

Crittografia Classica

a.a. 2019/20

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

<http://www.di-srv.unisa.it/~ads>



Marzo 2020

Steganografia

Occultamento
del messaggio



Steganografia

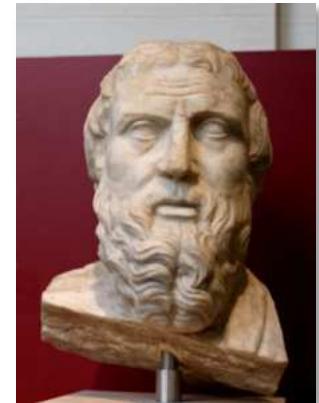
στεγανός = coperto

γραφία = scrittura

Steganografia: Esempi

Erodoto (libro V delle Storie)

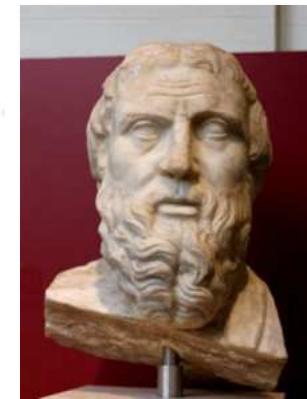
"Accadde che contemporaneamente gli giungesse anche da Susa da parte di Istieo il messaggero dalla testa segnata, che annunziava ad Aristagora di ribellarsi al re. Infatti Istieo, volendo dare ad Aristagora l'ordine di ribellarsi, non aveva alcun altro modo per annunziarglielo con sicurezza, essendo le strade sorvegliate; allora, fatta rasare la testa al più fidato degli schiavi, vi impresso dei segni e aspettò che ricrescessero i capelli. Non appena ricrebbbero, lo spedì a Mileto, non comandandogli null'altro se non che, quando giungesse a Mileto, dicesse ad Aristagora di fargli radere i capelli e di guardare la sua testa: i segni impressi ordinavano, come già prima ho detto, la rivolta. Istieo fece questo perché s'affliggeva assai d'essere trattenuto a Susa".



Steganografia: Esempi

Erodoto (libro VII delle Storie)

re (o perchè volesse in questo provvedere ai medesimi , o per insultarli , lo che io lascio che altri il pensino) appena Serse ebbe deliberato di far la spedizione in Grecia , ciò avendo saputo lo stesso Demarato , il quale era in Susa , stimò bene di farne avvisati i Lacedemonj ; e non potendo farlo altramente , poichè v'era timore che non fosse scoperto , servìssì di tale astuzia . Prese delle tavolette doppie , ne rase la cera , e poi scrisse sul legno delle medesime tavolette la risoluzione del Re . Fatto ch'ebbe ciò , distese la cera sopra le lettere , affinchè quelle tavolette , non essendo scritte , niente male arrecassero a chi le portava , per via dei custodi delle strade . Il messo di Demarato avendole ricapitate ai Lacedemonj , non potean essi da prima congetturar ciò che fossero , fino a che , come si dice , Gorgo figliuola di Cleomene , e moglie di Leonida , dopo aver pensato , insegnò loro , che togliendo la cera avrebbero trovate delle lettere sul legno . Così seguendo loro il di lei consiglio , furono ritrovate le lettere ; e dopo averle lette , le mandarono al rimanente dei Greci .



Steganografia: Esempi

- Plinio il vecchio (I secolo d.C.)
- Comunicazione mediante inchiostro simpatico ottenuto dal latice di titimabo

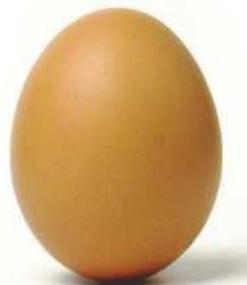


- Trasparente una volta asciutto, il latice cambia al marroncino se esposto a un calore moderato
- Comportamento legato alla presenza del carbonio, di cui le molecole organiche sono ricche

Steganografia: Esempi

Gian Battista Della Porta (XVI secolo)

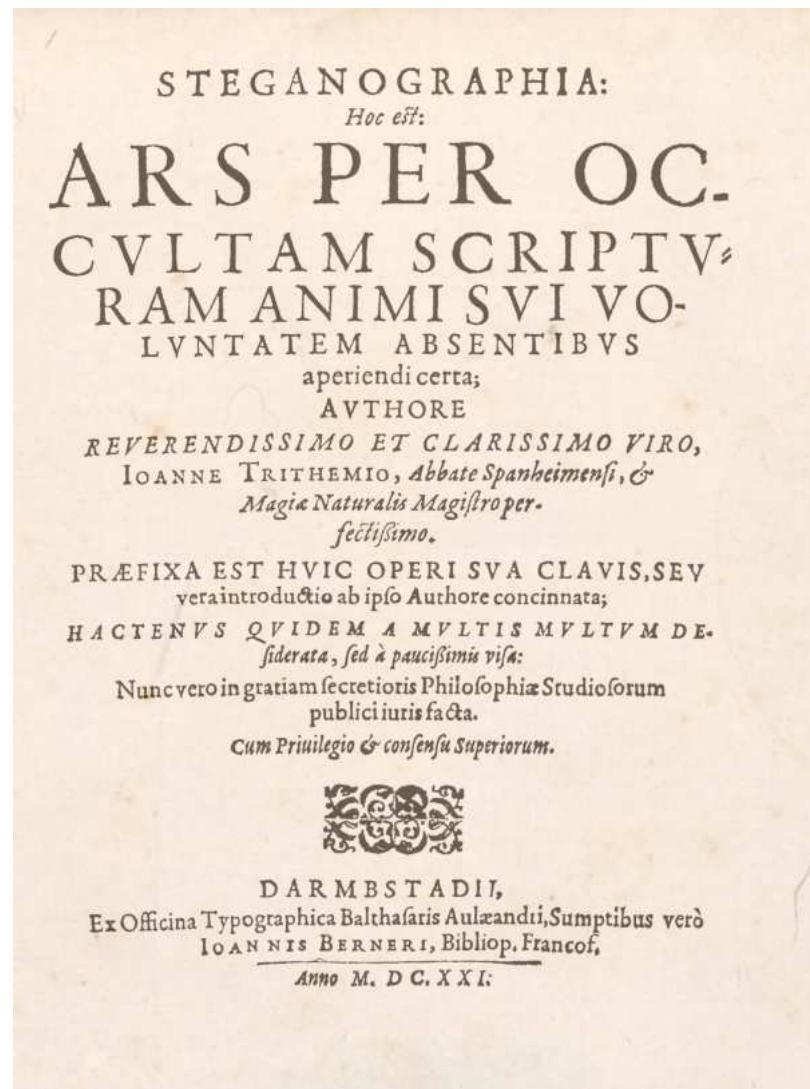
Comunicazione mediante uovo sodo e una sorta di “inchiostro simpatico”



- Si prepara un inchiostro con 30 grammi di allume in mezzo litro di aceto
- Si scrive sul guscio, che è poroso, senza lasciar traccia
- Questo tinge l'albumen solidificato
- Il messaggio si legge sbucciando l'uovo

Primo uso del termine Steganografia

Johannes Trithemius
1499



Steganografia: Problemi

Se il corriere è attentamente perquisito il messaggio può essere scoperto

- Raschiando tavolette di cera
- Rasando il capo al corriere
- Avvicinando il foglio ad una fonte di calore
- Sbucciando le uova

La segretezza è perduta al momento dell'intercettazione

Crittografia

Trasformazione

+

Segretezza



Crittografia

Cryptos = nascosto,
segreto

Grafiēn = scrittura

Alcuni metodi antichi di cifratura

Scitala

- Usata dai Greci antichi, in particolare dagli Spartani, nelle missioni militari
- Descritta da Plutarco (46-125 d.C.) in "Vita di Lisandro", *Le vite parallele* di Plutarco



Alcuni metodi antichi di cifratura

Quadrato di Polibio o Scacchiera di Polibio

➤ Descritto da Polibio (206-124 a.C.) nelle "Storie"

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I J	K
3	L	M	N	O P	
4	Q	R	S	T	U
5	V	W	X	Y	Z

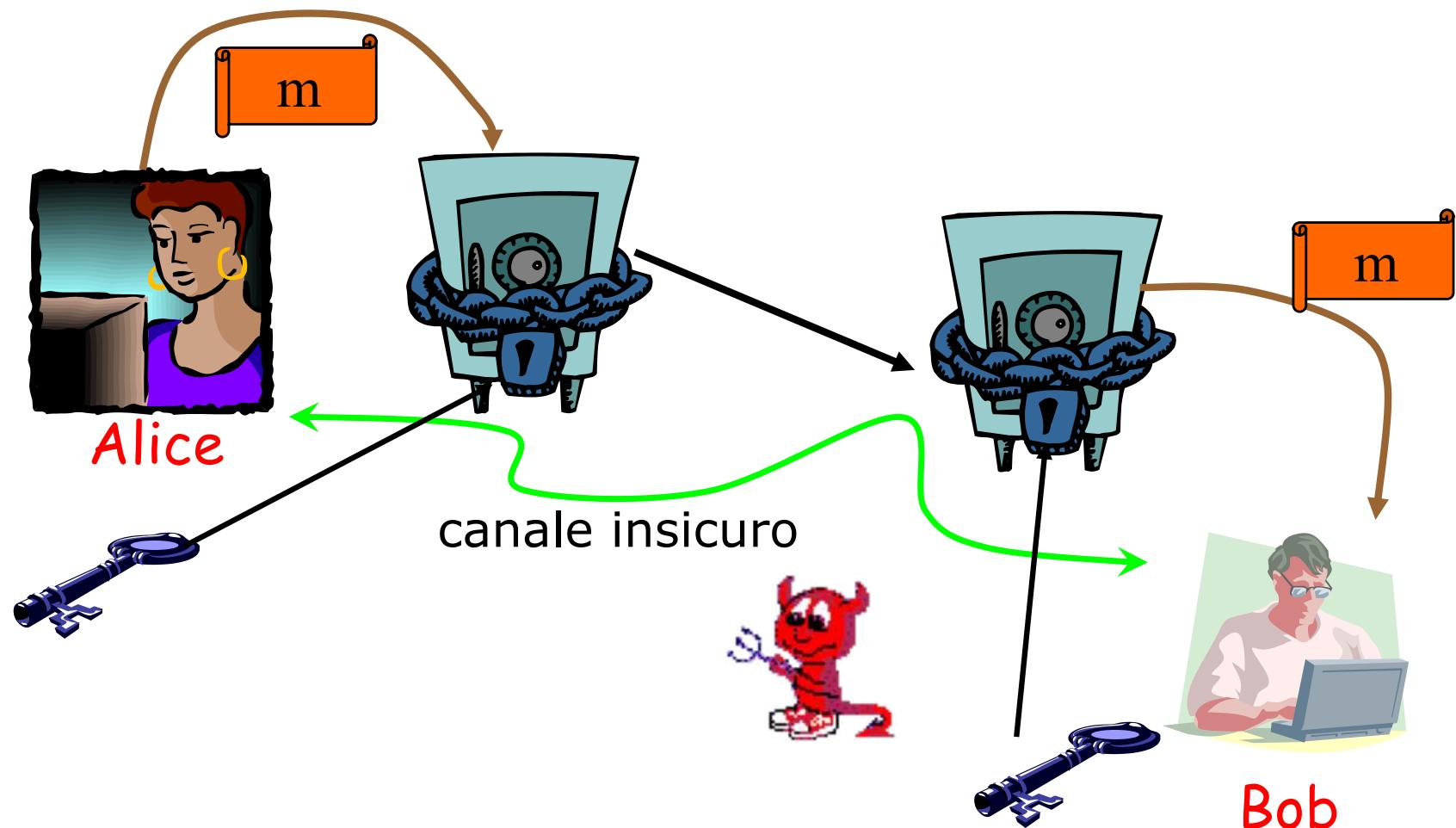


testo in chiaro: C A S A

testo cifrato: (1,3) (1,1) (4,3) (1,1)

Cifrari simmetrici

Operazioni:
trasposizioni e sostituzioni



Cifrari a trasposizione

Trasposizione:

- Permutazione del testo in chiaro

I simboli del testo in chiaro cambiano posizione
nel testo cifrato

Esempio

- MESSAGGIO SEGRETO

- MSAGOERTESGISGEO

MSAGOERT
ESGI SGEO

Tecniche di trasposizione

Basate su matrici

EGGSOESIRMGEOST

4	1	3	2	5
M	E	S	S	A
G	G	I	O	S
E	G	R	E	T
O				

Tecniche di trasposizione

Basate su matrici

EGGSOESIRMGEOST

4	1	3	2	5
M	E	S	S	A
G	G	I	O	S
E	G	R	E	T
O				

Come si decifra?

Tecniche di trasposizione

Basate su matrici

EGGSOESIRMGEOST

Ripetizione trasposizione

GSESRAGIOEEGTOMS

4	1	3	2	5
M	E	S	S	A
G	G	I	O	S
E	G	R	E	T
O				

4	1	3	2	5
E	G	G	S	O
E	S	I	R	M
G	E	O	A	S
T				

Tecniche di trasposizione

- Usate da sole sono facili da analizzare
 - Le lettere del testo in chiaro sono visibili
 - LTEETRE DEL TSETO IN CIHRAO SNOO VSIBILII
- Possono essere usate insieme a tecniche con sostituzione

Cifrario di Cesare

100-44 a.C.

Svetonio (*Vitae Caesarorum*): lettera di Cesare a Cicerone

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

testo in chiaro

$$X \leftarrow M + 3 \bmod 26$$

OMNIA GALLIA EST DIVISA IN PARTES TRES
RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV

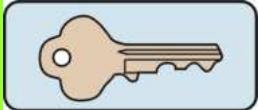
testo cifrato

Cifrari con shift

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cifrari con shift

Chiave K



$$X \leftarrow M+K \bmod 26 \quad K \in \{0, \dots, 25\}$$

Quante chiavi sono possibili?

Crittoanalisi

Dato un testo cifrato

- Provo tutte le possibili chiavi

Facile da fare

- Poco tempo

Una sola chiave mi darà un testo in chiaro con
senso compiuto

- È il messaggio originale

Crittanalisi

K	RX KTSXPBD HIPHTGP
1	SY LUTYQCE IJQIUHQ
2	TZ MVUZRDF JKRJVIR
3	UA NWVASEG KLSKWJS
4	VB OXWBTFH LMTLXKT
5	WC PYXCUGI MNUMYLU
6	XD QZYDVHJ NOVNZMV
7	YE RAZEWIK OPWOANW
8	ZF SBAFXJL PQXPBOX
9	AG TCBGYKM QRYQCPY
10	BH UDCHZLN RSZRDQZ
11	CI VEDIAMO STASERA
12	DJ WFEJBNP TUBTFSB

13	EK XGFKCOQ UVCUGTC
14	FL YHGLDPR VWDVHUD
15	GM ZIHMEQS WXEWIVE
16	HN AJINFRT XYFXJWF
17	IO BKJOGSU YZGYKXG
18	JP CLKPHTV ZAHZLYH
19	KQ DMLQIUW ABIAMZI
20	LR ENMRJVX BCJBNAJ
21	MS FONSKWY CDKCOBK
22	NT GPOTLXZ DELDPCL
23	OU HQPUMYA EFMEQDM
24	PV IRQVNZB FGNFREN
25	QW JSRWOAC GHOGSFO

Cifrari a sostituzione monoalfabetica

Alfabeto in chiaro

Alfabeto cifrante

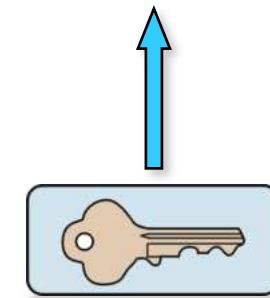
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	C	T	M	B	W	L	A	K	J	D	X	I	N	E	Y	S	U	P	F	Z	R	Q	H	V	G

testo in chiaro:

C A S A

testo cifrato:

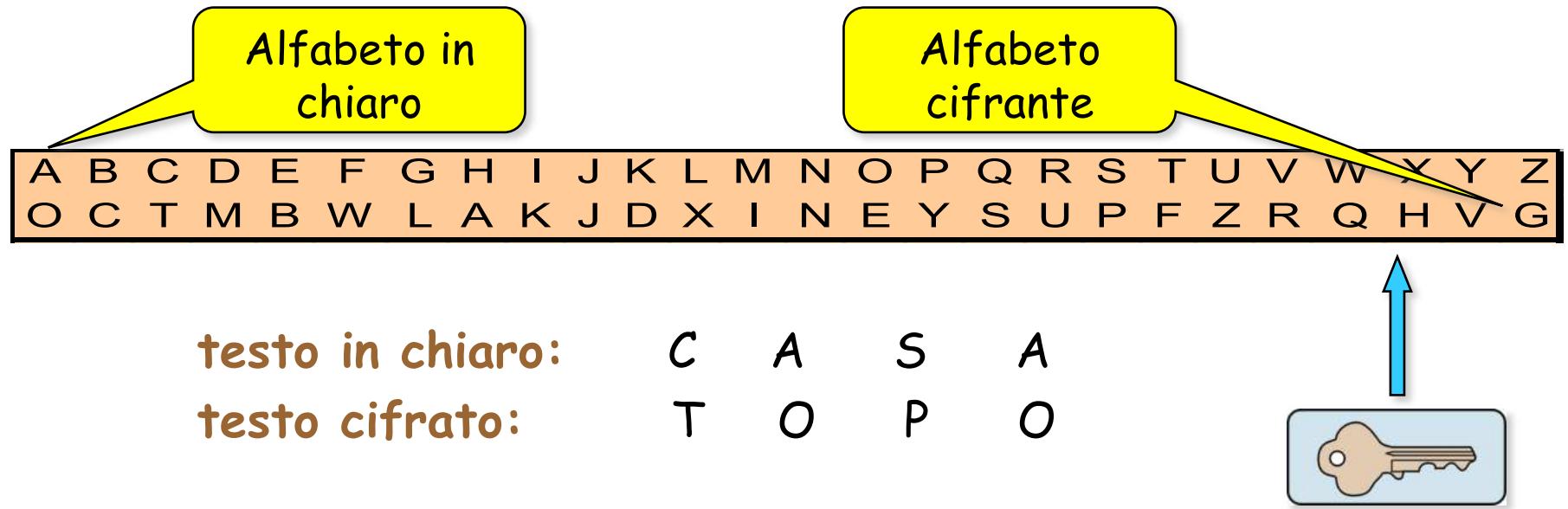
T O P O



Quante sono le possibili chiavi?



Cifrari a sostituzione monoalfabetica



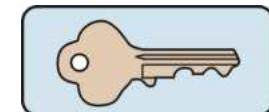
Numero di chiavi da provare: $26! \approx 4 \times 10^{26}$

Con 10^6 computer, ognuno che prova 10^9 chiavi al secondo, la ricerca esaustiva richiede $\approx 10^4$ anni

Improponebile!

Cifrari a sostituzione monoalfabetica con chiave

Frase chiave: JULIUS CAESAR



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

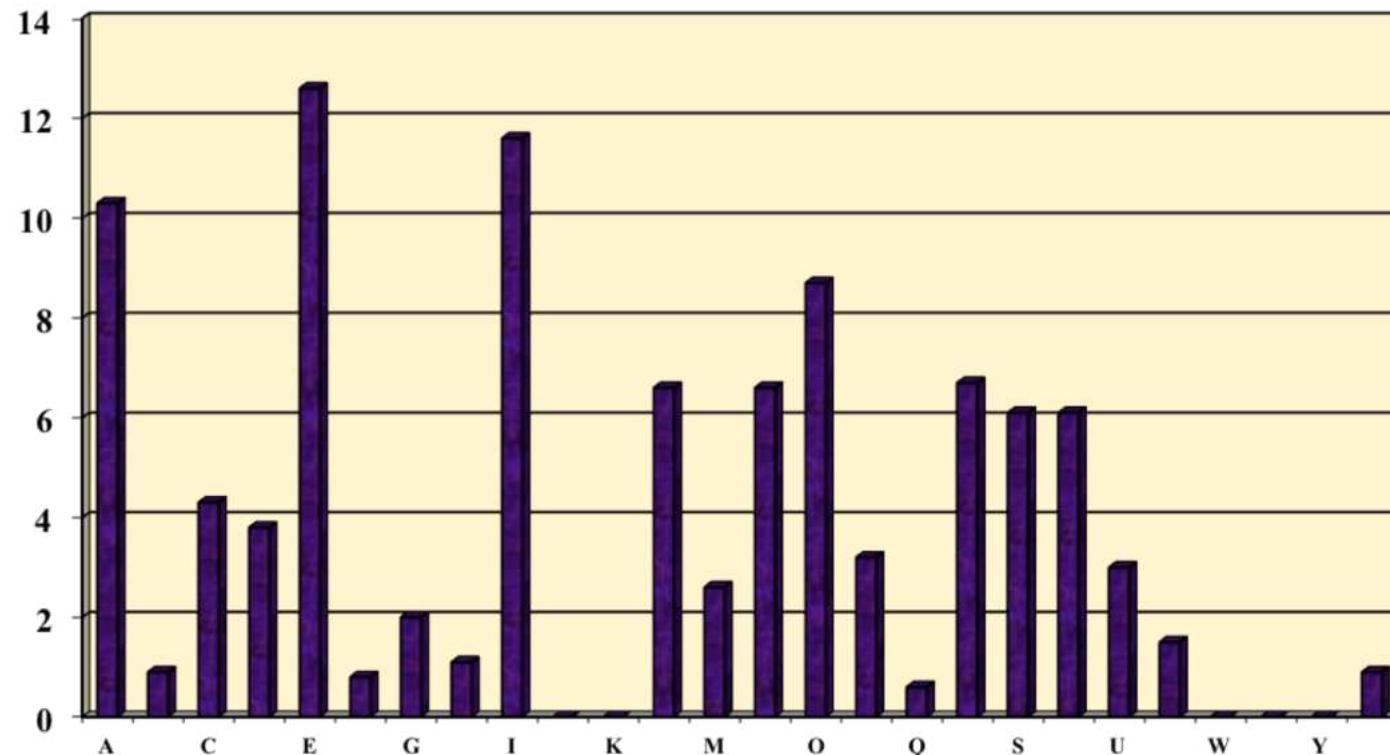
Quante chiavi sono possibili?

Più di 26, ma meno di 26!

Crittoanalisi

- Ogni lettera cambia “abito”, ma conserva la sua “identità”
 - Frequenza
 - Vicinanza con altre lettere (q è sempre seguita da u,...)
 - Altre regole
- Il cifrario può essere rotto considerando le regolarità del linguaggio
 - Calcolo della frequenza relativa delle lettere nel cfrato
 - Confronto con la distribuzione standard delle frequenze per quel linguaggio

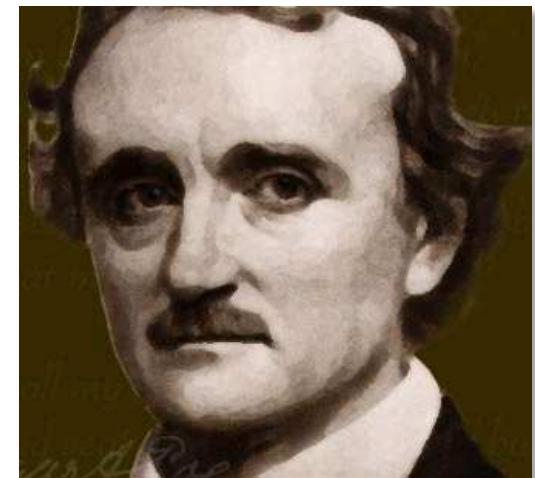
Frequenze occorrenze lettere



	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
italiano	10,3	0,9	4,3	3,8	12,6	0,8	2,0	1,1	11,6	0,0	0,0	6,6	2,6	6,6	8,7	3,2	0,6	6,7	6,1	6,1	3,0	1,5	0,0	0,0	0,0	0,9
inglese	7,3	1,3	3,5	4,3	12,8	3,0	2,0	3,5	7,8	0,3	0,5	3,7	2,8	7,8	7,5	2,8	0,5	8,5	6,0	9,3	3,0	1,5	1,5	0,5	2,3	0,3
francese	8,3	1,3	3,3	3,8	17,8	1,3	1,3	1,3	7,3	0,8	0,0	5,8	3,2	7,2	5,7	3,7	1,2	7,3	8,3	7,2	6,3	1,8	0,0	0,0	0,8	0,0

Crittoanalisi

Edgar Allan Poe, "Lo scarabeo d'oro" (1843)



53++!305))6*;4826)4+.)4+);806*;48!8`60))85;]8*:+*8!83(88)5*!;
46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8`8*; 4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;

Crittoanalisi

53++!305))6*;4826)4+.)4+);806*;48!8` 60))85;]8*:+*8!83(88)5*!;
46(;88*96*?;8)*+(:485);5*!2:*+(:4956*2(5*-4)8` 8*; 4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;



caratteri occorrenze

8	33
:	26
4	19
+)	16
*	13
5	12
6	11
! 1	8
0	6
9 2	5
: 3	4
?	3
`	2
- .	1

Crittoanalisi

53++!305))6*;4826)4+.)4+);806*;48!8` 60))85;]8*:+*8!83(88)5*!;
46(;88*96*?;8)*+(:485);5*!2:*+(:4956*2(5*-4)8` 8*; 4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;



caratteri occorrenze

8	33
:	26
4	19
+)	16
*	13
5	12
6	11
! 1	8
0	6
9 2	5
: 3	4
?	3
`	2
- .	1

Assumiamo che 8
corrisponda al carattere e

Crittoanalisi

53++!305))6*;4826)4+.)4+);806*;48!8` 60))85;]8*:+*8!83(88)5*!;
46(;88*96*?;8)*+(:485);5*!2: *+(:4956*2(5*-4)8` 8*; 4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;



caratteri occorrenze

8	33
:	26
4	19
+	16
*	13
5	12
6	11
!	8
1	8
0	6
9	5
2	5
:	4
3	4
?	3
`	2
-	1
.	1

Assumiamo che 8
corrisponda al carattere e

7 occorrenze di ;48

Crittoanalisi

53++!305))6*;4826)4+.)4+);806*;48!8` 60))85;]8*:+*8!83(88)5*!;
46(;88*96*?;8)*+(:485);5*!2: *+(:4956*2(5*-4)8` 8*; 4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;



caratteri occorrenze

8	33
:	26
4	19
+	16
*	13
5	12
6	11
!	8
1	8
0	6
9	5
2	5
:	4
3	4
?	3
`	2
-	1
.	1

Assumiamo che 8
corrisponda al carattere e

7 occorrenze di ;48
Assumiamo che ; ⇒ t
4 ⇒ h
8 ⇒ e

...poi

Crittoanalisi

53++!305))6*;4826)4+.)4+);806*;48!8` 60))85;]8*:+*8!83(88)5*!;
46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8` 8*; 4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;



5 rappresenta a

!	"	d
8	"	e
3	"	g
4	"	h
6	"	i
*	"	n
+	"	o
("	r
:	"	t

A good glass in the bishop's hostel in the devil's seat twenty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line from the tree through the shot fifty feet out.

Few persons can be made to believe
that it is not quite an easy thing to
invent a method of secret writing
which shall baffle investigation.
Yet it may be roundly asserted
that human ingenuity cannot
concoct a cipher which human
ingenuity cannot resolve.

Edgar Allan Poe

Tecniche per “evitare” analisi statistiche

- Nulle
- Omofoni

Null

- Aggiungere simboli meno frequenti
 - in posizioni da non alterare il significato

testo in chiaro: QUELQRAMODELQLAGO...

testo cifrato: ...

Aumento frequenze dei corrispondenti simboli

Omofoni

- Molti simboli per cifrare singoli caratteri frequenti

testo in chiaro: E

testo cifrato: Õ Ñ ® (scelti a caso!)

- Si abbassano le frequenze dei simboli del testo cifrato

12.6 per E → 3.15 per Õ Ñ ®

Nomenclatori

- In aggiunta all'alfabeto cifrante si usa un insieme di **parole in codice**
- Variante di cifrario a sostituzione
- Inizialmente ristretto a nomi di persone importanti
 - Il nomenclatore era un pubblico ufficiale che annunciava i titoli dei dignitari in visita alle corti reali
- Diffusi dall'inizio del XV secolo alla fine del XVIII secolo
- Raggiunsero i 50.000 simboli

Nomenclatori

- In aggiunta all'alfabeto cifrante si usa un insieme di **parole in codice**
- Un tipo di cifrario a sostituzione
- Inizialmente ristretto a nomi di persone importanti
 - Il nomenclatore era un pubblico ufficiale che annunciava i titoli dei dignitari in visita alle corti reali
- Svantaggi:
 - Compilazione e trasporto del repertorio
 - Se cade in mani ostili
 - Non molto più sicuro della singola sostituzione monoalfabetica

Crittoanalisi

Conseguenza tragica di una attività di crittoanalisi

Nel 1587 Maria Stuarda, (1542-1587), regina di Scozia, fu decapitata per aver cospirato contro la cugina Elisabetta



La congiura di Babington

- Maria Stuarda, regina di Scozia (dal 1542 al 1567),
 - al suo rientro in Inghilterra nel 1567 fu messa in prigione dalla cugina Elisabetta I
 - rimase in prigione per 19 anni
 - Anima del cattolicesimo inglese



- Anthony Babington, paggio di Maria Stuarda, ordì una congiura che prevedeva
 - La liberazione di Maria dalla prigione
 - L'uccisione di Elisabetta
 - Una ribellione alla religione protestante

La congiura di Babington

- Sir Francis Walsingham, segretario di stato, provò che Maria aveva preso parte alla congiura
- Dopo un lavoro di crittoanalisi, la decifrazione dei messaggi chiarì che Maria Stuarda condivideva il piano



La congiura di Babington

- Sir Francis Walsingham, segretario di stato, provò che Maria aveva preso parte alla congiura
- Dopo un lavoro di crittoanalisi, la decifrazione dei messaggi chiarì che Maria Stuarda condivideva il piano



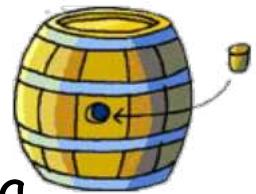
- Una considerazione:
Le comunicazioni sono molto più esplicite
se chi parla pensa di non essere intercettato!



La congiura di Babington

Maria e Babington comunicavano grazie a

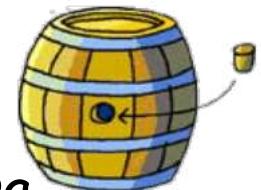
- Un corriere (Gilbert Gifford)
- Un birraio, che nascondeva i messaggi avvolti in un sacchetto di cuoio dentro lo zipolo delle botti di birra
- Un cifrario



La congiura di Babington

Maria e Babington comunicavano grazie a

- Un corriere (Gilbert Gifford)
- Un birraio, che nascondeva i messaggi avvolti in un sacchetto di cuoio dentro lo zipolo delle botti di birra
- Un cifrario, costituito da



23 simboli che sostituivano le lettere

a b c d e f g h i k l m n o p q r s t u x y z
○ † ↗ # a □ θ ∞ i ɔ n / / φ v s m f Δ E C 7 8 9

4 nulle

Nulles ff.—.—.d.

Dowbleth σ

un simbolo per le doppie

Un nomenclatore di 35 simboli, che sostituivano parole o frasi

and for with that if but where as of the from by
z 3 4 + 4 3 ɔ n m 8 x w
so not when there this in wiche is what say me my wyrt
ɔ x + w 6 x z b m n m m o
send lre receave bearer I pray you Mte your name myne
l s t T L R - R ɔ ss

La

ngton

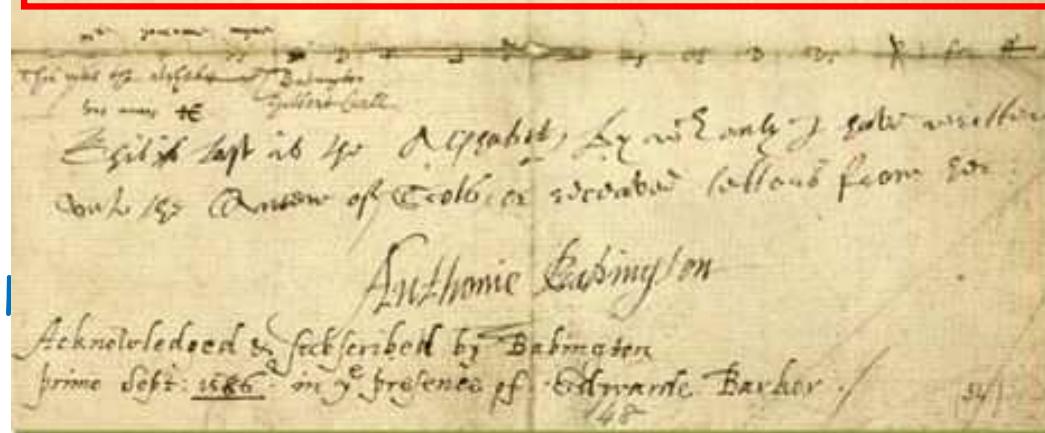
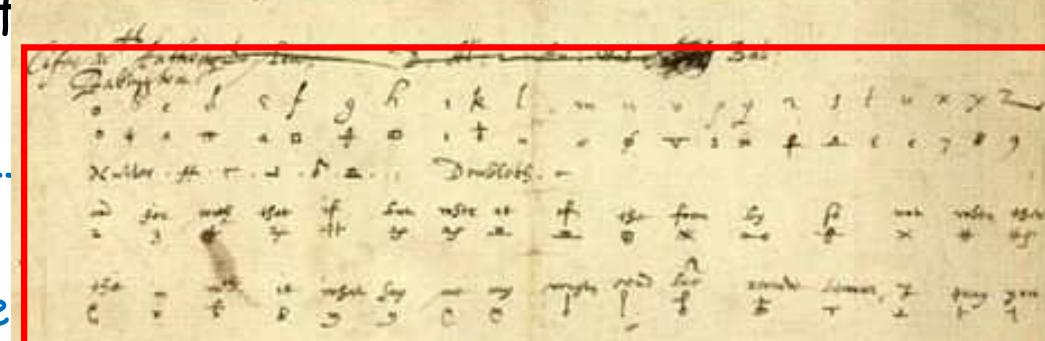
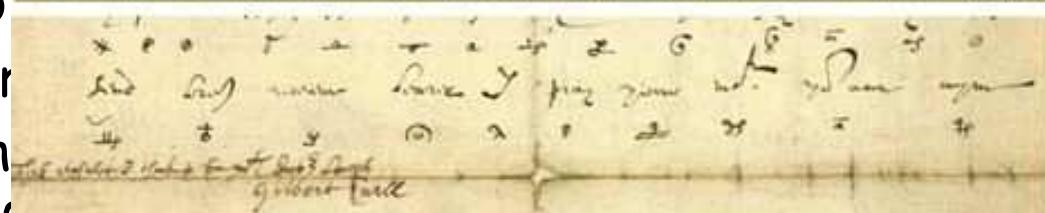
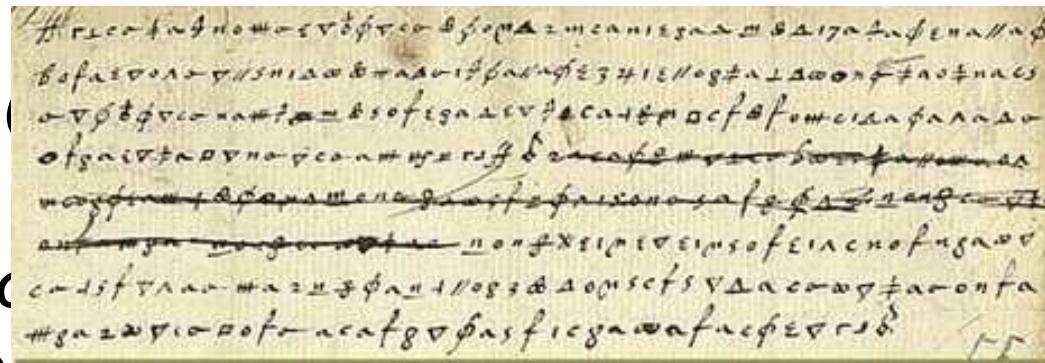
Maria e Bo

- Un co
- Un bir
- sacch
- Un cif

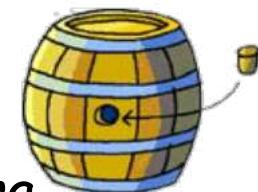
23 simboli che sostituivano le let-

4 nulle

Un nomenclatore
35 simboli, che sostituivano parole
frasi



in un
di birra



s t u x y z
Δ E C 7 8 9

un simbolo
per le doppie

rom by
X ∞

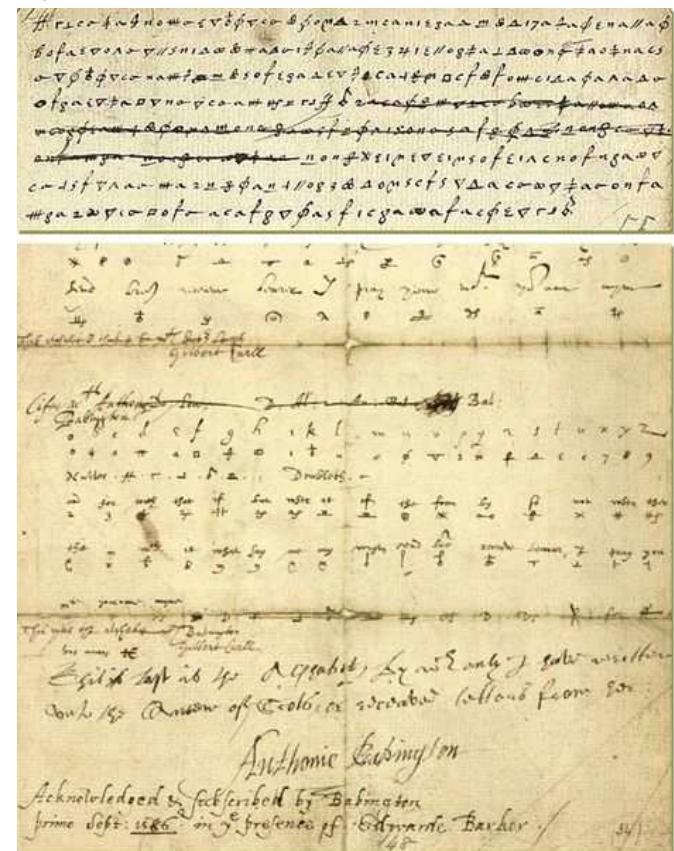
me my wyrt
M M O

ur name myne
ȝ SS

La congiura di Babington

Gifford consegnava a Walsingham tutti i messaggi, che venivano decifrati da Thomas Phelippes

- Maria firmò la sua condanna a morte rispondendo alla lettera di Babington
 - Babington e complici furono arrestati e squartati vivi
 - Maria fu decapitata l'8 febbraio 1587



Oltre la cifratura monoalfabetica

Due approcci:

- Utilizzo di cifrature di più lettere per volta
 - Playfair
 - Hill
- Utilizzo di più alfabeti cifranti
 - Leon Battista Alberti
 - Vigenère

Cifrario di Playfair

Cifratura multilettera di Playfair

- Cifra due simboli insieme
- Utilizza una matrice 5x5
 - Costruita a partire da una parola chiave per facilità di memorizzazione
 - I J equivalenti

Inventato da Charles Wheatstone, 1854
Divulgato dall'amico Lord Playfair

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

Cifrario di Playfair

Lettere di ogni coppia diverse

- Si introduce un simbolo fittizio
 - Pallone = pa lx lo ne

Si individuano le due lettere nella matrice

- Se individuano un rettangolo
 - Ciascuna lettera sostituita dalla lettera che si trova nella stessa riga del rettangolo
- Se individuano una colonna
 - Ciascuna lettera sostituita dalla seguente nella colonna
- Se individuano una riga
 - Ciascuna lettera sostituita dalla seguente nella riga

Cifrario di Playfair

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

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

testo in chiaro: AT TA CX CO

testo cifrato: RS

Cifrario di Playfair

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

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

testo in chiaro: AT TA CX CO

testo cifrato: RS SR

Cifrario di Playfair

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

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

testo in chiaro: AT TA CX CO

testo cifrato: RS SR BU

Cifrario di Playfair

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

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

testo in chiaro: AT TA CX CO

testo cifrato: RS SR BU HM

Cifrario di Playfair

- Migliore rispetto alla cifratura monoalfabetica: $26 \times 26 = 676$ digrammi
 - Ma la struttura del testo rimane!
- Analisi condotta in base alla frequenza dei digrammi più comuni nella lingua
 - Italiano: er, es, on, re, en, de, di, ti, si, al, ...

Cifrario di Playfair

- Frequenza digrammi inglese
- Esempio: th 315

	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	1	32	39	15		10	18		16	10	77	18	172		2	31	1	101	67	124	12	24	7		27	1			
B	8				58				6	2		21	1		11			6	5		25				19				
C	44		12		55	1		46	15		8	16			59	1		7	1	38	16		1						
D	45	18	4	10	39	12	2	3	57	1		7	9	5	37	7	1	10	32	39	8	4	9		6				
E	131	11	64	107	39	23	20	15	40	1	2	46	43	120	46	32	14	154	145	80	7	16	41	17	17				
F	21	2	9	1	25	14	1	6	21	1		10	3	2	38	3		4	8	42	11	1	4		1				
G	11	2	1	1	32	3	1	16	10		4	1	3	23	1		21	7	13	8		2		1					
H	84	1	2	1	251	2		5	72		3	1	2	46	1		8	3	22	2		7		1					
I	18	7	55	16	37	27	10			8	39	32	169	63	3		21	106	88		14	1	1		4				
J					2									4					4										
K					28				8				3	3				2	1		3		3						
L	34	7	8	28	72	5	1		57	1	3	55	4	1	28	2	2	2	12	19	8	2	5		47				
M	56	9	1	2	48			1	26			5	3	28	16			6	6	13		2		3					
N	54	7	31	118	64	8	75	9	37	3	3	10	7	9	65	7		5	51	110	12	4	15	1	14				
O	9	18	18	16	3	94	3	3	13	5	17	44	145	23	29		113	37	53	96	13	36		4	2				
P	21	1			40			7	8		29				28	26		42	3	14	7	1		2					
Q																			20										
R	57	4	14	16	148	6	6	3	77	1	11	12	15	12	54	8		18	39	63	6	5	10		17				
S	75	13	21	6	84	13	6	30	42	2	6	14	19	71	24	2	6	41	121	30	2	27		4					
T	56	14	6	9	94	5	1	315	128		12	14	8	111	8		30	32	53	22	4	16		21					
U	18	5	17	11	11	1	12	2	5		28	9	33	2	17		49	42	45					1	1				
V	15				53				19					6															
W	32		3	4	30	1		48	37		4	1	10	17	2		1	3	6	1	1	2							
X	3		5		1				4					1	4				1	1									
Y	11	11	10	4	12	3	5	5	18		6	4	3	28	7		5	17	21	1	3	14					1		
Z						5			2		1																		

Frequenza trigrammi in inglese

THE	1182	CON	114	UND	83	DIN	68	SAN	59
ING	356	NCE	113	INT	80	STI	68	STE	59
AND	284	ALL	111	ANT	79	NOT	67	ANY	58
ION	252	EVE	111	HOU	77	ORT	67	ART	58
ENT	246	ITH	111	MEN	76	THO	66	NTE	58
FOR	191	TED	110	WAS	76	DAY	65	RAT	58
TIO	188	AIN	108	OUN	75	ORE	65	TUR	58
ERE	173	EST	106	PRO	75	BUT	64	ICA	57
HER	170	MAN	101	STA	75	OUT	63	ICH	57
ATE	165	RED	101	INE	73	URE	63	NDE	57
VER	159	THI	100	WHI	71	STR	62	PRE	57
TER	157	IVE	96	OVE	71	TIC	62	ENC	56
THA	155	REA	95	TIN	71	AME	61	HAS	56
ATI	148	WIT	93	AST	70	COM	61	WHE	55
HAT	138	ONS	92	DER	70	OUR	61	WIL	55
ERS	135	ESS	90	OUS	70	WER	61	ERA	54
HIS	130	AVE	84	ROM	70	OME	60	LIN	54
RES	125	PER	84	VEN	70	EEN	59	TRA	54
ILL	118	ECT	83	ARD	69	LAR	59		
ARE	117	ONE	83	EAR	69	LES	59		

<http://jnicholl.org/Cryptanalysis/Data/EnglishData.php>

Frequenza parole in inglese

THE	15568	OR	1101	WHEN	603	ONLY	309
OF	9767	HER	1093	WHAT	570	ANY	302
AND	7638	HAD	1062	YOUR	533	THEN	298
TO	5739	AT	1053	MORE	523	ABOUT	294
A	5074	FROM	1039	WOULD	516	THOSE	288
IN	4312	THIS	1021	THEM	498	CAN	285
THAT	3017	MY	963	SOME	478	MADE	284
IS	2509	THEY	959	THAN	445	WELL	283
I	2292	ALL	881	MAY	441	OLD	282
IT	2255	THEIR	824	UPON	430	MUST	280
FOR	1869	AN	789	ITS	425	US	279
AS	1853	SHE	775	OUT	387	SAID	276
WITH	1849	HAS	753	INTO	387	TIME	273
WAS	1761	WHERE	752	OUR	386	EVEN	272
HIS	1732	ME	745	THESE	385	NEW	265
HE	1727	BEEN	720	MAN	383	COULD	264
BE	1535	HIM	708	UP	369	VERY	259
NOT	1496	ONE	700	DO	360	MUCH	252
BY	1392	SO	696	LIKE	354	OWN	251
BUT	1379	IF	684	SHALL	351	MOST	251
HAVE	1344	WILL	680	GREAT	340	MIGHT	250
YOU	1336	THERE	668	NOW	331	FIRST	249
WHICH	1291	WHO	664	SUCH	328	AFTER	247
ARE	1222	NO	658	SHOULD	327	YET	247
ON	1155	WE	638	OTHER	320	TWO	244

<http://jnicholl.org/Cryptanalysis/Data/EnglishData.php>

Cifrario di Hill

Lester S. Hill, 1929

Cifratura multi-lettera

- m lettere in chiaro successive
- m lettere di testo cifrato
- Sostituzione usando algebra lineare

Per $m=3$ la cifratura delle 3 lettere $p_1p_2p_3$ è

- $c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \text{ mod } 26$
- $c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \text{ mod } 26$
- $c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \text{ mod } 26$

Cifrario di Hill

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{12} & k_{22} & k_{23} \\ k_{13} & k_{32} & k_{33} \end{bmatrix} \times \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \text{ mod } 26$$

La chiave K è la matrice dei coefficienti k

Es. P = PAYMOREMONEY

Chiave

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

Cifrario di Hill

$m=3$, primi 3 caratteri

➤ PAY = (15, 0, 24)

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \times \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \text{ mod } 26$$

➤ Testo cifrato: (11,13,18) = LNS

Testo cifrato completo: LNSHDLEWMTRW

Cifrario di Hill

Per la decifratura si usa la matrice inversa

- Quindi K deve essere invertibile

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \quad K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

$$\begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} = \begin{bmatrix} k'_{11} & k'_{12} & k'_{13} \\ k'_{12} & k'_{22} & k'_{23} \\ k'_{13} & k'_{32} & k'_{33} \end{bmatrix} \times \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} \pmod{26}$$

Cifrario di Hill

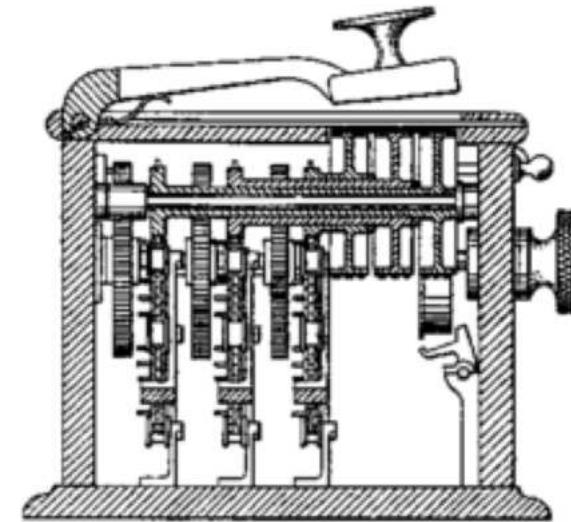
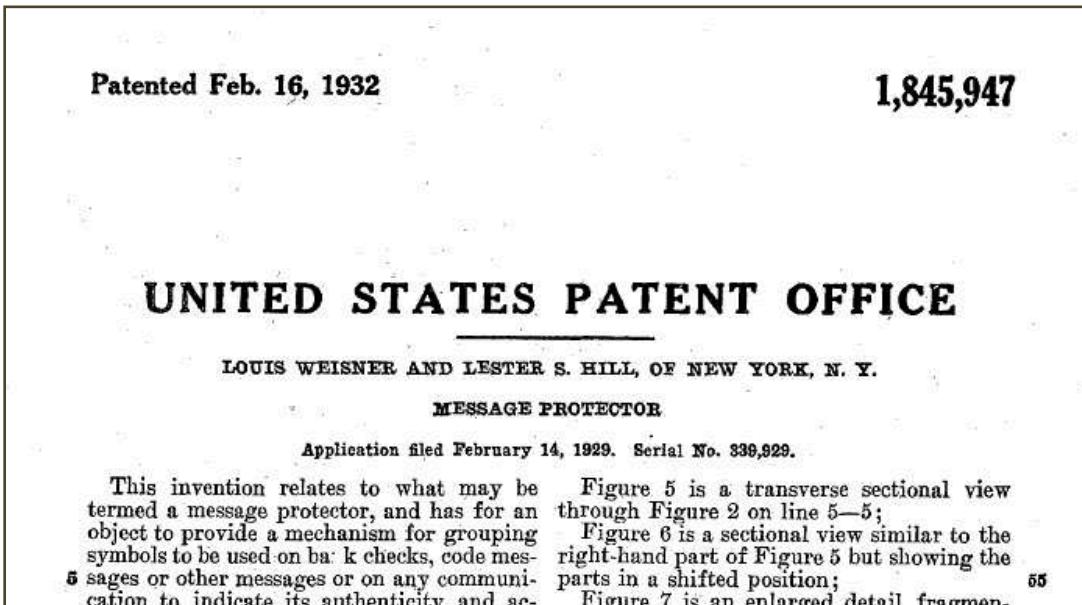
Come per Playfair la cifratura di Hill

- Nasconde le frequenze delle singole lettere

Attacchi possibili

- Se si conoscono m coppie testo in chiaro/cifrato
- Si riesce a recuperare la chiave!

Cifrario di Hill



- Era difficile fare i conti a mano
- Costruita macchina per moltiplicazione 6×6
- Sfortunatamente la chiave era fissata per ogni macchina ...
- Si suggeriva di usare una tripla cifratura seguita da altri passi
- Non ebbe successo commerciale

Cifrario di Alberti

Leon Battista Alberti, "De Cifris", 1466

Usa più alfabeti cifranti e li sostituisce durante la cifratura



- Disco esterno fisso (*stabilis*), 24 celle
- Disco interno mobile (*mobilis*), 24 celle

Cifrario di Alberti

Usa più alfabeti cifranti e li sostituisce durante la cifratura



I metodo (indice mobile)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234
disco interno mobile: gklnpr tuz&xy somqih fdbace



LE2ONE

Cifrario di Alberti

Usa più alfabeti cifranti e li sostituisce durante la cifratura



I metodi (indice mobile)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234
disco interno mobile: gklnpr tuz&xy somqih fdbace

g lettera indice
Allineare g-A

LE2ONE

A

Cifrario di Alberti

Usa più alfabeti cifranti e li sostituisce durante la cifratura



I metodi (indice mobile)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234
disco interno mobile: gklnpr tuz&xy somqih fdbace

g lettera indice
Allineare g-A

LE2ONE

AZ

Sostituzione
L con z

Cifrario di Alberti

Usa più alfabeti cifranti e li sostituisce durante la cifratura



I metodi (indice mobile)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234
disco interno mobile: gklnpr tuz&xy somqih fdbace

nulla

Allineare g-A

LE2ONE

Azpayxp

Cifrario di Alberti

Usa più alfabeti cifranti e li sostituisce durante la cifratura



I metodi (indice mobile)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234
disco interno mobile: gklnpr tuz&xy somaih fdbace

nulla

Allineare g-A

LE2ONE

Azpayxp

Adesso voglio
cambiare
alfabeto
cifrante!

Cifrario di Alberti

Usa più alfabeti cifranti e li sostituisce durante la cifratura



I metodi (indice mobile)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234
disco interno mobile: gklnpr tuz&xy somqih fdbace

Allineare g-A

nulla

LE2ONE

AzpayxpC

Allineare g-C

Cifrario di Alberti

Usa più alfabeti cifranti e li sostituisce durante la cifratura



I metodi (indice mobile)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234
disco interno mobile: gklnpr tuz&xy somqih fdbace

nulla

Allineare g-C

Allineare g-A

LE2ONE AL...

AzpayxpCct...

Cifrario di Alberti



II metodo (indice fisso)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234

disco interno mobile: gklnpr tuz&xy somqih fdbace



LEONE

Cifrario di Alberti



II metodo (indice fisso)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234

disco interno mobile: gklnpr tuz&xy somqih fdbace

Allineare g-A

LEONE

g

Cifrario di Alberti



II metodo (indice fisso)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234

disco interno mobile: gklnpr tuz&xy somqih fdbace

Allineare g-A

LEONE

Sostituzione
L con z

gz

Cifrario di Alberti



II metodo (indice fisso)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234

disco interno mobile: gklnpr tuz&xy somqih fdbace

Allineare g-A

LEONE
gzpyxp

Cifrario di Alberti



II metodo (indice fisso)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234

disco interno mobile: gklnpr tuz&xy somqih fdbace

Allineare g-A

LEONE
gzpyxp

Adesso voglio
cambiare
alfabeto
cifrante!

Cifrario di Alberti



II metodo (indice fisso)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234

disco interno mobile: gklnpr tuz&xy somqih fdbace

Allineare g-A

LEONE3

non è una nulla

gzpyxpc

Allineare c-A

Cambio alfabeto cifrante

Cifrario di Alberti



II metodo (indice fisso)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234

disco interno mobile: gklnpr tuz&xy somqih fdbace

Allineare g-A

LEONE3

non è una nulla

gzpyxpc

Allineare c-A

disco esterno: ABCDEF GILMNO PQRSTV XZ1234

disco interno mobile: cegkln prtuz& xysomq ihfdb

Cifrario di Alberti



II metodo (indice fisso)

disco esterno: ABCDEF GILMNO PQRSTV XZ1234

disco interno mobile: gklnpr tuz&xy somqih fdbace

Allineare g-A

Allineare c-A

LEONE3AI ...
gzpyxpcct...

disco esterno: ABCDEF GILMNO PQRSTV XZ1234

disco interno mobile: cegkln prtuz& xysomq ihfdb

Cifrario di Vigenère

Blaise de Vigenère, 1586

Cifrario a sostituzione polialfabetica

testo in chiaro

$M = M_0 M_1 M_2 \dots M_n$

$$C_i \leftarrow M_i + K_{i \bmod t} \bmod 26$$

testo cifrato

$C = C_0 C_1 C_2 \dots C_n$

chiave



$K = K_0 K_1 K_2 \dots K_{t-1}$

Cifrario di Vigenère

Blaise de Vigenère, 1586

Cifrario a sostituzione polialfabetica

testo in chiaro

$M = M_0 M_1 M_2 \dots M_n$

$$C_i \leftarrow M_i + K_i \bmod t \bmod 26$$

testo cifrato

$C = C_0 C_1 C_2 \dots C_n$

chiave

$K = K_0 K_1 K_2 \dots K_{t-1}$

esempio



Cifrario di Vigenère

Blaise de Vigenère, 1586

Cifrario a sostituzione polialfabetica

testo in chiaro

$M = M_0 M_1 M_2 \dots M_n$

$$C_i \leftarrow M_i + K_i \bmod t \bmod 26$$

testo cifrato

$C = C_0 C_1 C_2 \dots C_n$

chiave

$K = K_0 K_1 K_2 \dots K_{t-1}$

Testo in chiaro: CODICE MOLTO SICURO

Chiave: REBUS

Cifrario di Vigenère

Blaise de Vigenère, 1586

Cifrario a sostituzione polialfabetica

testo in chiaro

$M = M_0 M_1 M_2 \dots M_n$

$$C_i \leftarrow M_i + K_i \bmod t \bmod 26$$

testo cifrato

$C = C_0 C_1 C_2 \dots C_n$

chiave

$K = K_0 K_1 K_2 \dots K_{t-1}$

Testo in chiaro: CODICE MOLTO SICURO

Chiave: REBUS

CODIC EMOLT OSICU RO

testo in chiaro

REBUS

chiave

TSECU

testo cifrato

Cifrario di Vigenère

Blaise de Vigenère, 1586

Cifrario a sostituzione polialfabetica

testo in chiaro

$M = M_0 M_1 M_2 \dots M_n$

$$C_i \leftarrow M_i + K_i \bmod t \bmod 26$$

testo cifrato

$C = C_0 C_1 C_2 \dots C_n$

chiave

$K = K_0 K_1 K_2 \dots K_{t-1}$

Testo in chiaro: CODICE MOLTO SICURO Chiave: REBUS

CODIC EMOLT OSICU RO testo in chiaro

REBUS REBUS REBUS RE chiave

TSECU VQPFL FWJWM IS testo cifrato

Come si poteva fare la sostituzione efficientemente?



Cifrario di Vigenère

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

Cifrario di Vigenère

- Considerato inviolabile per molto tempo
 - Numero possibili chiavi = 26^t
- Resiste all'analisi delle frequenze
 - Una lettera cifrata corrisponde a più simboli in chiaro
- Babbage (1834) e Kasiski (1863) furono i primi a cimentarsi nella crittoanalisi
 - Studio delle ripetizioni per individuare la lunghezza della chiave
 - Analisi delle frequenze in ognuno degli alfabeti cifranti corrispondenti alle lettere della chiave

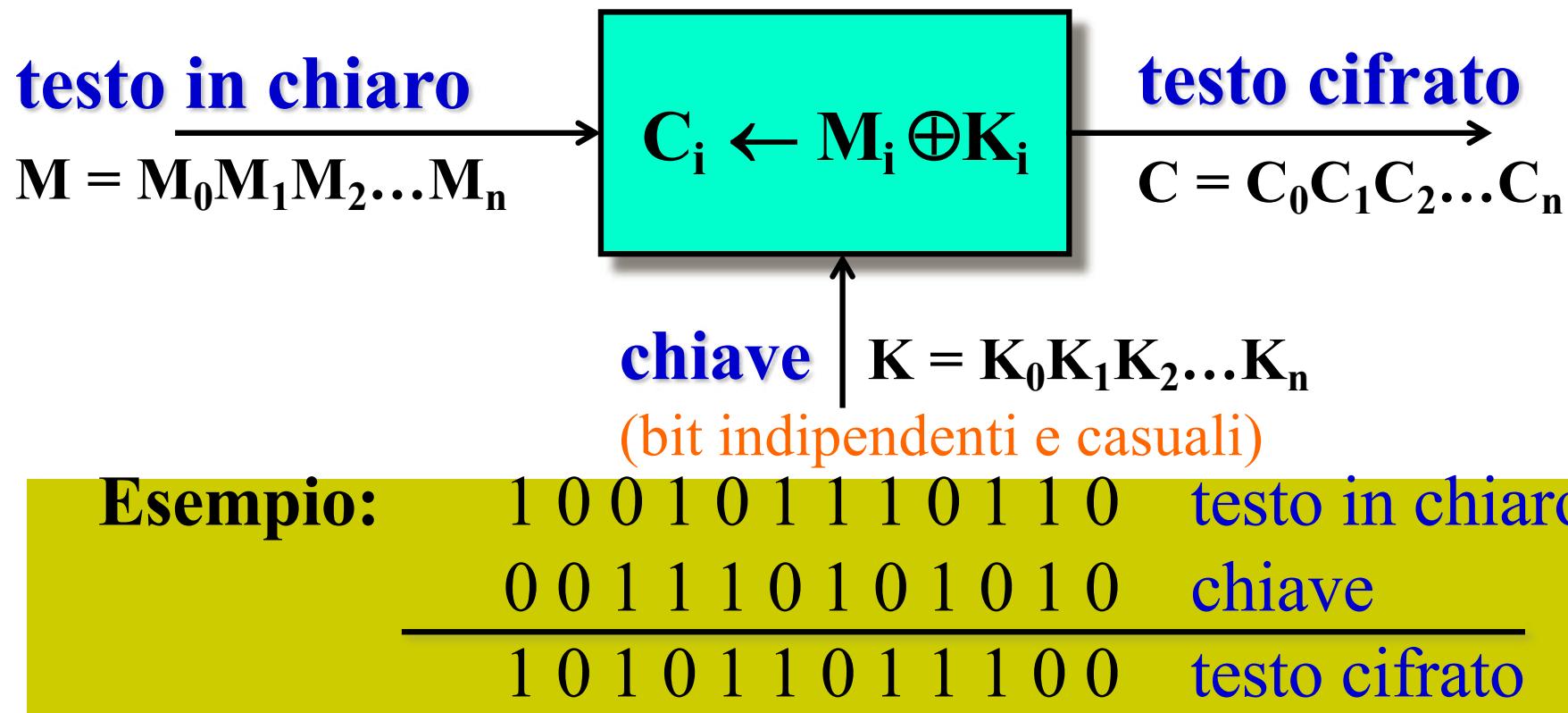
Blaise de Vigenère

- Traicté des Chiffres
- Libro del 1586
- Descrive lo stato dell'arte della Crittografia dell'epoca



Un cifrario perfetto

One-time pad, Gilbert Vernam, impiegato AT&T, 1917



One-time Pad

Unconditionally secure

- Indipendentemente dal tempo e dalle risorse a disposizione è **impossibile** decifrare il testo cifrato
- Esaminando tutte le chiavi possibili otteniamo anche tutti i messaggi possibili!
 - La casualità della chiave non ci consente di distinguere tra i messaggi ottenuti

One-time Pad

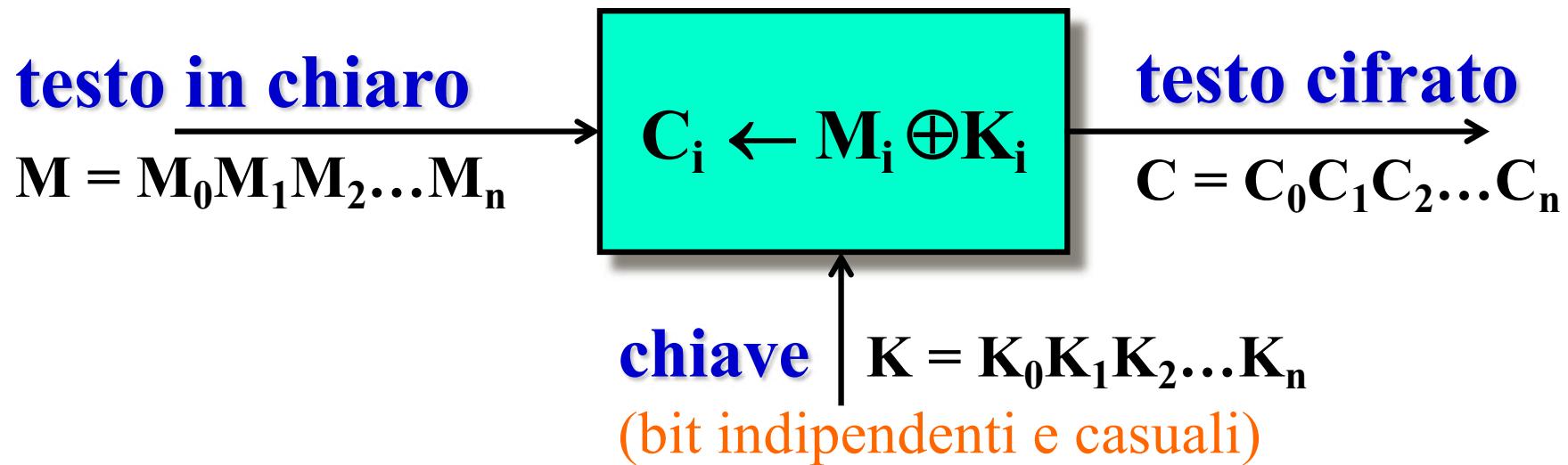
Supponiamo che il messaggio cifrato sia **10**

- Se la chiave è **00** allora il testo in chiaro è **10**
- Se la chiave è **01** allora il testo in chiaro è **11**
- Se la chiave è **10** allora il testo in chiaro è **00**
- Se la chiave è **11** allora il testo in chiaro è **01**

One-time Pad

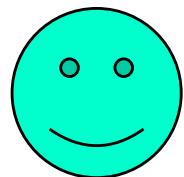
- Supponiamo che il messaggio **attaccarelavalleallalba** sia cifrato con la chiave **efthjzcokmflwpaqhctrows**
- Ad esempio, esiste una chiave che trasforma il testo cifrato nel messaggio **abbandonarevalleallalba**
- Trovatela!

One-time Pad



cifrario perfetto: M e C sono indipendenti

$$\text{Prob}(M=M') = \text{Prob}(M=M' | C=C')$$



Linea rossa Washington-Mosca

- Dopo la crisi dei missili di Cuba nel 1962
 - Necessità di una linea veloce e diretta tra Washington e Mosca
 - Messaggi impiegavano 6 ore tra ricezione, traduzione, preparazione ed invio

Linea rossa Washington-Mosca

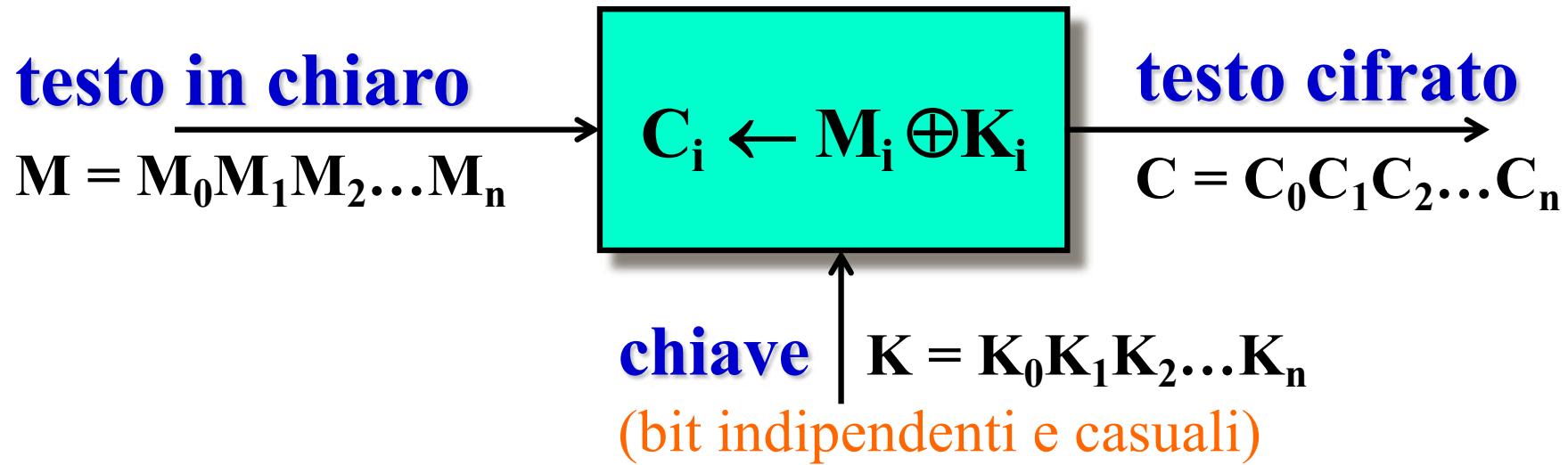
- Dopo la crisi dei missili di Cuba
- Necessità di una linea veloce e sicura tra Washington e Mosca
- Messaggi impiegavano 6 ore tra traduzione, preparazione ed invio



- Linea rossa nel 1963 con
 - 2 telescriventi
 - Device per la cifratura *Electronic Teleprinter Cryptographic Regenerative Repeater Mixer II* (ETCRRM II)



One-time Pad



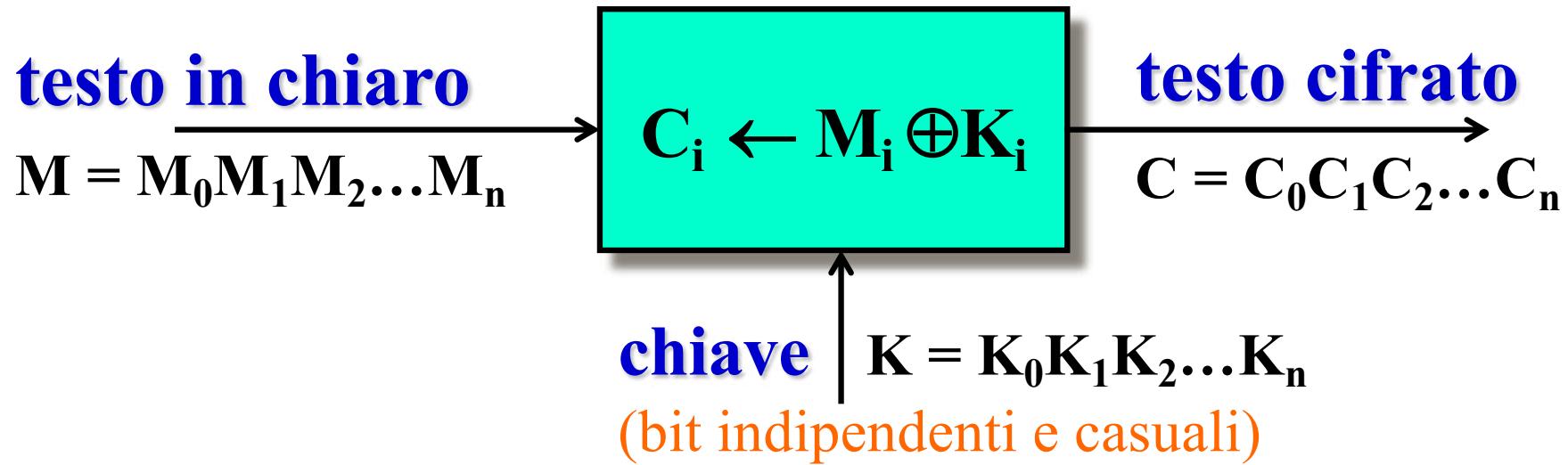
cifrario perfetto: M e C sono indipendenti

$$\text{Prob}(M=M') = \text{Prob}(M=M' | C=C')$$



Svantaggi?

One-time Pad



cifrario perfetto: M e C sono indipendenti

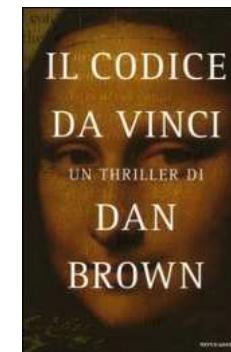
$$\text{Prob}(M=M') = \text{Prob}(M=M' | C=C')$$



lunghezza chiave = lunghezza testo in chiaro

Crittografia e Letteratura

- Jules Verne (1828-1905), "Mathias Sandorf"
 - messaggio cifrato dal conte Sandorf, coinvolto in una cospirazione anti-austriaca
- Edgar Allan Poe (1809-1849), "Lo Scarabeo d'Oro"
 - messaggio cifrato dal pirata Capitano Kidd, dice dove è nascosto il tesoro
- Dan Brown, "Il Codice Da Vinci"
 - O, Draconian Devil! Oh Lame Saint!
(Leonardo Da Vinci! The Mona Lisa!)
- Ian Caldwell, Thomas Dustin "Il Codice del Quattro"
 - Steganografia e crittografia all'interno di un antico testo



I crittogrammi Beale

- Un enigma crittografico non ancora risolto
- Tesoro nascosto nella Contea di Bedford, Virginia, USA
- Dibattito: verità o bufala?



I crittogrammi Beale

La vicenda inizia nel 1822 a Lynchburg, Virginia

Protagonisti:

- Thomas J. Beale, avventuriero del selvaggio West
- Robert Morris, gestore di un hotel di Lynchburg
- Un tesoro sepolto del valore di **20 milioni di dollari**
- Tre crittogrammi
- Un opuscolo pubblicato nel 1885



I crittogrammi Beale

Nel 1822 Beale affidò a Morris una scatola chiusa a chiave chiedendogli di custodirla

- La scatola conteneva documenti cifrati

Se Beale non fosse tornato entro 10 anni, Morris avrebbe dovuto aprirla

- La chiave necessaria alla decifratura sarebbe stata recapitata a Morris nel 1832



I crittogrammi Beale

Beale non tornò mai e Morris non ricevette la chiave di decifratura

Nel 1845 Morris aprì la scatola

- All'interno c'erano tre crittogrammi e una lettera per Morris
 - La lettera svelò che Beale aveva scoperto un giacimento d'oro
 - I tre crittogrammi indicavano
 - l'ammontare del tesoro
 - la sua ubicazione
 - la ripartizione del tesoro tra gli eredi
- 

I crittogrammi Beale

- Morris tentò per 20 anni di decifrare i crittogrammi, senza successo
- Nel 1862 mostrò i crittogrammi ad un amico che, dopo aver decifrato il secondo, pubblicò un opuscolo nel 1885
- Il secondo crittogramma fu decifrato usando come chiave la dichiarazione di indipendenza



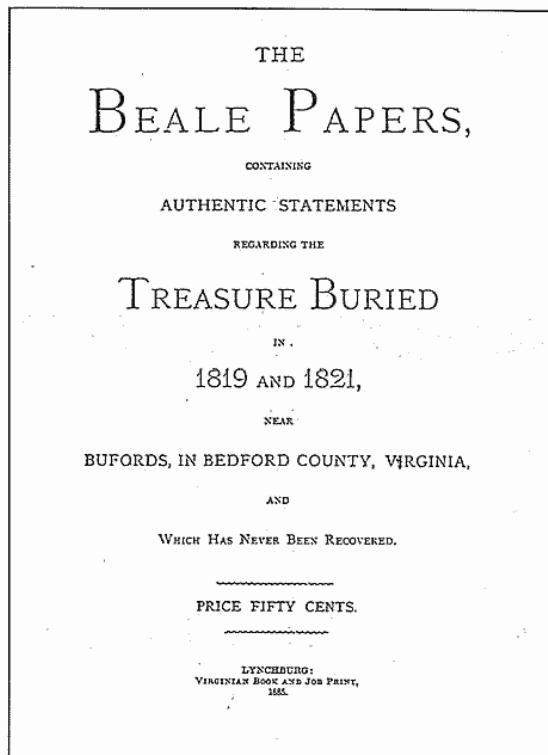
I crittogrammi Beale

22

The Beale Treasure

3.

The Beale Papers



L'opuscolo

3 — *The Beale Papers*

41

20

THE BEALE PAPERS.

peace, contract alliances, establish commerce, and to do all other acts and things which independent States may of right do. And for the support of this declaration, with a firm reliance on the protection of Divine Providence, we mutually pledge to each other our lives, our fortunes, and our sacred honor.

The letter, or paper, so often alluded to, and marked "2," which is fully explained by the foregoing document, is as follows.

115, 70, 24, 807, 37, 52, 49, 17, 31, 62, 647, 23, 7, 15, 140, 47, 29, 107, 79, 84, 56, 239, 10, 26, 511, 5, 196, 308, 85, 58, 169, 186, 59, 211, 86, 9, 46, 316, 554, 132, 106, 95, 58, 58, 2, 42, 7, 85, 122, 58, 81, 82, 77, 250, 196, 66, 98, 118, 71, 140, 287, 29, 833, 37, 1005, 65, 147, 807, 24, 3, 8, 18, 47, 48, 59, 807, 45, 816, 101, 41, 78, 154, 1005, 122, 135, 191, 16, 77, 49, 102, 37, 72, 84, 73, 85, 35, 871, 59, 190, 81, 23, 18, 106, 271, 60, 394, 220, 220, 308, 287, 68, 8, 6, 191, 128, 48, 10, 46, 46, 29, 39, 47, 56, 51, 90, 105, 15, 69, 101, 10, 201, 37, 105, 28, 248, 16, 150, 7, 35, 19, 301, 125, 110, 450, 287, 68, 117, 511, 62, 51, 220, 37, 118, 140, 597, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 29, 59, 511, 548, 107, 603, 220, 7, 69, 154, 41, 20, 50, 6, 575, 129, 154, 248, 110, 61, 53, 33, 30, 5, 38, 8, 14, 84, 37, 540, 217, 115, 71, 23, 81, 63, 49, 131, 59, 47, 73, 239, 569, 58, 59, 39, 18, 44, 21, 44, 21, 12, 12, 79, 73, 353, 105, 58, 107, 37, 211, 603, 129, 303, 134, 45, 101, 15, 284, 540, 250, 14, 203, 140, 344, 26, 811, 138, 115, 48, 73, 34, 295, 316, 601, 64, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121, 12, 93, 10, 15, 35, 12, 131, 62, 115, 102, 807, 40, 53, 135, 193, 80, 81, 03, 07, 41, 85, 63, 10, 106, 807, 138, 8, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 40, 59, 1, 35, 41, 21, 40, 7, 10, 3, 81, 600, 44, 400, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33, 37, 333, 287, 140, 47, 88, 60, 87, 49, 47, 64, 6, 7, 71, 39, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 140, 208, 230, 15, 101, 246, 85, 94, 511, 2, 270, 100, 53, 89, 47, 630, 68, 53, 7, 44, 30, 31, 250, 10, 51, 33, 106, 160, 113, 81, 102, 406, 330, 540, 330, 20, 66, 33, 101, 807, 138, 301, 310, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 30, 811, 7, 2, 118, 73, 16, 195, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 551, 138, 19, 85, 100, 48, 47, 77, 14, 27, 8, 47, 138, 63, 140, 44, 32, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 41, 48, 7, 25, 46, 110, 20, 807, 191, 31, 113, 29, 82, 33,

Il secondo crittogramma

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56, 239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122, 106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140, 287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41, 78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196, 81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 6, 191, 122, 43, 234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46, 10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28, 248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113, 140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107, 603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8, 14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53, 79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 505, 125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115, 48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121, 12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41, 85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49, 47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2, 270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31, 10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250, 557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106, 160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27, 8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 44, 48...

La chiave

DECLARATION OF INDEPENDENCE

When(1) in(2) the(3) course(4) of(5) human(6) events(7) it(8) becomes(9) necessary(10) for(11) one(12) people(13) to(14) dissolve(15) the(16) political(17) bands(18) which(19) have(20) connected(21) them(22) with(23) another(24) and(25) to(26) assume(27) among(28) the(29) powers(30) of(31) the(32) earth(33) the(34) separate(35) and(36) equal(37) station(38) to(39) which(40) the(41) laws(42) of(43) nature(44) and(45) of(46) nature's(47) god(48) entitle(49) them(50) a(51) decent(52) respect(53) to(54) the(55) opinions(56) of(57) mankind(58) requires(59) that(60) they(61) should(62) declare(63) the(64) causes(65) which(66) impel(67) them(68) to(69) the(70) separation(71) we(72) hold(73) these(74) truths(75) to(76) be(77) self(78) evident(79) that(80) all(81) men(82) are(83) created(84) equal(85) that(86) they(87) are(88) endowed(89) by(90) their(91) creator(92) with(93) certain(94) unalienable(95) rights(96) that(97) among(98) these(99) are(100) life(101) liberty(102) and(103) the(104) pursuit(105) of(106) happiness(107) that(108) to(109) secure(110) these(111) rights(112) governments(113) are(114) instituted(115) among(116) men(117) ...

La cifratura

Testo in chiaro: I have deposited ...

Chiave: instituted(115) hold(73) another(24) ...

Testo cifrato: 115, 73, 24, 807, 37, ...

Il crittogramma decifrato

"I have deposited in the county of Bedford, (Virginia) about four miles from Buford, in an excavation or vault, six feet below the surface of the ground, the following articles belonging jointly to the parties whose names are given in number three herewith. The first deposit consisted of ten hundred and fourteen pounds of gold and thirty eight hundred and twelve pounds of silver deposited Nov. Eighteen Nineteen. The second was made Dec. Eighteen Twenty one and consisted of nineteen hundred and eighty eight of silver, also jewels obtained in St. Louis in exchange to save transportation and valued at thirteen thousand dollars. The above is securely packed in iron pots with iron covers the vault is roughly lined with stone and the vessels rest on solid stone and are covered with others. Paper number one describes the exact locality of the vault so that no difficulty will be had in finding it."

Thomas Jefferson Beale

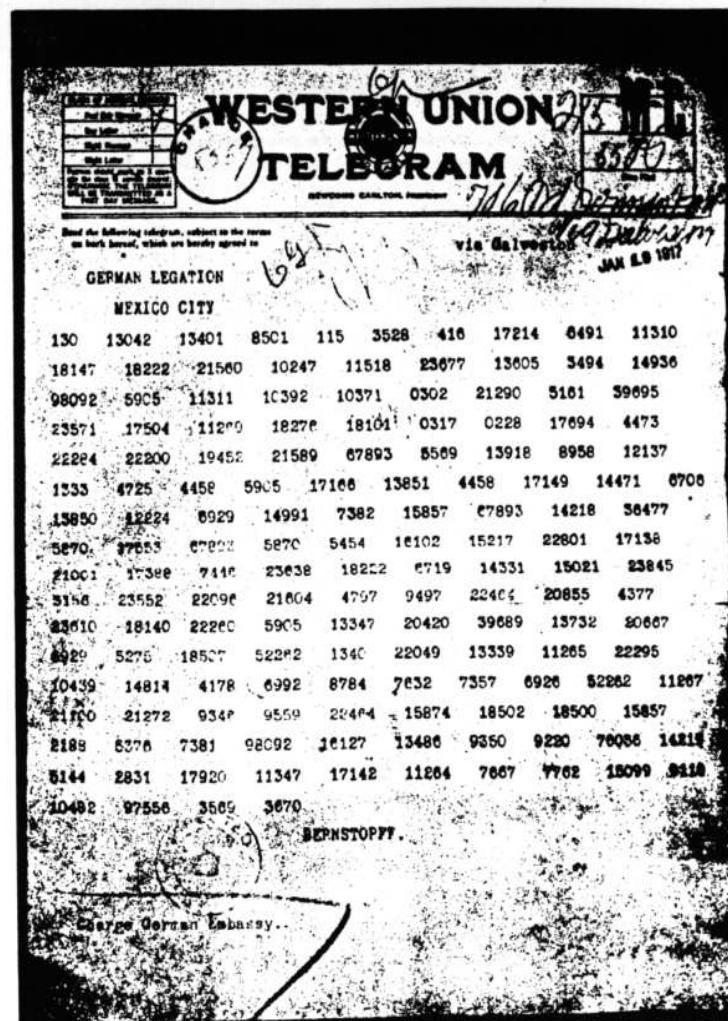
I crittogrammi Beale

- Il primo e il terzo crittogramma di Beale sono inviolati da più di un secolo
 - I crittogrammi potrebbero essere stati alterati dall'autore dell'opuscolo per impedirne la decifratura
- E il tesoro?
 - Qualcuno potrebbe averlo trovato utilizzando gli indizi dell'unico crittogramma decifrato
- L'intera storia potrebbe essere una montatura, ispirata dal romanzo di Edgar Allan Poe
- Ancora oggi crittoanalisti e cacciatori di tesori sono affascinati dalla vicenda
- Verità o bufala?



Il telegramma di Zimmermann

- La decifrazione di un telegramma tedesco, intercettato dagli inglesi nel 1917, influì sul corso della storia
- Il telegramma spinse gli Stati Uniti a riconsiderare la loro politica di neutralità



"All the News That's Fit to Print."

The New York Times.

EXTRA
8:30 A.M.

VOL. LXXV., NO. 7091. 1915.

NEW YORK, SATURDAY, MAY 8, 1915.—TWENTY-FOUR PAGES.

EIGHT CENTS. ADVERTISING, \$1.00 PER LINE.

Printed Saturday morning, New

LUSITANIA SUNK BY A SUBMARINE, PROBABLY 1,260 DEAD; TWICE TORPEDOED OFF IRISH COAST; SINKS IN 15 MINUTES; CAPT. TURNER SAVED, FROHMAN AND VANDERBILT MISSING; WASHINGTON BELIEVES THAT A GRAVE CRISIS IS AT HAND

SHOCKS THE PRESIDENT

Washington Deeply Stirred by the Loss of American Lives.

BULLETINS AT WHITE HOUSE

When Read: Then Deeply, but in Silence on the Nation's Course.

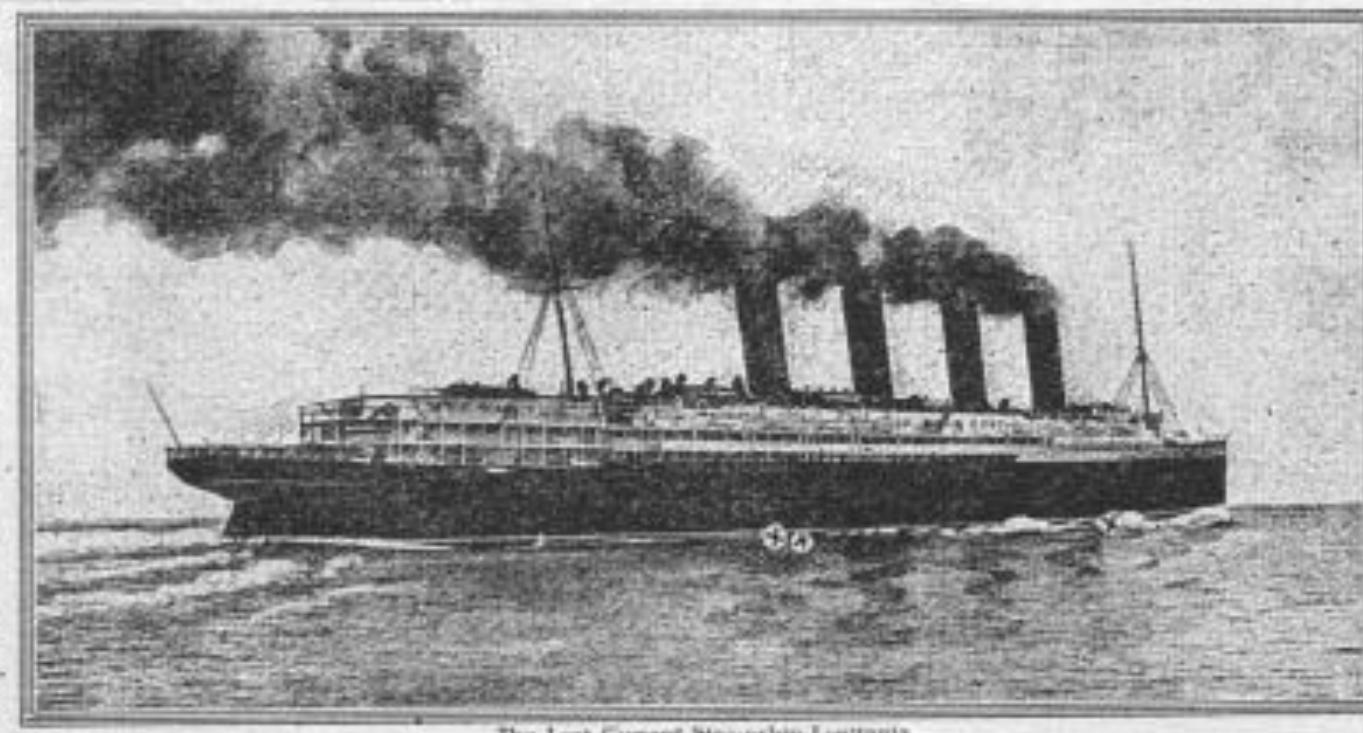
HINTS OF CONGRESS CALL

Loss of Lusitania Recalls Firm Ties of Our First War—Waging to Germany.

CAPITAL FULL OF RUMORS

Reports That Lives Were in Danger Before Submarine Came.

Special to the Sun Times.
WORCESTER, Mass., May 7.—"Never more than 2000 legs, never more than 2000 dead came from the Titanic had been given," said Worcester men who worked at it for months and for protection of the Americans. "The early reports said that lives had been in danger before the boat had been hit, but the belief that there had been no real attack made me say in the previous messages how little meaning there is in those rumors and that they look like noise."



The Lost Cunard Steamship Lusitania
X Where the First Torpedo Struck. II Where the Second Torpedo Struck.

SOME DEAD TAKEN ASHORE

Several Hundred Survivors at Queenstown and Rosslare.

STEAMROTTELLS OF OCEANIC

One Torpedo Crashes Into the Damaged Liner's Bow, Another Into the Empty Stern.

SHIP LISTS EVER TO PORT

Making it Impossible to Load Many Boats, Six Hundred Must Have Gone Down.

ATTACKED IN BROAD DAYLIGHT

Passenger at Luncheon Having Just Been Given by Germans to Save the Ship Left New York.

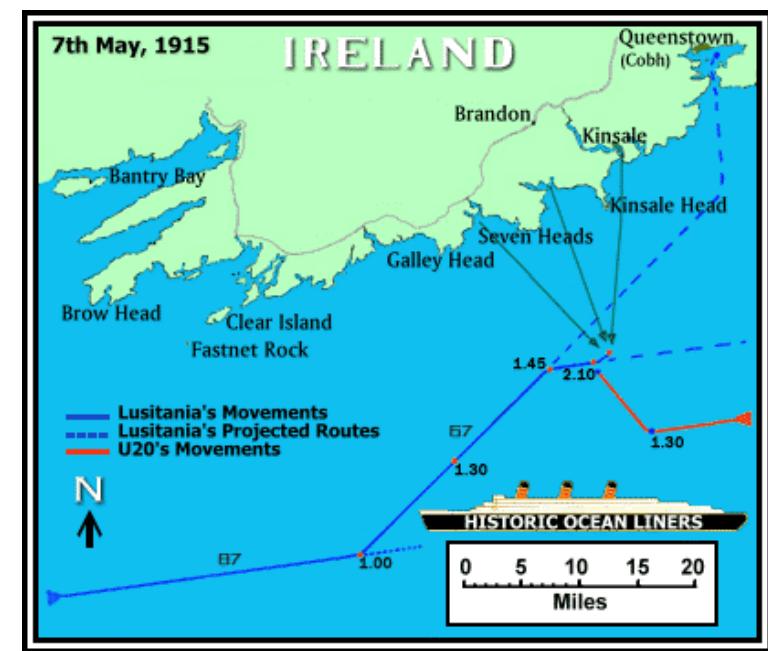
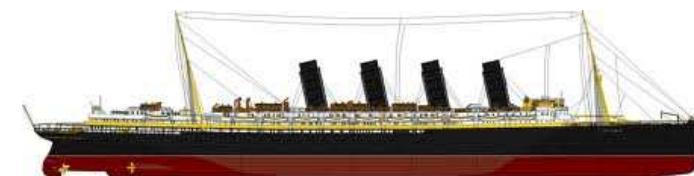
Only 659 Were Saved, First-Cabin Passengers

QUEENSTOWN, Saturday, May 8, 4:28 A.M.—Survivors of the Lusitania who have arrived here report that only about 600 of those aboard the steamer were saved, and not all of

New York Times, 8 maggio 1915



U-20



Il telegramma di Zimmermann

- Nel 1915 un U-boot tedesco in immersione affondò il transatlantico britannico Lusitania
 - 1.198 vittime, tra cui 128 civili americani
- Per evitare l'entrata in guerra degli USA, la Germania promise che gli U-boot sarebbero emersi prima di attaccare
- Nel 1917 la Germania decise di venir meno al suo impegno
 - L'impiego senza restrizioni della flotta sottomarina avrebbe costretto la Gran Bretagna alla resa
 - Bisognava fare presto ed evitare agli USA di entrare in guerra cambiando il corso del conflitto

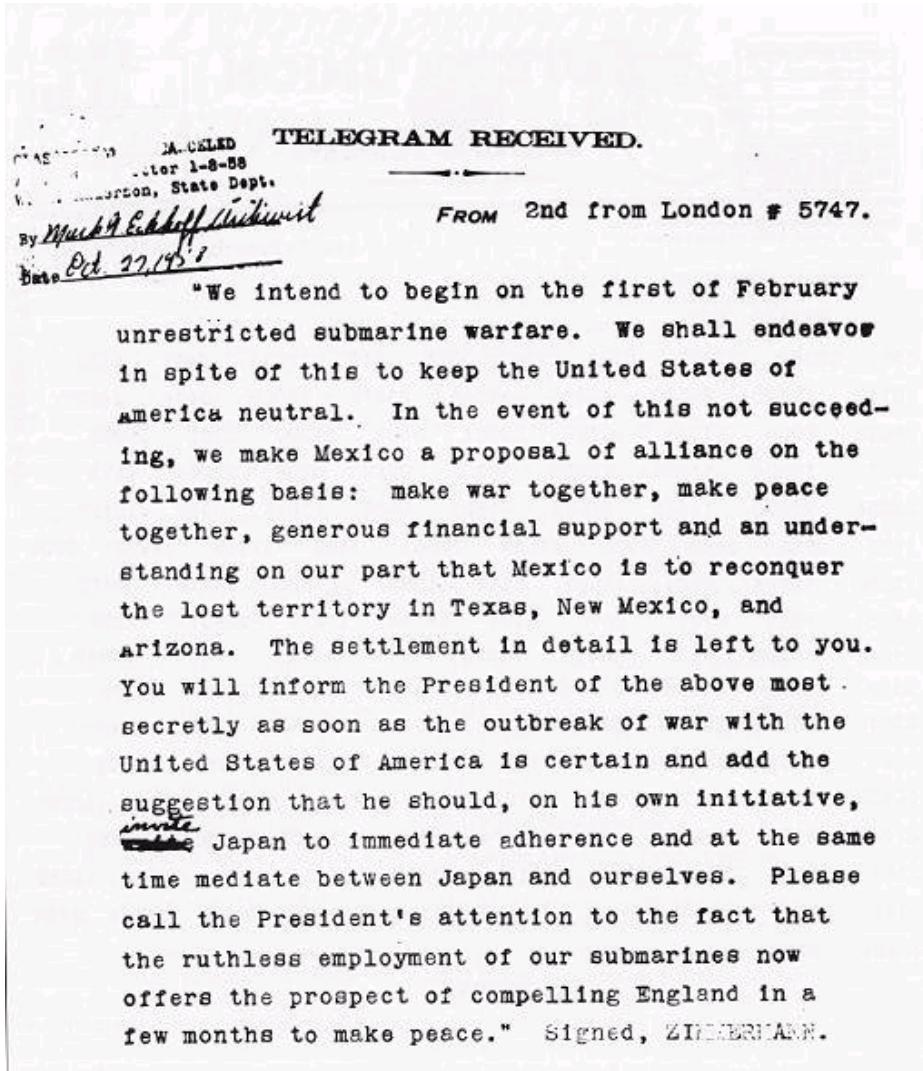
Il telegramma di Zimmermann



- Zimmermann, ministro tedesco degli esteri progettò un piano:
 - Indurre il Messico e il Giappone ad attaccare gli USA
 - In tal modo gli USA non avrebbero avuto il tempo di impegnarsi in Europa e la Gran Bretagna si sarebbe arresa
- Il 16 gennaio 1917, Zimmermann inviò un telegramma cifrato a von Bernstorff, ambasciatore tedesco a Washington
 - Il telegramma doveva essere ritrasmesso a von Eckhardt, ambasciatore tedesco a Città del Messico
 - L'ambasciatore lo avrebbe consegnato al presidente messicano

Il telegramma di Zimmermann

Il telegramma fu
intercettato dalla
Gran Bretagna e
decifrato dai suoi
crittoanalisti



Il telegramma di Zimmermann

- Il telegramma fu intercettato dalla Gran Bretagna e decifrato dai suoi crittoanalisti
 - Non fu inviato subito agli americani
- Il 1 febbraio 1917 la Germania comunicò agli USA la decisione sull'uso illimitato degli U-boot
 - Gli USA decisero di restare neutrali
 - Bisognava mostrare loro il contenuto del telegramma senza svelare il ruolo dei crittoanalisti britannici
- Un agente britannico in Messico trafugò la versione messicana del telegramma e la rese pubblica

Ad aprile 1917 gli USA decisero di entrare in guerra



Group-by-group decodement of the Zimmermann Telegram as sent by Ambassador Bernstorff to German Minister von Eckhardt in Mexico on January 19, 1917.

130	Nr. 3	13851	stop	18507	hinzufuegen
13042		4458	gemeinsamen	52262	Japan
13401	Auswaertiges Amt	17149	Friedensschluss	1340	von
8501	telegraphiert	14471	stop	22049	sich
115	vom 16ten Januar	6706	reichliche	13339	aus
3528	colon	13850	finanzielle	11265	zu
416	Nr. 1	12224	Unterstuetzung	22295	sofortiger
17214	Ganz geheim	6929	und	10439	Beitretung
6491	Selbst	14991	Einverstaendnis	14814	einladen
11310	zu	7382	unsererseits	4178	infinitive with zu
18147	entziffern	15857	dass	6992	und
18222	stop	67893	Mexiko	8784	gleichzeitig
21560	Wir	14218	in	7632	zwischen
10247	beabsichtigen	36477	Texas	7357	uns
11518	am	5870	comma	6926	und
23677	ersten	17553	Neu	52262	Japan
13605	Februar	67893	Mexiko	11267	zu
3494	un	5870	comma	21100	vermitteln
14936	eingeschraenkten	5454	Ar	21272	stop
98092	U-boot	16102	iz	9346	Bitte
5905	kreig	15217	on	9559	den

Parte del telegramma decifrato dalla Naval Intelligence Division (United Kingdom)

L7

7632 zwischen
7357 uns
6926 und
52262 Japan
11267 zu
21100 vermitteln
21272 Ⓛ
9346 Bitte
9559 den
22464 Präsident
15874 darauf
hinweisen
18562 Ⓛ
18500 Ⓛ
15857 dafs
2188 rücksichtslos
5376 anwendung
7381 unsrich
98092 Uboote
16127 pitgt
13486 Ansicht
9350 bietet
9220 Ⓛ
76036 England

4.

4458 gemeinsam
17149 Friedensschluss.
14471 Ⓛ
6706 reichlich
13850 finanziell
12224 unterstützung
6929 und
14991 einverständnis
73824 aussieverts.
158(5)7 da/3
67893 Mexico.
14218 in
36477 Texas
5670 Ⓛ
17553 neu
67693 Mexico.
5870 Ⓛ
5454 AR
16102 IZ
15217 ON
22801 A

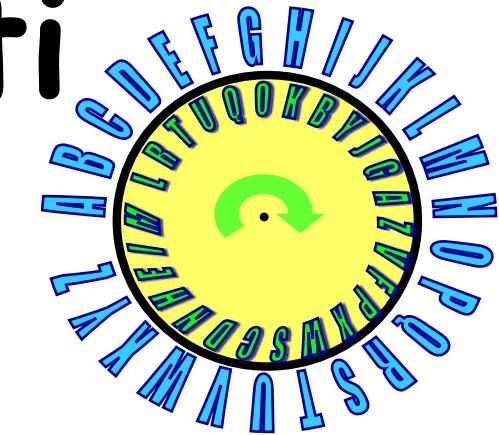
Macchine cifranti

Cifratura

- richiede tempo
- ripeterla aumenta il tempo

Meccanizzazione

- Disco di Alberti (1400)
- Cilindri cifranti (1600)
- Cilindri di Thomas Jefferson



Cilindro di Thomas Jefferson

Circa 1790 - 1800

(Terzo presidente USA)

Cilindro di 15cm e 36 dischi di legno



Numero possibili ordinamenti dei dischi = $36! \approx 3.72 \cdot 10^{41}$

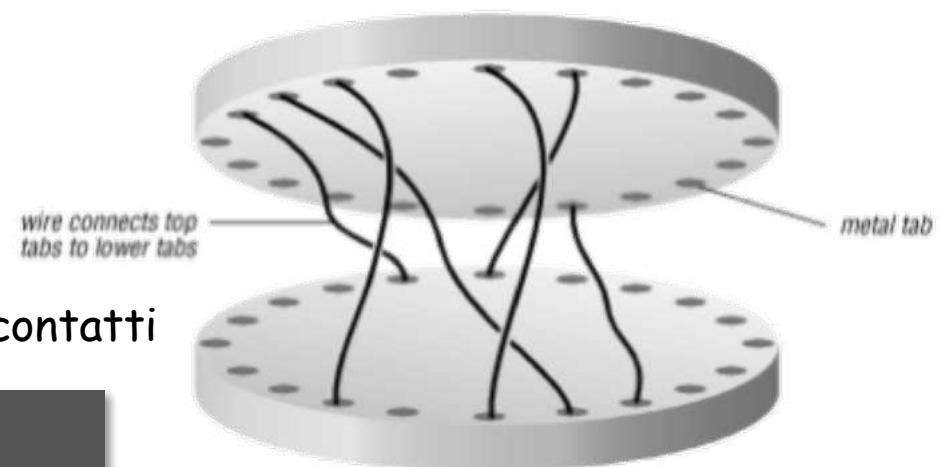
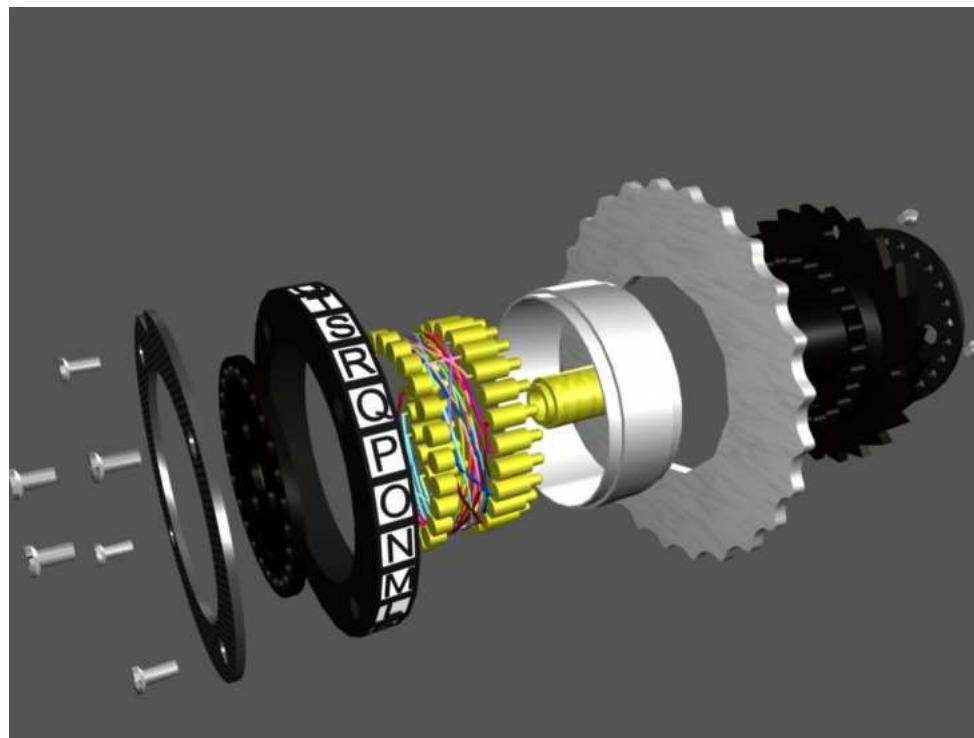
Macchine a Rotori

- Device elettro-meccaniche
- Costruite a partire dal 1918
- La più famosa è **Enigma**
- Implementano cifrari a sostituzione polialfabetica
 - La sostituzione cambiava automaticamente ad ogni lettera cifrata

Rotori

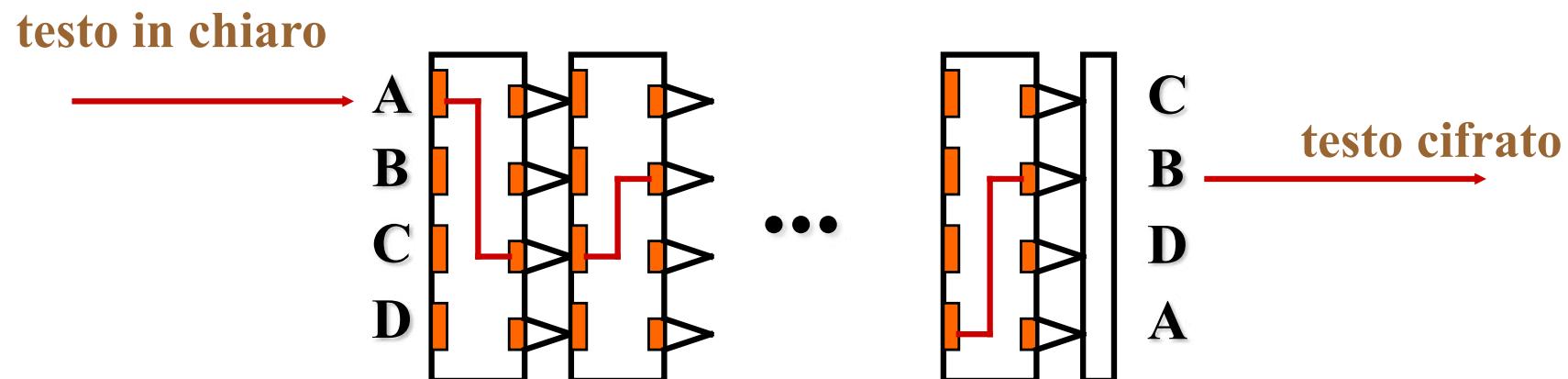
Dischi

- possono ruotare
- 26 contatti elettrici su ambo le parti
- materiale isolante
- fili elettrici interni che connettono i contatti



Macchine a Rotori

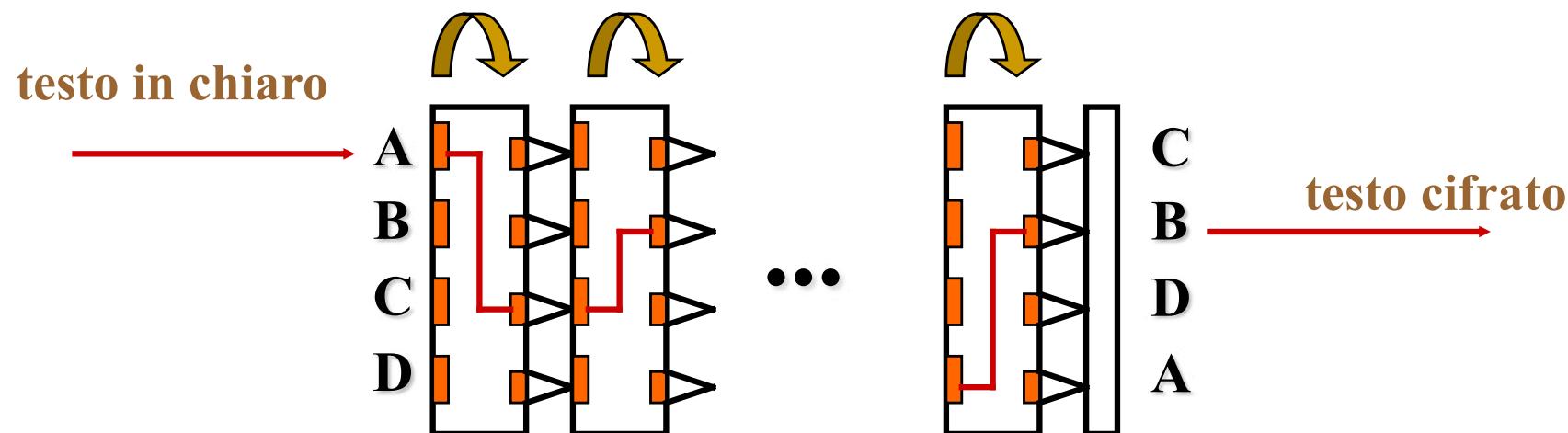
Ogni rotore opera una sostituzione monoalfabetica



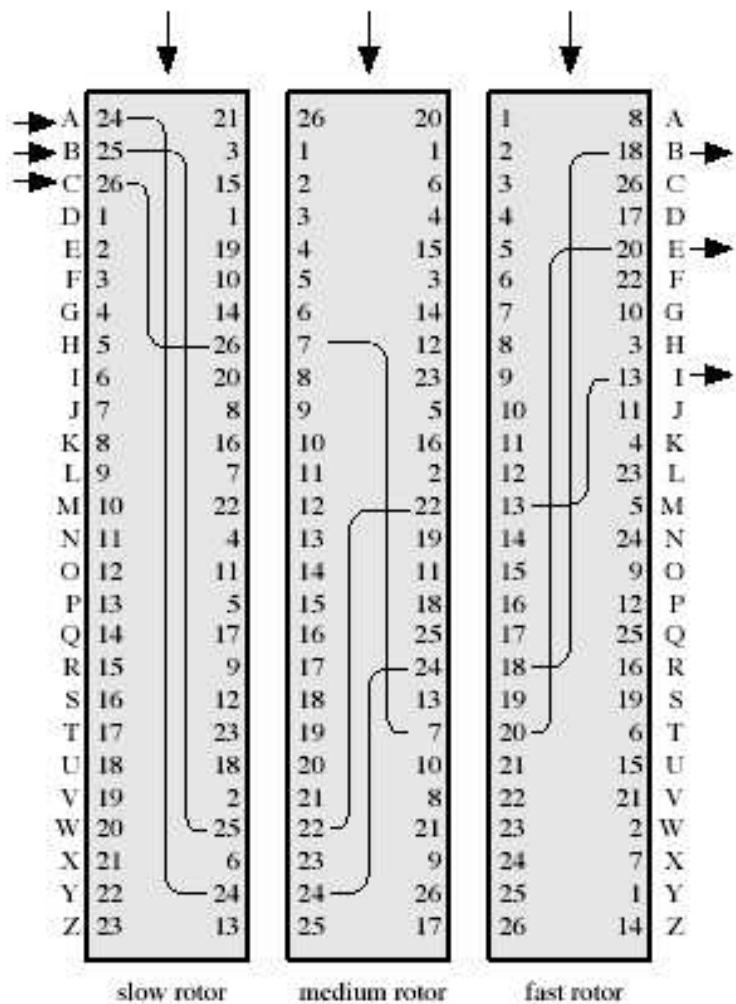
Macchine a Rotori

I dischi ruotano

- Quello più a destra ad ogni lettera cifrata
- Il secondo più a destra dopo 26 rotazioni del primo
- Il terzo più a destra dopo 26 rotazioni del secondo
- ... come un contachilometri

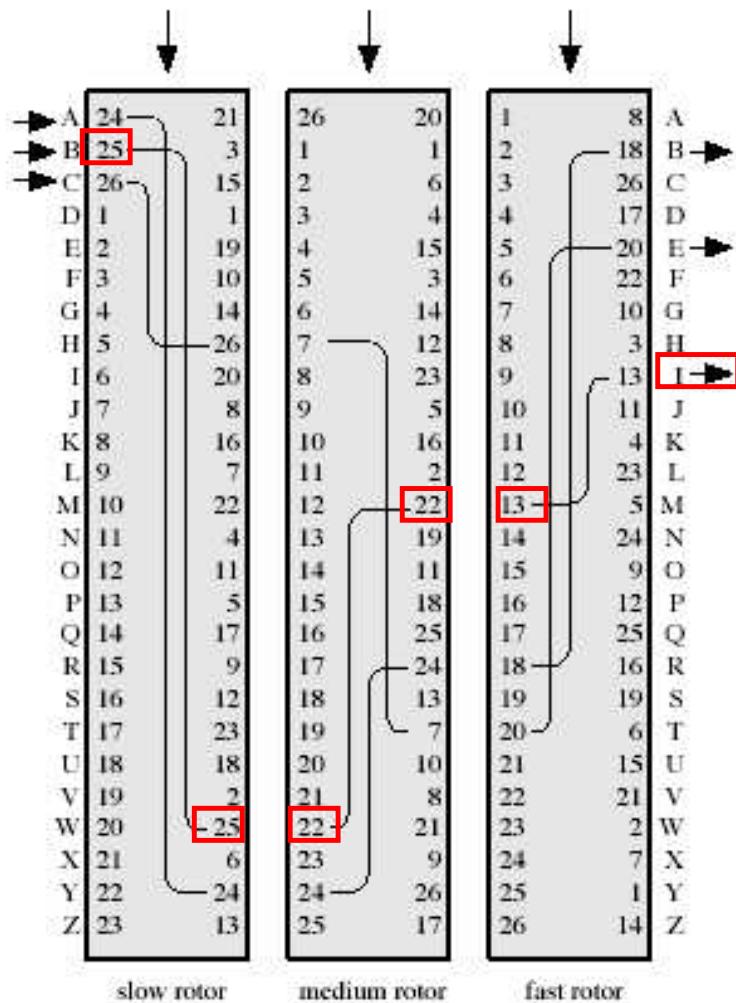


Esempio rotazione



Sostituzione
per una lettera

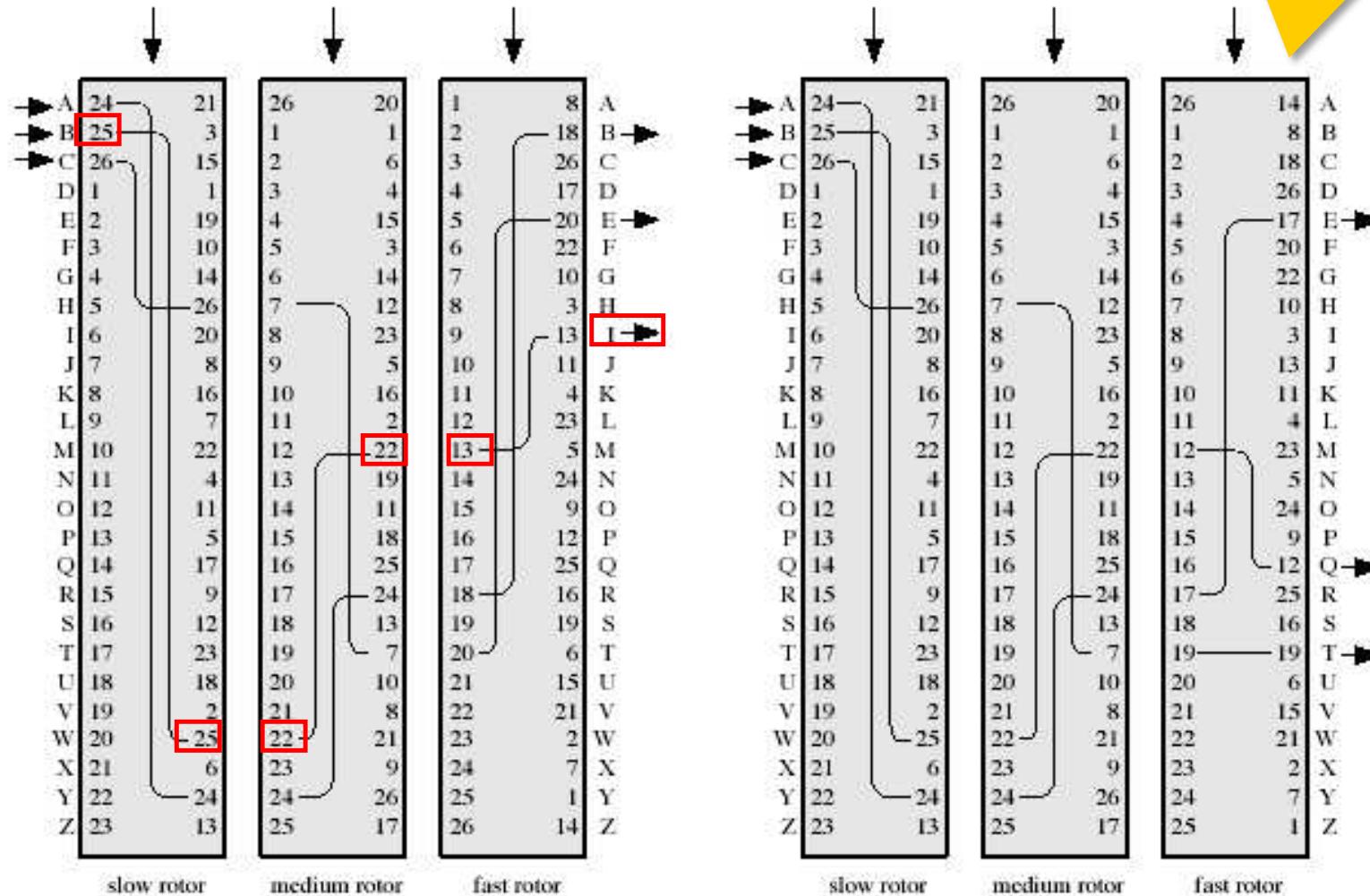
Esempio rotazione



Esempio B → I

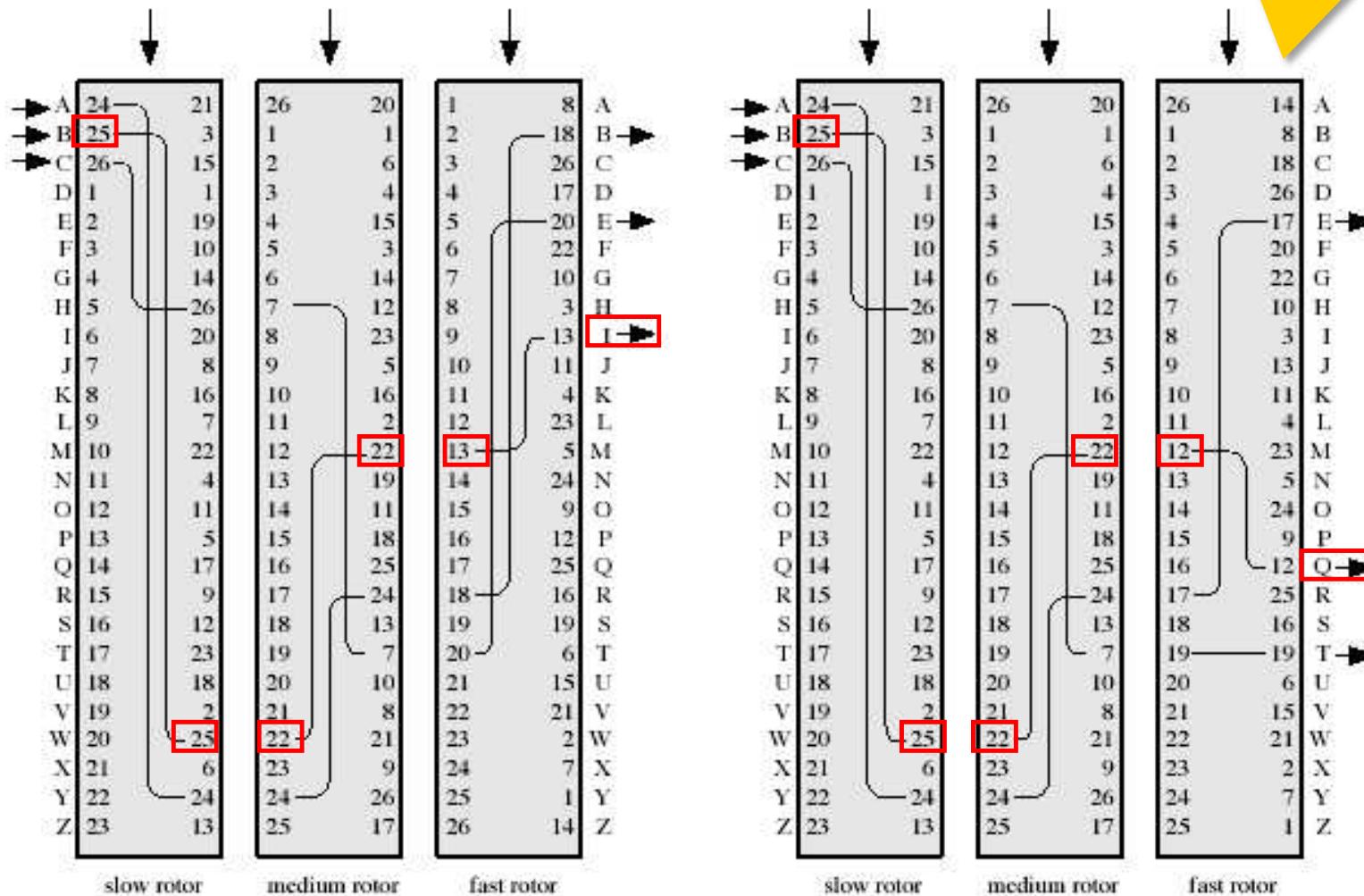
Esempio rotazione

Rotazione dopo la
cifratura di una
lettera



Esempio rotazione

Esempio B → Q

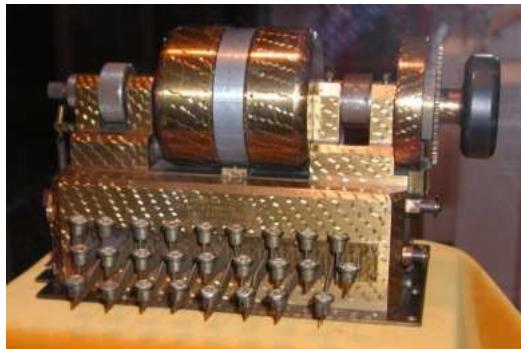


Rotori

- Con tre rotori: $26^3 = 17.576$ diversi alfabeti cifranti
- Si possono aggiungere altri rotori
 - con 4 rotori: $26^4 = 456.976$
 - con 5 rotori: $26^5 = 11.881.376$
- Supera la debolezza del cifrario di Vigenère
 - C'erano pochi alfabeti cifranti usati in ciclo
- Rotori: ciclo di sostituzione non si ripete quasi mai
 - Occorrerebbero dei testi di lunghezza enorme
(Come una intera enciclopedia con decine di volumi ciascuno con migliaia di pagine!)

Prime macchine a rotori

- Costruzione della prima macchina:
Edward Hugh Hebern [1918]
- Primo brevetto [1921]
- *Hebern Electric Code, Inc.* prima azienda crittografica americana, bancarotta [1926]
- U. S. Navy, usa macchine a 5 rotori della *Hebern* [1929-1930]





Macchine a rotori

Boris Hagelin, svedese, costruì:

- B-21 [1925], usata dall'esercito svedese



- B-211 [1932]



- C-36 per i Francesi [1934]



- C-48 (prodotte 140.000 macchine!), chiamate M-209 quando usate dall'esercito americano nella II guerra mondiale

- ... azienda svizzera dal 1948: C-52, CD-55, T-55, CD-57

Fialka

Russa M-125, nota
come Fialka [1956]

- 10 rotori



Enigma

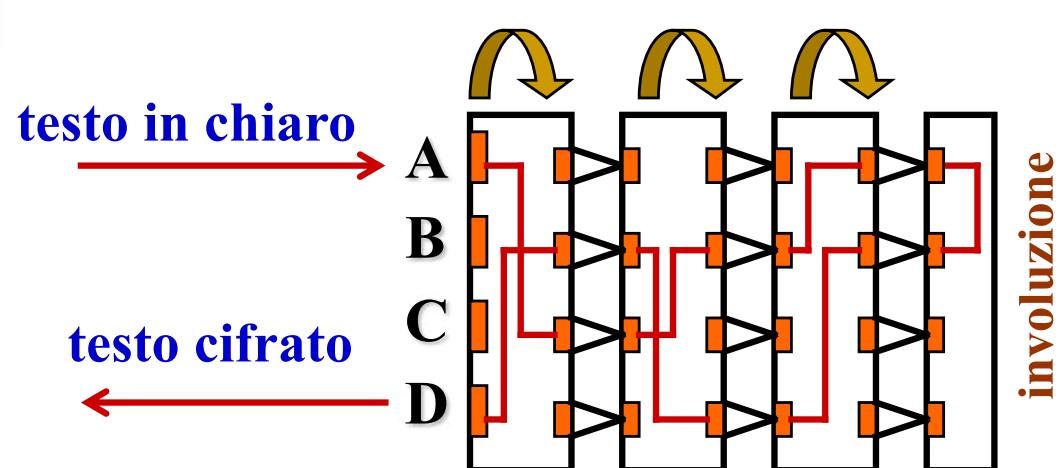
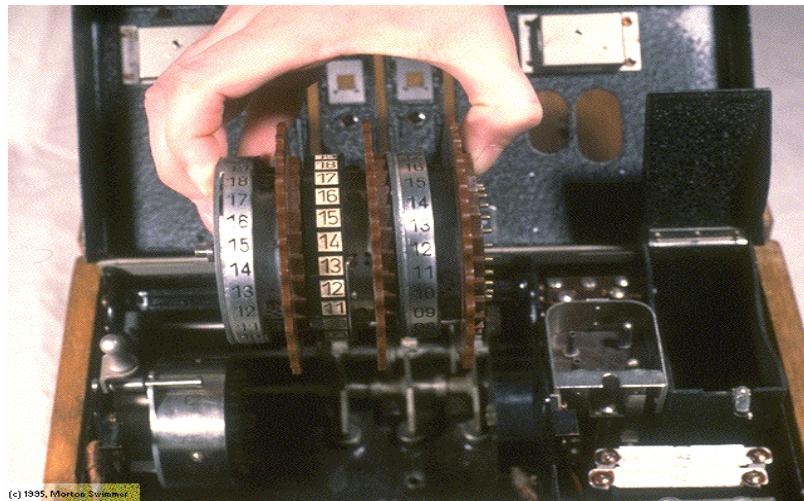
II Guerra Mondiale

Caratteristiche:

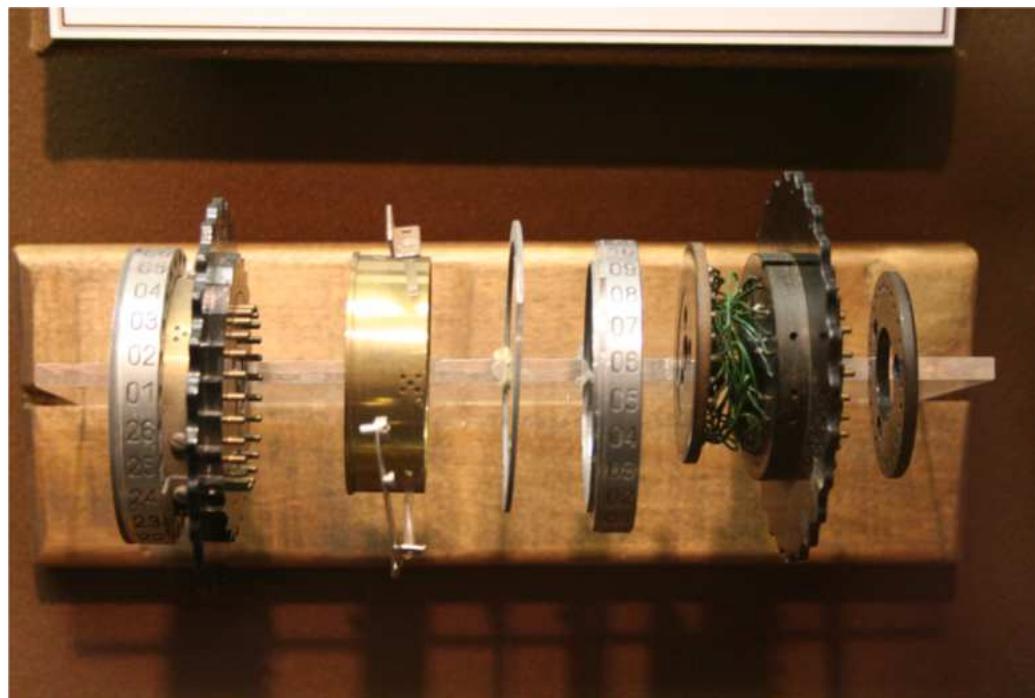
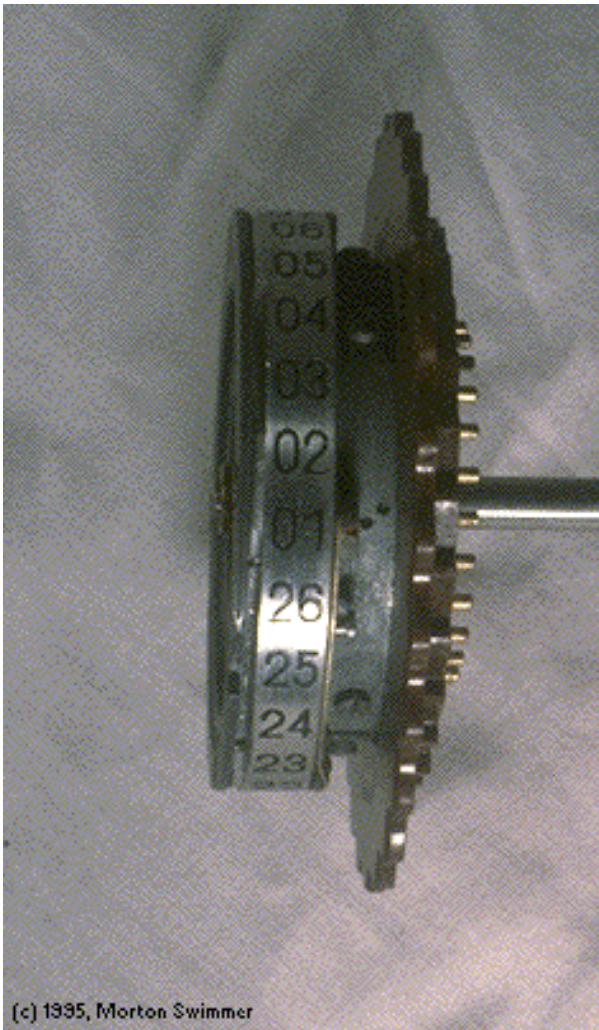
- 3 rotori
- Involuzione
- Pannello a prese multiple



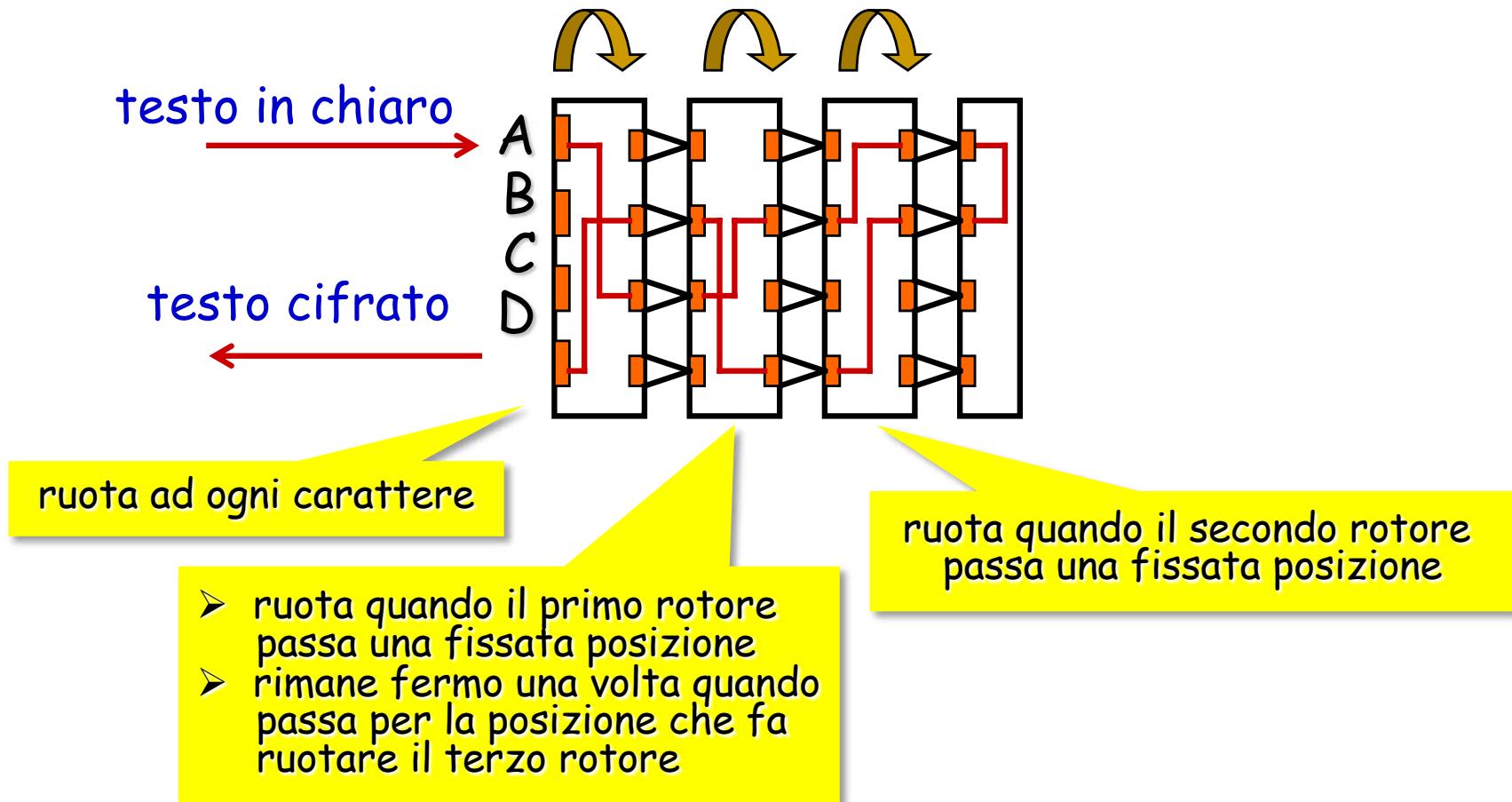
Enigma



Rotore Enigma



Enigma: odometro

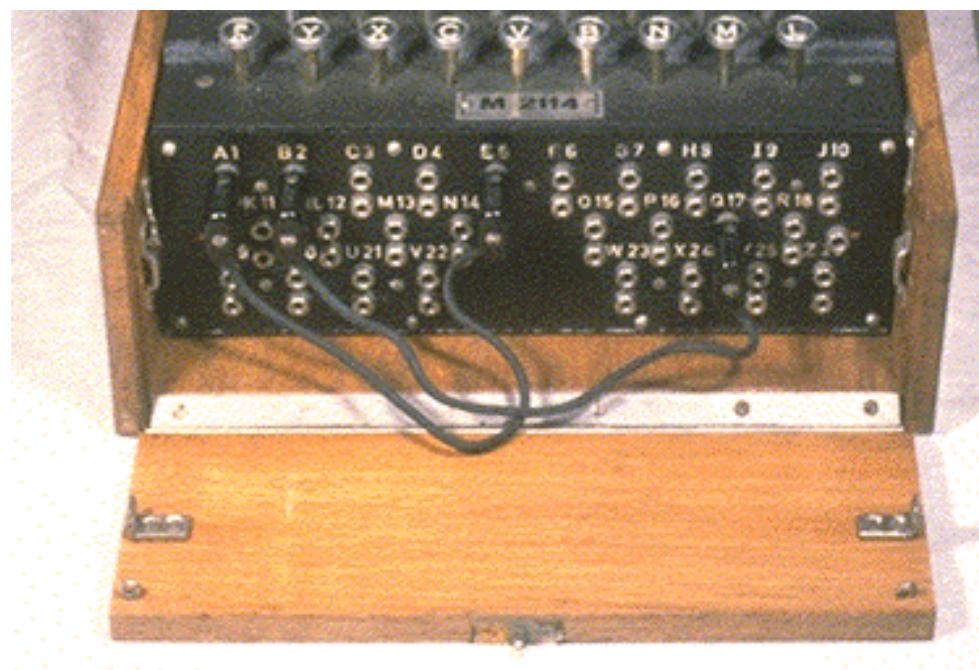


Ciclo: $26 \cdot 25 \cdot 26 = 16.900$ caratteri

Enigma pannello tavole di connessione

6 coppie di swap

- Lettere scambiate
- Cavo fra le due lettere da scambiare



Enigma pannello tavole di connessione

6 coppie di swap

- Lettere scambiate
- Cavo fra le due lettere da scambiare

Come funzionava il cavo?

Enigma pannello tavole di connessione

6 coppie di swap

- Lettere scambiate
- Cavo fra le due lettere da scambiare

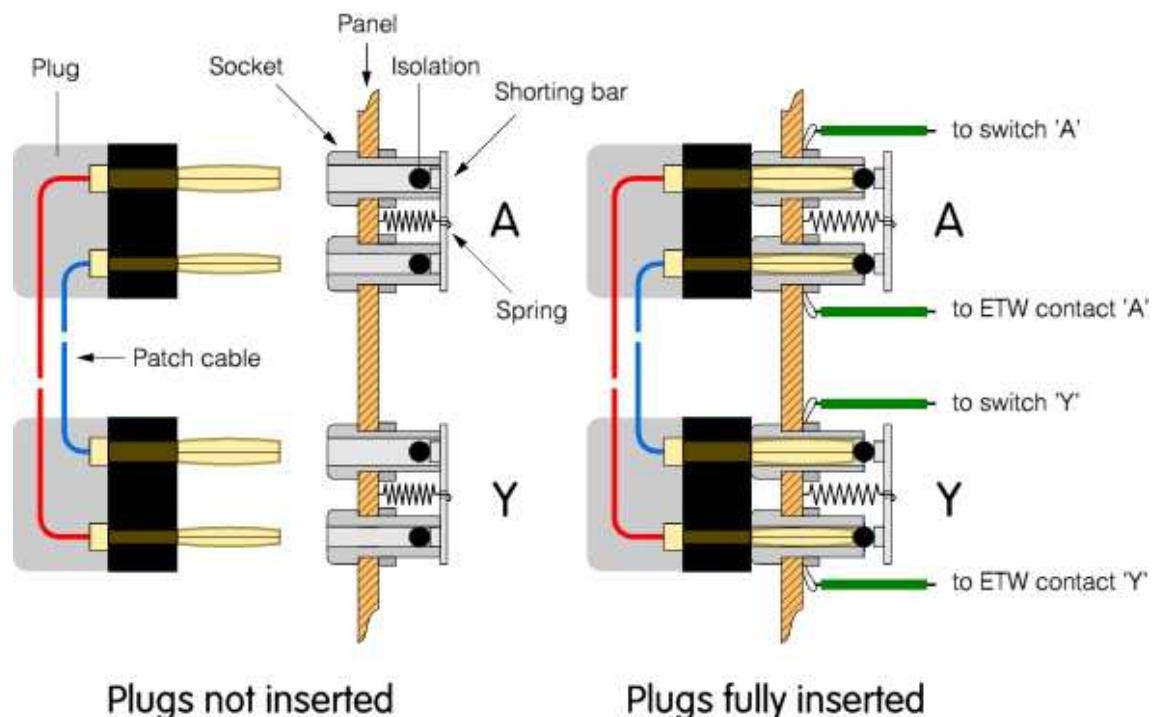
pin più sottile e
pin più doppio



Enigma pannello tavole di connessione

6 coppie di swap

- Lettere scambiate
- Cavo fra le due lettere da scambiare



Qualche ulteriore dettaglio

- Uso solo di 26 lettere
- Punteggiatura omessa oppure sostituita
 - In modi diversi da Esercito, Marina, ...
- Ad esempio
 - Spazio omesso oppure sostituito da "X"
 - ":" omesso oppure sostituito da "X"
 - "," codificata con "ZZ" o "Y"
 - "?" codificato con "FRAGE" o "FRAQ" o "UD"

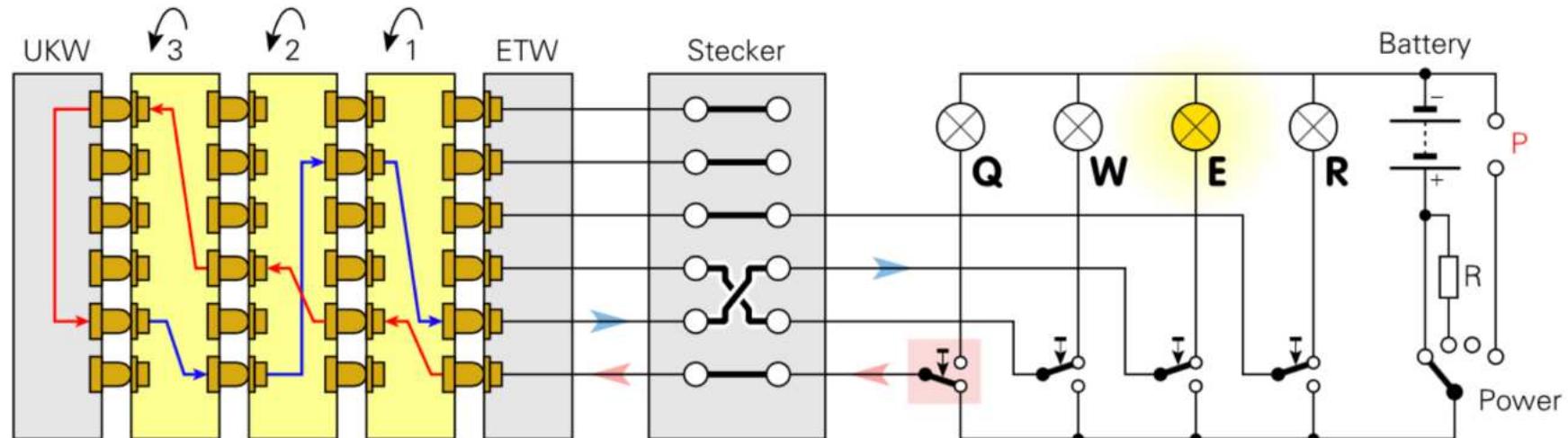
Rilevazione lettera cifratura

Come si rilevava la
lettera della cifratura?



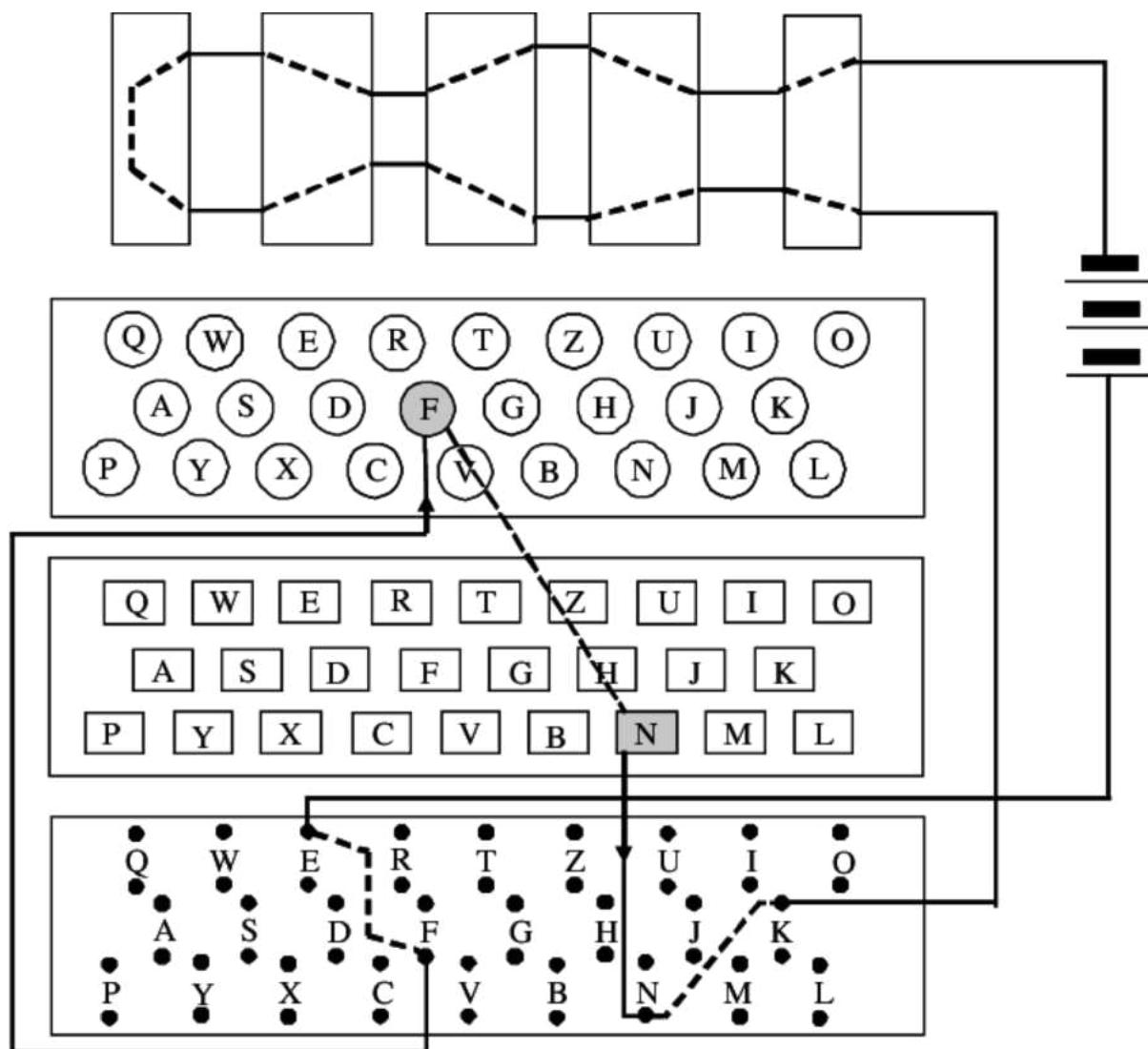
Rilevazione lettera cifratura

Come si rilevava la
lettera della cifratura?



Simplified circuit diagram of a 3-wheel Service Enigma

Diagramma funzionale



Enigma: inizializzazione

- **Walzenlage** scelta dei rotori e dell'ordine
 - 3 rotori tra 5 (Esercito e Aviazione) oppure tra 8 (Marina)
 - Marina M4, quarto rotore, "greco" e sottile
- **Umkehrwalze** scelta del riflettore
 - (possibile nelle versioni verso la fine della guerra)
- **Ringstellung** posizionamento di ogni singolo rotore
- **Steckerverbindungen** posizionamento coppie lettere in tavola di connessioni

Le chiavi di Enigma

Rotori o scambiatori:

- $26 \times 25 \times 26 = 16.900$ combinazioni possibili

Unità cifrante:

- I tre rotori (1,2,3) potevano essere inseriti in 6 diverse posizioni: 123, 132, 213, 231, 312, 321

Pannello a prese multiple:

- Gli abbinamenti di 6x2 lettere sono 12 su 26 cioè 100.391.791.500

Numero di chiavi totali: 10 milioni di miliardi...

Chiave giornaliera

- Assetto del pannello
 - Es. A/L - P/R - T/D - B/W - K/F - O/Y
- Disposizione dei rotori
 - 1 - 3 - 2
- Orientamento dei rotori
 - Q - C - W

Chiave giornaliera

- Assetto del pannello
 - Es. A/L - P/R - T/D - B/W - K/F - O/Y
- Disposizione dei rotori
 - 1 - 3 - 2
- Orientamento dei rotori
 - Q - C - W

Per maggiore sicurezza uso di una *chiave di messaggio*:

- Es. chiave giornaliera QCW
- Chiave messaggio PGH, ripetuta PGHPGH
- Cifratura di PGHPGH tramite QCW, → KIVBJE
- Cifratura e trasmissione del messaggio tramite PGH

Enigma: vari modelli

- Arthur Scherbius, inventore
- Brevetto ottenuto nel 1928
- Azienda a Berlino
- Costruite circa 100.000 macchine
- Versioni commerciali
 - Enigma A (1923)
 - Enigma B (1924)
 - Enigma C (1926)
 - Enigma D (1927)
 - Enigma H (1929)
 - ...



Enigma: vari modelli

- Arthur Scherbius, inventore
- Brevetto ottenuto nel 1928
- Azienda a Berlino
- Costruite circa 100.000 macchine
- Versioni commerciali
 - Enigma A (1923)
 - Enigma B (1924)
 - Enigma C (1926)
 - Enigma D (1927)
 - Enigma H (1929)
 - ...



Enigma H (1929)
8 rotori
Ritirata, non affidabile

Enigma: vari modelli

➤ Versioni militari

- Funkschlüssel C (1926)
- Enigma G (1928-1930)
- Wehrmacht Enigma I (1930-1938)
- M3 (1934)
 - Rotori in più (1938-1939) per esercito, aviazione e marina
- M4 (1942)

U.S. National
Cryptologic Museum

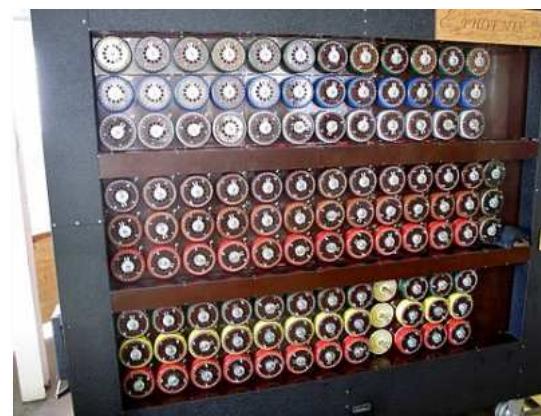
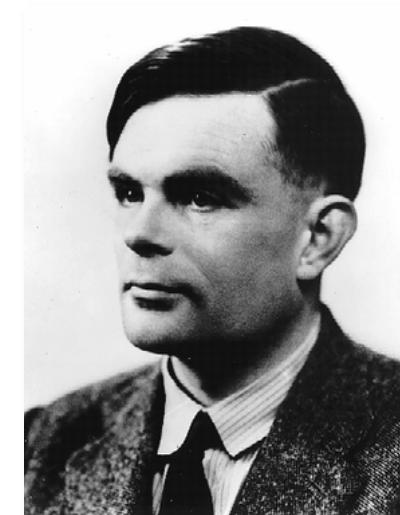


Enigma: alcuni punti deboli

- Nessuna lettera cifra se stessa
 - A causa del reflettore!
- Se L1 cifra L2 allora L2 cifra L1
- Utilizzo di *cillies*, chiavi semplici
 - Ad es., qweqwe
- Invio della posizione iniziale rotori
- ...

Enigma: crittoanalisi

- Marian Rejewski ed altri matematici polacchi, decifravano i messaggi cifrati della versione corrente, 1932
 - Creazione di una "bomba", device elettromeccanica
- Nel 1938 il numero di rotori passò da 3 a 5
- Alan Turing e altri matematici a Bletchley Park
 - Bombe inglesi 1939
 - Poiché i rotori potevano essere scelti e poi posti in posizioni diverse occorrevano $\binom{5}{3} = 36$ "bombe" che funzionavano in parallelo
- "bombe" forse a causa del ticchettio prodotto



Bomba ricostruita
The National Museum of Computing
on Bletchley Park

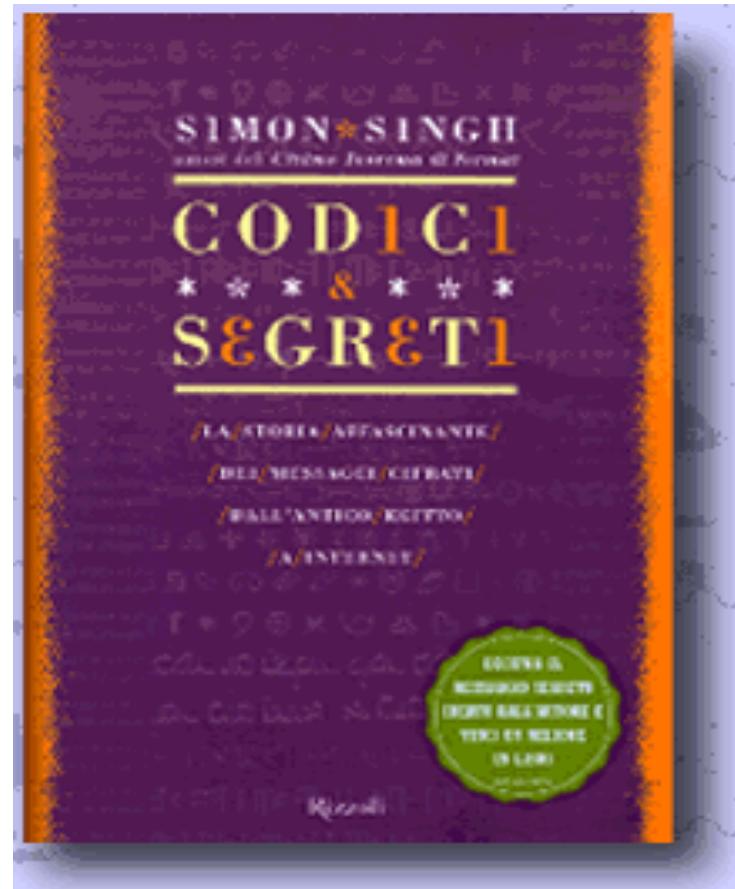
Cifratrice Lorentz e Colossus

- Telescrivente
- Comunicazione alto livello
 - Molti messaggi firmati "Adolf Hitler, Führer"
- 12 dischi che producevano una sequenza pseudocasuale, poi in xor con il testo in chiaro
- Costruzione di **Colossus**
 - Primo computer elettronico, programmabile
 - Primo prototipo, 1944, Bletchley Park
 - Erano 10 alla fine della guerra
 - Tutte distrutte dai servizi segreti inglesi
 - Replica funzionante, 2007, esposta The National Museum of Computing, Bletchley Park
 - Non per qualsiasi computazione



Bibliografia

Simon Singh,
Codici & Segreti
Rizzoli ed., 1999



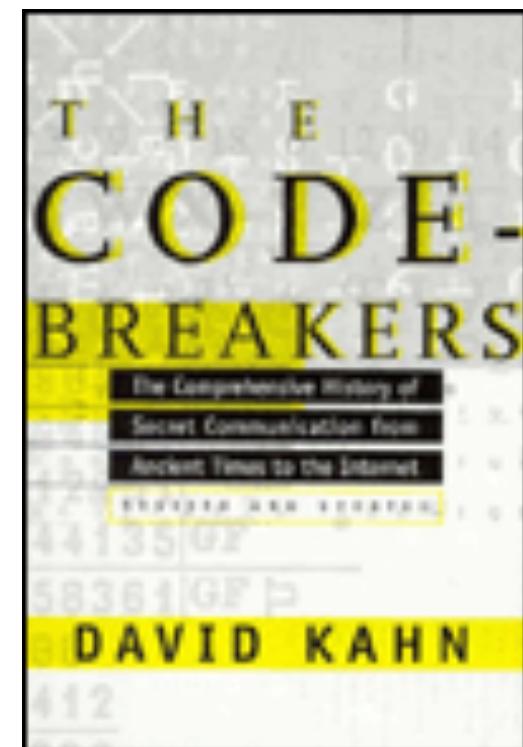
Bibliografia

David Kahn,

The codebreakers: the Story of Secret Writing

Macmillan, New York 1967

Simon & Schuster Trade
1200 pp., October 1996



Domande?

