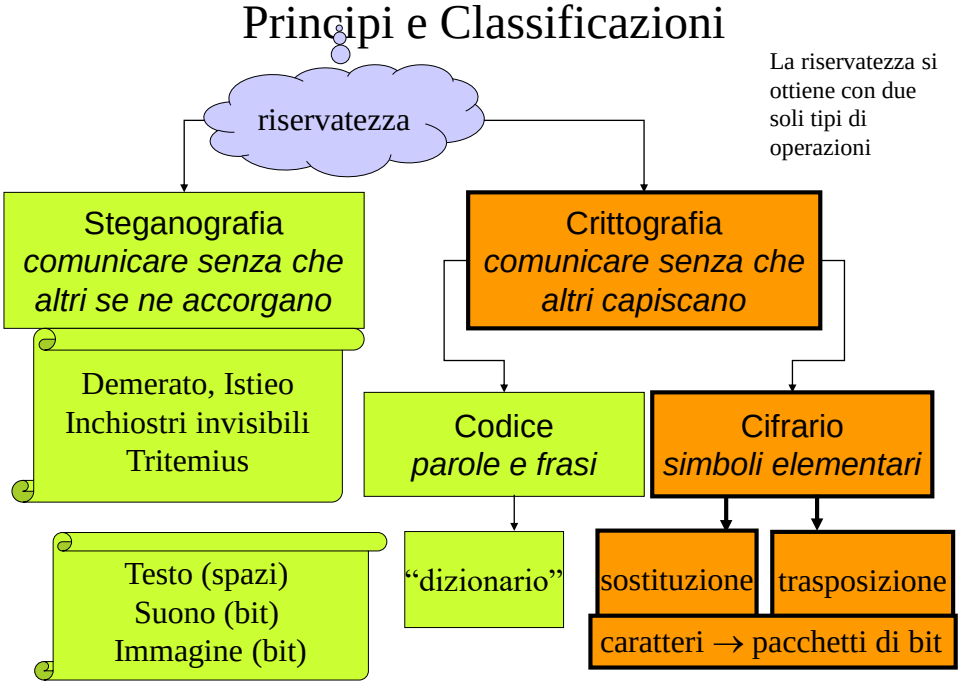
Crittologia classica

Crittografia classica: la storia

- 1900 a.c. Egitto: geroglifici non standard
- 1500 a.c Mesopotamia: Formula con molte interpretazioni
- 500 a.c Israele: Codice ATBASH per il libro di Geremia
- 500 a.c. Plutarco: Scitale degli Spartani
- 50 a.c. Svetonio: Cifrario di Giulio Cesare
- 300 d.c. Kama Sutra
- 725 d.c. Abu al Yahmadi: sostituzione e trasposizione
- XV°-XVI° sec: sostituzione polialfabetica
- 1917 Macchina di Vernam
- 1930-40 Macchine cifranti: Schrebius, Hagelin
- 1940-45 Macchine per crittanalisi: Turing, Shannon

Principi e Classificazioni



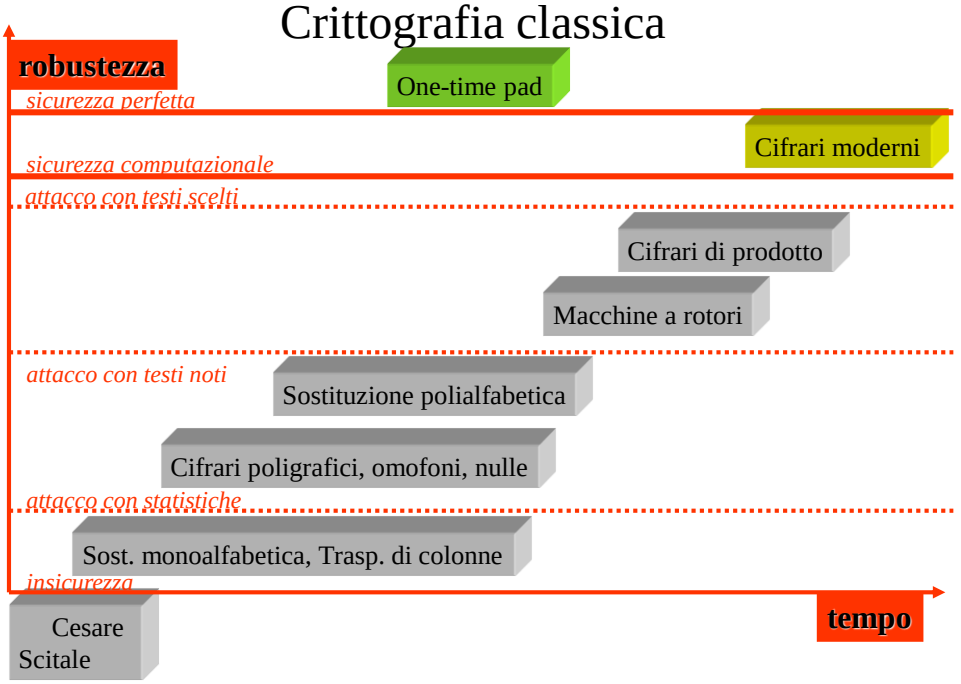
Decrittazione

Obiettivi dell'intruso:
•il testo in chiaro
•la chiave

ATTACCO	CONOSCENZE DELL'INTRUSO
con solo testo cifrato *ciphertext-only*	**linguaggio usato nel testo in chiaro e statistiche sull'occorrenza dei simboli**
con testo in chiaro noto *known plaintext*	**coppie di testo cifrato intercettato e testo in chiaro corrispondente**
con testo in chiaro scelto *chosen plaintext*	**testi cifrati corrispondenti a testi in chiaro di sua scelta**
con testo cifrato scelto *chosen ciphertext*	**testi in chiaro corrispondenti a testi cifrati di sua scelta**

Pericolosità *e quindi* **Robustezza**

Crittografia classica



Crittografia classica: la sostituzione monoalfabetica

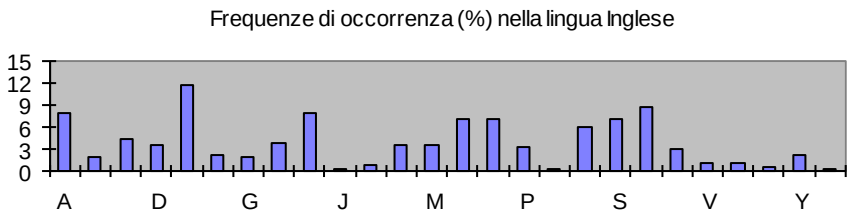
regola di sostituzione (o chiave)

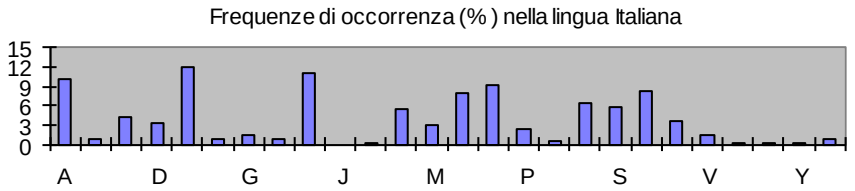
```
A B C  D E  F G H  I L M N O P Q R S T U  V Z
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
Q E M  R F  Z T B  L U P O N H A S C G V  D I
```

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 GQGXG 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 XHXXU JYQPU GOGMG TYOGA SXNYQ UJUAK UGDAN
MUGVA JJGDH TXGVA JSHYT GSYQP AANGS AODNA JHSXN GADGY TGBBG QYOAH TGQUJ UAKUG OGXHN GGDDA TGOGA SXNYQ UJUAK UGALL AMUSX YIHAJ DABBY VUJAK TYSUN GJJAK NYXHX XYAVG

frequenze dei caratteri % in italiano

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

A	B	C	D	E	F	**G**	H	I
13,52	2,41	0	2,78	0	0,74	**11,30**	4,26	0,74
J	K	L	M	N	O	P	Q	R
6,85	2,59	1,11	1,85	4,44	2,96	1,11	4,44	0
S	T	**U**	V	W	X	**Y**	Z	
4,44	7,78	**8,52**	2,78	0	6,48	**8,89**	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 QaJVa
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 QaJVa
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 QaJVa
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 × 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**
7	6	5	1	8	2	3	4

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

Simboli di riempimento

Ordine:

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 × 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
- RI → DF

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

- LP → ZL
- AK→ RX

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

- "doppia": regole varie

Sostituzione polialfabetica

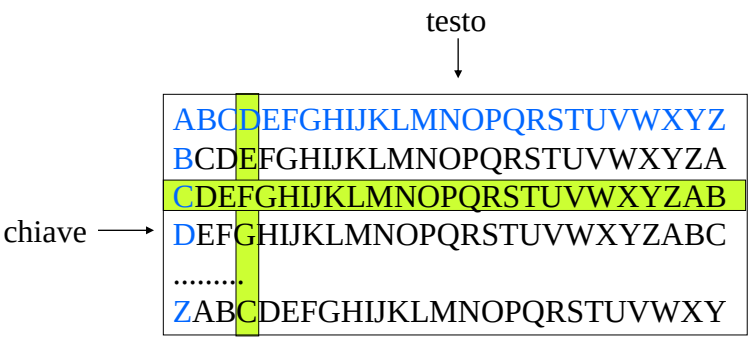
SOSTITUZIONE POLIALFABETICA

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:

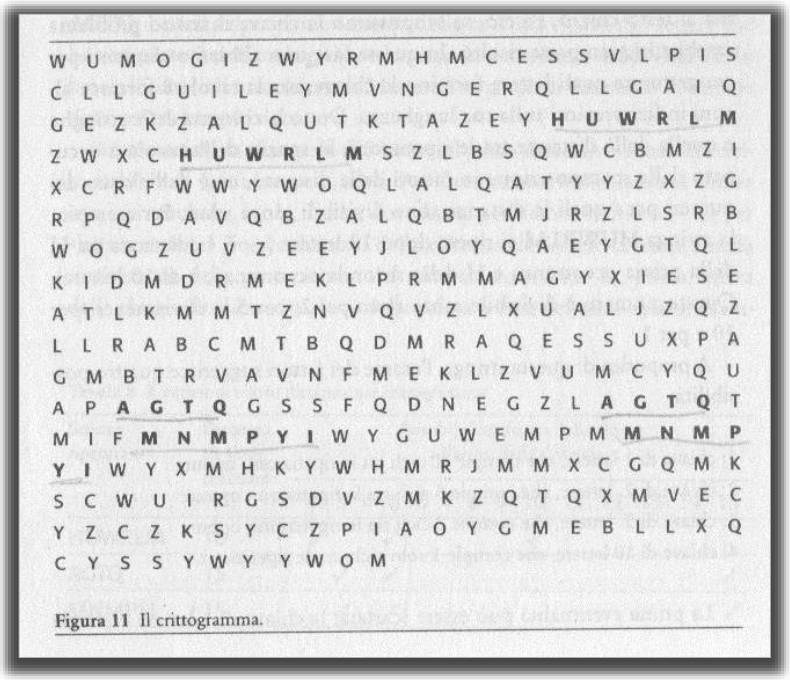
C	I	A	O	C	I	A	O	C	I	A	O	C	I
D	O	M	A	N	I	N	O	N	P	O	S	S	O
F	Z	M	O	P	S	N	C	P	A	O	H	U	Z

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**.

Chiaro	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	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
PERCHE'?



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

Figura 11 Il crittogramma.

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 ripetizioni:	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		✓		✓										✓

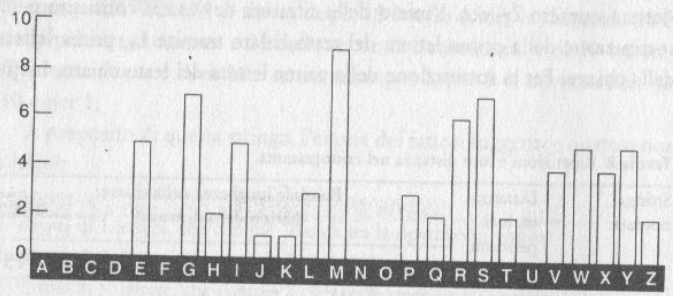


Figura 12 Distribuzione di frequenza delle lettere crittate tramite l'alfabeto cifrante L_1 (numero di occorrenze).

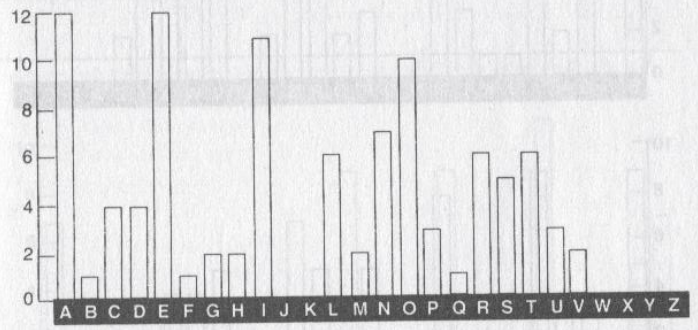


Figura 13 Distribuzione di frequenza della lingua italiana (occorrenze ogni 100).

* (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 freqenze molto basse, comprese tra l'1,5 e lo 0,5 per cento. *N.d.T.*)

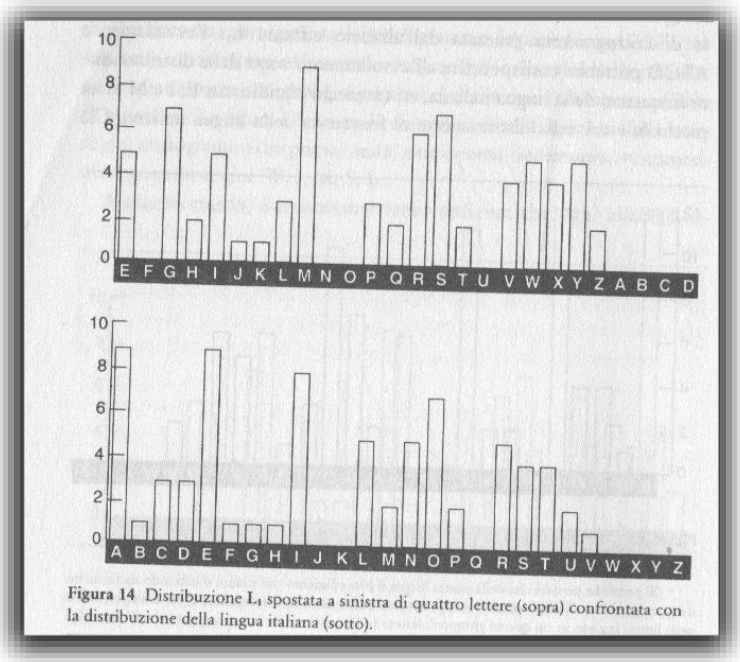


Figura 14 Distribuzione L_4 spostata a sinistra di quattro lettere (sopra) confrontata con la distribuzione della lingua italiana (sotto).

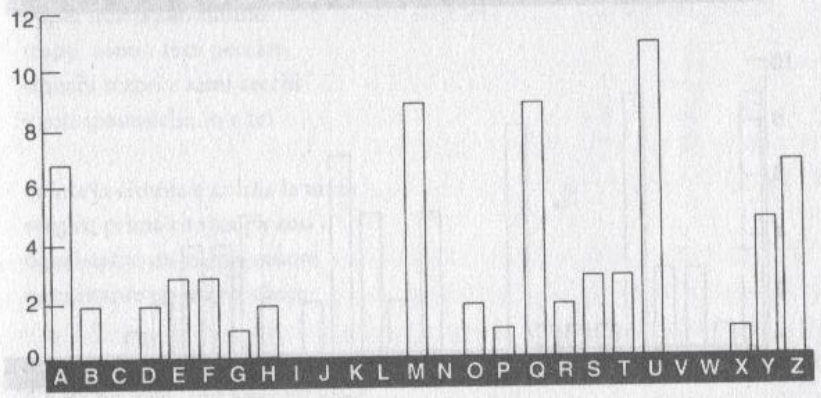


Figura 15 Distribuzione di frequenza delle lettere crittate tramite l'alfabeto cifrante L_2 (numero di occorrenze).

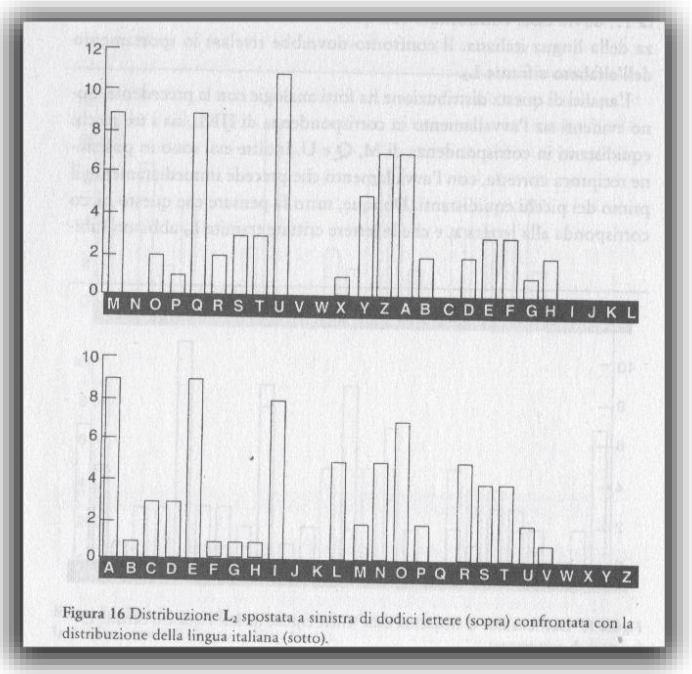
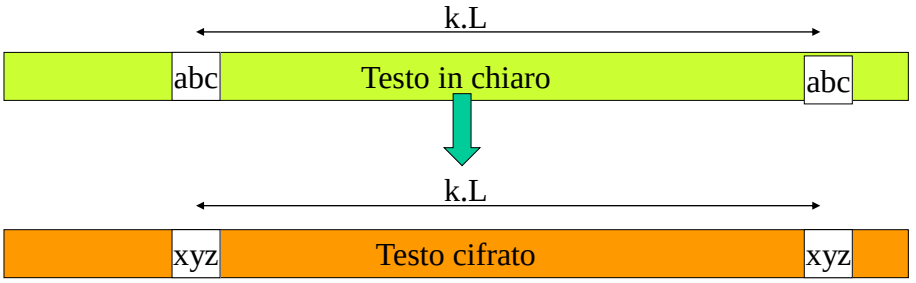


Figura 16 Distribuzione L_2 spostata a sinistra di dodici lettere (sopra) confrontata con la distribuzione della lingua italiana (sotto).

Il testo in chiaro inizia così:
Siedienontivergognareguanciaaguanciafiancoafianco….

Test di Kasiski



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 = MCD

Accorgimenti utili

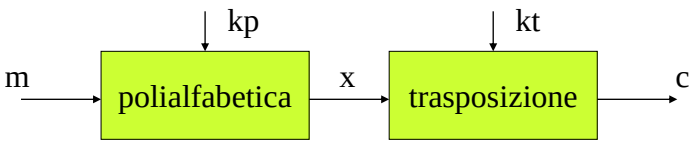
1: "*chiave lunga e scelta a caso"*

2: " *mai archiviare insieme testi cifrati e decifrazioni*".

3: " *mai lasciare incustodite macchine pronte per cifrare/decifrare*"

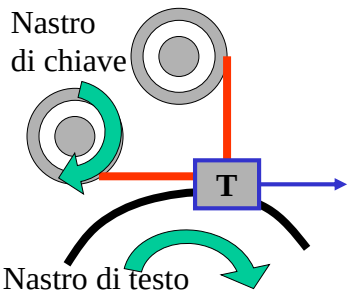
4: "*ogni simbolo del blocco in chiaro deve influire sul valore di tutti i simbolo del blocco cifrato*"

Iª Guerra Mondiale: **sopracifratura**



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*

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

•Addizione eseguiti sui singoli bit costitutivi il carattere

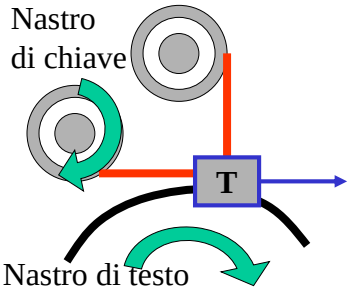
•Per la decrittazione si somma al carttere del testo cifrato di nuovo il carattere oscurante

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

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	FIGS	FIGS

Figure 3. The Baudot Code Set

Il Cifrario di Vernam (1917)



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

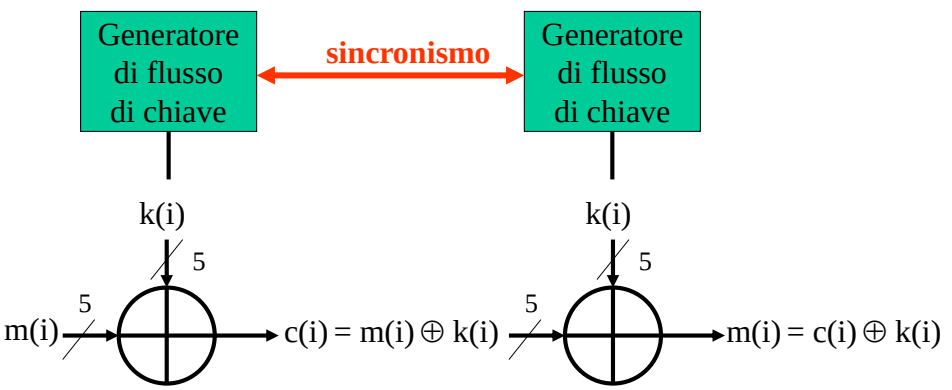
	Chiave							
Testo	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	110	111	001	000	011	010
110	110	111	100	101	010	011	000	001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

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

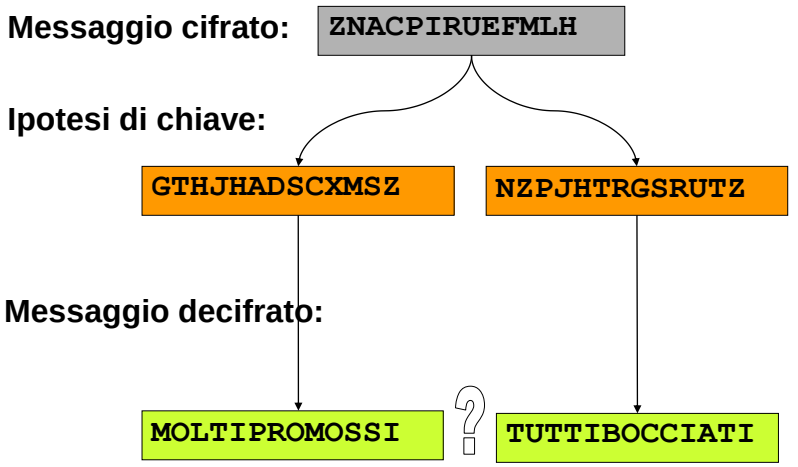
Mauborgne: *chiave scelta a caso e usata una sola volta*

Polialfabetica con *running key*

Il Cifrario di Vernam-Mouborgne



One-time pad: inviolabile con attacco passivo



Per trasmettere un messaggio riservato su un canale insicuro bisogna concordare una chiave altrettanto lunga su un canale sicuro

Problemi di one-time pad

•Accordo riservato su molte chiavi molto lunghe

•Uguale probabilità di occorrenza dei simboli di chiave

•Ricezione di tutto il testo cifrato in ordine

Bletchley Park

Spie russe

Telefono rosso

Attacco attivo

•Impiego di meccanismi di autenticazione (H, S)

Definizioni di sicurezza per un Cifrario

SEGRETEZZA PERFETTA

Un Cifrario è detto **perfetto**, o **assolutamente sicuro**, se, dopo aver intercettato un certo testo cifrato **C**, l'incertezza *a posteriori* sul testo in chiaro **M** corrispondente è uguale all'incertezza che si aveva *a priori* , cioè prima dell'intercettazione.

SICUREZZA

Un Cifrario è **sicuro** se dato un qualsiasi testo cifrato **C**, il trovare un **M** tale che $\mathbf{E_k(M) = C}$ è **impossibile** per chi non conosce **k**.

SICUREZZA COMPUTAZIONALE

Un Cifrario è detto **computazionalmente sicuro** se il calcolare **M** da un **C** è possibile, ma richiede una potenza di elaborazione superiore a quella a disposizione dell'attaccante.

Confusione & Diffusione (C. Shannon)

La **confusione** nasconde la relazione esistente tra testo in chiaro e testo cifrato e rende poco efficace lo studio del secondo basato su statistiche e ridondanze del primo.Rende difficile prevedere che cosa Accadrà al cifrato anche modificando un solo simbolo Del testo in chiaro
La **sostituzione** è il mezzo più semplice ed efficace per creare confusione.

Cifrario composto: S&T iterato

La **diffusione** nasconde la ridondanza del testo in chiaro spargendola all'interno del testo cifrato. Si impone ad ogni simbolo del testo in chiaro di influire su molti se non tutti i simboli del testo cifrato. Difficile prevedere quali e quanti si modificano se si modifica anche un solo simbolo del testo in chiaro
La **trasposizione** è il mezzo più semplice ed efficace per ottenere diffusione

Il cifrario composto