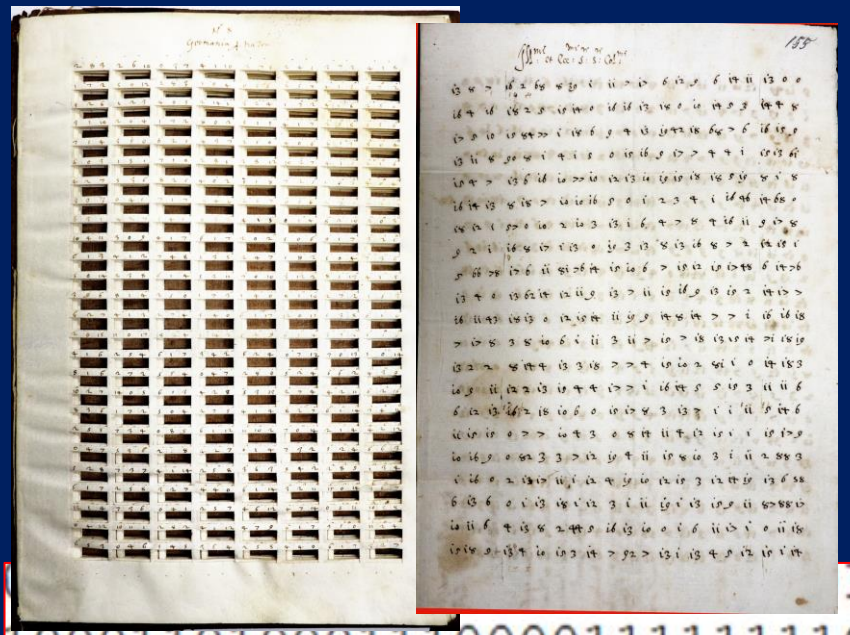


Dalla cifra delle caselle al cifrario di Vernam

Aritmetica modulare e sequenze casuali nella storia della crittografia

Chiaro c	A 11000	l 01001	e 10000	a 11000	00000	i 01100	a 11000	c 01110	t 00001	a 11000	00000	e 10000	s 10100	t 00001
Chiave k	11101	01101	00101	00001	10101	01111	11011	01011	00010	10110	01101	11100	01110	11000
Cifrato c XOR k	00101	00100	10101	11001	10101	00011	00011	00101	00011	01110	01101	01100	11010	11001

Associazione Patavina Mathesis

Mathesis Venezia

DIPARTIMENTO MATEMATICA

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

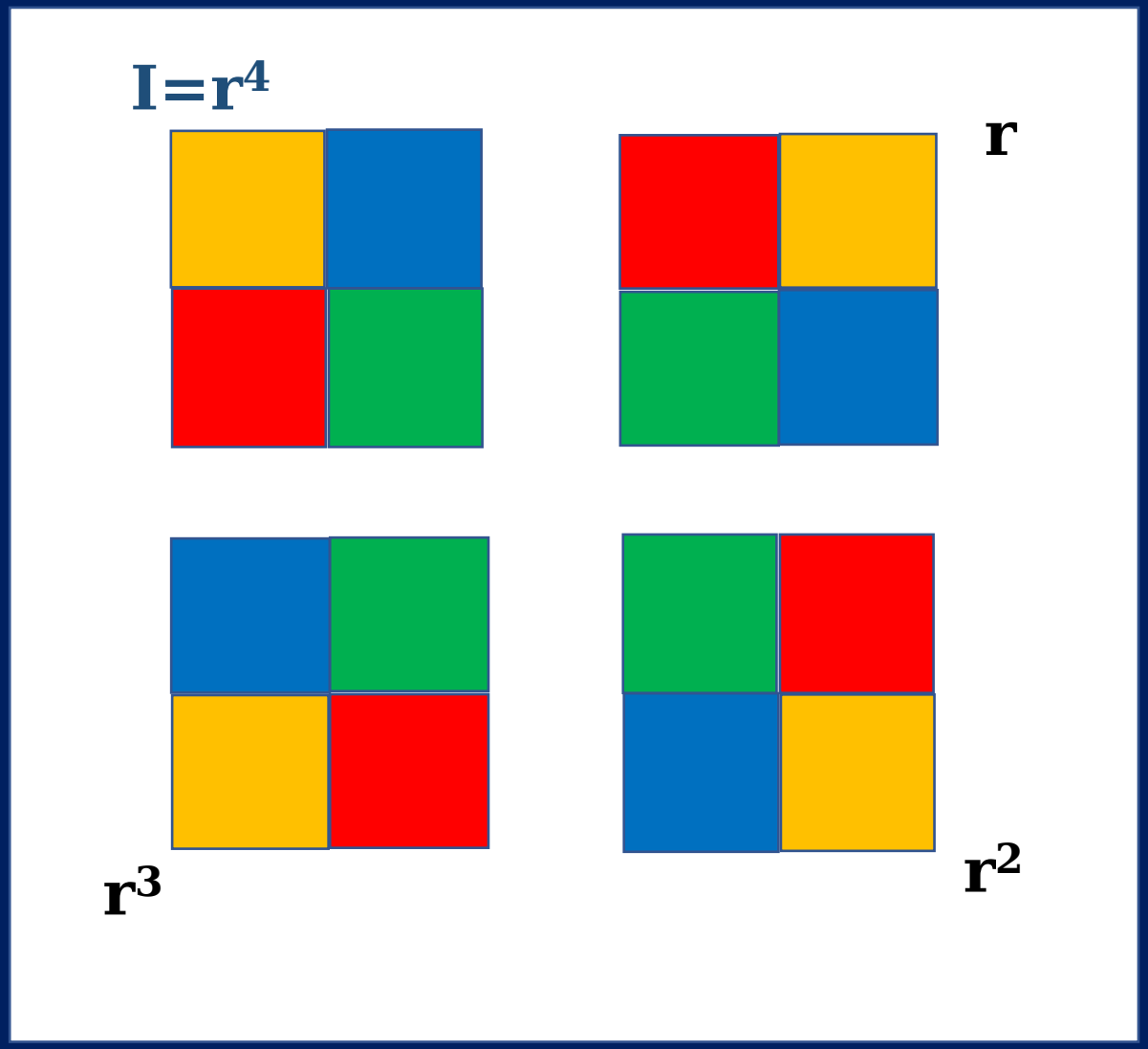
Gruppi e aritmetiche modulari

Rotazioni di un quadrato su se stesso

In quanti modi può essere posizionata una mattonella quadrata in una buca su misura?
In quanti modi può ruotare una quadrato su se stesso?

Chiamando I la posizione iniziale ed r la rotazione di un angolo retto sono possibili 4 rotazioni e quindi 4 posizioni del quadrato:

I r r^2 r^3 [$r^4 = I$]



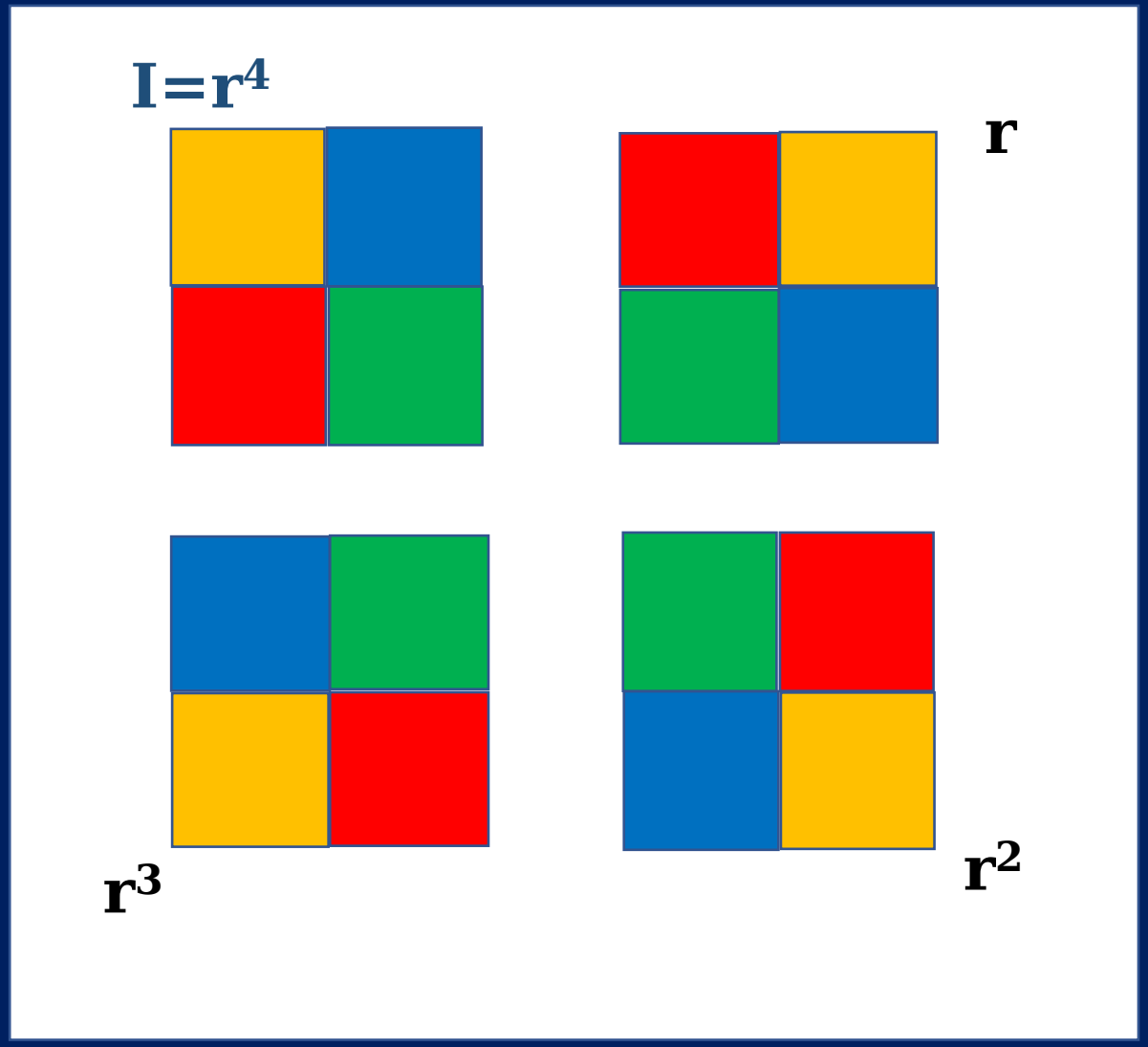
Il gruppo delle rotazioni di un quadrato

Chiusura *Concatenando* le 4 possibili rotazioni si ottiene ancora una delle 4 (L'operazione è **chiusa**)
Es. $r^2\, r^3 = r^5 = r$

Elemento neutro Esiste una rotazione **neutra** I a destra e sinistra
$Ir = rI = r$

Elemento inverso Per ogni rotazione esiste la rotazione **inversa**
Es. l'inverso di r è r^3 infatti
$r\, r^3 = I$

Associatività La concatenazione è **associativa** (xy)z = x)yz)



Un gruppo un po’ più complicato!

Cubo di Rubik: sei facce quadrate che possono ruotare in 4 posizioni diverse.

Facendo un po’ di calcoli le posizioni del cubo 3x3 possibili sono:

$12!\ 8!\ 3^7 2^{10} = 43\ 252\ 003\ 274\ 489\ 856\ 000$

43 252 003 274 489 856 000

Nonostante questo numero enorme tutto il cubo disordinato si può riordinare con 26 mosse; o in tempi inferiori ai 5 secondi!

Tavola pitagorica delle rotazioni

L’ insieme delle quattro rotazioni:

$R = \{I, r, r^2, r^3\}$

e l’operazione di concatenazione costituiscono un **gruppo**, che può rappresentarsi con una tavola pitagorica

Interpretando il tutto come somma di rotazioni di angoli retti si ottiene un gruppo sull’insieme {0, 1, 2, 3} e la somma di rotazioni.
La sua tavola pitagorica è quella a lato, ed è quella di un’aritmetica modulo 4. Per esempio 2 + 3 = 1 perché ruotare di 2 retti e poi di 3 retti, equivale a ruotare di 1 retto.

I due gruppi si dicono **isomorfi** nel senso che hanno la stessa identica struttura, sono quindi rappresentazioni di uno stesso **gruppo astratto**.

	I	r	r2	r3
I	I	r	r2	r3
r	r	r2	r3	I
r2	r2	r3	I	r
r3	r3	I	r	r2

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Ma c’è un’aritmetica ancora più piccola

- $\Phi = \{0, 1\}$

La più piccola aritmetica modulare, è quella con due soli numeri, 0 e 1.

Ci sono solo 4 addizioni possibili:

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

L’operazione inversa, sottrazione modulo 2, coincide con l’addizione:

$$0 - 0 = 0$$
$$0 - 1 = 1$$
$$1 - 0 = 1$$
$$1 - 1 = 0$$

$\oplus$ 2	0	1
0	0	1
1	1	0

Equivalente logico: lo XOR (aut aut)

L’addizione modulo 2 equivale a un connettivo logico tra due proposizioni, oggi chiamato XOR (eXclusive OR) ed equivalente al latino

AUT AUT

o l’una o l’altra ma non tutte e due.

V aut V = F

V aut F = V

F aut V = V

F aut F = F

XOR	F	V
F	F	V
V	V	F

Se dico:
O piove o nevica
?
?
?
?
Mento o dico la verità?

Aritmetiche modulari nelle cifre antiche e moderne

Crittografia antica : prima del medio evo
Crittografia classica: dal secolo XV (carta e penna comunicazioni lente)
Crittografia moderna: dal XIX secolo (telegrafo, radio, macchine)
Crittografia contemporanea: dopo il 1970 (computer)

Atbash la cifra più antica del mondo?

Nella Bibbia si accenna a un modo cifrato per scrivere il nome di Dio, usando l'alfabeto ebraico

		0123456789 … 19
p:	lettera chiara	ABCDEFGHILMNOPQRSTVX
c:	lettera cifrata	**XVTSRQPONMLIHGFEDCBA**

In fondo basterebbe
La lista dimezzata:

ABCDEFGHIL	ATBASH
XVTSRQPONM	XCVTDO

Alfabeto dimezzato, detto anche
lista involutoria o reciproca

Matematicamente:

$p + c = 19$

$p = 19 - c \quad c = 19 - p$
$p = 19 - (19 - p) = p$

L'operazione di cifra coincide con quella di decifra

Atbash la prima lista involutoria?

ABCDEFGHIL
XVTSRQPONM

SCESEMOSEDALSINAI
DTRDRLHDRSXMDNIXN

```
function Atbash(testo){
   cifrato = ‘’;
   foreach(testo as lettera){
        cifrato .= chr(19-ord(lettera));
   }
   return cifrato
}
```

```
    19-
V   16
B    3
```

È superfluo specificare il modulo 20

La funzione vale sia come cifra che come decifra.
Comodità operativa a costo di una riduzione della sicurezza

Cesare scrive in cifra (*Svetonio-Vita di Cesare § 56*)

Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, ***id est D pro A et perinde reliquas commutet***.

Augusto scrive in cifra (*Svetonio-Vita di Augusto § 88*)

Quotiens autem per notas scribit, ***B pro A, C pro B ac deinceps eadem ratione sequentis litteras ponit; pro X autem duplex A.***

Alfabeto latino antico

Lettera chiara	ABCDE FGHIL MNOPQ RSTVX
Lettera cifrata	DEFGH ILMNO PQRST VXABC

Il gruppo delle cifre di Cesare

Oggi con il nome di *cifra di Cesare* si intende una che cifra una lettera chiara con una spostata di *k* lettere avanti nell'alfabeto; per k = 1 si ha la cifra di Augusto, per k=3 la cifra di Cesare. Usando l'alfabeto internazionale a 26 lettere di oggi, abbiamo un insieme di 26 possibili cifrari di Cesare. Notevole che:

1. Esiste una cifra di Cesare neutra, quella con scarto k=0 (o k=26!!)
2. Componendo due cifre di Cesare (nel senso di cifrare due volte, prima con scarto ***h***, la seconda con scarto ***i***) si ottiene ancora una cifra di Cesare.
3. Per ogni cifra di Cesare ne esiste una inversa che composta con la prima dà la cifra neutra; per esempio se la prima ha scarto 3 la inversa avrà scarto 23, e in tutto sono 26, con il che si torna alla cifra neutra.
4. Vale la proprietà associativa.

E quindi l'insieme delle cifre di Cesare ha una struttura di gruppo.

La cifra di Cesare/Augusto è un’addizione modulo 20

Se Atbash si riduce a una sottrazione, Cesare si riduce a un'addizione modulo 20, usando gli ordinali delle singole lettere (A = 0; B =1 …X = 19):

$$c \equiv p + k \pmod{20}$$

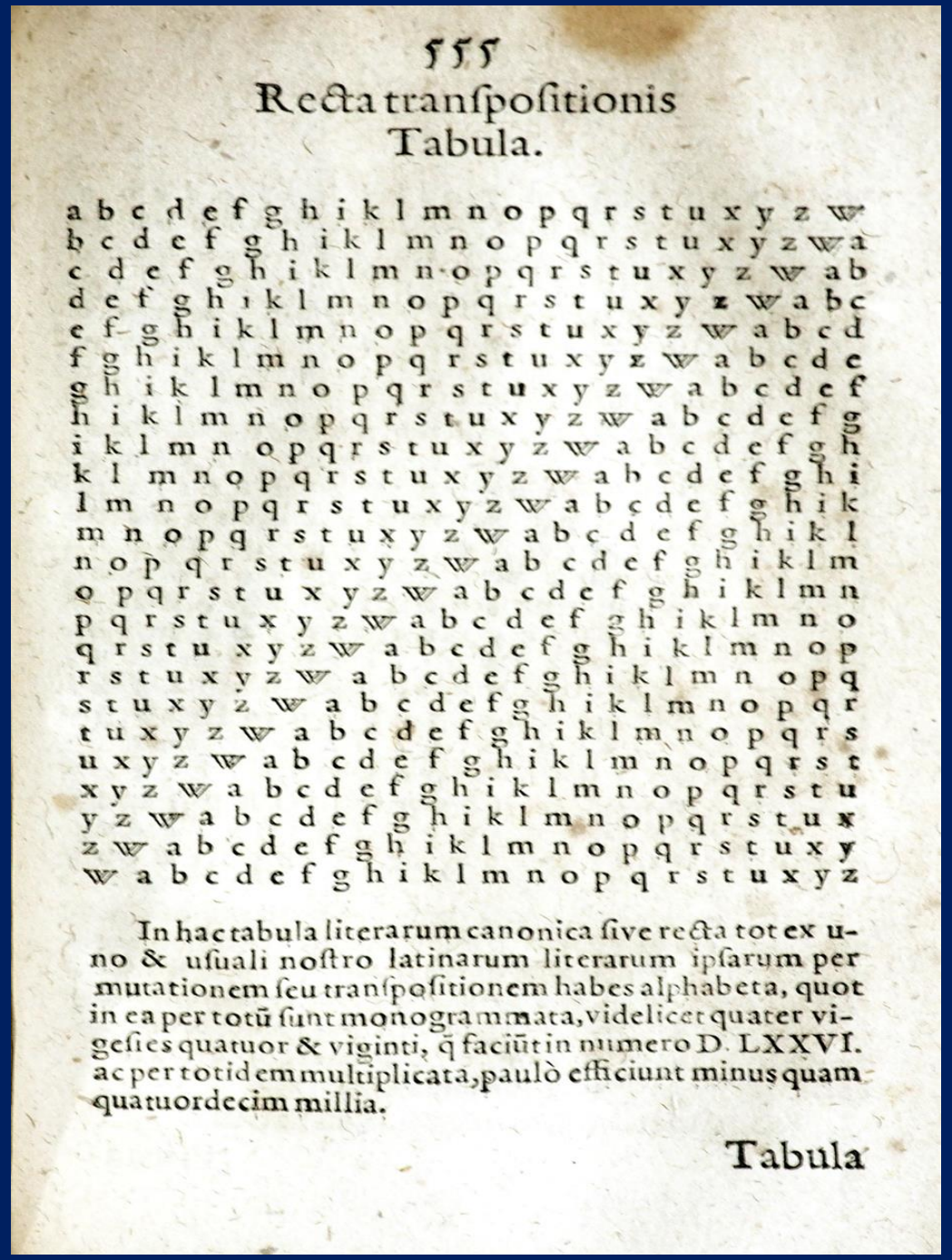
$$c \equiv p + k \pmod{N}$$

Dove

c = lettera del testo cifrato
p = lettera del testo chiaro
k = chiave (3 per Cesare, 1 per Augusto)
N = numerosità alfabeto

1507 La recta tabula dell'abate Tritemio

La ***recta tabula*** dell'Abate Tritemio è considerata il primo esempio di cifra polialfabetica nel senso che non usava sempre lo stesso alfabeto, ma anzi lo cambiava ad ogni passo.
Ogni colonna (o riga) della tabella è una cifra di Cesare, la prima a scarto **zero**, neutra; la seconda ha scarto **uno** come quella di Augusto ecc.ecc.
Ovviamente la sicurezza di questa cifra si basa essenzialmente sulla non conoscenza del metodo, chiunque avesse comprato il libro non avrebbe poi alcuna difficoltà a decrittare messaggi di questo tipo.



555

Recta tranſpoſitionis
Tabula.

a b c d e f g h i k l m n o p q r s t u x y z w
b c d e f g h i k l m n o p q r s t u x y z w a
c d e f g h i k l m n o p q r s t u x y z w a b
d e f g h i k l m n o p q r s t u x y z w a b c
e f g h i k l m n o p q r s t u x y z w a b c d
f g h i k l m n o p q r s t u x y z w a b c d e
g h i k l m n o p q r s t u x y z w a b c d e f
h i k l m n o p q r s t u x y z w a b c d e f g
i k l m n o p q r s t u x y z w a b c d e f g h
k l m n o p q r s t u x y z w a b c d e f g h i
l m n o p q r s t u x y z w a b c d e f g h i k
m n o p q r s t u x y z w a b c d e f g h i k l
n o p q r s t u x y z w a b c d e f g h i k l m
o p q r s t u x y z w a b c d e f g h i k l m n
p q r s t u x y z w a b c d e f g h i k l m n o
q r s t u x y z w a b c d e f g h i k l m n o p
r s t u x y z w a b c d e f g h i k l m n o p q
s t u x y z w a b c d e f g h i k l m n o p q r
t u x y z w a b c d e f g h i k l m n o p q r s
u x y z w a b c d e f g h i k l m n o p q r s t
x y z w a b c d e f g h i k l m n o p q r s t u
y z w a b c d e f g h i k l m n o p q r s t u x
z w a b c d e f g h i k l m n o p q r s t u x y
w a b c d e f g h i k l m n o p q r s t u x y z

In hac tabula literarum canonica ſive recta tot ex uno & uſuali noſtro latinarum literarum ipſarum permutationem ſeu tranſpoſitionem habes alphabeta, quot in ea per totū ſunt monogrammata, videlicet quater vigeſies quatuor & viginti, q̄ faciūt in numero D. LXXVI. ac per totidem multiplicata, paulò efficiunt minus quam quatuordecim millia.

Tabula

La recta tabula esempio

Matematicamente si riduce a una serie di cifrari di Cesare a passo variabile (crescente con A=0, B=1.. Z=22, W=23):

Colonna Lettera	Spost.	addizione	
A	0	$c = p \pmod{24}$	
B	1	$c = p+1 \ (mod\ 24)$	Augusto
C	2	$c = p+2 \ (mod\ 24)$	
D	3	$c = p+3 \ (mod\ 24)$	Cesare

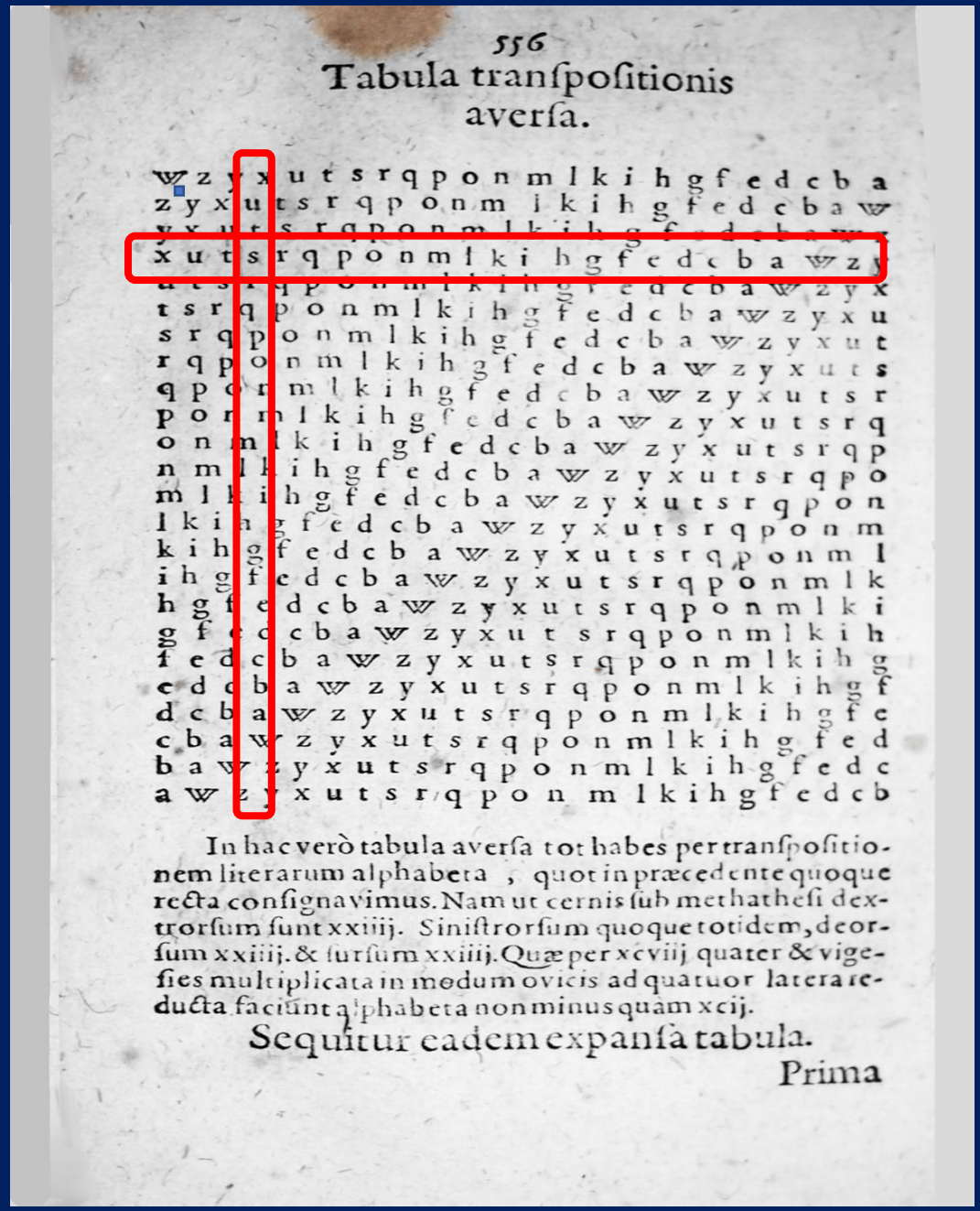
Non è affatto più sicura di Cesare, la sicurezza si basa sulla conoscenza del metodo (ossia del libro ..)

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

La tabula aversa dell'abate Tritemio

Matematicamente si riduce a una serie di liste involutorie tipo Atbash:

Colonna Lettera	Spost.	addizione	
W	23	$c = 23 - p$	Atbash
Z	22	$c = 22 - p \pmod{24}$	
Y	21	$c = 21 - p \pmod{24}$	
X	20	$c = 20 - p \pmod{24}$	



556

Tabula tranſpoſitionis averſa.

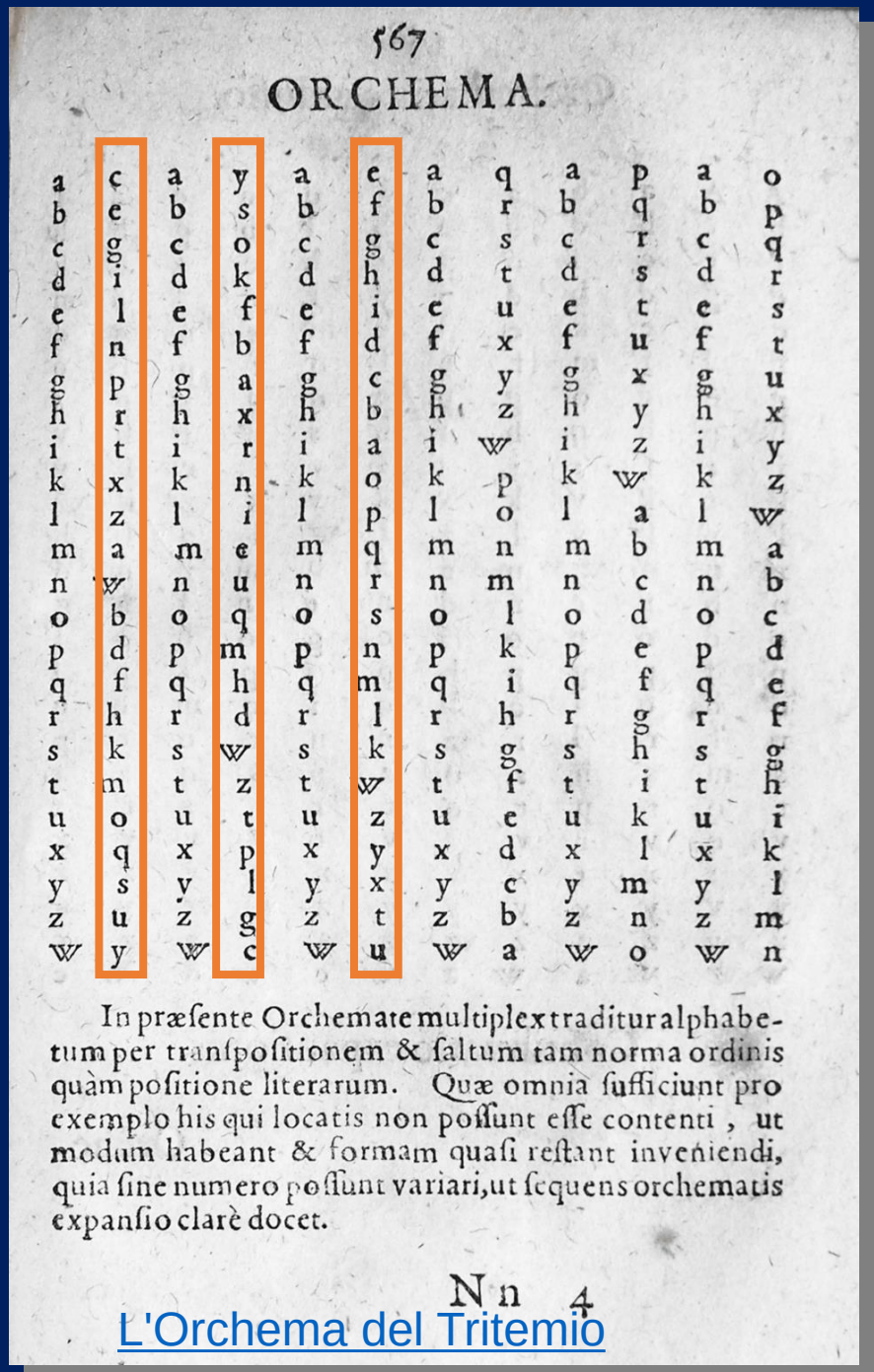
In hac verò tabula averſa tot habes per tranſpoſitionem literarum alphabeta, quot in præcedente quoque recta conſignavimus. Nam ut cernis ſub methathesi dextrorſum ſunt xxiiij. Siniſtrorſum quoque totidem, deorſum xxiiij. & ſurſum xxiiij. Quæ per xcviij quater & vigeſies multiplicata in modum ovicis ad quatuor latera reducta faciunt alphabeta non minus quam xcij.

Sequitur eadem expanſa tabula.

Prima

La Orchema dell'abate Tritemio

Tritemio si rendeva probabilmente conto che la ***recta tabula*** non era tanto sicura, in quanto troppo regolare.
Poche pagine più avanti, infatti, propone una cifra diversa che chiama ***orchema***, dal greco ***ορχημα*** che vuol dire ballo, danza.
Insomma le lettere invece di presentarsi in file ordinate, danzano e ballano scambiandosi di posto in vari modi, proprio come ballerine.
Modi che per la verità sono ancora un po' troppo ordinati ..
In sostanza ad ogni passo si usa un alfabeto diversamente ordinato.
Non c'è formula matematica ... e questo in crittografia è un bene ...



567

ORCHEMA.

In præſente Orchemate multiplex traditur alphabetum per tranſpoſitionem & ſaltum tam norma ordinis quàm poſitione literarum. Quæ omnia ſufficiunt pro exemplo his qui locatis non poſſunt eſſe contenti, ut modum habeant & formam quaſi reſtant inveniendi, quia ſine numero poſſunt variari, ut ſequens orchematis expanſio clarè docet.

Nn 4

L'Orchema del Tritemio

La cifra zero di G. B. Bellaso ritrovata a Venezia

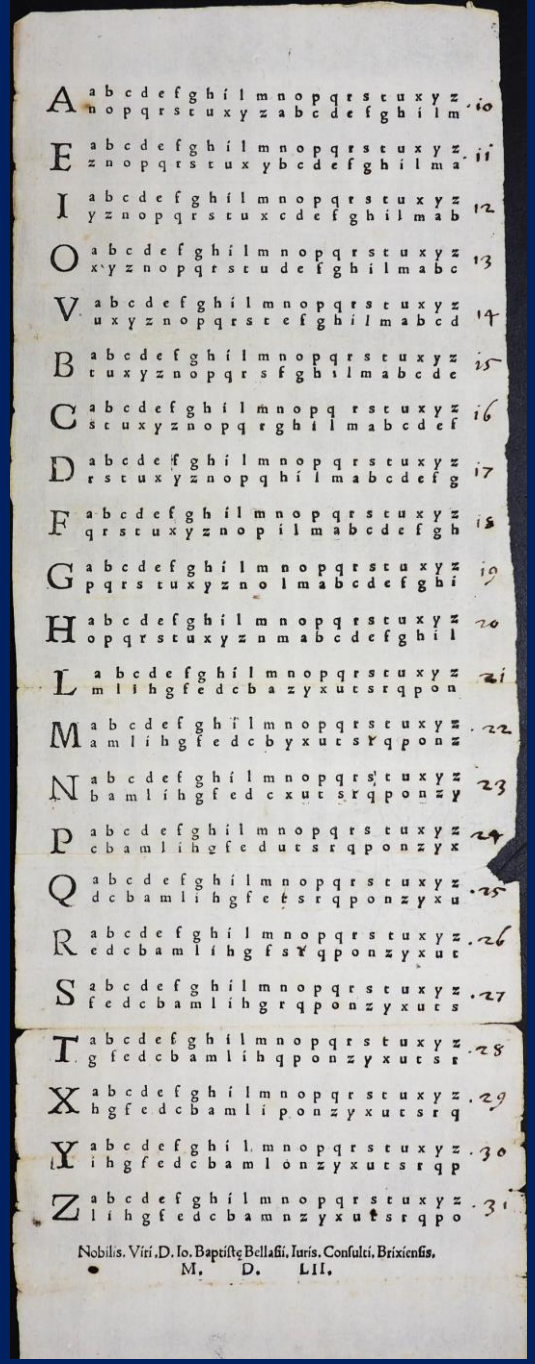
Giovanni Battista Bellaso pubblicò nel 1553 una sua cifra, scrivendo che l'anno precedente aveva distribuita ad amici e conoscenti una prima tavola della quale questa era un miglioramento.

Questa tavola del 1552 della quale si erano perse le tracce, è stata ritrovata da chi scrive nel novembre 2018 tra le carte dell'Archivio di Stato di Venezia.

La tavola equivale in buona parte alla tavola *aversa* del Tritemio, consistendo di 22 liste reciproche scritte però in un ordine diverso.

La cifra zero di G.B.Bellaso 1552

ASVe Cifre, chiavi e scontri di cifra, busta 3.



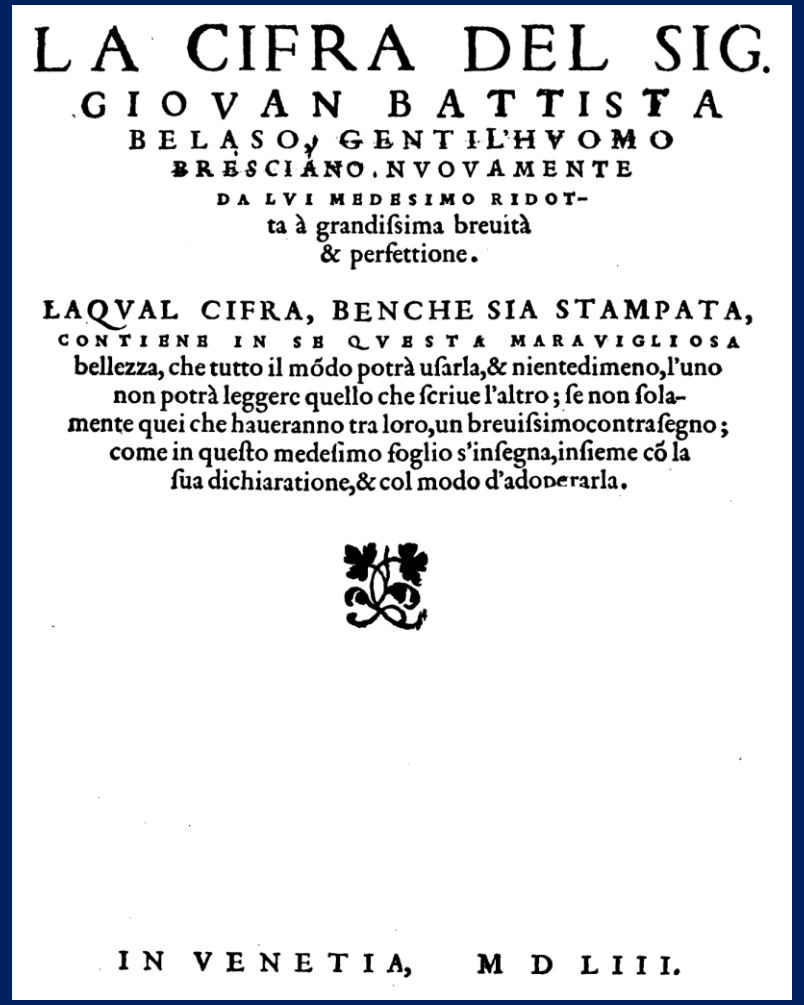
Le cifre di G. B. Bellaso

La vera grande invenzione del Bellaso è quella di un ***contrasegno*** una parola o versetto facile da ricordare a memoria da usare come **chiave** per la cifratura usando la tavola qui accanto: si cercherà la lettera della chiave nella colonna a sinistra, poi quella del chiaro nella lista a destra; la lettera sotto o sopra sarà la cifra.

```
Chiave   BRESCIABRESCIABRESCI
Chiaro   ARMATATVRCHESCAPARTE
Cifrato  TOYFBYGBOOLYHPTQZNBP
```

Bellaso sottolinea così, sin dalla copertina questa novità:

La qual cifra, benche sia stampata, contiene in se questa merauigliosa bellezza, che tutto il mondo potrà usarla, & nientedimeno, l'uno non potrà leggere quello che scriue l'altro, se non solamente quei che haueranno tra loro un breuissimo contrasegno […]



LA CIFRA DEL SIG.
GIOVAN BATTISTA
BELASO, GENTILHVOMO
BRESCIANO, NVOVAMENTE
DA LVI MEDESIMO RIDOT-
ta à grandiſsima breuità
& perfettione.

LAQVAL CIFRA, BENCHE SIA STAMPATA,
CONTIENE IN SE QVESTA MARAVIGLIOSA
bellezza, che tutto il mõdo potrà uſarla,& nientedimeno,l'uno
non potrà leggere quello che ſcriue l'altro; ſe non ſola-
mente quei che haueranno tra loro,un breuiſsimocontraſegno;
come in queſto medeſimo foglio s'inſegna,inſieme cõ la
ſua dichiaratione,& col modo d'adoperarla.

IN VENETIA, M D LIII.

[La cifra zero di G.B.Bellaso 1552]

[La cifra del 1553 di G.B. Bellaso]

Cifrare con il contrasegno di Bellaso (1553)

La cifra del 1553 non è altro che quella dell'anno prima con la lista involutoria compattata e le lettere raggruppate.

Usando come contrasegno BRESCIA il messaggio ***Armata turchesca parte*** si cifra così:

```
Chiave   BRESCIABRESCIABRESCI
Chiaro   ARMATATVRCHESCAPARTE
Cifrato  NBYPAYGHBOYZHPNMZCQP
```

Bellaso è per questo considerato il padre, o forse sarebbe meglio dire il nonno, della ***password***

[La cifra del 1553 di G.B. Bellaso]

A B	ABCDEFGHILM NOPQRSTVXYZ
C D	ABCDEFGHILM TVXYZNOPQRS
E F	ABCDEFGHILM ZNOPQRSTVXY
G H	ABCDEFGHILM STVXYZNOPQR
I L	ABCDEFGHILM YZNOPQRSTVX
M N	ABCDEFGHILM RSTVXYZNOPQ
O P	ABCDEFGHILM XYZNOPQRSTV
Q R	ABCDEFGHILM QRSTVXYZNOP
S T	ABCDEFGHILM PQRSTVXYZNO
V X	ABCDEFGHILM VXYZNOPQRST
Y Z	ABCDEFGHILM OPQRSTVXYZN

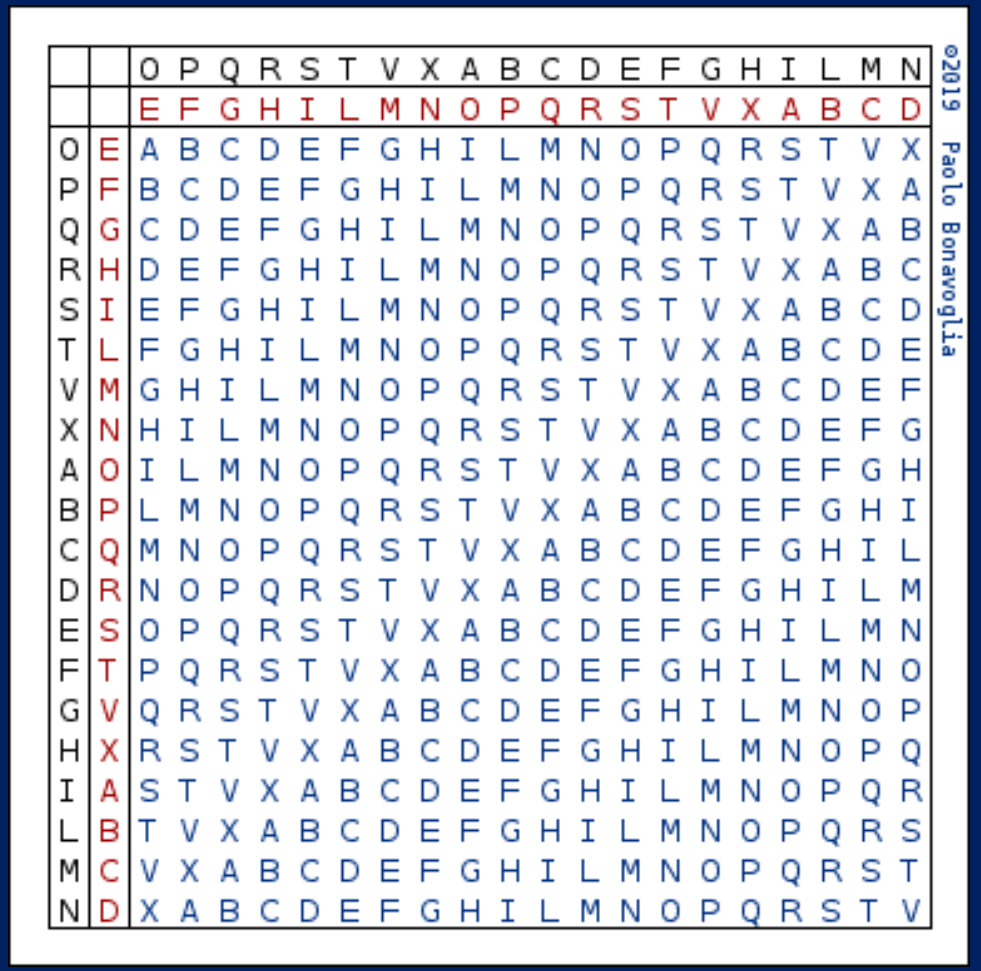
La Tavola di Vigènere

Blaise de Vigenère pubblicò nel 1586 un trattato di cifre nel quale proponeva una cifra che usava la ***recta tabula*** dell'abate Tritemio in combinazione con la parola chiave (***contrasegno***) proposta da G. B. Bellaso nella sua cifra del 1553, che Vigenère ripubblica in formato 20x20 usando l'alfabeto latino classico.

Oggi per «cifra di Vigenère» si intende di solito una cifra adattata all'alfabeto odierno a 26 lettere e senza le permutazioni previste da Vigenère.

Questa cifra, considerata per molto tempo indecifrabile in quanto confonde l'analisi delle frequenze, in realtà è debolissima per parole chiave brevi e da dizionario, una volta trovata la lunghezza N della chiave si riduce a N cifrati di Cesare di facile soluzione.

Molto diverso sarebbe il discorso se N fosse molto grande, e soprattutto se la chiave è una sequenza casuale di lettere o numeri. Ne riparlereo

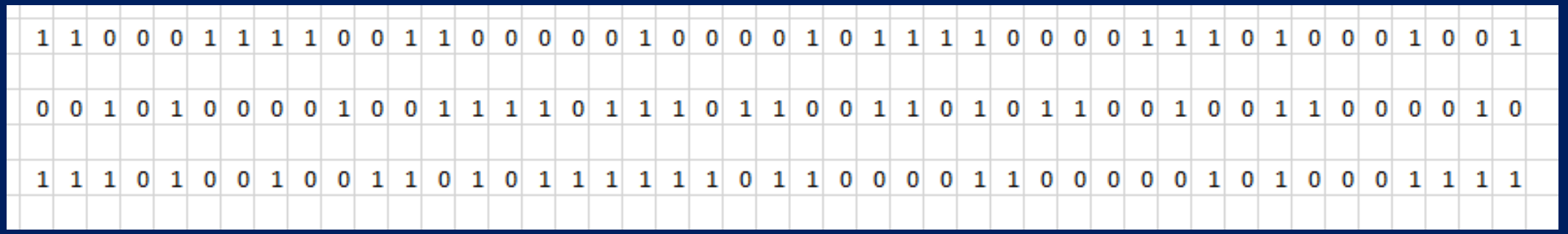


		O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N
		E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D
O	E	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X
P	F	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A
Q	G	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B
R	H	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C
S	I	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D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

La tavola di Vigenère

Ma cosa significa casuale?

Sequenze casuali



Quando possiamo dire che una sequenza è realmente casuale?

Quando il modo più breve per definirla … consiste nell’elencarla

Se invece esiste un algoritmo per generarla più breve della sequenza, allora ovviamente non è realmente casuale,

Tentativi di definire la casualità

- Casuale = imprevedibile.

- Conoscere i primi ***n*** termini di una sequenza non dà alcuna informazione sul termine ***n+1.***

- Casuale = indescrivibile.

- La miglior descrizione della sequenza è la sequenza stessa.

- Casuale = incomprimibile.

- Non esiste un algoritmo per generare la sequenza che sia più breve della sequenza stessa (Kolmogorov).

Come generare sequenze casuali

Metodi hardware

Sono metodi meccanici: lanciare dadi o monete, estrarre numeri dalla ruota del Lotto; la meccanica è troppo complicata per essere prevedibile. Perfetti ma in genere troppo lenti per produrre lunghe sequenze.

Pseudo-casuali: macchine con rotori

A partire dal 1920 furono create macchine cifranti a rotori; una parte dei rotori girando e facendo girare il rotore vicino producevano una sequenza di lettere o numeri con distribuzione apparentemente casuale, ma inevitabilmente avevano un periodo che doveva essere il più lungo possibile. Quindi erano pseudo-casuali.

Pseudo-casuali: algoritmi software

Destinati a girare sui computer, sono algoritmi che, un po' come i rotori producono sequenze apparentemente casuali, in realtà pseudocasuali.

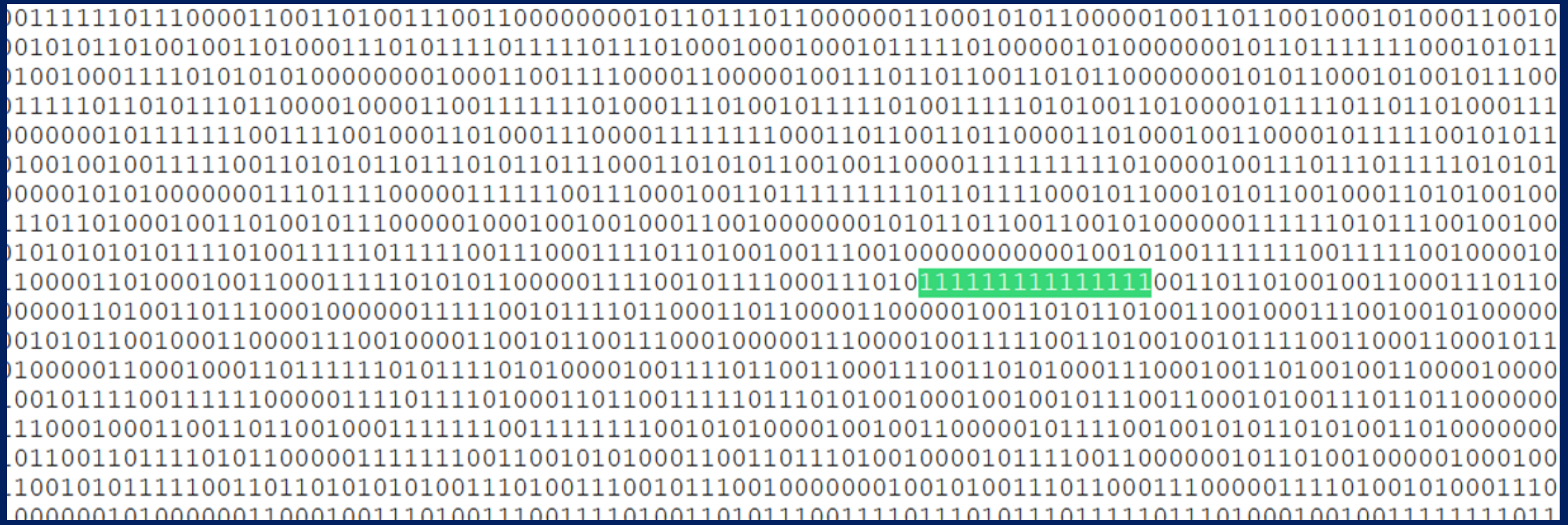
Sequenze casuali

È casuale questa sequenza 111111111111111 ?
(quindici 1 di seguito)?
Dipende dal contesto …

Numeri casuali

Sequenze casuali

È casuale questa sequenza 111111111111111 ?
(quindici 1 di seguito)?
Dipende dal contesto …



Numeri casuali

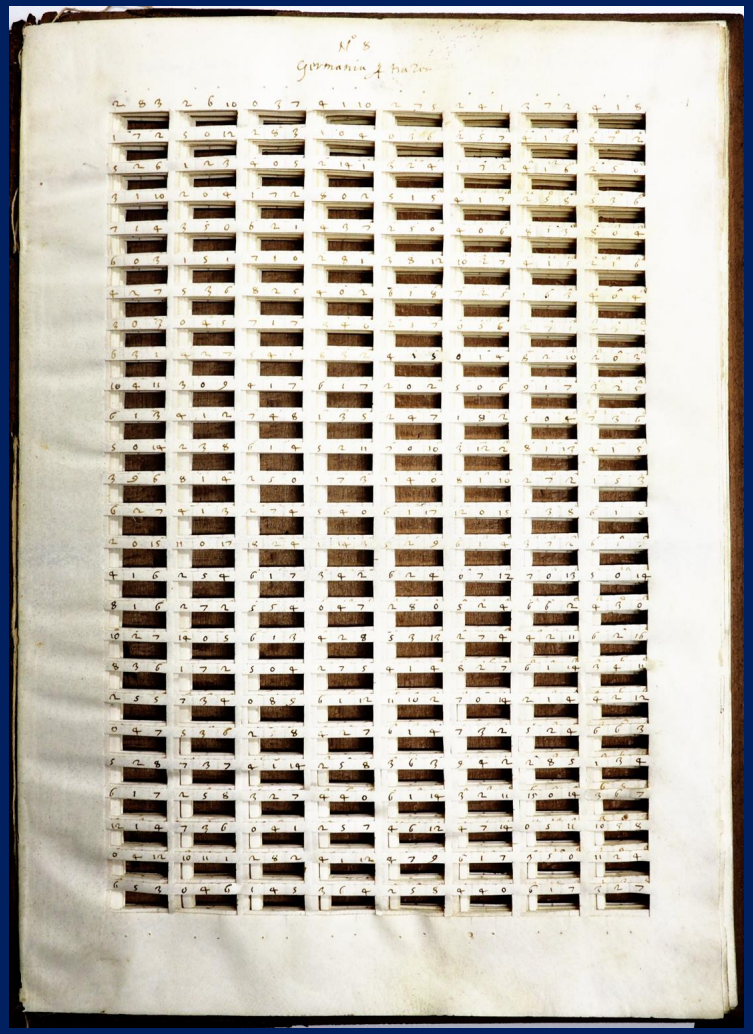
Le grate casuali della cifra delle caselle

La riscoperta della cifra delle caselle di Hieronimo di Franceschi

Quando nel 2018 riuscii a ricostruire il funzionamento la cosa che mi colpì maggiormente fu l'uso della sovra-cifratura, una cifra composta, a dir poco inusuale nel XVI secolo.

Ma in effetti altrettanto inusuale e ben più importante per la sicurezza, è l'uso di una cifra poli-alfabetica con chiave molto lunga, fino a 624 numeri apparente casuali!

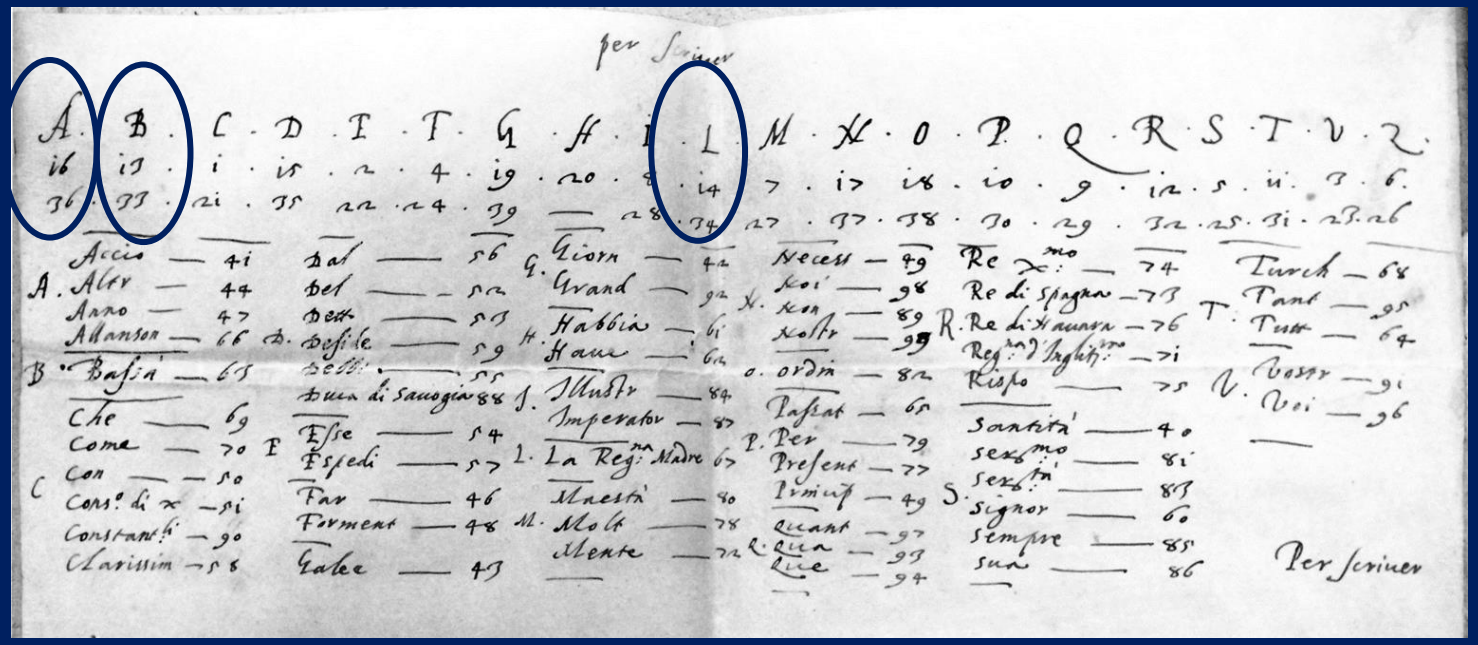
Cifra delle Caselle - Esempio interattivo



ASVe, Cifre, chiavi e scontri di cifra, busta 4 reg. 8

La cifra delle caselle di H. di Franceschi

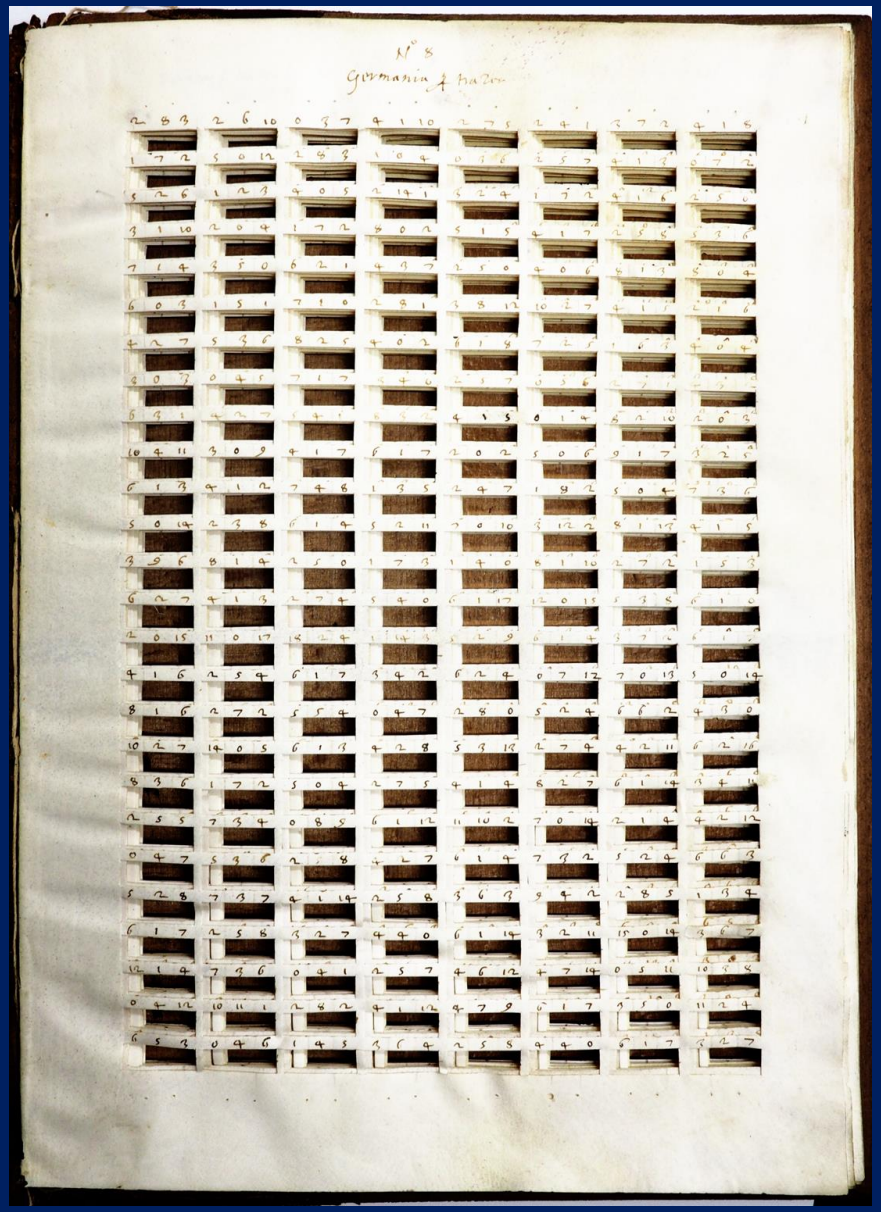
ASVe, Cifre, chiavi e scontri di cifra, b. 3, c. 32



Volendo cifrare ALBA Cifra di ALBA 8 15 10 19

P chiaro	K chiave	C cifrato p-k
A 16 36	8	16-8 = 8
L 14 34	19	14 -19 ? 34-19 = 15
B 13 33	3	13-3 = 10
A 16 36	17	16-17=? 36-17=19

Cifra delle Caselle - Esempio interattivo



Cifrare con le caselle:

Ed ecco uerso noi uenir per naue
un uecchio bianco per antico pelo
gridando guai a uoi anime praue

e	d	e	c	c	o	u	e	r	s	o	noi	u	e	n	i	r	per	n	a	u	e	u	n
2–	15–	2–	1–	1–	18–	3–	2–	12–	5–	18–	98–	3–	2–	17–	8–	12–	79–	17–	16–	3–	2–	3–	17–
2	8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2	4	1	8
0	7	19	19	15	8	3	19	5	1	17	88	1	15	12	6	8	78	14	9	1	18	2	9
u	e	c	c	h	i	o	b	i	a	n	c	o	per	a	n	t	i	c	o	p	e	l	o
3–	2–	1–	1–	20–	8–	18–	13–	8–	16–	17–	1–	18–	79–	16–	17–	11–	8–	1–	18–	10–	2–	14–	18–
1	7	2	5	0	12	2	8	3	1	0	4	0	3	6	2	5	7	4	1	3	0	7	2
2	15	19	16	20	16	16	5	5	15	17	17	18	76	10	15	6	1	17	17	7	2	7	16
g	r	i	d	a	n	d	o	g	u	a	i	a	uoi	a	n	i	m	e	p	r	a	u	e
19–	12–	8–	15–	16–	17–	15–	18–	19–	3–	16–	8–	16–	96–	16–	17–	8–	7–	2–	10–	12–	16–	3–	2–
5	2	6	1	2	3	4	0	5	2	14	1	3	2	4	1	7	2	4	1	6	2	5	0
14	10	2	14	14	14	11	18	14	1	2	7	13	94	12	16	1	5	18	9	6	14	18	2

Cifrato da trasmettere:

```
 0  7 19 19 15  8  3 19  5  1 17 88  1 15 12  6  8 78 14  9  1 18  2  9
 2 15 19 16 20 16 16  5  5 15 17 17 18 76 10 15  6  1 17 17  7  2  7 16
14 10  2 14 14 14 11 18 14  1  2  7 13 94 12 16  1  5 18  9  6 14 18  2
```

Testo chiaro
Cifra A16-36
Grata Germania

Cifra caselle

2	8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2	4	1	8
1	7	2	5	0	12	2	8	3	1	0	4	0	3	6	2	5	7	4	1	3	0	7	2
5	2	6	1	2	3	4	0	5	2	14	1	3	2	4	1	7	2	4	1	6	2	5	0
3	1	10	2	0	4	1	7	2	8	0	2	5	1	5	4	1	7	2	5	8	5	3	6
7	1	4	3	5	0	6	2	1	4	3	7	2	5	0	4	0	6	8	1	3	8	0	4
6	0	3	1	5	1	7	1	0	2	8	1	3	8	12	10	2	7	4	1	5	2	1	6
4	2	7	5	3	6	8	2	5	4	0	2	6	1	8	7	2	5	1	6	3	4	0	4
3	0	3	0	4	5	7	1	7	3	4	0	2	5	7	0	5	6	2	7	1	4	3	2
6	3	1	4	2	7	5	4	1	8	3	2	4	1	5	0	1	4	8	2	10	2	0	3
10	4	11	3	0	9	4	1	7	6	1	7	2	0	2	5	0	6	9	1	7	3	2	5
6	1	3	4	1	2	7	4	8	1	3	5	2	4	7	1	8	2	5	0	4	7	3	6
5	0	14	2	3	8	6	1	4	5	2	11	7	0	10	3	12	2	8	1	13	4	1	5
3	9	6	8	1	4	2	5	0	1	7	3	1	4	0	8	1	10	2	7	2	1	5	3
6	2	7	4	1	3	2	7	4	5	4	0	6	1	17	12	0	15	5	3	8	6	1	0
2	0	15	11	0	17	18	2	4	1	14	3	5	2	9	6	1	4	3	7	2	6	1	7
4	1	6	2	5	4	6	1	7	3	4	2	6	2	4	0	7	12	7	0	13	5	0	14
8	1	6	2	7	2	5	5	4	0	4	7	2	8	0	5	2	4	6	6	2	4	3	0
10	2	7	14	0	5	6	1	3	4	2	8	5	3	13	2	7	4	4	2	11	6	2	16
8	3	6	1	7	2	5	0	4	2	7	5	4	1	4	8	2	7	6	1	14	3	4	11
2	5	5	7	3	4	0	8	9	6	1	12	11	10	2	7	0	14	2	1	4	4	2	12
0	4	7	5	3	6	2	5	8	4	2	7	6	1	4	7	3	2	5	2	4	6	6	3
5	2	8	7	3	7	4	1	14	2	5	8	3	6	3	9	4	2	2	8	5	1	3	4
6	1	7	2	5	8	3	2	7	4	4	0	6	1	14	3	2	11	15	0	14	3	6	7
12	1	4	7	3	6	0	4	1	2	5	7	4	6	12	4	7	14	0	5	11	10	3	8
0	4	12	10	11	1	2	8	2	4	1	12	4	7	9	6	1	7	3	5	0	11	2	4
6	5	3	0	4	6	1	4	5	3	6	4	2	5	8	4	4	0	6	1	7	3	2	7

Cifra delle Caselle - Esempio interattivo

Quanto erano sicure le caselle?

La critica di Pietro Partenio

Partenio nel 1596 alla fine della disputa con Franceschi scrisse una lunga autodifesa al Consiglio di Dieci accanendosi contro la cifra delle caselle del Franceschi; i punti principali sono:

1. La prima cifra A 16-36 è poco più che un monoalfabetico, si cifra per singole lettere, e può essere forzata da un qualsiasi cifrista con un minimo di esperienza.
2. Le grate 24x26 con un massimo di 624 numeri sono sicurissime, ma possono essere rubate o copiate.
3. In conclusione, la cifra delle caselle vale poco più di quelle del Tritemio, vecchie ormai di 90 anni

Cifra delle Caselle - Esempio interattivo

Aveva ragione Partenio?

1. Verissimo, la prima cifra è debole e paradossalmente se ne potrebbe fare a meno.
2. Partenio deve ammettere che le grate 24x26 sono fortissime, praticamente indecifrabili. Si aggrappa al pericolo di furto o copiatura che è altro discorso ed esisteva anche per i nomenclatori. Più fattibile forse era corrompere un segretario.
3. Confondere la cifra delle caselle con la recta tabula del Tritemio può essere solo il frutto della tensione del momento. A meno che non si riferisse all'Orchema.

La vera forza delle caselle.

La vera forza della cifra delle caselle era nelle grate, che realizzavano un sistema polialfabetico a chiave molto **lunga** e **disordinata**. Si tratta di un autentico «Unicum» nella storia della crittografia, anche per il ricorso all'aritmetica, la cifratura richiedeva una sottrazione e la decifratura un'addizione.
La ben nota cifra di Vigenère equivaleva a un'addizione modulo 20, ma Vigenère non sembra aver realizzato la cosa, utilizzando una tavola equivalente a quella del Tritemio, per combinare facilmente senza calcoli testo chiaro e cifrato. E raccomanda l'uso di chiavi brevi e facili a ricordare.

L'importanza di questi due fattori, lunghezza della chiave e disordine non sembra fossero tanto chiari ai cifristi del Rinascimento. Anche Bellaso nel suo primo opuscolo del 1553 scrive che la chiave, che lui chiama *contrasegno*, può anche essere *breuissimo*, non è molto importante, ma poi nel secondo opuscolo raccomanda l'uso di chiavi più lunghe, usando versetti o parti di un poema che si ricordano a memoria, che però non sono affatto casuali.

Certo le grate erano lunghissime, ma non infinite e venivano riutilizzate ad ogni pagina.

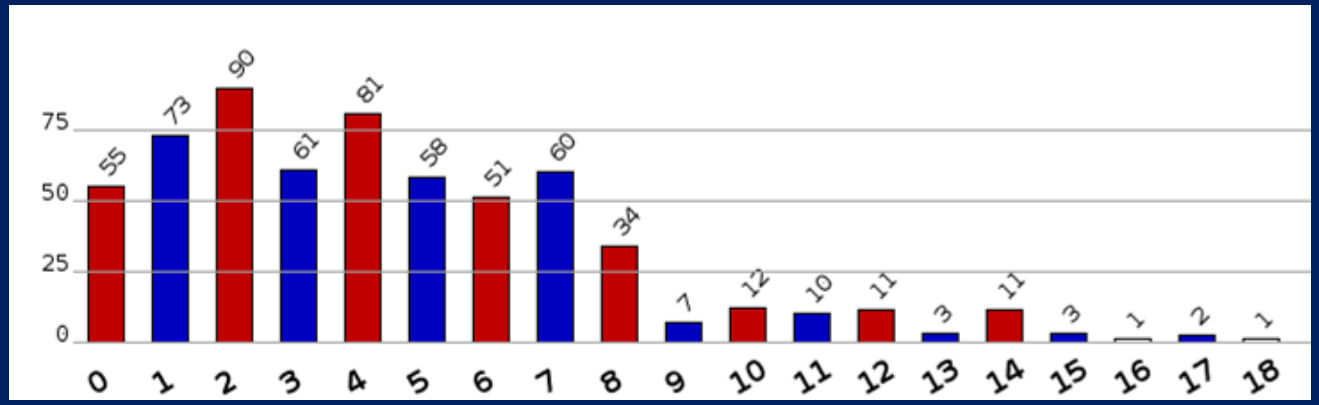
Resta l'altro punto da chiarire: quanto erano disordinate le chiavi, ossia le grate?

Cifra delle Caselle - Esempio interattivo

Quanto erano disordinate le grate?

Grata Germania
(Sacro Romano Impero, Praga, Vienna)

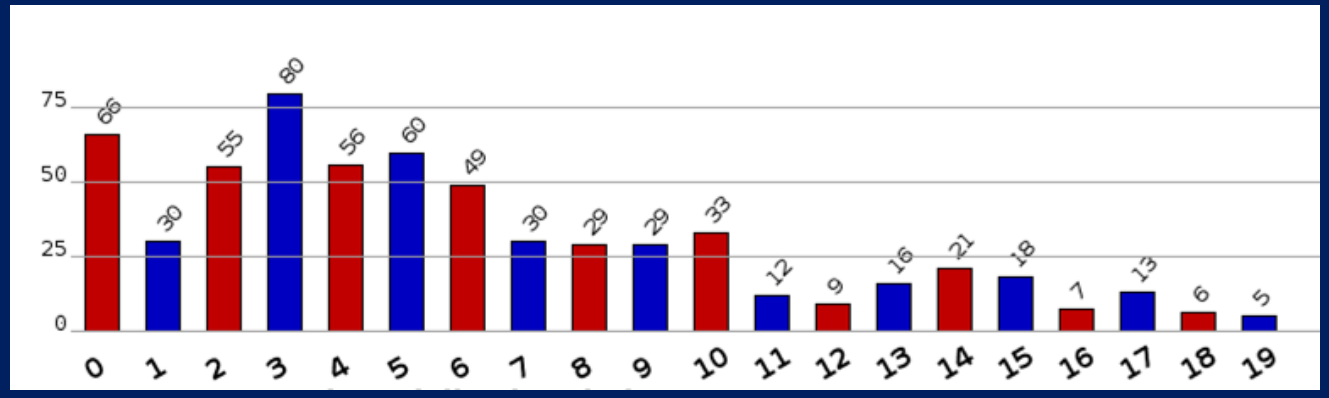
E’ disordinata o no?
26x24=624
Chiave di 624 numeri



2	8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2	4	1	8
1	7	2	5	0	12	2	8	3	1	0	4	0	3	6	2	5	7	4	1	3	0	7	2
5	2	6	1	2	3	4	0	5	2	14	1	3	2	4	1	7	2	4	1	6	2	5	0
3	1	10	2	0	4	1	7	2	8	0	2	5	1	5	4	1	7	2	5	8	5	3	6
7	1	4	3	5	0	6	2	1	4	3	7	2	5	0	4	0	6	8	1	3	8	0	4
6	0	3	1	5	1	7	1	0	2	8	1	3	8	12	10	2	7	4	1	5	2	1	6
4	2	7	5	3	6	8	2	5	4	0	2	6	1	8	7	2	5	1	6	3	4	0	4
3	0	3	0	4	5	7	1	7	3	4	0	2	5	7	0	5	6	2	7	1	4	3	2
6	3	1	4	2	7	5	4	1	8	3	2	4	1	5	0	1	4	8	2	10	2	0	3
10	4	11	3	0	9	4	1	7	6	1	7	2	0	2	5	0	6	9	1	7	3	2	5
6	1	3	4	1	2	7	4	8	1	3	5	2	4	7	1	8	2	5	0	4	7	3	6
5	0	14	2	3	8	6	1	4	5	2	11	7	0	10	3	12	2	8	1	13	4	1	5
3	9	6	8	1	4	2	5	0	1	7	3	1	4	0	8	1	10	2	7	2	1	5	3
6	2	7	4	1	3	2	7	4	5	4	0	6	1	17	12	0	15	5	3	8	6	1	0
2	0	15	11	0	17	18	2	4	1	14	3	5	2	9	6	1	4	3	7	2	6	1	7
4	1	6	2	5	4	6	1	7	3	4	2	6	2	4	0	7	12	7	0	13	5	0	14
8	1	6	2	7	2	5	5	4	0	4	7	2	8	0	5	2	4	6	6	2	4	3	0
10	2	7	14	0	5	6	1	3	4	2	8	5	3	13	2	7	4	4	2	11	6	2	16
8	3	6	1	7	2	5	0	4	2	7	5	4	1	4	8	2	7	6	1	14	3	4	11
2	5	5	7	3	4	0	8	9	6	1	12	11	10	2	7	0	14	2	1	4	4	2	12
0	4	7	5	3	6	2	5	8	4	2	7	6	1	4	7	3	2	5	2	4	6	6	3
5	2	8	7	3	7	4	1	14	2	5	8	3	6	3	9	4	2	2	8	5	1	3	4
6	1	7	2	5	8	3	2	7	4	4	0	6	1	14	3	2	11	15	0	14	3	6	7
12	1	4	7	3	6	0	4	1	2	5	7	4	6	12	4	7	14	0	5	11	10	3	8
0	4	12	10	11	1	2	8	2	4	1	12	4	7	9	6	1	7	3	5	0	11	2	4
6	5	3	0	4	6	1	4	5	3	6	4	2	5	8	4	4	0	6	1	7	3	2	7

Grata Costantinopoli
(Impero Ottomano)

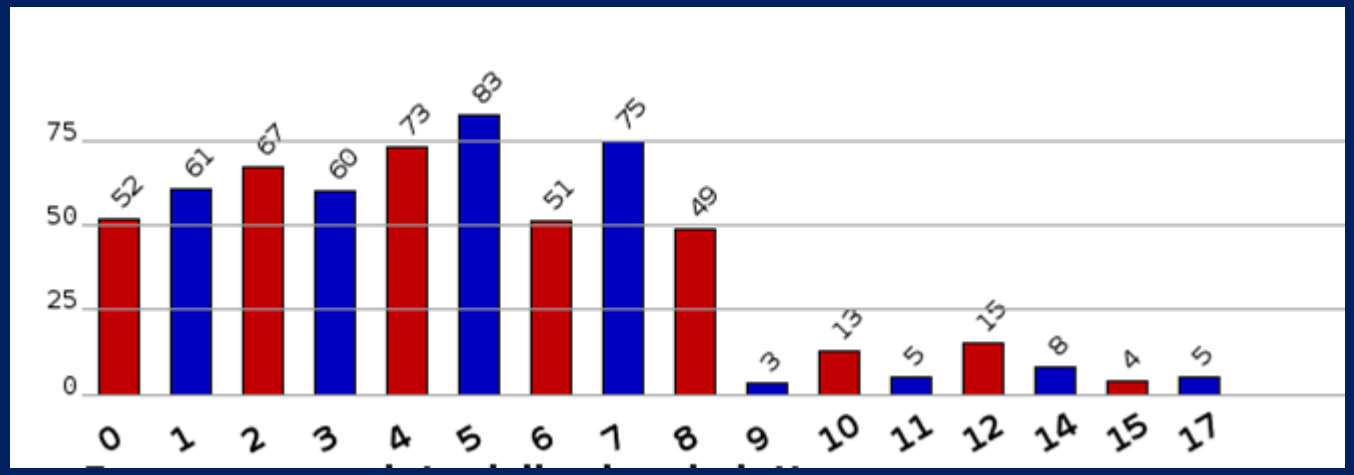
E’ disordinata o no?
26x24=624
Chiave di 624 numeri



3	5	7	8	0	6	4	16	5	17	7	5	3	0	1	9	3	0	18	15	11	4	8	11
10	3	1	5	9	7	8	3	2	17	12	8	19	4	1	2	6	8	10	2	3	6	9	1
5	7	6	0	7	0	5	14	6	3	7	2	4	15	6	13	0	7	9	13	4	10	7	0
19	5	3	14	3	5	6	2	18	4	1	0	7	11	9	6	3	8	11	9	1	4	7	9
7	14	2	15	5	4	2	0	15	10	4	9	6	8	2	4	3	6	1	10	9	0	3	2
3	0	2	16	17	8	19	4	10	2	15	6	3	14	12	9	2	3	8	16	14	19	4	11
8	17	0	13	3	1	17	14	5	3	0	17	8	2	6	5	14	5	3	0	4	4	0	0
17	13	2	5	3	0	9	8	7	5	3	12	7	1	5	4	13	4	2	1	3	3	1	5
15	14	1	16	2	5	8	8	5	3	6	7	8	2	4	13	0	7	7	5	3	9	0	6
14	3	2	15	0	4	7	6	3	2	5	0	7	1	2	12	17	3	4	3	5	8	1	4
11	7	9	4	13	3	3	0	1	9	3	0	6	2	5	4	7	6	8	15	3	17	4	1
5	3	8	15	4	7	6	18	7	14	7	9	5	3	5	4	7	3	5	17	0	0	7	6
14	3	5	6	3	9	14	13	10	7	0	0	9	8	17	15	3	5	1	3	2	4	2	13
6	2	4	5	3	8	15	3	9	11	7	5	8	7	13	12	5	3	1	10	2	6	3	8
7	5	3	3	0	1	9	7	17	10	10	8	6	5	14	11	3	5	13	3	2	5	0	0
10	0	4	5	0	2	8	6	16	9	14	0	5	4	15	10	2	6	14	2	6	4	10	3
0	12	3	4	6	3	0	5	15	6	13	6	3	2	10	9	1	4	13	1	5	3	9	2
6	11	0	3	5	1	6	4	10	3	11	5	2	4	9	0	17	3	10	2	4	1	0	5
2	0	3	0	2	5	4	10	6	13	5	0	1	3	8	6	16	2	9	4	3	2	6	5
4	0	2	6	3	2	5	11	4	0	6	0	5	4	15	8	0	10	6	3	0	4	6	6
15	2	4	10	8	14	0	10	10	9	12	5	3	3	0	4	5	15	5	2	0	3	6	0
10	0	3	18	14	4	16	1	0	3	0	4	2	10	5	3	4	14	0	3	6	0	6	3
5	15	12	14	3	2	15	4	2	2	6	3	1	9	4	2	3	5	6	2	4	6	5	2
2	3	6	10	2	4	10	3	0	2	6	5	10	10	10	4	5	10	8	18	4	3	0	3
9	4	5	9	1	3	14	13	0	18	5	0	10	0	6	2	13	0	0	10	3	2	4	8
9	5	6	0	0	4	12	11	10	19	0	1	2	3	0	1	10	4	3	14	2	1	3	5

Grata Spagna
(Madrid)

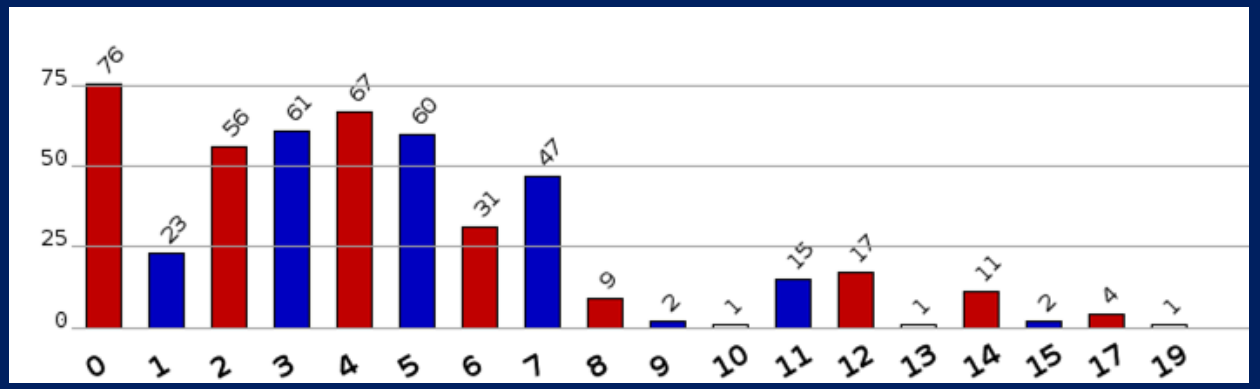
E’ disordinata o no?
26x24=624
Chiave di 624 numeri



4	3	1	7	10	2	6	1	5	3	8	9	1	2	7	10	0	0	5	2	0	4	3	7
5	4	3	3	2	1	10	5	3	4	0	6	7	0	12	15	0	4	6	3	3	2	5	7
1	6	8	5	2	4	3	4	1	14	3	12	5	8	0	4	6	2	17	1	9	6	4	0
1	7	10	3	12	4	5	8	3	7	2	5	10	10	0	4	7	2	5	8	3	0	5	4
12	10	3	6	1	4	7	2	5	4	4	0	11	2	7	6	3	0	5	2	7	10	1	4
14	2	7	5	8	3	6	1	4	3	7	2	4	8	2	5	0	4	7	2	5	6	1	7
6	3	2	7	4	8	5	0	7	3	6	1	2	5	0	4	2	6	1	5	7	5	2	0
6	6	4	2	6	8	1	7	4	5	8	3	4	7	6	1	0	3	5	2	7	0	6	0
12	2	6	5	8	7	3	10	1	0	7	0	4	6	5	2	5	2	4	7	6	5	0	7
0	5	3	1	7	8	6	8	4	2	5	8	1	7	5	2	8	0	3	1	7	4	1	12
5	0	1	6	3	0	8	1	5	5	2	0	4	5	6	7	17	4	12	1	1	5	0	7
7	4	2	5	8	3	2	5	0	4	6	0	6	1	4	7	0	8	5	2	7	4	1	5
6	7	3	2	8	1	5	3	1	4	7	2	5	8	0	4	3	6	1	7	4	2	5	0
4	4	2	5	2	0	8	1	7	6	1	0	5	3	4	5	8	2	6	1	5	0	7	5
14	1	4	5	0	17	2	15	3	12	2	14	1	4	6	5	8	3	1	7	8	0	5	8
7	4	2	5	7	0	6	7	4	0	7	5	0	5	3	6	1	4	12	7	15	7	1	4
14	1	7	5	0	6	1	7	5	6	1	4	3	7	0	8	1	4	3	5	8	1	4	2
5	0	5	4	7	2	8	1	9	6	4	1	7	3	6	5	8	2	3	4	6	7	3	2
8	2	10	11	2	5	7	4	1	6	2	7	0	4	3	17	2	5	1	7	0	4	6	1
7	8	2	4	7	1	5	8	3	2	7	5	8	1	2	14	3	7	5	3	7	2	5	8
12	3	6	1	14	2	11	3	4	5	8	12	6	3	5	4	8	1	7	3	6	5	3	7
10	11	2	4	5	8	2	7	3	8	1	4	7	3	1	6	2	8	5	3	6	2	7	4
6	3	8	12	4	7	5	3	4	14	5	8	12	1	4	8	5	3	1	7	6	4	3	0
4	4	0	5	8	1	2	7	6	5	3	2	8	1	12	7	3	8	10	2	5	3	7	4
10	7	5	2	7	3	4	8	5	11	2	6	5	3	4	2	7	5	0	5	8	1	7	2
6	0	5	2	5	0	7	3	4	12	8	1	15	2	4	17	0	5	6	1	8	4	2	7

Grata Francia, Savoia
(Parigi, Torino)

E’ disordinata o no?
26x21=546
Chiave di 546 numeri



3	5	7	12	4	6	9	3	7	4	12	2	6	0	8	4	7	3	6	2	0
6	5	3	4	0	7	11	2	5	6	0	7	12	4	5	2	0	3	7	8	5
4	2	3	5	0	6	4	14	7	3	6	4	5	0	17	2	5	8	4	14	3
0	7	14	2	5	17	3	6	4	2	5	7	12	6	0	7	3	0	5	0	4
19	2	3	5	0	14	2	5	11	3	17	4	13	0	6	5	4	12	2	3	8
4	6	14	2	5	7	3	4	6	5	0	7	3	5	0	12	1	4	3	2	5
4	2	5	3	7	2	4	0	2	5	7	0	2	12	3	4	7	5	8	3	6
5	8	0	6	3	7	4	2	0	5	11	3	0	4	0	8	7	3	4	6	0
7	5	12	3	4	14	6	5	12	11	3	6	12	4	1	5	2	3	1	4	11
3	1	0	4	0	7	2	5	4	3	11	2	6	7	0	5	0	12	4	5	3
14	3	5	0	7	2	0	4	11	5	2	7	6	3	1	0	0	2	5	1	2
7	5	1	4	12	2	4	11	0	7	0	4	5	14	2	7	3	6	3	4	4
0	7	0	5	1	2	3	0	4	15	2	7	4	15	11	2	0	3	5	0	6
5	0	4	0	7	3	5	0	2	0	6	1	7	5	0	4	7	3	0	4	1
8	2	12	1	5	8	0	7	0	2	0	5	2	0	1	7	3	4	11	1	3
5	2	12	3	4	11	3	0	5	0	4	10	2	4	0	3	7	0	12	2	0
4	7	3	1	0	2	0	3	4	7	6	12	3	7	5	0	6	3	4	5	14
2	11	4	5	7	11	4	6	0	5	3	12	2	5	0	3	4	1	4	3	0
4	0	7	5	0	14	3	0	5	2	7	0	4	3	2	4	5	0	7	4	1
11	3	4	0	6	2	4	3	2	0	4	3	1	5	7	0	4	2	3	1	4
5	0	7	4	2	5	0	7	3	0	5	2	4	1	2	11	2	17	0	3	4
2	14	6	3	0	7	6	2	4	5	7	3	0	2	5	6	0	2	1	3	4
7	0	6	2	4	5	1	0	4	3	2	5	6	1	4	3	5	0	7	1	2

Il cifrario di Vernam

1917-19 : Gilbert Vernam

Nel 1917 Gilbert Vernam, un ingegnere americano inventa e poi brevetta nel 1919 un dispositivo elettrico che realizza un’operazione XOR (o addizione modulo 2), che permette di cifrare un messaggio chiaro sommandolo con lo XOR con una chiave costituita da una sequenza casuale di 0 e 1, da non riutilizzare.

Ma come fare uno XOR con un testo che è una sequenza di lettere dell’alfabeto con una fila di 0 e 1?

Occorre un codice che trasformi le lettere in bit.

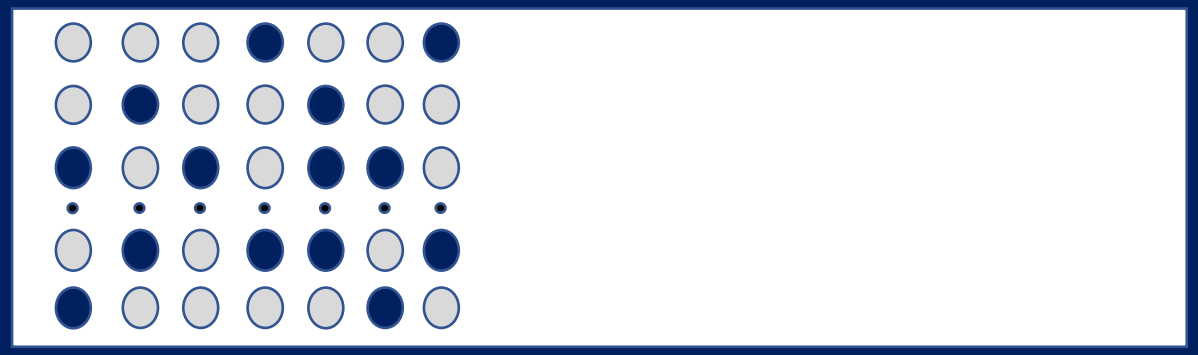
Non è necessario che questo codice sia segreto! Basta un codice pubblico come era l’alfabeto Morse che codificava ogni lettera con un gruppo di segnali lunghi e brevi o il più recente codice Baudot che codificava ogni lettera con un gruppo di 5 bit.

Il dispositivo inventato da Vernam usava appunto il codice Baudot.
Oggi sarebbe più conveniente usare il codice ASCII.

Il codice Baudot

Inventato nel 1870 dal francese Emile Badot, venne usato nei decenni successivi per le comunicazioni telegrafiche e soprattutto per le telescriventi.

Usa un nastro di carta forata; ogni linea ha cinque caselle che possono essere forate o no. Cinque bit permettono di codificare simboli; Baudot usa uno dei 32 simboli come segnale per commutare dalle lettere dell'alfabeto a numeri ed altri segni arrivando a 59 caratteri stampabili.



Codice	Binario	Lettera	Numero	Codice	Binario	Lettera	Numero
0	00000			24	11000	A	-
19	10011	B	?	14	01110	C	:
18	10010	D	$	16	10000	E	3
22	10110	F	!	11	01011	G	&
5	00101	H	#	12	01100	I	8
26	11010	J	'	30	11110	K	(
9	01001	L	)	7	00111	M	.
6	00110	N	,	3	00011	O	9
13	01101	P	0	29	11101	Q	1
10	01010	R	4	20	10100	S	{bel}
1	00001	T	5	28	11100	U	7
15	01111	V	;	25	11001	W	2
23	10111	X	/	21	10101	Y	6
17	10001	Z	"	4	00100	[sp]	[sp]
27	11011	{cifr}	{cifr}	2	00010	{cr}	{cr}
31	11111	{lett}	{lett}	8	01000	{lf}	{lf}

Il cifrario di Vernam

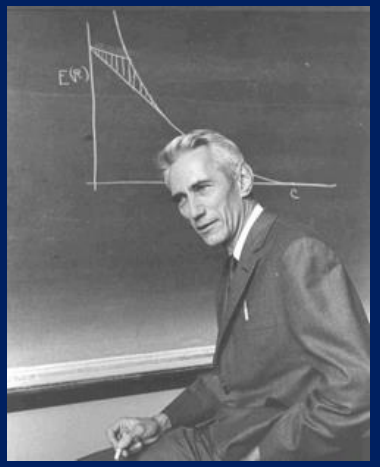
Chiaro c	A 11000	l 01001	e 10000	a 11000	 00000	i 01100	a 11000	c 01110	t 00001	a 11000	 00000	e 10000	s 10100	t 00001
Chiave k	11101	01101	00101	00001	10101	01111	11011	01011	00010	10110	01101	11100	01110	11000
Cifrato c XOR k	00101	00100	10101	11001	10101	00011	00011	00101	00011	01110	01101	01100	11010	11001

In generale per cifrario di Vernam si intende un cifrario basato su uno XOR tra bit del chiaro e bit del cifrato, ma soprattutto su una chiave di lunghezza infinita ed ancora più importante del tutto casuale; in pratica una chiave molto lunga generata in modo casuale, imprevedibile e che una volta usata, non venga più riutilizzata, ma se ne generi una ex-novo.

In altre parole il principio dell'**usa e butta**, usa una volta sola, in inglese **One Time Pad,** abbreviato in **OTP**, ormai diventato l'acronimo che identifica questo tipo di cifre.

Sopra: esempio, si cifra il messaggio ***Alea iacta est*** codificato in Baudot e cifrato con una chiave OTP.

L’articolo di Shannon (1949)



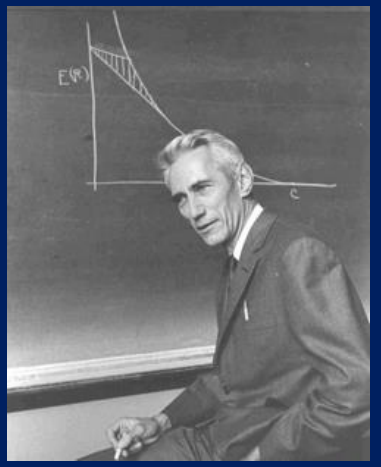
Claude Shannon (1916-2001) nel 1949 pubblica l’articolo ‟*A mathematical theory of Cryptography*” che si rifà a quello dell’anno precedente:‟*A mathematical theory of communications*”

Shannon nell’articolo del 1948 aveva definito l’incertezza di un testo, visto come una sequenza di caratteri (in effetti una catena markoviana).

$$H = -K \sum_{i=1}^{n} p_i \log p_i$$

Dove p_i è la probabilità dell’ i-esimo evento possibile, nel caso di un testo, una lettera. Il meno iniziale compensa il valore negativo del logaritmo di una probabilità (per definizione minore di 1) sempre negativo, mentre K è una costante che dipende dalle unità di misura come la base del logaritmo. Scegliendo 2 come base, l’unità di misura di H è il bit, l’unità di misura dell’informazione.
L’incertezza H infatti è una misura dell’informazione che abbiamo su un testo.
H=0 equivale alla conoscenza perfetta del testo, un solo evento ha probabilità 1 con logaritmo 0, tutti gli altri hanno probabilità zero, incertezza nulla, certezza assoluta!
Il valore massimo di H significa massima incertezza e minima conoscenza del testo, quando tutte le probabilità sono uguali a $\frac{1}{n}$, insomma non ne sappiamo nulla.

Il teorema di Shannon



Shannon introduce le seguenti definizioni:

- **Cifrario perfetto**: testo chiaro e cifrato sono completamente indipendenti: la incertezza del cifrato non cambia in alcun modo l'incertezza del chiaro e viceversa.
- **Indipendenza della chiave**: testo chiaro e chiave sono completamente indipendenti: l'incertezza della chiave non cambia in alcun modo l'incertezza del chiaro e viceversa.

Shannon dimostra che un **cifrario tipo Vernam è perfetto e indipendente dalla chiave**, e viceversa un cifrario perfetto e indipendente dalla chiave è necessariamente un Vernam.

Per esempio: venire in possesso di una o più coppie chiaro - cifrato permette di ricostruire banalmente il segmento di chiave usato, ma questo non dà alcuna informazione sul resto della chiave, in poche parole non serve a nulla.

Tutto risolto? Basta usare un Vernam?

Tutto risolto allora? Basta usare un Vernam ed abbiamo un cifrario perfetto, questa volta veramente indecifrabile?

Non è così semplice.

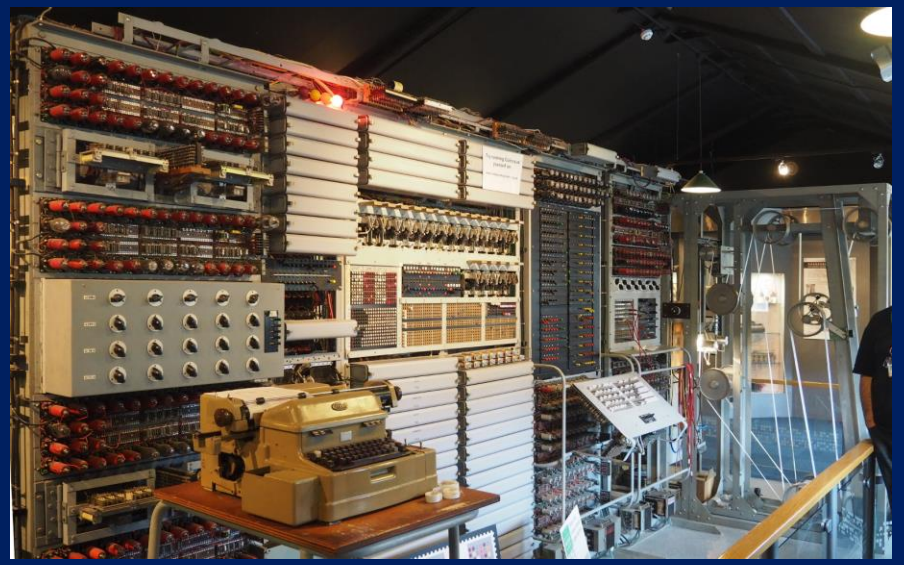
Innanzitutto va detto che il teorema di Shannon non si applica solo al Vernam (uso dello XOR) ma anche alle cifre polialfabetiche con chiave, come quelle di Bellaso, Vigenère (addizioni modulo N) e tante altre … a condizione che la chiave non sia breve ma piuttosto infinita, che si possa prolungare all'infinito, mai riutilizzata, **OTP**, e soprattutto realmente casuale, questo è il punto cruciale.

La stessa cifra delle caselle sarebbe stata indecifrabile se avesse rinnovato la grata ad ogni pagina, cosa praticamente irrealizzabile in tempi nei quali le informazioni viaggiavano alla velocità dei corrieri a cavallo o per mare.

Comunque dopo il 1920 il paradigma OTP ispirò un'intera generazione di macchine cifranti che realizzassero o per lo meno approssimassero da vicino un Vernam.

La macchina Lorenz

Il più noto esempio di macchina cifrante, che realizzasse un Vernam e fosse quindi di fatto indecifrabile, è la Lorenz usata dagli alti comandi tedeschi nella II guerra mondiale.
Usava una serie di rotori con tacche distribuite in modo *disordinato* che ogni tanti passi fanno girare il rotore successivo generando una sequenza che soddisfa i requisiti di casualità.
Ma inevitabilmente dopo n passi, la macchina tornerà allo stato iniziale e riprenderà la sequenza tale e quale.
Quella che genera è una sequenza pseudo-casuale, non è un vero OTP. Essendo n molto grande la sicurezza era considerata molto buona, ma non assoluta.
Tanto è vero che la Lorenz fu forzata dagli inglesi a Bletchley Park, che pure non ne avevano mai avuta una per mano. E che dovettero inventare i Colossus, i primi computer per ridurre i tempi di calcolo a livelli accettabili



Macchina Lorenz

La macchina Hagelin RT

Questa macchina prodotta dalla ditta svedese Hagelin, poi passata in Svizzera come **Crypto AG**, aveva due moduli intercambiabili, uno con la tradizionale serie di rotori che generavano una sequenza pseudocasuale, e uno che si limitava a leggere la chiave da un nastro Baudot che era la chiave di cifratura: la sequenza di fori (e quindi numeri) era generata con un procedimento hardware realmente imprevedibile come il lancio di una moneta, niente software; pare si trattasse di procedimenti chimici basati sul moto caotico.

L'unica macchina cifrante realmente indecifrabile? Sembra proprio di sì se è vero che gli americani diffidarono la Crypto AG dal vendere la macchina a paese non alleati degli USA.

Ma la vera forza di questo sistema non sta nella macchina ma nel metodo usato per produrre i nastri

Macchina Hagelin RT

Foto 2015, P. Bonavoglia. Esemplare al Ministero degli Affari Esteri, Roma.

DIANA, un OTP usata in Vietnam, e nella guerra fredda

Trasmettere: I Vietcong attaccheranno stasera

One Time Pad	Blocco indicatore a pos. 175
	NFHQI RWVAE GBUNJ KHNHP DJLXH NMIVV AJAIZ JAVFA ZMCTZ MEHZM
	WCVHZ DVLLQ HMZHU ZRUUW VUIXO IJTPI FMLBU KFQWR GDDGL YGDSA
	ZNVIL KQUDG DJTPL OAQEW HLAKS MIYPB ZPPUX AFOVI VZSPO DDOTI
	LATML LYTJO VJDKD BLJQH RMGKC **VNFJG OVHHH** SSGLC UHLYR PADYR
	KQEQB GLOMV VARCH YUAEG DZNPY FFYIE QSUUJ WAVKN QFNHH VGCVL
	IZKWP JBUHJ YXCTS LPSGZ FXFTF NOLPK XYKHU ZQWTY GRWIL OUAHA
	ANYFG DTVPJ FMHPU COLZI JFAGO LVILD IMQGS XKLTZ UYMCO GFDRE
	LBJLI XWDFI HOUYV MVGYO FSNRU CYZFP ERRNC ZLZDR IKGCI BPEHN
	TNGHF BJDAP TFGKT JJEJM WRXCU FEJJM XDADK FETJF ICKOM DYWIH
	JEYGH SLMCV YZYZD IEHBN MKQXZ CBXYJ EHODO VWZIZ VGZTF CCKJE
	YWOOU NQVLP FQXTU LPQLX PHEOA KRDUB HTYWH SKYOV OTMLM GXCWJ
	AMQEB RPTUK UCDSY KLJJZ FXSRJ FXHHU QIHHM IYBBT LWVPO UZZDJ
	YJHRA QWXYE SPMZW ZIVBK PMGLB VFBUJ LTSSL TIIRH NJWZI TZROA
	BDNIP PDVRY ECSXU DRDLI KYRHY AAYSO YTSMC HBFCT DHVVF QZXTL
	FEKXL JYLHQ AFKTS MBURE NVMIR SZQPS CUXMR IVQUC GVIQO ACQUU
	UIQHQ HZPYO IAJGN BPIRJ LXFTO TUQKP LFXBM OILEH ZNIIT VKIDB

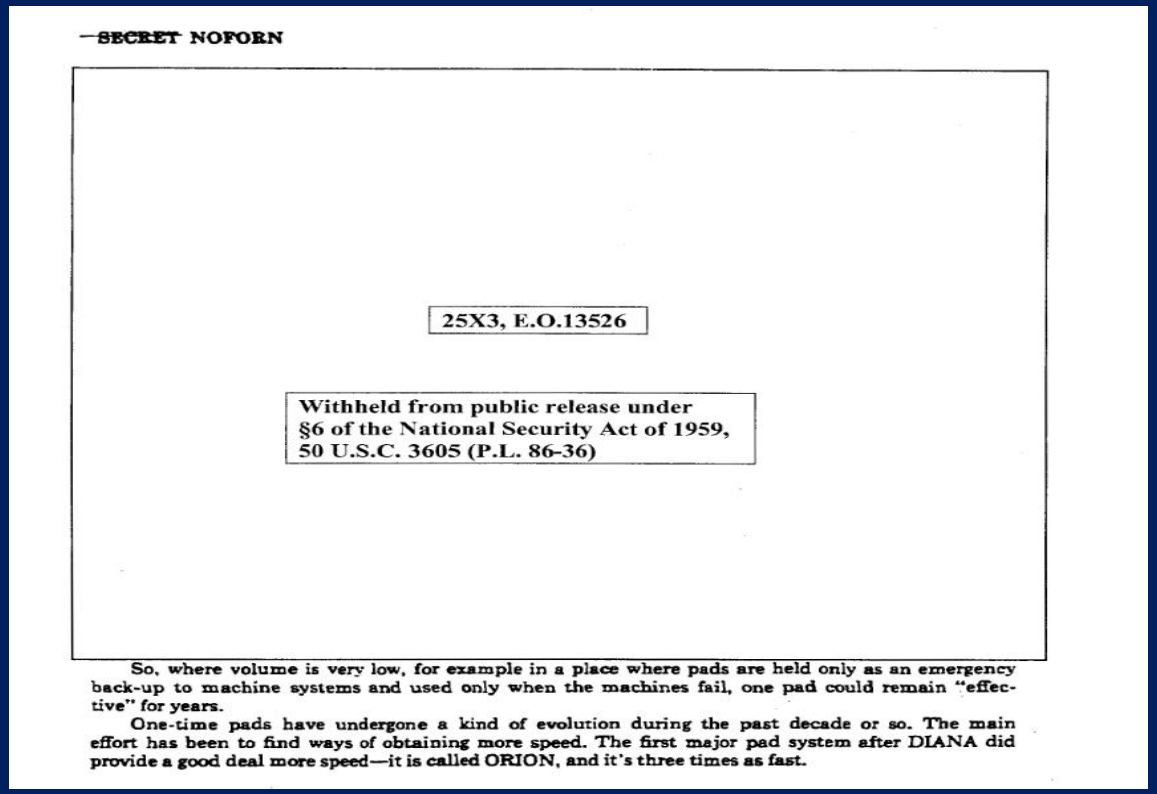
chiave da OTP	VNFJG OVHHH SSGLC UHLYR PADYR KQEQB GLOMV VARCH YU
testo chiaro	----- ----- IVIET CONGA TTACC HERAN NOQUE STASE RA
testo cifrato	VNFJG OVHHH ZMLKE DEBVI RGWZG IFEJL GAVTA MGIFO KF

[Diana cryptosystem: la cifra in dettaglio]

Tavola nel formato originale, simile a Bellaso 1552	
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 Z Y X W V U T S R Q P O N M L K J I H G F E D C B A
B	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 Y X W V U T S R Q P O N M L K J I H G F E D C B A Z
C	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 X W V U T S R Q P O N M L K J I H G F E D C B A Z Y
D	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 W V U T S R Q P O N M L K J I H G F E D C B A Z Y X
E	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 V U T S R Q P O N M L K J I H G F E D C B A Z Y X W
F	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 T S R Q P O N M L K J I H G F E D C B A Z Y X W V
G	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 T S R Q P O N M L K J I H G F E D C B A Z Y X W V U
H	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 S R Q P O N M L K J I H G F E D C B A Z Y X W V U T
I	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 R Q P O N M L K J I H G F E D C B A Z Y X W V U T S
J	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 Q P O N M L K J I H G F E D C B A Z Y X W V U T S R
K	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 P O N M L K J I H G F E D C B A Z Y X W V U T S R Q
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 O N M L K J I H G F E D C B A Z Y X W V U T S R Q P
M	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 N M L K J I H G F E D C B A Z Y X W V U T S R Q P O
N	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 M L K J I H G F E D C B A Z Y X W V U T S R Q P O N
O	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 L K J I H G F E D C B A Z Y X W V U T S R Q P O N M
P	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 K J I H G F E D C B A Z Y X W V U T S R Q P O N M L
Q	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 J I H G F E D C B A Z Y X W V U T S R Q P O N M L K
R	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 I H G F E D C B A Z Y X W V U T S R Q P O N M L K J
S	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 G F E D C B A Z Y X W V U T S R Q P O N M L K J I
T	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 G F E D C B A Z Y X W V U T S R Q P O N M L K J I H
U	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 F E D C B A Z Y X W V U T S R Q P O N M L K J I H G
V	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 E D C B A Z Y X W V U T S R Q P O N M L K J I H G F
W	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 C B A Z Y X W V U T S R Q P O N M L K J I H G F E
X	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 C B A Z Y X W V U T S R Q P O N M L K J I H G F E D
Y	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 A Z Y X W V U T S R Q P O N M L K J I H G F E D C
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 Z Y X W V U T S R Q P O N M L K J I H G F E D C B

Era sicura Diana?

Dipende dalla chiave OTP,
era realmente casuale?
Come era generata?



~~SECRET~~ NOFORN

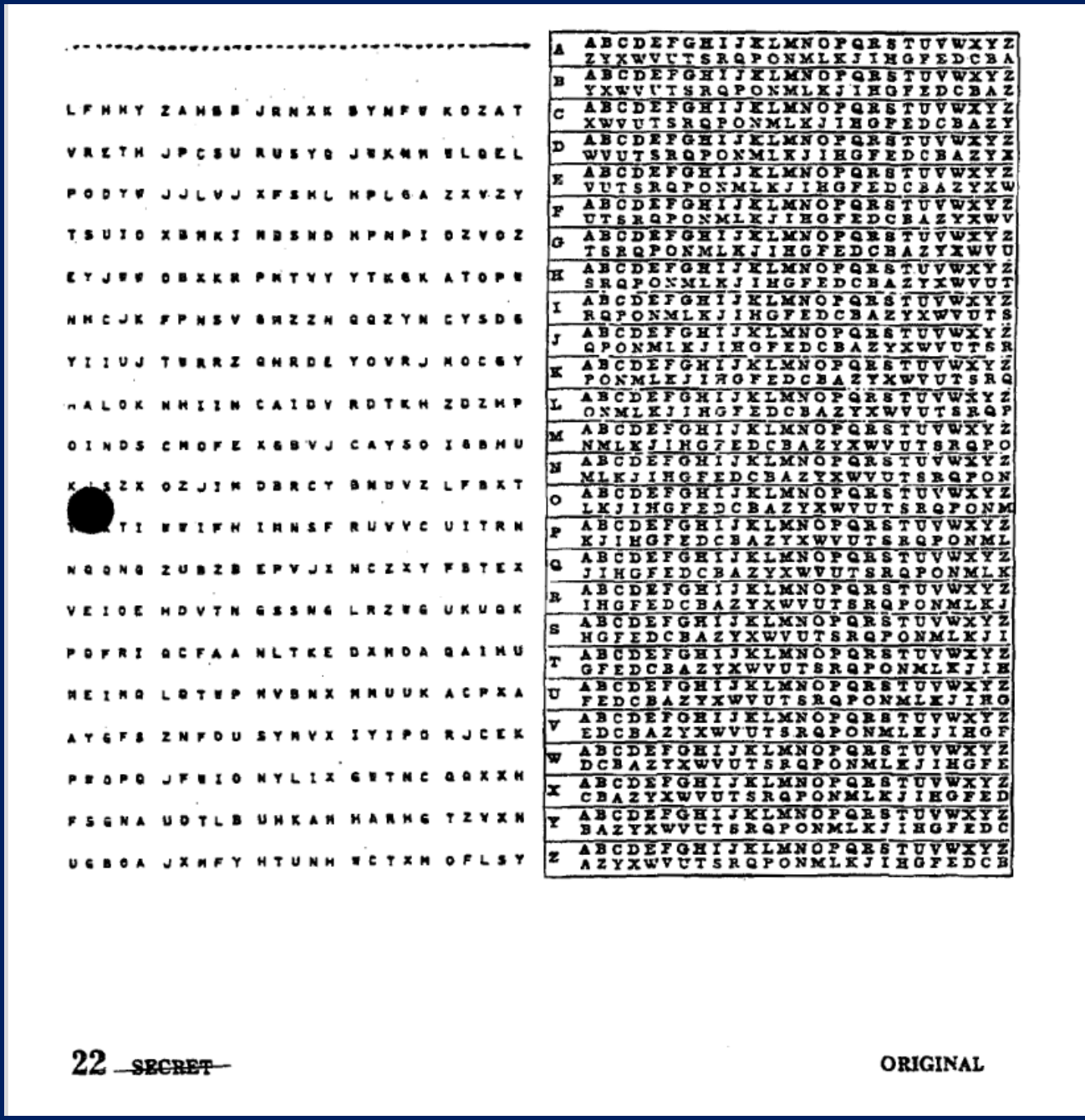
25X3, E.O.13526

Withheld from public release under §6 of the National Security Act of 1959, 50 U.S.C. 3605 (P.L. 86-36)

So, where volume is very low, for example in a place where pads are held only as an emergency back-up to machine systems and used only when the machines fail, one pad could remain "effective" for years.

One-time pads have undergone a kind of evolution during the past decade or so. The main effort has been to find ways of obtaining more speed. The first major pad system after DIANA did provide a good deal more speed—it is called ORION, and it's three times as fast.

David G. Boak, *A History of U.S. Communications Security* (Volumes I and II), National Security Agency, , 1973 − 2008, pag. 22 - 23 → eBook



22 ~~SECRET~~ ORIGINAL

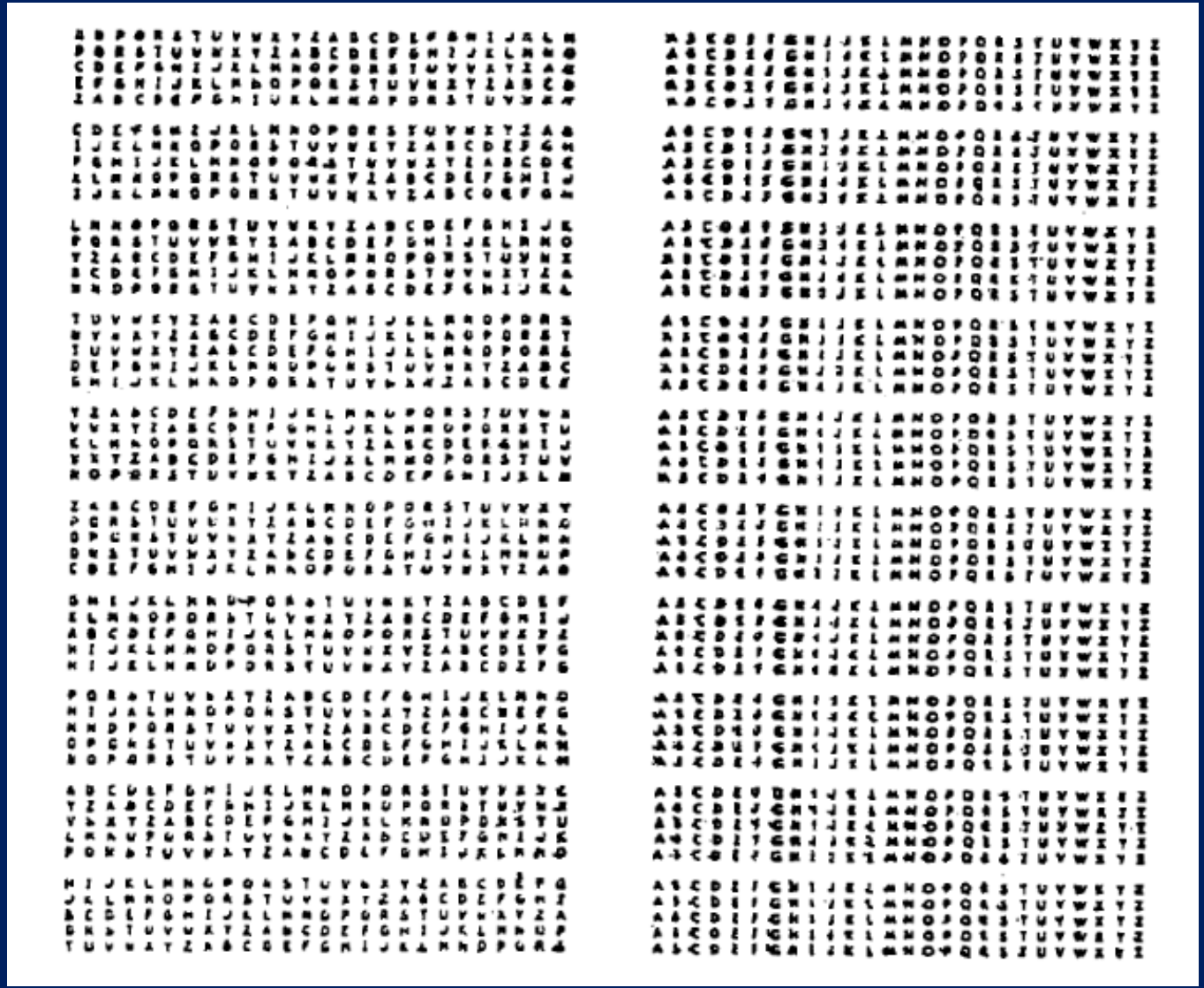
La cifra Orion: Orion come Orchema?

Questa cifra fu adottata dal NSA in sostituzione di DIANA considerata troppo lenta.

Sul recto di un foglio ci sono 50 linee con alfabeti ordinati, sul retro ci sono perfettamente allineati 50 alfaberi disordinati e sotto un foglio di carta carbone con il lato inchiostrato verso l'alto.
Il cifrista per ogni linea segnerà con un cerchietto la lettera corrispondente; automaticamente verrà cerchiata sul retro la cifra, velocissimo ma molto ingombrante

http://www.crittologia.eu/critto/cifraORION.html

David G. Boak, *A History of U.S. Communications Security* (Volumes I and II), National Security Agency, , 1973 − 2008, pag. 22 - 23 → eBook



E alla fine il cerchio si è chiuso.

Dall’Orchema di Tritemio avevamo cominciato e all’Orchema siamo tornati!

Ora però abbiamo le idee un po’ più chiare sulla effettiva sicurezza dei cifrari.

Tanto è vero che dopo il 1970 si è presa una strada diversa, si è rinunciato al mito del cifrario perfetto, e si sono realizzati cifrari che non sono perfetti, sarebbero decifrabili ma in tempi proibitivi. Come RSA, DH, El Gamal e …

le ***curve ellittiche***, oggetto delle prossima conferenza della prof. Angela Zottarel.

Grazie per l’attenzione!

Riferimenti

- **Testi base**
  - F. L. Bauer, *Decrypted Secrets,* Springer, Berlin, 1997-2007
  - D.Kahn, *Codebreakers,* Scribner, New York, 1966-1996
  - L. Sacco, *Manuale di Crittografia,* Roma 1947, e Lecce 2014

- **Testi originali**
  - *(oggi disponibili e spesso scaricabili da Google-Libri e altre librerie on-line)*
  - I. Tritemius, *Polygraphiae libri VI,* 1518-1613
  - G. B. Bellaso, *La cifra del Sig. Giovan Battista Bellaso*, Venezia, 1553
  - B. de Vigenère, *Traicté des chiffres ou secrètes manières d'escrire,* Paris, 1586-1587
  - C. Shannon, «A Mathematical Theory of Communication», *Bell System Technical Journal*, Vol. XXVII, no. 3, July 1948
  - C. Shannon, «Communication Theory of Secrecy Systems», *Bell System Technical Journal*, Vol. XXVIII, no. 4, October 1949

Riferimenti

- **Articoli su riviste specializzate**
  - David G. Boak, *A History of U.S. Communications Security* (Vol. I and II), National Security Agency, 1973 – 2008
  - P. Bonavoglia, «Bellaso's 1552 cipher recovered in Venice», *Cryptologia* 43-6, 2019
  - P. Bonavoglia, «The cifra delle caselle a superencrypted XVI century cipher», *Cryptologia* 44-1, 2020
  - A. Buonafalce, "Bellaso's reciprocal ciphers», *Cryptologia*, 2006
  - A. Buonafalce, *Giovan Battista Bellaso e le sue cifre polialfabetiche,* Lerici 1997