Introducción a la Criptografía

Criptografía clásica

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
KISA

Criptografía clásica

- Algunos autores consideran que la Criptografía comienza con la escritura ideográfica y jeroglífica.

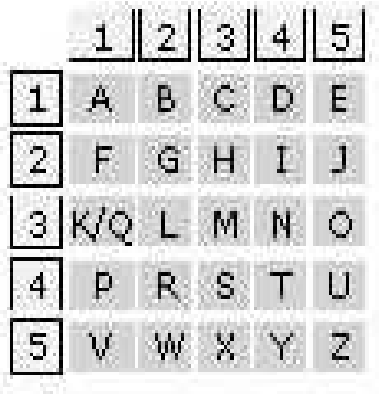
- Esteganografía: ocultación de un mensaje secreto dentro de otro inteligible.

Nota: Las imágenes de esta sección están obtenidas de Wikipedia.

- Siglo V a.C. Escitalo de los Lacedemonios. Cilindro de madera más cinta enrollada sobre la que se escribe. Se trata de una *transposición*.

Técnica de transposición: consiste en cambiar la posición de los caracteres del mensaje.

- Siglo II a. C. Polybios. Disposición del alfabeto en matriz 5×5. *Sustitución* de la letra a_{ij} por los números i j.



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

Mensaje en claro: METODO DE SUSTITUCION
Mensaje cifrado: 331544351435 1415 . . .

Mensaje cifrado: 4135325412243543
Mensaje en claro: POLYBIOS

Técnica de sustitución: consiste en sustituir cada carácter del mensaje por otro diferente.

- Cifrado de César (emperador romano 100-44 a.C.): *sustitución* de cada letra de un texto por otra situada tres posiciones más adelante en el abecedario.

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	

$$A \mapsto D,\ B \mapsto E,\ \ldots,\ W \mapsto Z,\ X \mapsto A,\ Y \mapsto B,\ Z \mapsto C.$$

Mensaje en claro: PRIMERA PRUEBA
Mensaje cifrado: SULOHUD SUXHED

Mensaje cifrado: B ÑD VLJXLHPWH
Mensaje en claro: Y LA SIGUIENTE

Este método permitió eliminar el aparato cifrador.

- Los árabes (1300), contribución significativa a la Criptografía:
  - Reemplazo de unas letras por otras (*sustitución*).
  - Escritura de palabras al revés (*transposición*).
  - Correlación con valores numéricos: dar a las letras un valor numérico.
  - Sustitución digrámica: asignar a cada letra un número y sustituir cada letra por dos, cuyo valor numérico suma el de la primera.
  - Sustitución de una letra por símbolos (utilizan libros de códigos).

- Disco de Alberti (1466). Modificación del cifrado de César utilizando discos concéntricos.

Permite multiplicidad de claves (tantas como ajustes posibles de los discos).

En 1593, De la Porta modificó el disco de Alberti cambiando uno de los dos alfabetos por una serie de símbolos.

- 1595, Cifrado de Vigenère: asigna a cada letra del alfabeto un valor entero y suma una palabra clave al mensaje, módulo el número de letras del alfabeto.

Alfabeto: $N = 27$. Clave: SOL

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
14	15	16	17	18	19	20	21	22	23	24	25	26	

Cifrado:

E	S	T	A	E	S	L	A	C	L	A	V	E
4	19	20	0	4	19	11	0	2	11	0	22	4
S	O	L	S	O	L	S	O	L	S	O	L	S
19	15	11	19	15	11	19	15	11	19	15	11	19
23	7	4	19	19	3	3	15	13	3	15	6	23
W	H	E	S	S	D	D	O	N	D	O	G	W

- Aumento del periodo: si volvemos a cifrar con otra palabra, el resultado es equivalente a cifrar con una clave de longitud el mínimo común múltiplo de las longitudes de las palabras usadas.

Por ejemplo, ciframos primero con la clave SOL y a continuación con la clave CABO. El resultado es el mismo que si cifráramos con una palabra clave de longitud 12.

E	S	T	A	E	S	L	A	C	L	A	V	E
4	19	20	0	4	19	11	0	2	11	0	22	4
S	O	L	S	O	L	S	O	L	S	O	L	S
19	15	11	19	15	11	19	15	11	19	15	11	19
23	7	4	19	19	3	3	15	13	3	15	6	23
W	H	E	S	S	D	D	O	N	D	O	G	W
C	A	B	O	C	A	B	O	C	A	B	O	C
2	0	1	15	2	0	1	15	2	0	1	15	2
25	7	5	7	21	3	4	3	15	3	16	21	25
Y	H	F	H	U	D	E	D	O	D	P	U	Y

- Cifrado encadenado: actual CFB *(Cipher FeedBack)*. Se cifra el primer bloque del mensaje en claro con la palabra clave y cada uno de los bloques siguientes se cifra utilizando como clave el resultado del cifrado del bloque anterior.

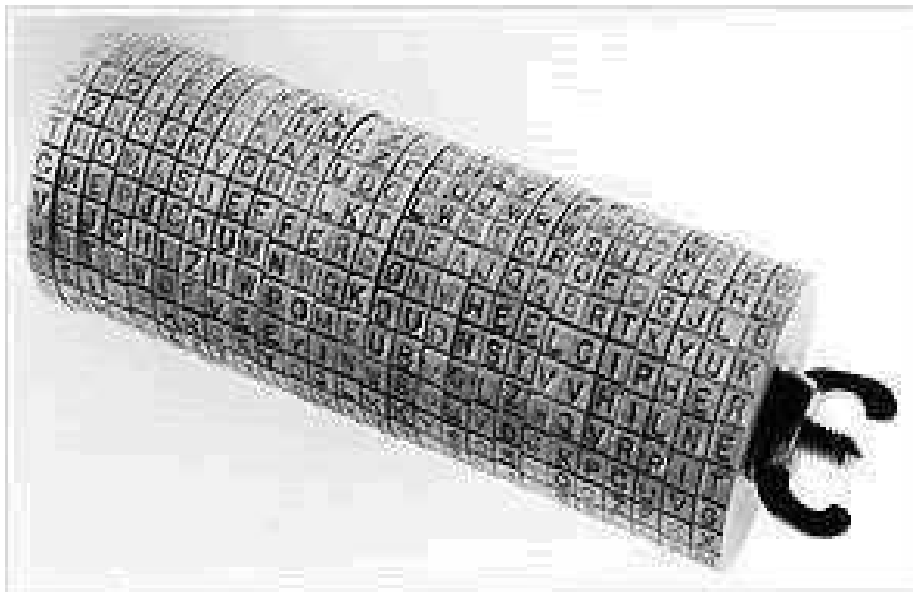
E	S	T	A	E	S	L	A	C	L	A	V	E
4	19	20	0	4	19	11	0	2	11	0	22	4
S	O	L	W	H	E	W	L	W	H	L	Y	R
19	15	11	23	7	4	23	11	23	7	11	25	18
23	7	4	23	11	23	7	11	25	18	11	20	22
W	H	E	W	L	W	H	L	Y	R	L	T	V

El trabajo de Vigènere contiene numerosas ideas que han sido posteriormente desarrolladas y están vigentes en la Criptografía actual.

- Cilindro de Jefferson, 1790. Similar al disco de Alberti, pero utilizando una serie de 26 cilindros concéntricos.

  El mensaje se escribe a lo largo de una de las generatrices del cilindro ajustando los discos en la posición deseada.

  La lectura a lo largo de otra generatriz es el criptograma.



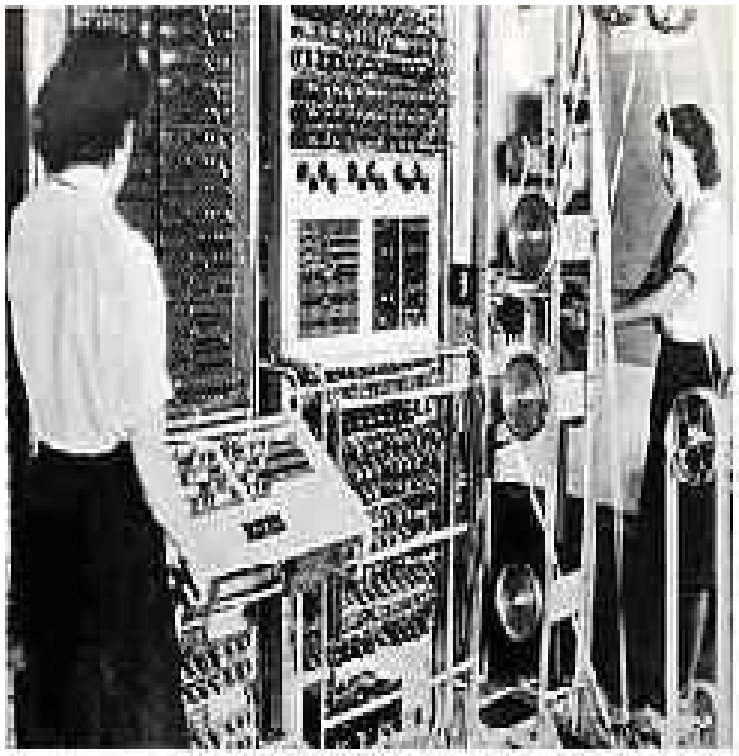
- 1854. Wheatstone diseña el cifrado de Playfair que consiste en una sustitución digrámica donde un par de letras del texto en claro se convierten en otro par distinto. Se escribe el alfabeto en una matriz cuadrada y cada pareja de letras se sustituye por otra siguiendo unas ciertas reglas.
- En 1863, un oficial del ejército prusiano (F. W. Kasiski) descubrió un criptoanálisis capaz de violar el cifrado de Vigenère si el texto que se va a cifrar es mayor que la longitud de la clave.
- 1867. Otra aportación de Wheatstone a la criptografía fue la mecanización del disco de Alberti.

- 1919. Vernam (ingeniero de los laboratorios Bell y de AT&T) descubrió que para que el cifrado de Vigenère fuera seguro la clave debía ser más larga que el mensaje y ser usada una sola vez ("one time pad "). Con estas dos condiciones se consigue un cifrado perfecto, como lo probó Shanon (Teoría de las Comunicaciones Secretas, 1949).
  Es prácticamente imposible de implementar.

- 1921. Hagelin diseña una máquina de cifrado basada en el cilindro de Jefferson. En 1935 se mecaniza. Dio lugar a la máquina ENIGMA, utilizada en la segunda guerra mundial.

- ENIGMA fué criptoanalizada por el ordenador Colossus (1943-1945). Este criptoanálisis se mantuvo secreto hasta 1972.

Enigma



Colossus

- 1976. La Oficina de estándares de Estados Unidos acepta el algoritmo DES (*Data Encrytion Standard*) para el cifrado de la información estatal no confidencial. Nace la Criptografía moderna.
- 1977. Aparece la criptografía de clave pública.

Fin de la sección