CRIPTOLOGÍA

¿cómo volvernos locos con los códigos ?

Carole Percier

caromathiques@gmail.com

Taller de Talento Matemático

9 de Marzo de 2012

Criptología
"la ciencia del secreto"

Criptografía

Disciplina que consiste en estudiar algóritmos, protocolos y sistemas para **proteger mensajes**

Criptoanalísis

Disciplina que consiste en **atacar los mensajes codificados** para descifrarlos

CRIPTOLOGÍA SENCILLA

Sustitución simple / monoalfabética : cada letra está cifrada por otra, pero esta no cambia en todo el mensaje.
Estos cifrados son "sencillos" de atacar : se puede estudiar la frecuencia de algunas letras, la repetición de otras, etc.

1. La cifra de César

El método está basado en un desfase fijo de las letras del alfabeto. Consiste en sustituir cada letra por otra, distante de una cantidad constante (n) y siguiendo el orden cíclico de las letras. El desfase n es la clave del método (César utilizaba un desfase de 3 letras).
Para descifrar el mensaje, se aplica el mismo algoritmo pero al revés.

Aplicaciones :

1. Con la clave $n=3$, cifrar la palabra TALENTO y descifrar la palabra SLULQHR

2. Descifrar el mensaje FKMKMSYXOC, cifrado con la clave 10.

3. Descifrar el mensaje siguiente : CJ FMLMP NPMFGZC YAAGMLCQ OSC JY JCW RMJCPY (cita de Séneca).

2. El cuadrado de Polybe

El método consiste en sustituir cada letra por sus coordenadas en un cuadrado 5 x 5. Esta técnica fue utilizada para transmitir mensajes a distancia, utilizando varias linternas : unas a la derecha, que indicaban la primera coordenada, y otras a la derecha, que indicaban la segunda coordenada.
En un principio es un cifrado muy sencillo, se puede complicar utilizando una clave : una palabra, que se pone al principio del cuadrado. Las siguientes casillas se rellenan por orden alfabético, sin repetir las de la clave.

Aplicación :
Construir el cuadrado de Polybe con la clave MATES (quitar la letra K), y descifrar este mensaje : 14 34 31 41 11 21 44 14 14 15 45 35 12 35 32 11 12 34 44 12 22 32 41 35 12 34

3. La cifra de los republicanos españoles

Esta técnica de cifrado fue utilizada durante la guerra civil. Su funcionamiento es muy similar al de Polybe. Se colocan en una tabla de 10 columnas y 3 filas las letras del alfabeto por orden (empezando por la clave). Para evitar confusiones, en la primera fila se rellenan solamente 8 casillas. Cada letra estará entonces cifrada por una o dos cifras, según su posición en la tabla.

4. El cifrado afín

Un cifrado afín consiste en cifrar cada letra del alfabeto (x), y a sustituir ese número por el número y, resto de la división de $ax+b$ por 26 (a y b : números enteros naturales, representan la clave del cifrado). Por fín, se sustituye y por la letra que le corresponde en el alfabeto. Este método no permite utilizar muchas claves, es bastante complicado de poner en marcha y no ofrece mucha más seguridad que otros cifrados más sencillos.

Aplicación :

Completar esta tabla, que utiliza como clave (3;7), y cifrar el mensaje “La palabra es el índice del pensamiento”.

	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			

	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		

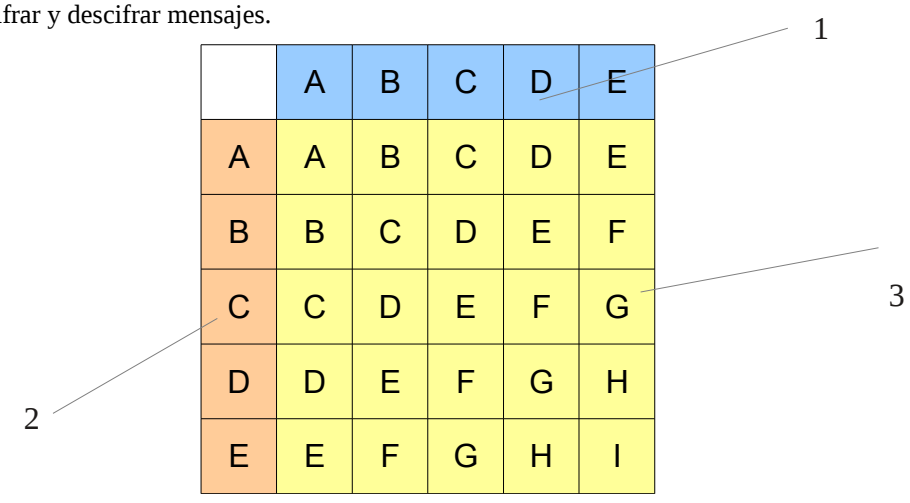
CRIPTOLOGÍA MÁS COMPLEJA

Hasta el siglo XVI, y a pesar de sus debilidades bien reconocidas, el cifrado de César fue el más utilizado : era sencillo, cómodo y bastante seguro. Fue entonces cuando un diplomata francés, Blaise de Vigenère, inició una nueva técnica de cifrado que dominó durante más de tres siglos.

Sustitución polialfabética : Al contrario de los métodos de sustitución simple, esta técnica, mucho más compleja, cifra, en un mismo mensaje, una misma letra por otras distintas, según su posición en el criptosistema. El cifrado de la máquina Enigma era un cifrado polialfabético. Uno de los más famosos es el cifrado de Vigenère.

El cifrado de Vigenère :

El método está basado en el del cifrado de César, pero el desfase de letra cambia siempre. Una tabla, constituida de 28 alfabetos, permite cifrar y descifrar mensajes.



- Se elige una clave (una palabra).
- Se escribe esta clave debajo del mensaje, repitiendola tantas veces como necesario para ir hasta el final del mensaje.
- Para cifrar una letra :
  - buscar en (1) la letra del mensaje
  - buscar en (2) la letra correspondiente de la clave
  - encontrar en (3) la letra cifrada
- Para descifrar una letra :
  - buscar en (2) la letra de la clave
  - buscar en su fila en (3) la letra cifrada
  - encontrar en esa columna en (1) la letra inicial

Ventajas :

Cada letra, en un mismo mensaje, con una única clave, puede ser cifrada por distintas letras. Por tanto, es imposible descifrar un mensaje por análisis frecuencial. Este cifrado es mucho más solido que todos los que se habían utilizado hasta ese momento. Además, a pesar de parecer complicado al principio, es bastante sencillo de utilizar.

SEGURIDAD + SENCILLEZ = EXÍTO !

Aplicaciones :

1. Con la clave COLUCHE, descifrar el mensaje siguiente :

   KRPUASFCPFOBRFCECGUINCBOGOEESQUNAEGGDUDLVWHTFKGETZLM
2. Eligiendo una clave, cifrar un mensaje de 10-12 palabras y pasarlo a otro grupo para que lo descifre.

SALIDAS PROFESIONALES

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

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

Estudios : en Francia, existen varios masters (4º y 5º curso universitario), accesibles después de haber cursado 3 años de matemáticas, o después de un título de ingeniero

- Master Professionnel Sécurité de l'Information, Cryptographie, Internet - UNIVERSITÉ DE LIMOGES
- CRYPTIS – UNIVERSITÉ DE LIMOGES

- Mathématiques et Informatique appliqués à la cryptologie - UNIVERSITÉ PARIS DIDEROT
- Cryptologie et protocoles – UNIVERSITÉ PARIS DIDEROT
- Cryptologie et Sécurité Informatique - UNIVERSITÉ DE BORDEAUX
- Mathématiques de l'information, Cryptographie – UNIVERSITÉ DE RENNES
- SeCReTS – UNIVERSITÉ DE VERSAILLES
- ...

Anexo : Tabla de Vigenère

Clé utilisée \ Lettre chiffrée	A	B	C	D	E	F	G	H	I	J	K	L	M	N	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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
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
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	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	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	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	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	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	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	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	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	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	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	O	P	Q	R	S	T	U	V	W	X	Y