

# *VI Jornada de les ciències*

*Dijous 22 de març del 2007*

## *Joc d'espies*



*Taller de matemàtiques*

*Christine Torre*

*Margarita García de Cortázar Nebreda*

*M<sup>a</sup> Pilar Caveró Castillo*

*Joan Antoni Alfaro Pérez*

# Taller ?

## El xifrat Cèsar i el xifrat Vigènere

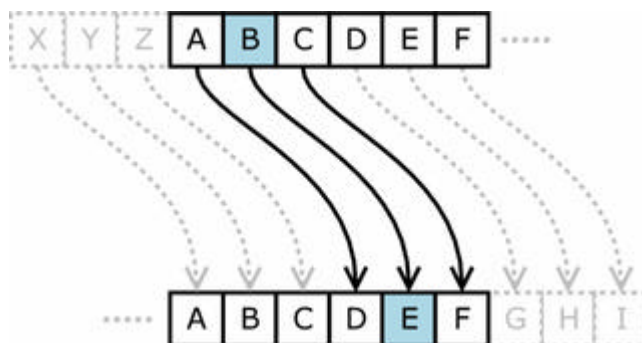
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z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



$$E_n(x) = x + n \pmod{27}.$$

VI Jornada de les ciències  
Dijous 22 de març del 2007  
Taller de matemàtiques; Joc d'espies  
El xifrat Cèsar

També conegut com xifrat per desplaçament, és una de les tècniques més simples i utilitzades. Pertany al grup de xifrat per substitució, és a dir, cada lletra del text original és substituïda per una altra lletra que es troba un nombre determinat de llocs més endavant en l'alfabet. Per exemple, amb un desplaçament de 3, la A seria canviada per la D, la B per la E, etc.



La transformació es pot representar alineant els dos alfabetes. Per exemple, aquest seria el xifrat Cèsar amb un desplaçament envers la dreta de tres espais:

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

Per tal de codificar un missatge només cal buscar cada lletra de la línia del text original i escriure la lletra corresponent en la línia codificada. Per descodificar, cal fer el contrari.

La codificació també es pot representar utilitzant l'aritmètica modular, transformant les lletres en números d'acord amb els següent esquema:

A	B	C	Ç	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

La codificació de la lletra x amb un desplaçament n es pot descriure com

$$E_n(x) = (x + n) \pmod{27} \text{ (mod indica mòdul, és a dir, el residu de la divisió entera)}$$

Per exemple:  $E_3(1) = (1 + 3) \pmod{27} = 4$  (la A es substitueix per la Ç)

La descodificació es fa de manera semblant:  $D_n(x) = (x - n) \pmod{27}$

Aquest mètode rep el nom per Juli Cèsar ja que sembla que l'utilitzava, amb un desplaçament de tres, per comunicar-se confidencialment amb els seus generals, i, sembla ser que era raonablement segur doncs pocs enemics del Cèsar haurien sabut llegir i molts menys podrien haver fet l'anàlisi corresponent.

En el segle XIX, la secció d'avisos personals dels diaris servia a vegades per intercanviar missatges codificats. David Kahn (1967) descriu alguns exemples de comunicació secreta entre amants en el periòdic The Times.

*VI Jornada de les ciències*  
*Dijous 22 de març del 2007*  
*Taller de matemàtiques; Joc d'espies*

Al 1915 l'armada russa l'emprava en substitució d'altres xifrats més complicats que havien resultat molt difícils d'utilitzar per les seves tropes: els criptoanalistes alemanys i austríacs no varen tenir gaires problemes per descodificar els missatges.

El xifrat Cèsar és part de sistemes més complexos de codificació com el xifrat Vigenère, i també té aplicació en el sistema ROT13.

Com tots els xifrats de substitució alfabètica simple, el xifrat Cèsar es desxifra amb facilitat i a la pràctica no ofereix molta seguretat a la comunicació.

### *Exemple*

Imaginem que hem captat el següent missatge: **EYEGEWJR EQ GEUAJXUWJ UJW QE WEFEXXE**

Si sabem o sospitem que està codificat amb el xifrat Cèsar, només ens caldrà saber el desplaçament per poder desxifrar el missatge. Com comencem? Una bona manera serà fer-ho amb paraules de poques lletres i veure amb quin desplaçament tenen sentit. Aquest és un mètode de força bruta.

Provem-ho!

	<b>E</b>	<b>Q</b>	
Amb un desplaçament de 1	D	P	No té sentit
Amb un desplaçament de 2	Ç	O	No té sentit
Amb un desplaçament de 3	C	N	No té sentit
Amb un desplaçament de 4	B	M	No té sentit
Amb un desplaçament de 5	A	L	Té sentit

Fem la comprovació amb una paraula més llarga:

<b>E</b>	<b>Y</b>	<b>E</b>	<b>G</b>	<b>E</b>	<b>W</b>	<b>J</b>	<b>R</b>
A	T	A	C	A	R	E	M

Ara que ja tenim el desplaçament, podem desxifrar-ho tot:

<b>E</b>	<b>Y</b>	<b>E</b>	<b>G</b>	<b>E</b>	<b>W</b>	<b>J</b>	<b>R</b>	<b>E</b>	<b>Q</b>	<b>G</b>	<b>E</b>	<b>U</b>	<b>A</b>	<b>J</b>	<b>X</b>	<b>U</b>	<b>W</b>	<b>J</b>
A	T	A	C	A	R	E	M	A	L	C	A	P	V	E	S	P	R	E
<b>U</b>	<b>J</b>	<b>W</b>	<b>Q</b>	<b>E</b>	<b>W</b>	<b>E</b>	<b>F</b>	<b>E</b>	<b>X</b>	<b>X</b>	<b>E</b>							
P	E	R	L	A	R	A	B	A	S	S	A							

## *El xifrat Vigenère*

Utilitza el xifrat Cèsar però amb un desplaçament diferent en cada posició del text; el valor del desplaçament es defineix amb una paraula clau repetitiva.

Va ser considerat un xifrat segur, fins que Kasiski va trobar un mètode d'atac.

El mètode Kasiski consisteix en determinar la longitud de la clau i es basa en la recerca de paraules repetides en el text xifrat.

Quan es troben paraules repetides és molt probable que les paraules coincideixin en el text pla i que la clau hagi coincidit en la mateixa posició. La distància entre les paraules repetides és un múltiple de la longitud de la paraula clau. Cercant parelles de paraules repetides i calculant el màxim comú divisor de la distància que les separa es pot trobar la longitud de la clau o un múltiple de la mateixa. Un cop coneguda la longitud de la clau només cal dividir el document en blocs de la mateixa mida i aplicar el mètode estadístic.

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

*VI Jornada de les ciències*  
*Dijous 22 de març del 2007*  
*Taller de matemàtiques; Joc d'espies*

*Exemple*

Es vol codificar el missatge: “els nombres governen el món” amb la paraula clau Pitagoras, Primer s’escriu la frase i a sota la paraula clau repetida tantes vegades com calgui:

E	L	S		N	O	M	B	R	E	S		G	O	V	E	R	N	E	N		E	L		M	O	N
P	I	T		A	G	O	R	A	S	P		I	T	A	G	O	R	A	S		P	I		T	A	G

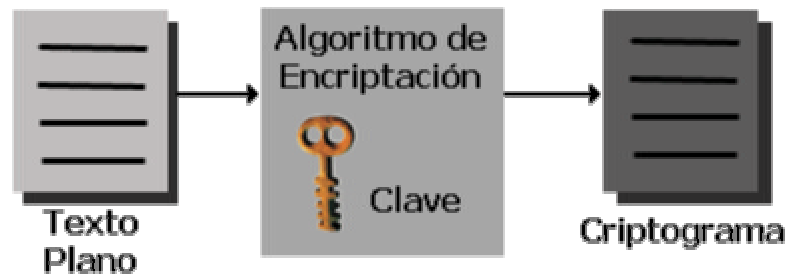
A la primera columna es busca P i a la primera fila la E; en la intersecció de la fila i la columna es troba el valor del criptograma: U

E	L	S		N	O	M	B	R	E	S		G	O	V	E	R	N	E	N		E	L		M	O	N
P	I	T		A	G	O	R	A	S	P		I	T	A	G	O	R	A	S		P	I		T	A	G
U	U	L		N	V	B	S	R	X	H		P	H	V	L	F	E	E	F		U	U		F	O	U

Com es pot veure, a una mateixa lletra del text pla li corresponen diferents lletres en el text xifrat.

# Taller ?

# Criptoanàlisis



VI Jornada de les ciències  
 Dijous 22 de març del 2007  
 Taller de matemàtiques; Joc d'espies  
**Introducción**

El criptoanálisis es una rama de la criptología en la que se estudian los principios y métodos de transformar un mensaje cifrado en su texto original sin conocer la clave. Es decir, mediante el criptoanálisis se intenta pasar del **texto cifrado o criptograma**, que no parece tener sentido, al **texto en claro o texto plano**.

**Texto cifrado o criptograma:**

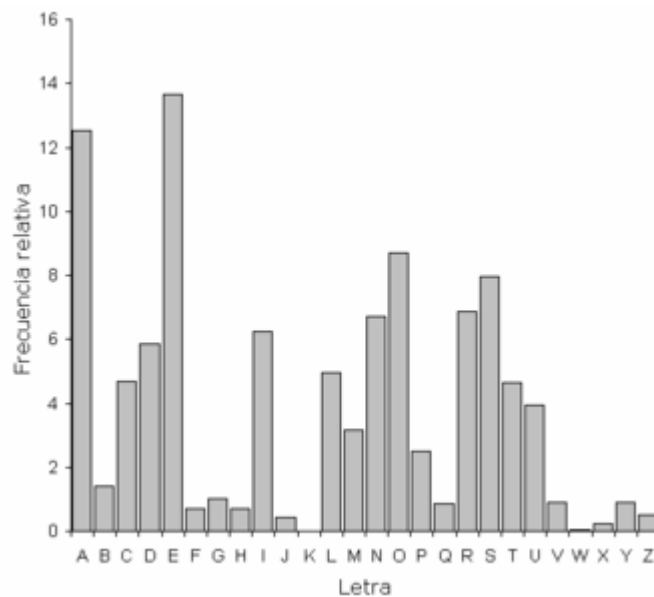
↑↱ ↱↱ ↱↱↑↱↱ ↱↑ ↱↱ ↱↱↱↱↱↱ ↱↑ ↱↱↱↱ ↱↱↑↱↱↑ ↱↱  
 ↱ ↱↱↱↑↱↱ ↱↱↱↱↱↱↱↱

**Texto plano**

EN UN LUGAR DE LA MANCHA DE CUYO NOMBRE NO QUIERO ACORDARME

Uno de los métodos auxiliares utilizado para descifrar un mensaje encriptado según las técnicas clásicas, es el llamado **análisis de frecuencias** o estudio de la frecuencia de aparición de las letras o grupos de letras en un criptograma y su comparación con la frecuencia de aparición de las letras en un idioma dado.

Dado un texto, ciertas letras o combinaciones de letras aparecen más a menudo que otras. Es más, existe, para un idioma determinado, una distribución característica de las letras que es prácticamente la misma en la mayoría de ejemplos de este lenguaje. El cálculo de frecuencias de las letras o combinaciones de letras en un lenguaje es difícil y esta sujeto a interpretación, ya que en los resultados de la distribución de frecuencias influyen varios parámetros. Teniendo en cuenta estas salvedades, la distribución de las letras en castellano viene dada por el siguiente gráfico y su correspondiente tabla, dada en porcentaje:



Porcentaje de aparición de las letras en castellano

*VI Jornada de les ciències*  
*Dijous 22 de març del 2007*  
*Taller de matemàtiques; Joc d'espies*

POR FRECUENCIA	
LETRA	PORCENTAJE
E	13.68
A	12.53
O	8.68
S	7.98
R	6.87
N	6.71
I	6.25
D	5.86
L	4.97
C	4.68
T	4.63
U	3.93
M	3.15
P	2.51
B	1.42
G	1.01
V	0.90
Y	0.90
Q	0.88
H	0.70
F	0.69
Z	0.52
J	0.44
X	0.22
W	0.02
K	0.00

A partir de los datos anteriores, se puede decir que:

- Las vocales ocuparán a lrededor del 45% del texto.
- La E y la A son identificables fácilmente dado su alto porcentaje de aparición.
- Las consonantes más frecuentes son: S, R, N, D, L (aparecen con una frecuencia de un 32%)
- Las seis letras menos frecuentes son: F, Z, J, X, W, K (sumadas tienen una frecuencia que no llega al 2%)

A la hora de aplicar el análisis de frecuencias a un criptograma habrá que tener en cuenta igualmente cuestiones como:

*VI Jornada de les ciències*  
*Dijous 22 de març del 2007*  
*Taller de matemàtiques; Joc d'espies*

- a) La aparición de palabras formadas por dos letras: *de, el, le, al, yo, mi, la, si, es, en, me, etc.*
- b) La aparición de palabras formadas por tres letras: *que, con, sin, del, por, con, los, las, les, etc.*
- c) La aparición de consonantes dobles: *ll, rr,*
- d) La aparición de palabras formadas por una letra: *a, o, e, y, u.*
- e) Las posibles terminaciones de palabra: *a, e, o, i, u, s, r, l, n, m, z, etc.*

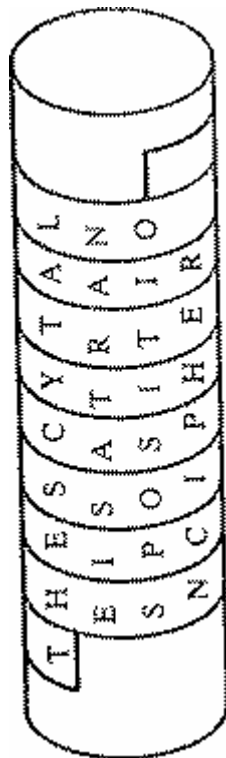
### *Análisis de frecuencias para algoritmos de sustitución simple*

En un algoritmo de sustitución simple cada letra del texto plano se reemplaza por otra y una letra del texto plano siempre será transformada en la misma letra del mensaje cifrado. Por ejemplo, si la cifra consiste en sustituir la **e** por la **x**, todas las letras **e** del texto se convertirán en **x** y una frecuencia elevada de **x** en el criptograma podría sugerir que se trata de una **e**.

El uso básico del análisis de frecuencias consiste primero en calcular la frecuencia de las letras que aparecen en el texto cifrado, comparar la frecuencia con la distribución del idioma en que se encuentra el texto en claro y asignar, de acuerdo con esta comparación, unos símbolos a otros. Así, una gran frecuencia de **X** podría sugerir que se trata de la **E**, pero también podría ser la **A** o la **O**.

# Taller ?

## *La scytale spartiate et le Transposition rectangulaire*



## La scytale spartiate

Le premier dispositif de cryptographie militaire connu, **la scytale spartiate**, date du V siècle avant JC.

La scytale est un bâton de bois autour duquel est entourée une bande de bois de cuir ou de parchemin. Il faut deux bâtons exactement de même dimensions.

- L'expéditeur écrit son message sur toute la longueur de la scytale et déroule ensuite la bande sur laquelle apparaît une suite de lettres sans signification.
- La plupart du temps, le messenger emportait la bande de cuir en l'utilisant comme ceinture, avec les lettres tournées vers l'intérieur.
- Le destinataire enroulera alors cette bande sur son bâton (de même diamètre) pour lire le message en clair.



## Transposition rectangulaire

Ici la clef est un mot que doivent connaître l'expéditeur et le destinataire.

La méthode consiste à écrire dans un tableau :

- Le mot de passe sur la première ligne,
- Le rang des lettres dans l'alphabet sur la deuxième ligne. Si une lettre est répétée, on les numérote de la gauche vers la droite.
- On écrit ensuite le message en mettant une lettre par case.
- On ordonne les colonnes dans l'ordre des numéros.
- Le message qui sera envoyé s'écrit par colonne dans l'ordre des numéros.
- Pour déchiffrer les messages, on utilise le processus à l'envers.

### Exemple 1

Si le mot de passe est : **autobus**

<b>A</b>	<b>U</b>	<b>T</b>	<b>O</b>	<b>B</b>	<b>U</b>	<b>S</b>
<b>1</b>	<b>6</b>	<b>5</b>	<b>3</b>	<b>2</b>	<b>7</b>	<b>4</b>
N	O	S	V	E	M	O
S	A	L	A	S	S	I
E	T	E	E	N	T	U
C	A	S	A			

*VI Jornada de les ciències*  
*Dijous 22 de març del 2007*  
*Taller de matemàtiques; Joc d'espies*

A	B	O	S	T	U	U
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>
N	E	V	O	S	O	M
S	S	A	I	L	A	S
E	N	E	U	E	T	T
C		A		S	A	

Le message envoyé sera: **NSEC ESN VAEA OIU SLES OATA MST.**

*Exemple 2*

Si le mot de passe est : **colegio**

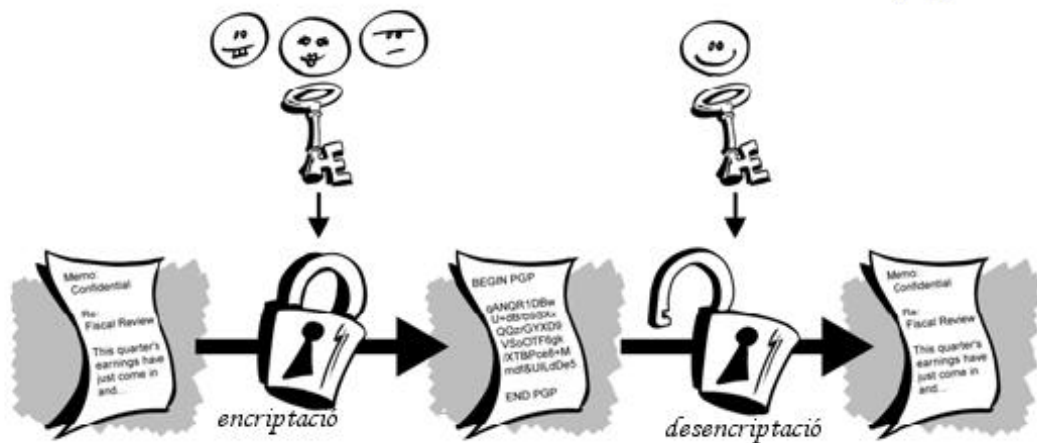
<b>C</b>	<b>O</b>	<b>L</b>	<b>E</b>	<b>G</b>	<b>I</b>	<b>O</b>
<b>1</b>	<b>6</b>	<b>5</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>7</b>
N	O	S	V	E	M	O
S	A	L	A	S	S	I
E	T	E	E	N	T	U
C	A	S	A			

C	E	G	I	L	O	O
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>
N	V	E	M	S	O	O
S	A	S	S	L	A	I
E	E	N	T	E	T	U
C	A			S	A	

Le message envoyé sera : **NSEC VAEA ESN MST SLES OATA OIU**

# Taller ?

## Criptografia asimètrica



## Criptografia asimètrica. Sistema RSA o de clau pública

La criptografia asimètrica és un mètode criptogràfic que utilitza un parell de claus per enviar missatges. Aquestes dues claus pertanyen a l'emissor.

Una clau és privada i s'ha de guardar de manera que ningú tingui accés. L'altra clau és pública i es pot lliurar a qualsevol persona

L'emissor xifra el missatge amb la clau pública. El receptor desxifra el missatge amb la seva clau privada.

La criptografia asimètrica sorgeix per solucionar el problema de la distribució de claus. Com aquesta s'ha de fer mitjançant un canal segur, això és difícil. Una solució en aquest problema la van donar "Diffie" i "Hellman" l'any 1976 i consisteix en utilitzar "funcions d'una via o d'un sentit"

Les funcions d'una via compleixen el següent:

- És fàcil de calcular  $y = f(x)$ , conegut  $x$ .
- Conegut  $y$  és computacionalment impossible el càlcul de  $x = f^{-1}(y)$

Per exemple, és fàcil de trobar dos nombres primers i fer-ne el producte; és difícil, donat un nombre molt gran, factoritzar-ho en dos nombres primers.

La criptografia asimètrica soluciona el problema d'intercanvi de claus dels sistemes de criptografia simètrica, l'escitala, la xifra Cèsar, la xifra Vigènere, ... ja que en aquest sistema no cal que l'emissor i el receptor es posin d'acord amb la clau a utilitzar, només cal que l'emissor aconseguixi una còpia de la clau pública del receptor

Els algorismes més habituals que es basen en la criptografia asimètrica són: Diffie-hellmann, RSA, DSA, ElGamal, la criptografia de corbes el·líptiques.

En resum, les principals característiques de la criptografia asimètrica són:

- Els seus algorismes s'implementen eficientment
- No cal el secret previ compartit
- El nombre de claus creix linealment amb el nombre de receptors
- Hi ha pocs algorismes
- A nivell informàtic és molt costós ja que les claus són molt grans (1000-4000 bits)
- La seva seguretat molt elevada ja que com es basa en la teoria de nombres i en la factorització, cal tenir molts bons coneixements sobre aquestes àrees i un ordinador potent per a poder-hi treballar.

## L'algorisme RSA

Aquest algorisme és de clau pública i deu el seu nom als seus inventors: Ron Rivest, Adi Shamir i Leonard Adleman

### Com funciona?

- S'agafen dos nombres primers P i Q de 200 dígits aproximadament. I es fa el seu producte  $n: P \cdot Q = n$
- Es cerca un nombre E que sigui primer amb  $F(n) = (P-1) \cdot (Q-1)$
- Com E i  $F(n)$  són primers entre si, aleshores existeix un nombre D de manera que  $E \cdot D - 1$  és múltiple de  $F(n)$
- Aquest D es pot calcular mitjançant l'algorisme d'Euclides
- Amb això ja tenim dues claus:
  - Clau pública ( E, n )
  - Clau privada ( D, n )

Un cop que s'ha trobat D cal mantenir en privat P, Q,  $F(n)$  i D. Si algú coneix aquestes dades, podrà desxifrar el vostre missatge.

Ara, hem de convertir el nostre missatge en un nombre, hi ha diverses maneres però és important que aquest nombre sigui més petit que N.

Un cop hem transformat en numèric el nostre missatge, per xifrar, utilitzem la fórmula:  **$C = M^E \text{ mòdul } n$**

Per desxifrar el missatge, emprem la fórmula:  **$M = C^D \text{ mòdul } n$**

### Exemple :

Prendrem nombres primers petits (2, 3, 5, 7, 11, ...) per facilitar el càlcul. Per exemple,  $P = 7$  i  $Q = 5$ ; llavors calculem:

$$n = 7 \cdot 5 = 35 \quad \text{i} \quad F(35) = (7 - 1) \cdot (5 - 1) = 24$$

Ara hem de trobar E de manera que E sigui primer amb 24. Podem triar entre 5, 7, 11, 13, 17, 19, 23 i escollim  $E = 13$

Cal trobar D de manera que  $13 \cdot D - 1$  sigui un múltiple de 24. Com es troba D? Amb l'algorisme d'Euclides, és a dir, basant-nos en el fet que:

$$\text{MCD}(\text{dividend}, \text{divisor}) = \text{MCD}(\text{divisor}, \text{residu})$$

En el nostre exemple, tenim:  $E = 13$  i  $F(35) = 24$

L'algorisme d'Euclides és el següent:

Quocient 1	Quocient 2	Quocient 3	Quocient 4	
<b>Dividend</b>	<b>Divisor</b>	Residu 1	Residu 2	<b>Residu 3 = MCD</b>
Residu 1	Residu 2	Residu 3	Residu 4= 0	

VI Jornada de les ciències  
Dijous 22 de març del 2007  
Taller de matemàtiques; Joc d'espies

Un cop que s'arriba a residu 0, s'acaba l'algorisme i el MCD és el darrer número pel qual s'ha dividit. En el nostre exemple:

1	1	5	2	
<b>24</b>	<b>13</b>	11	2	1
11	2	1	0	

El MCD (24, 13) = 1

Ara observeu que passa amb les proves de les divisions efectuades:

☆  $24 = 13 \cdot 1 + 11$ ;  $11 = 24 - 1 \cdot 13$ ;

☆  $13 = 11 \cdot 1 + 2$ ;  $2 = 13 - 1 \cdot 11 = 13 - 1 \cdot (24 - 1 \cdot 13) = 13 - 1 \cdot 24 + 1 \cdot 13$ ;  
 $2 = 2 \cdot 13 - 1 \cdot 24$

☆  $11 = 2 \cdot 5 + 1$ ;  $1 = 11 - 2 \cdot 5$ ;  $1 = (24 - 13 \cdot 1) - (2 \cdot 13 - 1 \cdot 24) \cdot 5 =$   
 $= 24 - 13 \cdot 1 - 10 \cdot 13 + 5 \cdot 24$ ;  $1 = 6 \cdot 24 - 11 \cdot 13$

Resumint:  $1 = 6 \cdot 24 - 11 \cdot 13$  Aquesta darrera expressió que hem obtingut s'anomena *Identitat de Bézout* (el seu enunciat és el següent: si **a** i **b** són nombres enters amb màxim comú divisor **d** [ $MCD(a, b) = d$ ], aleshores existeixen enters **x** i **y** tals que  $ax + by = d$ )

D'aquí, tenim que  $D = -11$  o  $D = -11 + 24 = 13$

Clau pública = (13,35)

Clau privada = (13,35)

Suposem que el missatge a codificar és MATES. Per convertir les lletres en nombres habitualment s'utilitza un codi com l'ASCII:

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

*Codi ASCII de les lletres majúscules*

Fem l'equivalència següent: MATES  $\leftrightarrow$  77 65 84 69 83

Ara elevem aquests nombres al nombre  $E=13$  i els calculem mòdul 35 (cal que feu la divisió del nombre entre 35 i trobeu el residu)

$77^{13} = C1$ ;  $C1 \bmod 35 = 18$

$65^{13} = C2$ ;  $C2 \bmod 35 = 30$

$84^{13} = C3$ ;  $C3 \bmod 35 = 14$

$69^{13} = C4$ ;  $C4 \bmod 35 = 34$

$83^{13} = C5$ ;  $C5 \bmod 35 = 13$

El missatge és ( 18,30,14,34,13 )

En aquest taller, farem només xifrat, ja que el desxifrat cal molt temps.

*VI Jornada de les ciències*  
*Dijous 22 de març del 2007*  
*Taller de matemàtiques; Joc d'espies*

*Taula de codis ASCII (0-127)*

Caràcteres no imprimibles			Caràcteres imprimibles					
Nombre	Dec	Car.	Dec	Car.	Dec	Car.	Dec	Car.
Nulo	0	NUL	32	Espacio	64	@	96	`
Inicio de cabecera	1	SOH	33	!	65	A	97	a
Inicio de texto	2	STX	34	"	66	B	98	b
Fin de texto	3	ETX	35	#	67	C	99	c
Fin de transmissió	4	EOT	36	\$	68	D	100	d
enquiry	5	ENQ	37	%	69	E	101	e
acknowledge	6	ACK	38	&	70	F	102	f
Campanilla (beep)	7	BEL	39	'	71	G	103	g
backspace	8	BS	40	(	72	H	104	h
Tabulador horizontal	9	HT	41	)	73	I	105	i
Salto de línia	10	LF	42	*	74	J	106	j
Tabulador vertical	11	VT	43	+	75	K	107	k
Salto de pàgina	12	FF	44	,	76	L	108	l
Retorno de carro	13	CR	45	-	77	M	109	m
Shift fuera	14	SO	46	.	78	N	110	n
Shift dentro	15	SI	47	/	79	O	111	o
Escape línia de datos	16	DLE	48	0	80	P	112	p
Control dispositivo 1	17	DC1	49	1	81	Q	113	q
Control dispositivo 2	18	DC2	50	2	82	R	114	r
Control dispositivo 3	19	DC3	51	3	83	S	115	s
Control dispositivo 4	20	DC4	52	4	84	T	116	t
neg acknowledge	21	NAK	53	5	85	U	117	u
Sincronismo	22	SYN	54	6	86	V	118	v
Fin bloque transmitido	23	ETB	55	7	87	W	119	w
Cancelar	24	CAN	56	8	88	X	120	x
Fin medio	25	EM	57	9	89	Y	121	y
Sustituto	26	SUB	58	:	90	Z	122	z
Escape	27	ESC	59	;	91	[	123	{
Separador archivos	28	FS	60	<	92	\	124	
Separador grupos	29	GS	61	=	93	]	125	}
Separador registros	30	RS	62	>	94	^	126	~
Separador unidades	31	US	63	?	95	_	127	DEL