CRIPTOLOGÍA

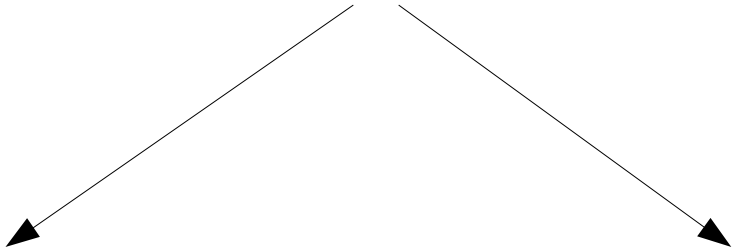
¿Cómo volvernos locos con tantos códigos ?

Carole Percier – Lycée Français Molière
caromathiques.moliere@gmail.com

-Taller de Talento Matemático-
9 de Marzo de 2012

CRIPTOLOGÍA

« la ciencia del secreto »



Criptografía
proteger mensajes

Criptoanálisis
descubrir mensajes

Descifrar

Cifrado por transposición

Cifrado por sustitución

Clave

Criptograma

Criptografía simétrica

Cifrado

Ataque

I. La ciencia del secreto atraviesa la historia

II. Criptología sencilla

III. Criptología más compleja

IV. Salidas profesionales

La ciencia del secreto atraviesa la historia

- **Técnica griega (X – VII a.C)**

  técnica de cifrado por transposición

- **Técnica hebraica (V a.C)**

  el método Atbash : sustitución alfabética inversa

- **Nabuchodonosor, rey de Babilonia (600 a.C)**

  escondía mensajes con sus esclavos

- **A partir de -200**

  aparición de verdaderas claves

- **Gabriele de Lavinde (1379)**

  recopilación de códigos y claves

- **Blaise de Vigenère (1586)**

  cifrado por sustitución polialfabética

- **Primera Guerra Mundial (1914 – 1918)**

  Segunda Guerra Mundial (1939 – 1945)

  Siglo XX

guerras & criptología...

Enigma

...victorias & tecnología

La bomba

Lorenz

Colossus

Criptología sencilla

- **Sustitución simple**

  cada letra del mensaje está sustituida por otra, igual durante todo el cifrado

- **Ataques**

  con un texto bastante largo: observación de las frecuencias de las letras y de las repeticiones

LA CIFRA DE CÉSAR

- **Método :** Cada letra se desplaza de un número fijo en el alfabeto → permutaciones circulares

- **Clave :** *n*, el valor del desplazamiento

  (César funcionaba con $n = 3$).

	A	B	C	D	E	F	G	H	I	J	K	L
n=3	D	E	F	G	H	I	J	K	L	M	N	O
n=10	K	L	M	N	O	P	Q	R	S	T	U	V
n=24	Y	Z	A	B	C	D	E	F	G	H	I	J

	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
n=3	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
n=10	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
n=24	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

EL CUADRADO DE POLYBE

- **Método :** cada letra está sustituida por sus coordenadas en un cuadrado de 5x5

- **Clave :** una palabra que inicia el relleno del cuadrado

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

Clave :
MATES

LA CIFRA DE LOS REPUBLICANOS

- **Método :** similar al de Polybe, pero la tabla es distinta : 3x9

- **Clave :** una palabra que inicia el relleno de la tabla

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

Clave :
VALIENTE

1 y 2 :

→ asociados a números de dos cifras

→ descifrado facilitado

CIFRADO AFÍN

- **Método :**

  1. cifrar cada letra por un número x (entre 0 y 25)

  2. calcular el resto de $(ax+b):26$ → valor y

  3. sustituir y por la letra que le corresponde en el alfabeto

- **Clave :** $(a;b)$

	A	B	C	D	E	F	G	H	I	J	K	L	M
x	0	1	2	3	4	5	6	7	8	9	10	11	12
ax+b		10			19					34			
y		10			19					8			
cifrado		K			T					I			

(a;b)=(3;7)

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
x	13	14	15	16	17	18	19	20	21	22	23	24	25
ax+b			52								76		
y			0								24		
cifrado			A								Y		

CIFRADO ALEATORIO

- **Método :** cifrar cada letra de manera aleatoria
- **Clave :** no tiene !
- **Ventaja :** se pueden crear muchísimos códigos !

Criptología más compleja

- **Sustitución polialfabética**

  cada letra de un mismo mensaje, cifrado con una misma clave, está cifrada por distintas letras

- **Ataques**

  análisis frecuencial casi imposible !

LA CIFRA DE VIGENÈRE

- **Método :** basado en la cifra de César, pero con desfases que cambian en función de la posición de la letra en el mensaje

- **Clave :** una palabra

Letra inicial

Letra de la clave

	A	B	C	D	E
A	A	B	C	D	E
B	B	C	D	E	F
C	C	D	E	F	G
D	D	E	F	G	H
E	E	F	G	H	I

Letra cifrada

Cifrado de la palabra MATEMATICAS con la clave TALENTO :

M	A	T	E	M	A	T	I	C	A	S
T	*A*	*L*	*E*	*N*	*T*	*O*	*T*	*A*	*L*	*E*
F	A	E	I	Z	T	H	W	C	L	W

Salidas profesionales

- **Sectores**

  defensa, informática, telecomunicaciones, redes, protección de documentos multimedia, editores de softwares, tarjetas electrónicas...

- **Puestos**

  ingeniero, investigador, consultor, espía (!!!)