUCCION E HISTORIA

|    |    |    |    |    |  |     |     |     |     |     |
|----|----|----|----|----|--|-----|-----|-----|-----|-----|
| ma | me | mi | mo | mu |  | na  | ne  | ni  | no  | nu  |
| pa | pe | pi | po | pu |  | qua | que | qui | quo | quu |
| ra | re | ri | ro | ru |  | sa  | se  | si  | so  | su  |
| ta | te | ti | to | tu |  | xa  | xe  | xi  | xo  | xu  |
| ya | ye | yi | yo | yu |  | za  | ze  | zi  | zo  | zu  |
| ba | be | bi | bo | bu |  | bra | bre | bri | bro | bru |
| ca | ce | ci | co | cu |  | cha | che | chi | cho | chu |

CIFRA USADA POR FELIPE II (S. XVI) (2/6)

# La cifra de Felipe II

INTRODUCCION E HISTORIA

|         |     |         |     |         |     |         |     |     |     |                |
|---------|-----|---------|-----|---------|-----|---------|-----|-----|-----|----------------|
| era     | ere | eri     | ero | eru     |     | dra     | dre | dri | dio | dru            |
| É       | E   | Ē       | F   | R       |     | Ĝ       | g   | ĝ   | g   | g <sup>e</sup> |
| fla     | fle | fli     | flo | flu     |     | fra     | fre | fri | fro | fru            |
| h'      | h   | h       | h   | he      |     | h       | h   | h   | h   | he             |
| gla     | gle | gli     | glo | glu     |     | gra     | gre | gri | gro | gru            |
| p'      | p   | p       | p   | pe      |     | p       | p   | p   | p   | p              |
| pla     | plo | pri     | plo | plu     |     | pro     | pro | pri | pro | pru            |
| q'      | q   | q       | q   | qe      |     | q       | q   | q   | q   | q              |
| tra     | tre | tri     | tro | tru     |     |         |     |     |     |                |
| R       | R   | R       | R   | R       |     |         |     |     |     |                |
| - A -   |     |         |     |         |     |         |     |     |     |                |
| Almanax | er  | Almanax | mo  | Almanax | lia | Almanax | ri  |     |     |                |
| Almanax | er  | Almanax | qui | - B -   |     | Almanax | um  |     |     |                |
| Almanax | er  | Almanax | qui | Almanax | qui | Almanax | er  |     |     |                |
| Almanax | er  | Almanax | qui | Almanax | qui | Almanax | er  |     |     |                |
| Almanax | er  | Almanax | qui | Almanax | qui | Almanax | er  |     |     |                |
| Almanax | er  | Almanax | qui | Almanax | qui | Almanax | er  |     |     |                |

CIFRA USADA POR FELIPE II (S. XVI) (3/6)

INTRODUCCION E HISTORIA

|            |      |             |     |           |      |            |    |
|------------|------|-------------|-----|-----------|------|------------|----|
| - C -      |      | - D -       |     | Lorenz    | not  | Francis    | 22 |
| Consejo    | ui   | Dios        | ion | Orque de  | test | Francis    | 23 |
| Catholico  | us   | Orque       | gi  | Orque de  | test | Francis    | 24 |
| Cardinal   | aut  | Orquesa     | tur | Orque de  | test | - C -      |    |
| Chenilles  | sla  | Origno      | ne  | Vandoux   | test | Gente      | 25 |
| Chailles   | bi   | Orpacho     | que | - E -     |      | Gente      | 26 |
| Conde      | lus  | Orine       | sol | Emperador | not  | Gobernador | 28 |
| Christian  | es   | Origenes    | sum | Esperanza | ubi  | General    | 27 |
| Christiano | le   | Orque de la | not | Esperanza | am   | Gente      | 29 |
| Campo      | vi   | Orque de la | sus | Embaxador | or   | Gente      | 30 |
| Campo      | que  | Orque de la | sus | Embaxador | not  | Gente      | 31 |
| Council    | lit  | Orque de la | neg | Embaxador | in   | Gente      | 32 |
| Capitay    | quon | Orque de la | neg | Embaxador | est  | Gente      | 33 |
| Cavallos   | il   | Orque de la | su  | Embaxador | et   | Gente      | 34 |
| Cavallos   | lud  | Orque de la | su  | Embaxador | et   | Gente      | 35 |
| Cavos      | q    | Orque de la | ore | Embaxador | et   | Gente      | 36 |
| Cavos      | am   | Orque de la | ore | Embaxador | et   | Gente      | 37 |
| Cavos      | ci   | Orque de la | ore | Embaxador | et   | Gente      | 38 |
| Cavos      | lia  | Orque de la | ore | Embaxador | et   | Gente      | 39 |
| Cavos      | ed   | Orque de la | ore | Embaxador | et   | Gente      | 40 |

CIFRA USADA POR FELIPE II (S. XVI) (4/6)

# La cifra de Felipe II

## INTRODUCCION E HISTORIA

|             |    |           |     |           |            |    |
|-------------|----|-----------|-----|-----------|------------|----|
| Italia      | 59 | Ministro  | lum | P         | Rey        | 79 |
| Inglaterra  | 60 | Moultan   | id  | Papa      | Reyno      | 81 |
| Ingleses    | 61 | Montigni  | mel | Principe  | Republica  | 82 |
| Infantes    | 62 | Mas       | la  | Principe  | Remedio    | 83 |
| Infancia    | 63 | Menos     | oct | Principe  | Respetado  | 84 |
| Inglaterra  | 64 | N         |     | Principe  | Resolucion | 85 |
| Indulgencia | 65 | Negocio   | 51  | Porque    | Reverencia | 86 |
| Importancia | 66 | Necesidad | 52  | Pera      | Reyna      | 87 |
| I           |    | Nenio     | 53  | Parque    | S          |    |
| Lussemburg  | 67 | Nuncio    | 54  | Pas       | Su Magd    | 87 |
| Lugares     | 68 | Nuncio    | 55  | Punto     | Su Maest   | 88 |
| Liga        | 69 | Nuncio    | 56  | Q         | Su Exe     | 89 |
| Libertad    | 70 | Nuncio    | 57  | Quanto    | Sonoya     | 90 |
| Lorena      | 71 | O         |     | Quanto    | Suget      | 91 |
| Licencia    | 72 | Obispo    | 58  | Qualidad  | Suyos      | 92 |
| Luzo        | 73 | Obispo    | 59  | Quantidad | Sin V      | 93 |
| M           |    | Obispo    | 60  | Qual      | Servicio   | 94 |
| Memoranda   | 74 | Officio   | 61  | Quon      | Servicio   | 95 |
| Mengue      | 75 | Obispo    | 62  | R         | Serone     | 96 |

CIFRA USADA POR FELIPE II (S. XVII) (5/6)

## INTRODUCCION E HISTORIA

|         |     |         |     |          |     |        |     |
|---------|-----|---------|-----|----------|-----|--------|-----|
| Eneso   | 97  | Oratado | 99  | O. Magd  | cre | Villa  | 101 |
| Siempre | 98  | Oratado | 100 | O. Maest | cri | Vivros | 102 |
| T       |     | Oratado | 101 | O. Maest | cro | Vivros | 103 |
| Orato   | 99  | Oratado | 102 | O. Maest | cro | Vivros | 104 |
| Vieno   | 100 | Oratado | 103 | O. Maest | cro | Vivros | 105 |
| Vieno   | 101 | Oratado | 104 | O. Maest | cro | Vivros | 106 |

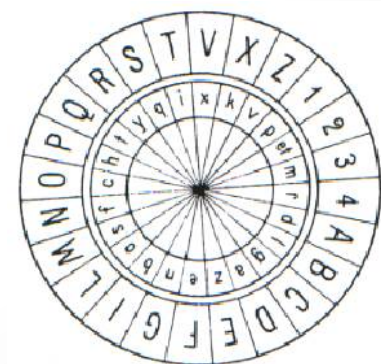
En las segundas, todas las letras, dictiones o numeros despues de los quales se sigue una S entre dos puntos y todo el renglon que comienza en una N entre dos puntos, o parte del fin de la letra una +.

CIFRA USADA POR FELIPE II (S. XVII) (6/6)



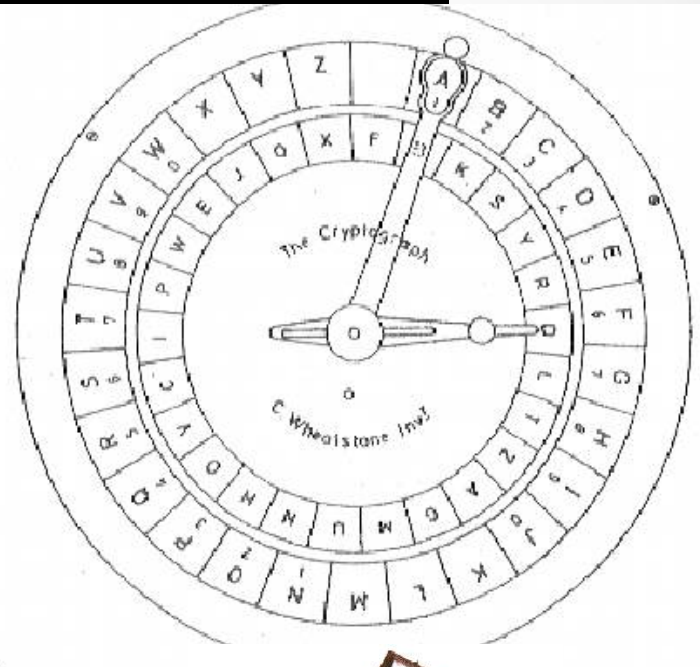
# El cifrado de Alberti

- En los siglos XVI y XVII se utiliza muy activamente la Criptología, pero no hay grandes progresos en la aparición de nuevos métodos, todos están basados en la sustitución.
- Leon Battista Alberti diseña en el siglo XVI un disco para cifrar en el que ya no hay una correspondencia única entre el carácter del texto en claro a cifrar y el criptograma obtenido.
- Como este tipo de cifradores hacía uso de más de un alfabeto, se les conoce como polialfabéticos; en contraste con los anteriores que se denominan monoalfabéticos.
- En este caso, se hace uso ya de una clave secreta al ajustar en una posición los discos antes de cifrar



# Cifradores del siglo XIX

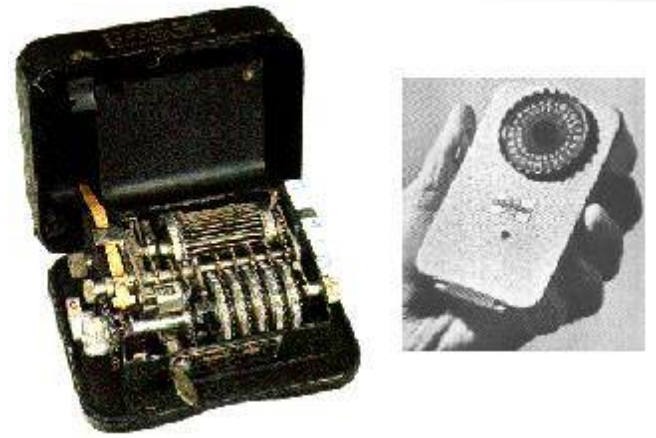
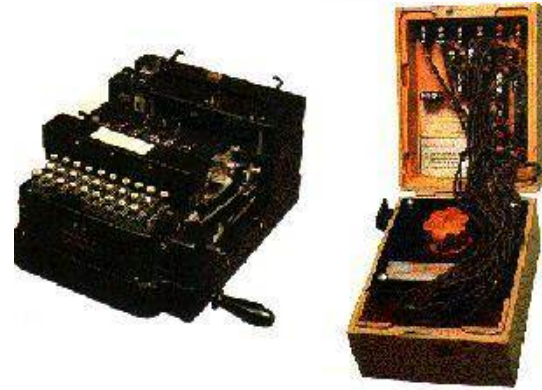
- En el siglo XIX aparece una nueva técnica (ya utilizada en cierto modo por los griegos) consistente en la alteración del orden de los símbolos del mensaje. Esta técnica es combinada con la sustitución.
- Se utilizan máquinas de cifrar, como las de *Wheatstone* y *Brazeries*.





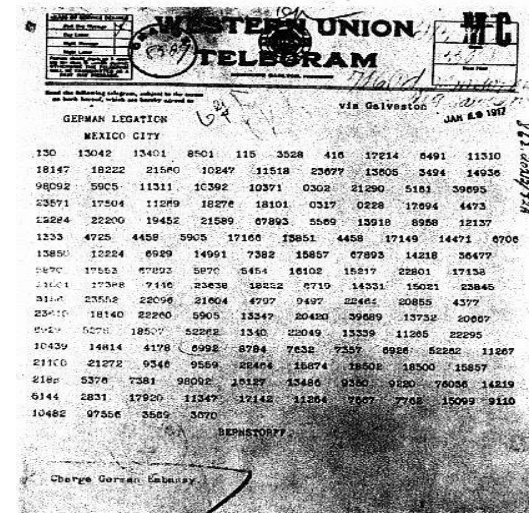
# Siglo XX: antes del ordenador

- El empujón decisivo para la criptología se produce en el siglo pasado con motivo de las Guerras Mundiales.
- Se desarrollan diversas máquinas de cifrado con rotores que permiten un cifrado polialfabético.
- De estas máquinas, cuyo papel principal fue su utilización para enviar mensajes cifrados precisamente en la Segunda Guerra Mundial, destacan tanto por sus características como por el halo de misterio que rodeaba a dos de ellas:
  - la máquina Enigma y la de Hagelin.



# Siglo XX: antes del ordenador

- Durante la Primera Guerra Mundial los ingleses consiguieron averiguar el método de cifrado del telegrama **Zimmerman**.
  - Utilizado por los alemanes, usaba un código para asignar cifras a las palabras de acuerdo con un libro de claves que poseían el emisor y el receptor del mensaje.
- Los franceses desmantelaron otro método utilizado por los alemanes, el sistema **ADFGX**.
  - Usaba tan solo esas letras para sustituir cada letra del mensaje sin cifrar por una combinación de dos de esas cinco letras, realizando posteriormente una transposición de longitud 20. La sustitución se hacía con la tabla



|   | A | D | F | G | X |
|---|---|---|---|---|---|
| A | n | b | x | r | u |
| D | q | o | k | d | v |
| F | a | h | s | g | f |
| G | m | z | c | l | t |
| X | e | i | p | j | w |

# Siglo XX: antes del ordenador

ADFGX

El mensaje

*PETAİN MONTAG ATTENTAT*

(Petain Lunes Atentado)

una vez hecha la sustitución, quedaría como

*AFXAGXFAXDAA GGAXAAGX / FAFG FAGXGXXAAAGXFAGX*

y realizando la transposición

*AFXAGXFAGGFXAFGAXXGDXAXAAGAGAAGXXAFAAGGXX*

# Siglo XX: después del ordenador

- Aparecen los ordenadores:
  - los métodos de cifrado anteriores resultan sumamente vulnerables por la capacidad de cálculo de los mismos.
- Los criterios utilizados para cifrar mensajes:
  - se establecen pensando en el posible ataque al sistema mediante un ordenador.
- Se habla así de sistemas:
  - computacionalmente seguros
  - computacionalmente inseguros

# Visión histórica

- La criptografía clásica abarca desde tiempos inmemoriales hasta la mitad del siglo XX.
- El punto de inflexión en esta clasificación la marcan tres hechos relevantes:
  - En el año 1948 se publica el estudio de C. Shannon sobre la Teoría de la Información.
  - En 1974 aparece el estándar de cifrado DES.
  - En el año 1976 se publica el estudio realizado por W. Diffie y M. Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifra, denominado cifrado con clave pública.

# Terminología

- Cifrar / Descifrar

*(no se **usaba** encriptar, pero ahora lo admite la RAE, desencriptar no está aceptado)*

- Texto en claro /  
Texto cifrado (o criptograma)

*el texto en claro se cifra para obteniendo texto cifrado y viceversa*

- Criptosistema / Cifrador

*todo algoritmo de cifrado es un criptosistema, también hay otras primitivas criptográficas (herramientas útiles en criptografía) que no son cifradores*

- Clave / Espacio de claves

*La clave es la entrada que determina la transformación realizada por un criptosistema, una contraseña es una entrada del usuario (que generalmente se transforma en una clave).*

*El espacio de claves es el número de claves posibles y determina la dificultad inicial de romper el criptosistema por fuerza bruta (búsqueda exhaustiva)*

- Criptología / Criptografía /  
Criptoanálisis

*La criptografía estudia el diseño de criptosistemas y el cifrado de mensajes; el criptoanálisis estudia como romper criptosistemas y obtener los mensajes cifrados sin conocer la clave; la criptología es la ciencia que combina el estudio de ambas.*

# Primitivas criptográficas

Disponemos de las siguientes primitivas o herramientas que estudiaremos a lo largo del curso:

- Criptografía simétrica (clave privada):
  - Cifrado en flujo
  - Cifrado en bloque
- Criptografía asimétrica (clave pública):
  - Cifrado
  - Firma digital
- Primitivas auxiliares:
  - PRNG (pseudoaleatoriedad)
  - Funciones Hash (resumen)
  - Funciones MAC (autenticación)
  - PBKDF (contraseñas)

# Ampliación

## Otros materiales

- Se puede consultar el capítulo 9 del libro de Lucena (en los materiales de UACloud)

## Cuestiones

- ¿Serían seguros los esquemas de criptografía clásica en la actualidad? ¿Por qué?
- ¿Cuáles son las principales diferencias entre los algoritmos clásicos y los modernos basados en computación?