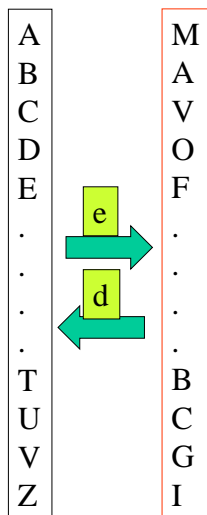


# Crittologia classica

## Sostituzione di caratteri

I due alfabeti



Trasformazioni possibili:  
 $n \times (n-1) \times (n-2) \times (n-3) \dots$

$$|T| = n!$$

$$n = 21 \rightarrow 5,1 \times 10^{19}$$
$$n = 26 \rightarrow 4 \times 10^{26}$$

Nessuno uguale a se stesso!

$$|T| = \sum_{j=0}^n (-1)^j \times \frac{n!}{j!}$$

$$> (n-1)!$$

La tabella come chiave

# Sostituzioni facili da ricordare

Cifrario di Cesare

Cifrario ATBASH

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHILMNOPQRSTUVWXYZABC

DE BELLO GALLICO  
IL GLQQT NFQQPHT

al più 20 chiavi

ABCDEFGHIJKLMNOPQRSTUVWXYZ

ZYXWVUTSRQPONMLIHGFEDCBA

BABILONIA  
VZVONILOZ

## Trasposizione di caratteri e la scitale

S<sub>1</sub>S<sub>2</sub>S<sub>3</sub>S<sub>4</sub>S<sub>5</sub>S<sub>6</sub>S<sub>7</sub>S<sub>8</sub>S<sub>9</sub>

↑ ↓

S<sub>3</sub>S<sub>8</sub>S<sub>1</sub>S<sub>2</sub>S<sub>6</sub>S<sub>5</sub>S<sub>9</sub>S<sub>7</sub>S<sub>4</sub>

chiave

1 2 3 4 5 6 7 8 9  
3 4 1 8 6 5 8 2 7

n lunghezza della stringa

$|T| = n!$

Scitale

Chiave: diametro e lunghezza

Θεμιστοκλες μεν ταυτα ενεγραφε

Θ	τ	σ	α	γ
ε	ο	τ	ρ	
μ	κ	μ	α	ε
ι	λ	ε	υ	φ
σ	ε	ν	τ	ε

▶

Θτο αγεο τ ρμκμαεαιλευνφσεντες



## Crittografia e Crittanalisi

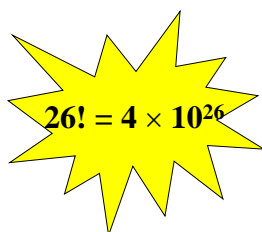
### Crittografia classica: la sostituzione monoalfabetica

regola di sostituzione (o chiave)

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

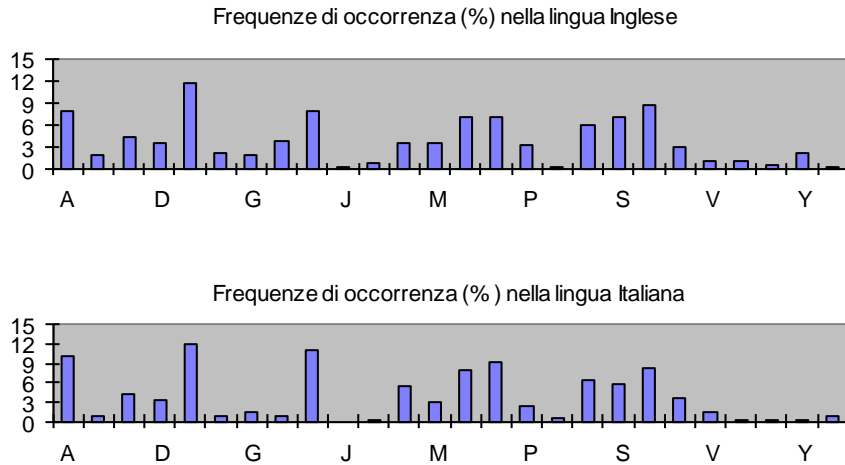
testo in chiaro: CRITTOGRAFIA

testo cifrato: MSLGGNTSQZLQ



$$26! = 4 \times 10^{26}$$

## Statistiche dei caratteri



Probabilità di occorrenza

## Statistiche di digrammi e trigrammi

Lingua inglese

TH 3,16%,

IN 1,54%

ER 1,33%

RE 1,3%

ecc.

THE 4,72

ING 1,42

ecc.

- un linguaggio naturale è ridondante
- la probabilità di occorrenza di stringhe corte è indipendente dal testo
- in un testo lungo le frequenze di occorrenza approssimano le probabilità

## Il punto debole della monoalfabetica

Le proprietà statistiche di ogni carattere del testo in chiaro vengono trasferite immutate sul carattere che lo sostituisce nel testo cifrato



Un grande spazio delle chiavi può non servire a nulla!

Come decifrare un codice monoalfabetico

- Sapendo che il testo è in italiano, è facile che l'ultima lettera di ciascuna parola sia una vocale (questa osservazione non è essenziale per il metodo, ma lo rende più breve)
- Si cercano i simboli più frequenti nel testo cifrato
- Si provano a sostituire con le lettere più frequenti in italiano
- Si cerca di vedere se si riesce a “intravedere” delle parti di parole
- Qualche tentativo può portare a parole improbabili, in tal caso si deve rivedere alcune scelte

Crittoanalisi di un Cifrario a Sostituzione

Dobbiamo decrittare il testo

QANGH TGMYJ XGHTN AVUNG TTYSH LUXYU OUAUD  
UQQYJ UJAXX YNUTY NGKGB BUGMA XASLG KJUGX  
YQANG HTGMY JXGHT DABBY VUJAK TYTYT ANGHT  
JAKTY VUJHS SYOGH TSAOD JUQAD ABBYV GQGXXG  
SXGVU IHAJJ UQPAV UTMAN TYSUO AXXYT YTAJJ ASXHF  
AATAU QGOUT AXXUD ANGQQ ATVAN AUJFH YQYAD  
ANNUS QGJVG NAJAS XGTBA TYTSY QYOAG TVGSS AOGUJ  
FGXXY KJUAQ PAHTL AJKUY NTYIH ASXYD ABBYV UJAKT  
YQGDU XYTAJ JGLYX XAKGV UHTMA QQPUY FGJAK  
TGOAU JIHGJ AGMAM GTYOA OGSXN GTXYT UYSAT YTQPA  
XHHXU JYQPU GOGMG TYOGA SXNYQ UJUAK UGDAN  
MUGVA JJGDH TXGVA JSHYT GSYQP AANGS AODNA JHSXN  
GADGY TGBBG QYOA H TGQUJ UAKUG OGXHN GGDDA  
TGOGA SXNYQ UJUAK UGALL AMUSX YIHAI DABBY VUJAK  
TYSUN GJJAK NYXHX XYAVG

frequenze dei caratteri % in italiano								
A 10,41	B 0,95	C 4,28	D 3,82	E 12,62	F 0,75	G 2,01	H 1,10	I 11,62
J 0	K 0	L 6,61	M 2,58	N 6,49	O 8,71	P 3,20	Q 0,75	R 6,70
S 6,04	T 6,06	U 3,04	V 1,51	W 0	X 0	Y 0	Z 0,93	

Digrammi frequenti in italiano (nell'ordine):

er, es, on, re, el, en, de, di, si, ti, la, al

frequenze dei caratteri % nel nostro testo

<b>A</b> 13,52	B 2,41	C 0	D 2,78	E 0	F 0,74	<b>G</b> 11,30	H 4,26	I 0,74
J 6,85	K 2,59	L 1,11	M 1,85	N 4,44	O 2,96	P 1,11	Q 4,44	R 0
S 4,44	T 7,78	<b>U</b> 8,52	V 2,78	W 0	X 6,48	<b>Y</b> 8,89	Z 0	

proviamo A=e

QeraH naMoJ XaHnr eVira nnoSH LiXoi OieiD iQqoJ iJeXX  
orino raKaB BiaMe XeSLa KJiaX oQera HnaMo JXaHn DeBBo  
ViJeK nonon eraHn JeKno ViJHS SoOaH nSeOD JiQeD eBBoV  
aQaXa SXaVi IHeJJ iQPeV inMer noSiO eXXon oneJJ eSXHF  
eenei QaOin eXXiD eraQQ enVer eiJFH oQoeD erriS QaJV  
reJeS XanBe nonSo QoOea nVaSS eOaiJ FaXXo KJieQ PeHnL  
eJKio rnoIH eSXoD eBBoV iJeKn oQaDi XoneJ JaLoX XeKaV  
iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe OaSXr anXon  
ioSen onQPe XHXXi JoQPi aOaMa noOae SXroQ iJieK iaDer  
MiaVe JJaDH nXaVe JSHon aSoQP eeraS eODre JHSXr aeDao  
naBBa QoOeH naQiJ ieKia OaXHr aaDDe naOae SXroQ iJieK  
iaeLL eMiSX oIHeJ DeBBo ViJeK noSir aJJeK roXHX XoeVa

QeraH naMoJ XaHnr eVira nnoSH LiXoi OieiD iQqoJ iJeXX  
 orino raKaB BiaMe XeSLa KJiaX oQera HnaMo JXaHn DeBBo  
 ViJeK nonon eraHn JeKno ViJHS SoOaH nSeOD JiQeD eBBoV  
 aQaXa SXaVi IHeJJ iQPeV inMer noSiO eXXon oneJJ eSXHF  
 eenei QaOin eXXiD eraQQ enVer eiJFH oQoeD erriS QaJV  
 reJeS XanBe nonSo QoOea nVaSS eOaiJ FaXXo KJieQ PeHnL  
 eJKio rnoIH eSXoD eBBoV iJeKn oQaDi XoneJ JaLoX XeKaV  
 iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe OaSXr **anXon**  
**ioSen** onQPe XHXXi JoQPi aOaMa noOae SXroQ iJieK iaDer  
 MiaVe JJaDH nXaVe JSHon aSoQP eeraS eODre JHSXr aeDao  
 naBBa QoOeH naQiJ ieKia OaXhr aaDDe naOae SXroQ iJieK  
 iaeLL eMiSX oIHeJ DeBBo ViJeK noSir aJJeK roXHX XoeVa

X=t

QeraH naMoJ taHnr eVira nnoSH Litoi OieiD iQqoJ iJett  
 orino raKaB BiaMe teSLa KJiat oQera HnaMo JtaHn DeBBo  
 ViJeK nonon eraHn JeKno ViJHS SoOaH nSeOD JiQeD eBBoV  
 aQata StaVi IHeJJ iQPeV inMer noSim etton oneJJ eStHF  
 eenei QaOin ettiD eraQQ enVer eiJFH oQoeD erriS QaJV  
 reJeS tanBe nonSo QoOea nVaSS eOaiJ Fatto KJieQ PeHnL  
 eJKio rnoIH eStoD eBBoV iJeKn oQaDi toneJ JaLot teKaV  
 iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe maStr anton  
 ioSen onQPe tHtti JoQPi aOaMa noOae StroQ iJieK iaDer  
 MiaVe JJaDH ntaVe JSHon aSoQP eeraS eODre JHStr aeDao  
 naBBa QoOeH naQiJ ieKia OatHr aaDDe naOae StroQ iJieK  
 iaeLL eMiSt oIHeJ DeBBo ViJeK noSir aJJeK rotHt toeVa

aMeM anoOe OaStr anton  
 ioSen onQPe tHtti JoQPi aOaMa noOae StroQ iJieK iaDer

M=v, S=s, O=m.....



la sostituzione è

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 L Q V A F K P U - - J O T Y D I N S X H M - - - B

il testo in chiaro è:

cerau navol taunr edira nnosu bitoi mieip iccol ilett  
orino ragaz ziave tesba gliat ocera unavo ltaun pezzo  
dileg nonon eraun legno dilus somau nsemp licep ezzod  
acata stadi quell iched inver nosim etton onell estuf  
eenei camin ettip eracc ender eilfu ocoep erris calda  
reles tanze nonso comea ndass email fatto gliec heunb  
elgio rnoqu estop ezzod ilegn ocapi tonel labot tegad  
iunve cchio faleg namei lqual eavev anome mastr anton  
iosen onche tutti lochi amava nomae stroc ilieg iaper  
viade llapu ntade lsuon asoch eeras empre lustr aepao  
nazza comeu nacil iegia matur aappe namae stroc ilieg  
iaebb evist oquel pezzo dileg nosir alleg rotut toeda

## Crittografia classica: la trasposizione di colonne

Tabella  $5 \times 8$  e chiave 76518234:

Testo in chiaro: ALLE PROSSIME ELEZIONI MI PRESENTO

A	L	L	E	P	R	O	S
S	I	M	E	E	L	E	Z
I	O	N	I	M	I	P	R
E	S	E	N	T	O	X	X

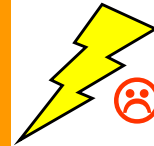
Statistiche dei digrammi e dei trigrammi alterate dall'operazione di affiancamento delle colonne

Ordine: 7 6 5 1 8 2 3 4

Simboli di riempimento

Testo cifrato: EEIN RLIO OEPX SZRX LMNELIOSASIE

Ogni carattere del testo cifrato mantiene le proprietà statistiche che ha nel linguaggio naturale, quindi poco utile. Quale info sfrutto? Le statistiche dei digrammi nel linguaggio naturale permettono invece di individuare quali sequenze di due simboli non sono naturali ma derivano dalla scrittura in colonne del testo in chiaro



## Crittografia classica: la trasposizione di colonne

Tabella  $5 \times 8$  (PxQ) e chiave 76518234:

Ordine: 1 2 3 4 5 6 7 8

E	R	O	S	L	L	A	P
E	L	E	Z	M	I	S	E
I	I	P	R	N	O	I	M
N	O	X	X	E	S	E	T

Chiave: 7 6 5 1 8 2 3 4

Ora si spostano le colonne in modo che l'indice di ricezione corrisponda ai numeri nella chiave

# Mascheramento della ridondanza

equiprobabilità di occorrenza di ogni simbolo del testo cifrato

## CRITTOGRAFIA CLASSICA

- **Eliminazione delle spaziature e dei segni di interpunzione**
- **Nulle:** caratteri non significativi
- **Omofoni:** più simboli per i caratteri più frequenti
- **Cifrari poligrafici:** cifratura di due o tre caratteri consecutivi
- **Cifrari polialfabetici:** trasformazioni variabili

CRITTOGRAFIA MODERNA usa spesso la sostituzione

almeno 8 caratteri alla volta (64 bit)

trasformazione dipendente da tutti i “blocchi” precedenti

Compressione senza perdita

R24: “non bisogna mai cifrare troppo testo con la stessa chiave”

## Playfair Cipher (sostituzione di digrammi)

CHIAVE

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

o si elimina la doppia o  
carattere improbabile

- J sostituito da I

Il digramma in chiaro identifica la diagonale di un rettangolo: il digramma cifrato è dato dai caratteri posti all'estremità dell'altra diagonale

- AI → RO

Se i digrammi sulla stessa riga -> quelli nelle casella alla destra

- RI → DF

- LP → ZL

Se i digrammi sulla stessa colonna -> quelli nelle casella sottostanti

- AK → RX

- “doppia”: regole varie



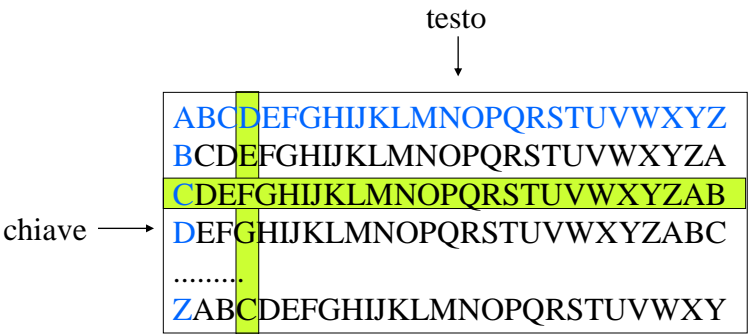
## SOSTITUZIONE POLIALFABETICA

Blaise de Vigenère pubblicò nel 1586 un trattato di cifre nel quale proponeva tra gli altri un codice che ebbe grande fortuna e che è ricordato con il suo nome. Si tratta del più semplice codice di sostituzione polialfabetica e proprio per la sua semplicità ha goduto per secoli di grande fama. Tale fortuna è durata fino a molti decenni dopo che era stato pubblicato un primo metodo di decrittazione.

La cifratura di Vigenère fu sconfitta solo nel XIX secolo.

A **Charles Babbage** (noto per aver progettato il precursore dei calcolatori elettronici) e a **Friedrich Wilhelm Kasiski** (ufficiale in pensione dell'esercito prussiano) si deve la scoperta del metodo di crittoanalisi.

# La sostituzione polialfabetica (Vigenere)



Chiave: CIAO

testo in chiaro : DOMANI NON POSSO

Cifratura:

C	I	A	O	C	I	A	O	C	I	A	O	C	I
D	O	M	A	N	I	N	O	N	P	O	S	S	O
F	Z	M	O	P	S	N	C	P	A	O	H	U	Z

Tavola 7 Tavola di Vigenère usata per la parola-chiave SOLE. La parola-chiave definisce quattro diversi alfabeti cifranti, cosicché la lettera n può essere crittata come F, B, Y e R.

Chiario	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

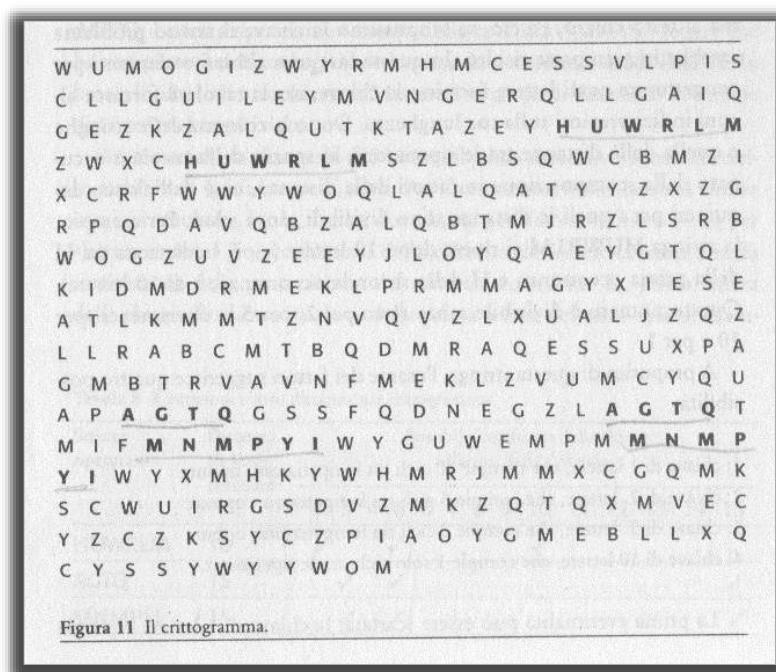
Chiave:	S O L E S O L E S O L E S O L E S O L E S O L
Testo in chiaro:	n o n v e d o n o n s e n t o n o n p a r l o
Testo cifrato:	F C Y Z W R Z R G B D I F H Z R G B A E J Z Z

**COSA SI NOTA? => una ripetizione**

Tra la n del secondo non e la n del terzo non la  
distanza è 8 lettere, multiplo esatto della  
lunghezza della chiave

Appiglio formidabile!

**PERCHE’?**



La stringa HUWRLM si ripete

Quattro possibilità:

1. chiave di 1 lettera che compie 10 cicli tra le ripetizioni
2. chiave di 2 lettere che compie 5 cicli tra le ripetizioni
3. chiave di 5 lettere che compie 2 cicli tra le ripetizioni
4. chiave di 10 lettere che compie 1 ciclo solo tra le ripetizioni

Tavola 8. Ripetizioni e loro distanza nel crittogramma.

Stringa ripetuta:	Distanza tra le ri- petizioni:	Possibile lunghezza della chiave: (fattori della distanza)													
		2	3	4	5	6	7	8	9	10	11	12	13	14	15
HUWRLM	10		✓		✓					✓					
AGTQ	15		✓		✓										✓
MNMPYI	15		✓		✓										✓

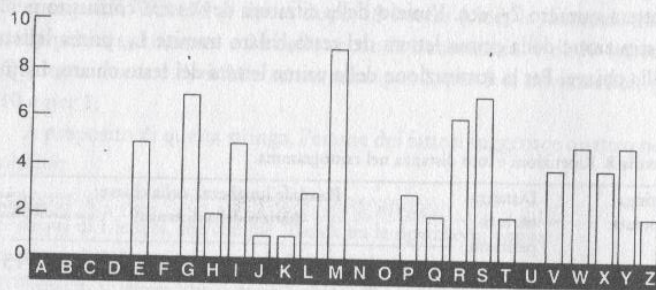


Figura 12 Distribuzione di frequenza delle lettere crittate tramite l'alfabeto cifrante  $L_1$  (numero di occorrenze).

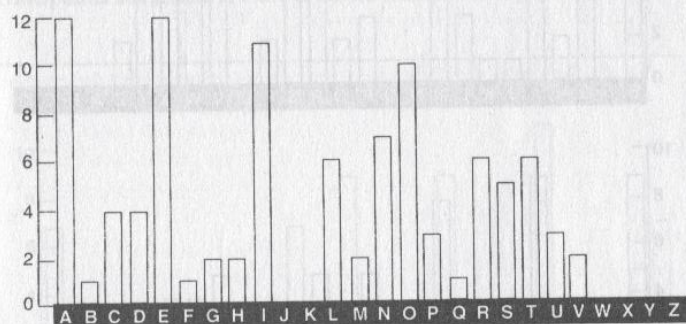


Figura 13 Distribuzione di frequenza della lingua italiana (occorrenze ogni 100).

\* (Si potrebbe pensare che nella nostra lingua il procedimento che stiamo illustrando sia facilitato dall'estrema rarità di lettere come w, x e y; ma l'avvallamento è ben riconoscibile, per esempio, anche nella lingua inglese, in cui questo gruppo di lettere ha frequenze molto basse, comprese tra l'1,5 e lo 0,5 per cento. *N.d.T.*)

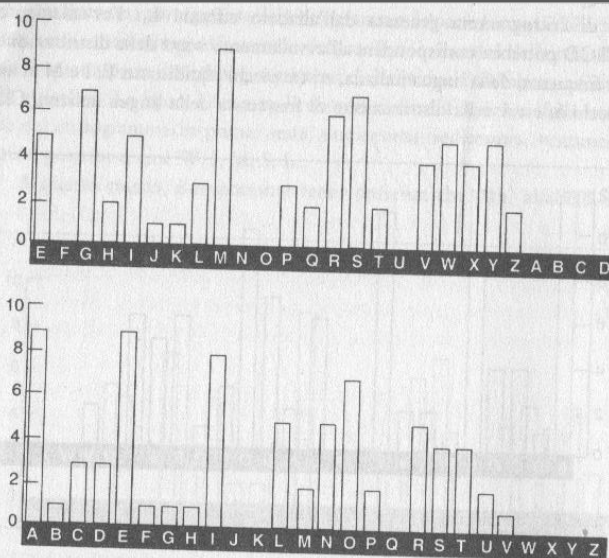
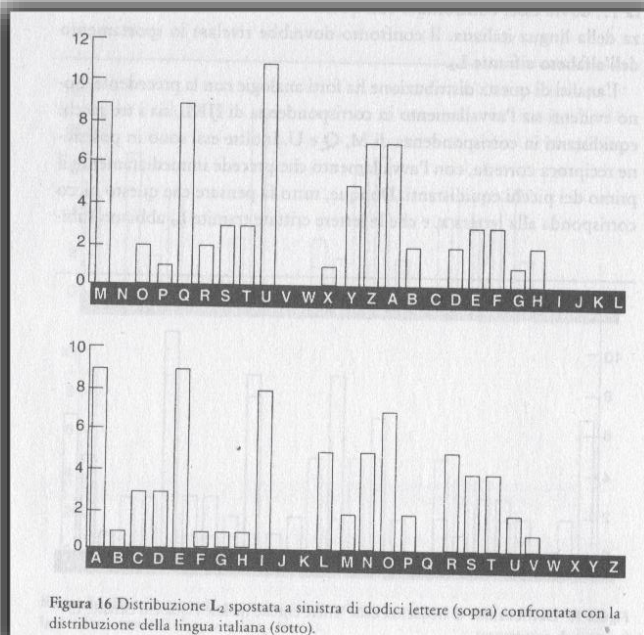
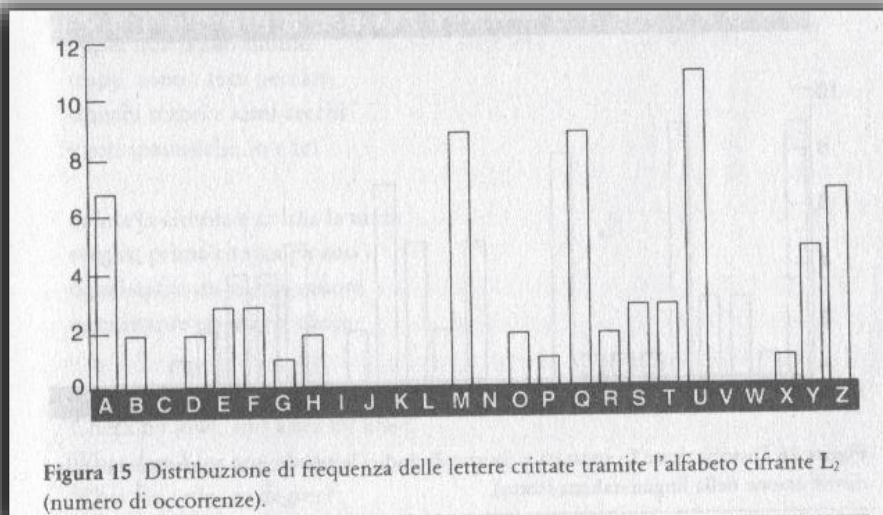


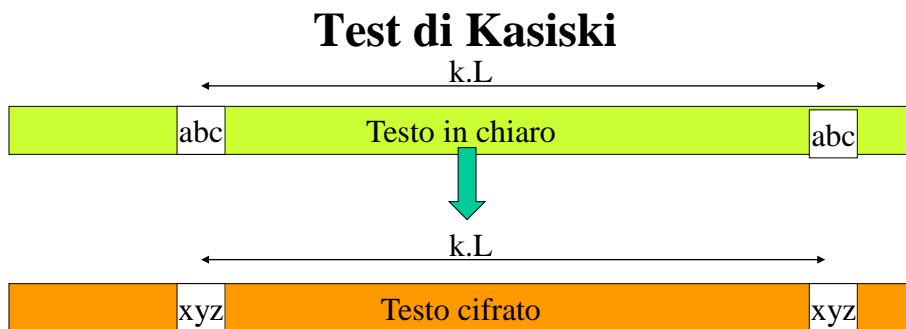
Figura 14 Distribuzione  $L_1$  spostata a sinistra di quattro lettere (sopra) confrontata con la distribuzione della lingua italiana (sotto).





Il testo in chiaro inizia così:

Siedienontivergognareguanciaaguanciafiancoafianco....



Chiave: ciao

Testo in chiaro: domani non puo domani deve andare a scuola

Due poligrammi identici presenti nel testo in chiaro ad una distanza uno dall'altro pari a un multiplo della lunghezza della chiave sono necessariamente sostituiti da poligrammi identici nel testo cifrato. Per sapere con buona probabilità la lunghezza di una chiave occorre:

- 1: ricerca nel cifrato di sequenze identiche
- 2: annotazione delle distanze
- 3: fattorizzazione e scelta delle distanze con un fattore comune
- 4:  $L = \text{MCD}$

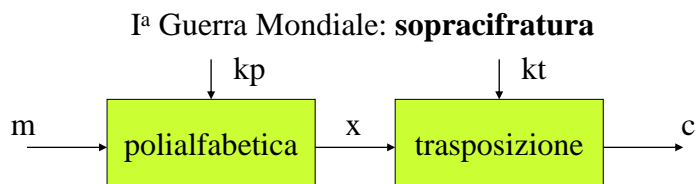
## Accorgimenti utili

•1: *“chiave lunga e scelta a caso”*

•2: *“mai archiviare insieme testi cifrati e decifrazioni”.*

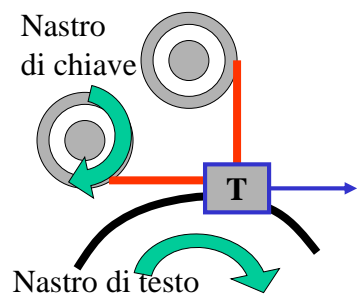
•3: *“mai lasciare incustodite macchine pronte per cifrare/decifrare”*

•4: *“ogni simbolo del blocco in chiaro deve influire sul valore di tutti i simbolo del blocco cifrato”*



**Il cifrario Vernam  
One time pad**

# Il Cifrario di Vernam (1917)



## Telegrafo di Vernam

- *codifica binaria (5 bit) codice di baudot a 32 bit per telescriventi)*
- *chiave lunga quanto il testo*

Binary value	Letters	Figures
00011	A	-
11001	B	?
01110	C	:
01001	D	\$
00001	E	3
01101	F	!
11010	G	&
10100	H	STOP
00110	I	8
01011	J	'
01111	K	{
10010	L	}
11100	M	.
01100	N	,
11000	O	9
10110	P	0
10111	Q	1
01010	R	4
00101	S	BELL
10000	T	5
00111	U	7
11110	V	;
10011	W	2
11101	X	/
10101	Y	6
10001	Z	"
00000	n/a	n/a
01000	CR	CR
00010	LF	LF
00100	SP	SP
11111	LTRS	LTRS
11011	FGS	FGS

Figure 3. The Baudot Code Set

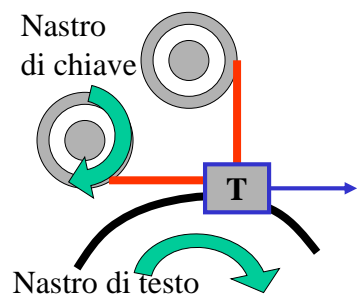
•Ogni carattere cifrato aggiungendo (somma modulo 2 – funzione invertibile) un carattere oscurante

•Addizione eseguiti sui singoli bit costitutivi il carattere

•Per la decrittazione si somma al carttere del testo cifrato di nuovo il carattere oscurante

es. T (00001) carattere in chiaro  
+ (addizione modulo 2 , XOR )  
C (01110) carattere oscurante  
-----  
V (01111) carattere cifrato

# Il Cifrario di Vernam (1917)



## Telegrafo di Vernam

- *codifica binaria (5 bit)*
- *chiave lunga quanto il testo*

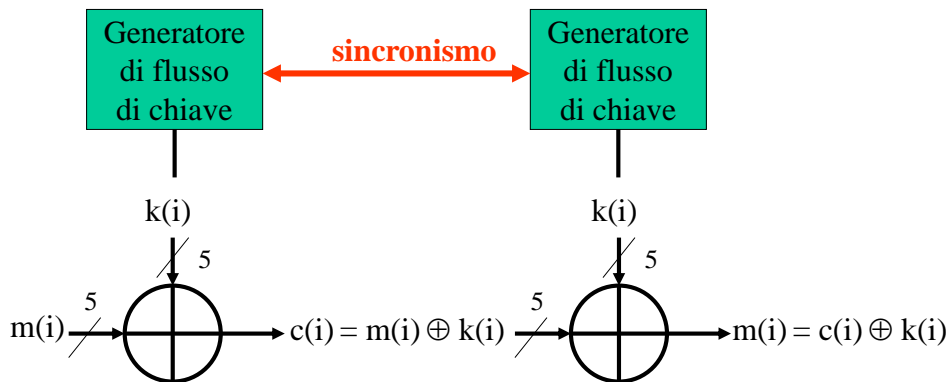
	Chiave							
Testo	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	110	111	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

**Mauborgne: chiave scelta a caso e usata una sola volta**

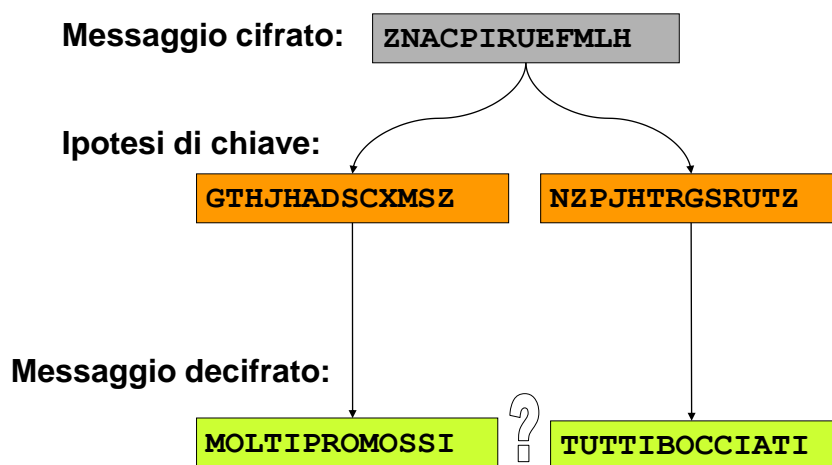
**Polialfabetica con running key**

8 righe: 8 permutazioni di {0,1,...,7}

## Il Cifrario di Vernam-Mouborgne



## One-time pad: inviolabile con attacco passivo



## Problemi di one-time pad

- Per trasmettere un messaggio riservato su un canale insicuro bisogna concordare una chiave altrettanto lunga su un canale sicuro
- Ricezione di tutto il testo cifrato in ordine

Bletchley Park

Spie russe

Telefono rosso

Attacco attivo

- Impiego di meccanismi di autenticazione (H, S)