

OCULTACIÓ D'INFORMACIÓ

El telegrama Zimmermann

CLASS OF SERVICE DESIRED									
Fast Day Message	<input checked="" type="checkbox"/>								
Day Letter	<input type="checkbox"/>								
Night Message	<input type="checkbox"/>								
Night Letter	<input type="checkbox"/>								

Please check mark on it according the above if correctly desired. OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

WESTERN UNION TELEGRAM
NEWSPAPER CARLTON, PRESIDENT

5587

3300

via Galveston

JAN 20 1917

GERMAN LEGATION
MEXICO CITY

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

130	13042	13401	8501	115	3528	416	17214	8491	11310
18147	18222	21560	10247	11518	23677	13805	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11269	18276	18101	0317	0228	17894	4473	
22284	22200	19452	21589	87893	5569	13918	8958	12137	
1333	4725	4458	5905	17186	13851	4458	17149	14471	6706
13850	12224	6929	14991	7382	15857	67893	14218	36477	
5870	17553	87893	5870	5454	16102	15217	22801	17138	
21001	17388	7440	23638	18222	8719	14331	15021	23845	
3156	23552	22096	21604	4797	9497	22464	20855	4377	
23610	18140	22260	5905	13347	20420	39689	13732	20667	
6929	5275	18507	52262	1340	22049	13339	11265	22295	
10439	14814	4178	6992	8784	7832	7357	6926	52262	11267
21100	21272	9346	9559	22464	15874	18502	18500	15857	
2188	5376	7381	98092	16127	13486	9350	9220	76036	14219
5144	2831	17920	11347	17142	11264	7667	7762	15099	9110
10482	97556	3589	3670						

BEPNSTORFF.

Charge German Embassy.

TÈCNIQUES CLÀSSIQUES

- 1) Amagar la informació compromesa a dins d'altra informació inofensiva: **esteganografia**.
- 2) Barrejar les lletres del missatge original: mètodes de **permutació**.
- 3) Aplicar algun canvi de símbols: mètodes de **substitució**.

ESTEGANOGRAFIA

Acrònims:

- “Viva Verdi” = “Viva Vittorio Emmanuelle
Re d'Italia” (Itàlia, s. XIX)

- Primers cristians: símbol del peix (*ictus*)

IXΘΥΣ = Υησους Χριστος Θεου Υιος Σωτηρ

= “Jesús Crist, Fill de Déu, Salvador”

Acròstics:

- Beatles, 1970: Lucy in the Sky with Diamonds

- E.A. Poe, *An enigma*:

Seldom we find, says Solomon Don Dunce,

Half an idea in the profoundest sonnet.

Through all the flimsy things we see at once

As easily as through a Naples bonnet

–Trash of all trash!– how can a lady don it?

.... "Sarah Anna Lewis"

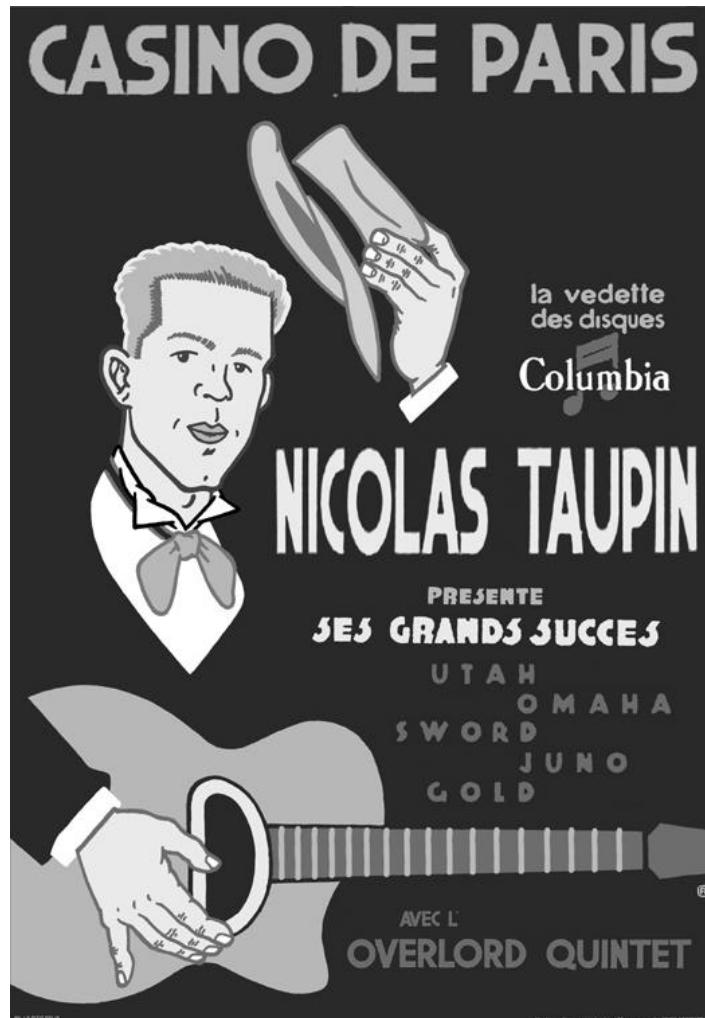
- Rector de Vallfogona, *Sonet set vegades acróstich*

SONET
EN FORMA DE LABIRINTO

Christo: H an H a H emor, H eresa, H an H a pena,
 H ntre H xc H ssiv H s glòri H s, i al H gries!
 R epa R a, i mi R a, que ag R avia R pod R ries
 H sta H sp H rança d H ma llum s H r H na.
 S os S ega, e S po S a ca S ta, i as S erena
 V queix V pen V , que h A n b A st V t les mies
 D ar D ura D or D escans D e infinits D ies
 H n les H tern H s sal H s, per H str H na

Teresa: J a la I ntr I cada, I fosca n I t in I ca
 H n b H ll H sa d H glòria v H ig s H 'm muda.
 S ou, S en S dubte, S enyor, S ol de Tere S a,
 V ostra esclava, ab V n cla V se V i V ifica,
 S egura, e S pò S , que S ou vó S en S a ajuda,
 T orrE glòR ia, d E scanS , i fortAlesa.

L'estranya desaparició de Nicolas Taupin



MÈTODES DE PERMUTACIÓ

Exemple: "mètode de les caixes"

Missatge: ELS ESDEVENIMENTS ES PRECIPITEN

Clau: PIRÀMIDE = (7,4,8,1,6,5,2,3)

1	2	3	4	5	6	7	8
E	L	S	E	S	D	E	V
E	N	I	M	E	N	T	S
E	S	P	R	E	C	I	P
I	T	E	N				

ETI / EMRN / VSP / EEEI / DNC / SEE / LNST / SIPE

Text xifrat: ETIEMRNVSP EEEIDNCSEELNSTSIPE

Agost 1610. Correspondència Galileo – Kepler.

Agost, Galileo:

SMAISMIRMILMEPOETALEVMIBVNENVGTTAVIRES

[Combinacions: 960302721204184355302136832000000]

Novembre, Kepler:

SALVE VMBISTINEVM GEMINATVM MARTIA PROLES

“Salve, ardents bessons, progenitors de Mart”

Solució correcta:

ALTISSIMVM PLANETAM TERGEMINVM OBSERVAVI

“Vaig observar que el planeta més alt era triple”

Galileo, desembre:

HAEC IMMATVRA A MEJAM FRVSTRA LEGVNTVR

“Recullo debades el que no està madur”

Kepler, març:

MACVLA RUFA IN JOVE EST GIRATVM MATHEM

“Hi ha una taca roja a Júpiter que gira matemàticament”

Solució correcta:

CINTHIAE FIGVRAS AEMVLATUR MATER AMORUM

“La mare de l’amor imita la forma de Cinthia (la Lluna)”

PRINCIPI DE KERCKHOFFS (1883): La seguretat d’un mètode criptogràfic no ha de dependre de mantenir secret el protocol, sinó només de mantenir secreta la clau.

MÈTODES DE SUBSTITUCIÓ

Mètode de Juli Cèsar (s. I aC)

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
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

Text inicial: ESTAN BOJOS, AQUESTS ROMANS

Text xifrat: *HVWDQ ERMRV, DTXHVWV URPDQV*

Matemàticament: $f(x) = x + 3 \pmod{26}$

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

Transformem la Y = 24:

$$f(24) = 24 + 3 \pmod{26} = 27 \pmod{26} = 1 = B.$$

Es pot mantenir el protocol (Cèsar) i canviar la clau:

Mètode Cèsar de clau 7:

$$f(x) = x + 7 \pmod{26}$$

Netscape v2.0 : "ROT13" $f(x) = x + 13 \pmod{26}$.

Mètode afí: $f(x) = mx + n \pmod{26}$:

Exemple: $f(x) = 3x + 7 \pmod{26}$

La clau secreta és "3 i 7".

Transformem la K:

$$K = 10$$

$$f(10) = 3 \cdot 10 + 7 \pmod{26} = 37 \pmod{26} = 11 = L$$

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

Compte!! No totes les fórmules són vàlides!

$$f(x) = 4x + 5 \pmod{26}$$

Transformem la A:

$$A = 0$$

$$f(0) = 4 \cdot 0 + 5 \pmod{26} = 5 = F.$$

Transformem la N:

$$N = 13$$

$$f(13) = 4 \cdot 13 + 5 \pmod{26} = 57 \pmod{26} = 5 = F !!!$$

Tant la A com la N es transformen en F !!! ...

Canvi qualsevol de lletres (sense fórmula matemàtica):

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

El cas més general (canvi de lletres per símbols):

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
6	*	;	>	%	?	\	&	+		/	:	"	¡	4	<	±	¾	÷	µ	ƒ	ø	¥	Á	Ñ	¿

Exemple clàssic: *L'escarabat d'or*, E.A. Poe.

53‡‡+305))6* ;4826)4‡.)4‡);806* ; 48+8
¶(60))85;1‡(;:‡* 8+83(88)5*+;46(;88*96*
?;8)*‡(;485);5*+2:*‡(;4956*2(5*-4)8¶8*
;4069285);)6+8)4‡‡;1(‡9;48081;8:8‡1;48
+85;4)485+528806*81(‡9;48;(88;4(‡?34;
48)4‡;161;:188;‡?;

REALMENT ESTEM OCULTANT LA INFORMACIÓ?

Tècnica de l'anàlisi de freqüències

(Abu Iusuf Al-Kindi, s. IX)

Català:

E (13,89%), A (12,55%), S (8,43%), R (7,74%),
I (6,99%), L (6,76%), N (6,40%), T (6,11%), O (5,71%),
U (4,18%), D (3,94%), C (3,60%), M (3,16%), P (2,72%),
V (1,40%), Q (1,35%), B (1,32%), G (1,28%), Ç (1,06%),
F (1%), H (0,72%), X (0,52%), J (0,30%), Y (0,18%),
Z (0,006%), K (0,004%), W (0,001%)

*ldvehmoedm iw lijlk zzluwdj mwqe, flhgkl vlk hliezj
zldwubm w mwqe nez cwh gkl tmbwdlk mbo fmiim
alhbm flz tmbw clz nlhwjmozl w ikfhlb tedlwqlbldj,
mgklzz gkl ldmzjlwq, wzzkbwdm w ukmhlwq jeji lzi
bmzi. xm gkl debli vw vm kd clk, mzm, w bmvebm li
lz ilk fhealjm.*

Símbol	Freqüència	Símbol	Freqüència
<i>l</i>	33	<i>q</i>	5
<i>m</i>	24	<i>g</i>	5
<i>w</i>	19	<i>t</i>	3
<i>z</i>	17	<i>c</i>	3
<i>k</i>	14	<i>u</i>	3
<i>b</i>	12	<i>o</i>	3
<i>i</i>	12	<i>n</i>	2
<i>d</i>	11	<i>x</i>	1
<i>e</i>	11	<i>a</i>	2
<i>h</i>	9	<i>r</i>	0
<i>j</i>	9	<i>s</i>	0
<i>f</i>	5	<i>p</i>	0
<i>v</i>	5	<i>y</i>	0

	<i>m</i>	<i>l</i>	<i>w</i>	<i>k</i>
<i>b</i>	8	4	4	3
<i>i</i>	3	7	4	1
<i>d</i>	3	7	4	1
<i>e</i>	0	0	0	0
<i>h</i>	2	6	2	1
<i>j</i>	4	3	1	0

*EdHOhAoOda il EijEU LLEuidj AiqO, fEhQUE HEU
hEiOLj LEdlubA I AiqO nOL clh QUE tAbIdEU Abo
fAiiA aEhbA fEL tAbI cEL nEhljAoLE I iUfhEb
tOdEIqEbEdj, AQUELL QUE EdALjEIq, ILLUblDA I
uUAhEIq jOji ELi bALi. xA QUE dObEi HI HA Ud cEU,
ALA, I bAHObA Ei EL iEU fhOaEjA*

AiqO = AIXO : q = X

fEhQUE = PERQUE: f = P, h = R

Solució final:

ENHORABONA SI ESTEU LLEGINT AIXÒ, PERQUÈ
HEU RESOLT L'ENIGMA I AIXÒ VOL DIR QUE
CAMINEU AMB PASSA FERMA PEL CAMÍ DEL
VERITABLE CONEIXEMENT, AQUELL QUE
ENALTEIX, IL·LUMINA I GUAREIX TOTS ELS
MALS. JA QUE NOMÉS HI HA UN DÉU, ALÀ, I
MAHOMA ÉS EL SEU PROFETA.

CRIPTOGRAFIA MODERNA: MÈTODES DE FLUX

Són un intent d'aproximar-se al “sistema del secret perfecte” (Teorema del Secret Perfecte de Shannon).

Quin és aquest “sistema perfecte”?

Cal tenir una clau formada per una seqüència infinita de nombres enters (entre 0 i 25), totalment aleatòria:

(1, 10, 4, 8, 13, 2, 17, 7, 6, 22, 19, 21, 12, 18, 14, 9, 20, 5, 15, 16, 0, 3, ...)

Aleshores, a cada lletra del missatge se li aplica un Juli Cèsar, utilitzant cada vegada un nombre diferent de la seqüència:

HOLA QUÈ TAL = 7, 14, 11, 0, 16, 20, 4, 19, 0, 11

Missatge: 7, 14, 11, 0, 16, 20, 4, 19, 0, 11

Clau: 1, 10, 4, 8, 13, 2, 17, 7, 6, 22

Cèsar: 8, 24, 15, 8, 3, 22, 21, 0, 6, 7

= I, X, P, I, D, W, V, A, G, H

Una aproximació d'aquest "sistema perfecte" dóna lloc a la famosa "xifra llibre":

Clau secreta: el Quixot.

Text xifrat:

1, 1, ASGTD LOKKQ JR YHHD...

Vol dir que la clau comença la pàgina 1, línia 1 del Quixot, i per tant és "EN UN LUGAR DE LA MANCHA, DE CUYO NOMBRE NO QUIERO ACORDARME..." = (4,13,20,13,11,20,6,0,17,3...)



pàgina 22, línia 3 de *Acción Libertadora*: “nuestros criterios para alcanzar el frente único...” = (13, 20, 4, 18, 19, 17, 14, 18, 2, 17, 8, 19, 4, 17, 8...)

Obtenim VILAVILACANTONADACARRERA.

Però la xifra llibre encara no és el sistema perfecte, perquè la clau, tot i que es pot considerar "infinita", no és gens aleatòria!

Els mètodes de flux (telefonía mòbil, televisió de pagament) implementen aquestes idees: van sumant, bit a bit, una clau infinita formada per 0's i 1's distribuïts aleatòriament (aparentment...).

SUCCESSIONS ALEATÒRIES

(1,25,3,1,25,3,1,25,3,...) és periòdica: NO aleatòria

(1,2,1,1,2,1,1,1,2,...) no és periòdica, però NO és aleatòria

(1, 10, 4, 8, 13, 2, 17, 7, 6, 22, 19, 21, 12, 18, 14, 9, 20, 5, 15, 16, 0, 3, ...) sembla aleatòria!!

$$f(x) = 7x + 3 \pmod{23}$$

$f(1) = 10$, $f(10) = 4$, $f(4) = 8$

1 és la **llavor** (el nombre inicial, que determina tota la seqüència).

De fet, el següent nombre de la seqüència és 1: $f(3) = 7 \cdot 3 + 3 \pmod{23} = 24 \pmod{23} = 1$. Per tant, es tornarà a repetir tota la seqüència a partir d'aquí!!

Com a molt, el període de la seqüència serà 23, perquè només hi ha 23 nombres diferents.

La solució és agafar una funció com:

$$f(x) = 1103515245x + 12345 \pmod{2147483648}$$

Els 3 nombres d'aquesta fórmula són la clau que comparteixen la companyia telefònica i l'abonat.

Però... són aquestes seqüències realment aleatòries?

NO, en absolut. No verifiquen els tres POSTULATS DE GOLOMB.

Postulats de Golomb per provar el grau d'aleatorietat d'una seqüència binària generada per ordinador (i, per tant, periòdica):

període 15: (0,0,0,1,1,1,1,0,1,0,1,1,0,0,1)

- 1) Hi ha d'haver el mateix nombre de 0's que de 1's.
- 2) El nombre de ràfegues de longitud k és $n/2^k$, on n és el nombre total de ràfegues.
- 3) El valor de $A(k)$ és constant i independent de k , on $A(k)$ = nombre d'elements de la seqüència que coincideixen amb el que està situat k llocs endavant.

COMPARTICIÓ DE SECRETS

Un secret important no pot ser guardat per una sola persona.

Un "esquema de compartició de secrets" és una situació en la qual el secret està repartit entre N persones, i coneixent els fragments d'informació de només M d'elles ($M < N$) es pot recuperar el secret.

Exemple:

Combinació caixa forta d'un banc: (12,13,14).

Hi ha 5 empleats i volem que almenys en facin falta 3 per recuperar la combinació.

$$\text{empleat 1: } -x + y - z = -13$$

$$\text{empleat 2: } 2x - y + z = 25$$

$$\text{empleat 3: } x - z = -2$$

$$\text{empleat 4: } x + 2y - 2z = 10$$

$$\text{empleat 5: } x + y - z = 11$$

CLAU PÚBLICA

Cada usuari té 2 claus, pública i secreta:

Usuaris	Claus públiques	Claus secretes
Alícia	P_A	S_A
Benet	P_B	S_B
Carles	P_C	S_C
...

Les claus públiques apareixen en un directori (obert a tothom). Tothom qui vulgui enviar un missatge xifrat a Alícia utilitzarà la seva clau pública P_A . Quan Alícia rebí el missatge xifrat, el desxifrarà amb la seva clau secreta S_A .

Un espia necessitarà saber S_A per desxifrar el missatge. Però no es pot deduir S_A de P_A . Hi ha una fórmula que les relaciona, però calen milions d'anys de càlculs per trobar la relació. Només Alícia, i ningú més, coneix la clau secreta S_A .

El sistema de clau pública més utilitzat és el RSA (Rivest, Shamir, Adleman, 1977).

Clau pública:

$N = 4041150417805697835589261226970036951192661609691747096108485682493033053$.

$N = p \cdot q$, on p i q són dos nombres primers, que precisament són la clau secreta:

$p = 872365845684756847456438756485787699$
 $q = 4632403294782394832648736483768748847$.

El premi de 100 dòlars de Rivest (1977): trobar els 2 factors p i q que componen el nombre

$N = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541$.

26 d'abril de 1994: 600 PC's via Internet (8 mesos de càlculs):

$p = 32769132993266709549961988190834461413177642967992942539798288533$

$q = 3490529510847650949147849619903898133417764638493387843990820577$