Cifrari storici

Cifrari storici

Scopo:

consentire comunicazioni **"sicure"** tra poche persone

➔ ma sono stati tutti forzati

Cifratura e decifrazione:

realizzate con carta e penna

Messaggi da cifrare:

frasi di senso compiuto in linguaggio naturale

Alfabeto: 26 lettere A, B, C, ..., X, Y, Z

Principi di Bacone

XIII secolo

1. Le funzioni C e D devono essere facili da calcolare
2. È impossibile ricavare la D se la C non è nota
3. Il crittogramma c = C (m) deve apparire *"innocente"*

Antichi esempi

Il metodo più antico di cui si ha notizia fu inventato dagli spartani nel V secolo a.C.

Scitale: asta cilindrica, costruita in due esemplari identici posseduti dai due corrispondenti

Chiave segreta: diametro della scitale

Antichi esempi

Erodoto: *Storie* (V secolo a. C.)

Cifrari storici: altri esempi

Enea Tattico, Grecia, IV secolo a.C.:

opera militare con un capitolo dedicato ai messaggi segreti

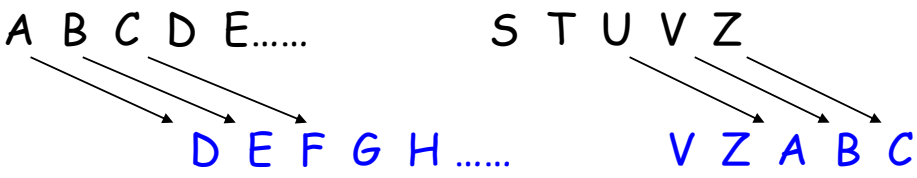
- inviare un libro qualsiasi sottolineandovi un sottoinsieme di lettere che costituiscono il messaggio
- sostituire le vocali di un testo con altri simboli grafici

Cifrario di Cesare

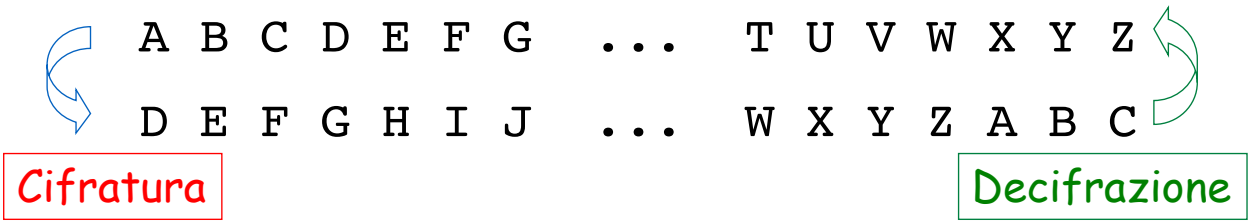
È il più antico cifrario di concezione moderna (Svetonio, *Le vite di dodici Cesari)*

Idea di base:

Il crittogramma c è ottenuto dal messaggio in chiaro m sostituendo ogni lettera di m con quella tre posizioni più avanti nell'alfabeto



Cifrario di Cesare



ATTENTO A EVE

DWWHQWR D HYH

Cifrario di Cesare

Non ha una chiave segreta

La segretezza dipendeva dalla conoscenza del metodo

Scoprire il metodo di cifratura significa comprometterne irrimediabilmente l'impiego

Il cifrario era destinato all'uso ristretto di un gruppo di conoscenti

Cifrario di Cesare generalizzato

Può essere trasformato aumentandone la sicurezza

- invece di rotare l' alfabeto di 3 posizioni, possiamo rotarlo di una quantità arbitraria k, $1 \leq k \leq 25$ (26 lascia inalterato il messaggio)
- in questo caso k è la chiave segreta del cifrario

Formulazione matematica

pos(X): posizione nell' alfabeto della lettera X
(pos(A) = 0, pos(B) = 1, ..., pos(Z) = 25)

chiave k, $1 \leq k \leq 25$

Cifratura di X

lettera Y tale che pos(Y) = (pos(X) + k) mod 26

Decifrazione di Y

lettera X tale che pos(X) = (pos(Y) - k) mod 26

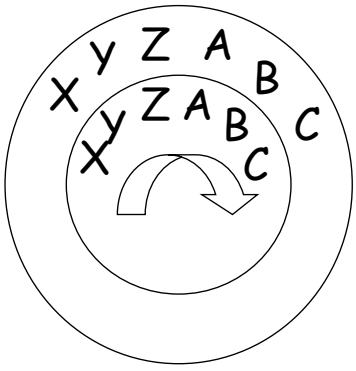
Esempio:

k = 10, cifratura di R, pos(R) = 17
(17 + 10) mod 26 = 1 = pos(B) R → B

Realizzazione fisica

Due dischi concentrici:

- disco interno: lettere dell'alfabeto in chiaro
- disco esterno: lettere cifrate



Crittoanalisi

Se si conosce la struttura del cifrario, si possono applicare in breve tempo tutte le chiavi possibili (25) a un crittogramma

- per decifrarlo
- e scoprire contemporaneamente la chiave segreta.

Cifrario inutilizzabile a fini crittografici

Osservazioni

Gode della proprietà commutativa

- data una sequenza di chiavi e di operazioni di cifratura e decifrazione, l'ordine delle operazioni può essere permutato arbitrariamente senza modificare il crittogramma finale

Date due chiavi, k_1 e k_2, e una sequenza s

$$C\,(C\,(s, k_2), k_1) = C\,(s, k_1 + k_2)$$

$$D\,(D\,(s, k_2), k_1) = D\,(s, k_1 + k_2)$$

una sequenza di operazioni di cifratura e decifrazione può essere ridotta ad una sola operazione di cifratura o decifrazione

Osservazioni

Inoltre, date due chiavi e una sequenza s

$C(D(s, k_2), k_1) = C(s, k_1 - k_2)$ se $k_1 \geq k_2$

$C(D(s, k_2), k_1) = C(s, k_2 - k_1)$ se $k_1 < k_2$

Comporre più cifrari non aumenta la sicurezza del sistema

Classificazione dei cifrari storici

Cifrari a sostituzione

sostituiscono ogni lettera del messaggio in chiaro con una o più lettere dell'alfabeto secondo una regola prefissata

Cifrari a trasposizione

permutano le lettere del messaggio in chiaro secondo una regola prefissata

Cifrari a sostituzione

Sostituzione monoalfabetica

alla stessa lettera del messaggio corrisponde sempre una stessa lettera nel crittogramma

Esempio: cifrario di Cesare

Sostituzione polialfabetica

alla stessa lettera del messaggio corrisponde una lettera scelta in un insieme di lettere possibili, secondo con una regola opportuna

a seconda della posizione o del contesto in cui appare la lettera nel messaggio

Sostituzione monoalfabetica

Si possono impiegare funzioni di cifratura e decifrazione più complesse dell'addizione e della sottrazione in modulo

Lo spazio delle chiavi è molto più ampio

La sicurezza è comunque molto modesta

Esempio: il cifrario affine

CIFRATURA

una lettera in chiaro X viene sostituita con la lettera cifrata Y che occupa nell' alfabeto la posizione

$$pos(Y) = (a * pos(X) + b) \bmod 26,$$

k = <a,b>: chiave segreta del cifrario

Esempio

k = <3,1>

"IL NOSTRO TEMPO"

⇓

"ZI OREGAR GNBUR"

Decifrazione

$$pos(X) = a^{-1} * (pos(Y) - b) \bmod 26$$

a^{-1}: l' inverso di a modulo 26

$(a \times a^{-1} = 1 \bmod 26)$

Vincoli

L'inverso di un intero a modulo m esiste ed è unico se e solo se MCD(a, m) = 1

Vincolo forte sulla definizione della chiave

Se MCD(a, 26) ≠ 1, la *funzione di cifratura non è iniettiva, e la decifrazione diventa impossibile*

ESEMPIO: k = < 13, 0 >

- tutte le lettere in posizione pari verrebbero trasformate in A (pos(A) = 0)
- tutte le lettere in posizione dispari in N (pos(N) = 13)

Chiavi segrete

- a e 26 devono essere co-primi
  - i fattori primi di 26 sono 2 e 13
  - a può assumere qualsiasi valore dispari tra 1 e 25, ad eccezione di 13 (12 valori possibili)
- b può essere scelto liberamente tra 0 e 25
  - dunque può assumere 26 valori
- Le chiavi legittime sono tutte le possibili < a, b >
- In totale 12 × 26 = 312 chiavi (troppo poche...)
  - in realtà 311 (la coppia <1,0> lascia inalterato il messaggio)

Le chiavi segrete

Se la segretezza dipende unicamente dalla chiave

il numero delle chiavi deve essere così grande da essere praticamente immune da ogni tentativo di provarle tutte

la chiave segreta deve essere scelta in modo causale

Cifrario completo

Si può prendere una permutazione arbitraria dell'alfabeto come chiave:

lettera in chiaro di posizione i

⇓

lettera di posizione i nella permutazione

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

testo: BOBSTAIATTENTOAEVE

messaggio cifrato: DEDFWSRSWWBYWESBGB

Cifrario completo

Chiave di 26 lettere

contro 2 numeri interi del cifrario affine

Spazio delle chiavi

esteso a $26! - 1$ ($\sim 4 \cdot 10^{26}$) chiavi

vasto e inesplorabile con metodi esaurienti

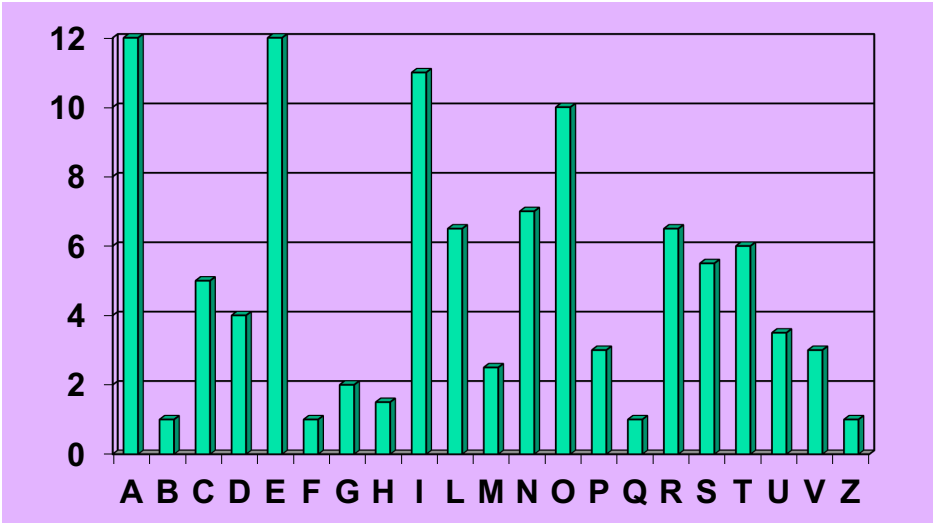
Ma il cifrario non è sicuro:

si può forzare (senza ricorrere a un attacco esauriente) sfruttando

- struttura logica dei messaggi in chiaro
- occorrenza statistica delle lettere

il sistema è attaccabile facilmente con un'analisi statistica sulla frequenza dei caratteri

Frequenze dei caratteri in italiano



Cifrari a sostituzione polialfabetica

- Una stessa lettera che si incontra in punti diversi del messaggio in chiaro ammette un insieme di lettere sostitutive possibili scelte con una regola opportuna
- L'esempio più antico risale ai tempi di Roma imperiale (archivio cifrato di Augusto)

Cifrario di Augusto

Svelato dall'imperatore Claudio

- I documenti dell' archivio erano scritti in numeri, non in lettere
- Augusto li scriveva in greco, poi metteva in corrispondenza la sequenza di lettere del documento con la sequenza di lettere del primo libro dell'Iliade
- Sostituiva ogni lettera del documento con il numero che indicava la distanza, nell'alfabeto greco, di tale lettera con quella in pari posizione nell'Iliade

Esempio:

lettera in posizione i nel documento: α
lettera in posizione i nell' Iliade: ε
carattere in pos. i nel crittogramma: 4 (distanza tra α e ε)

Cifrario di Augusto

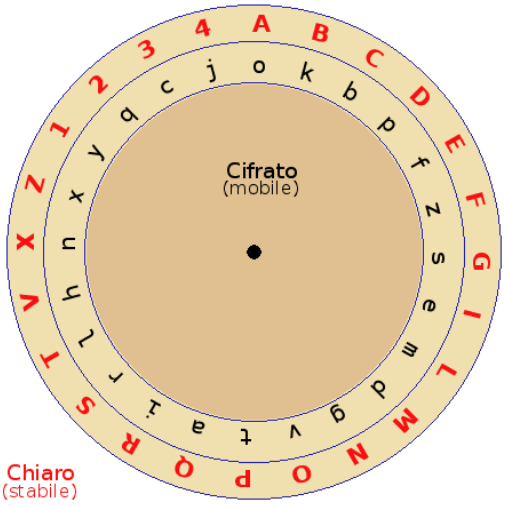
Cifrario difficile da forzare se la chiave è lunghissima

Utilizzato nella seconda guerra mondiale prendendo come chiave una pagina prefissata di un libro, e cambiandola di giorno in giorno

Svantaggio: registrazione per iscritto della chiave

Nascita dei cifrari polialfabetici

il disco di Leon Battista Alberti (XV secolo)



Alfabeto esterno
lettere (alcune) e numeri, per formulare il messaggio

Alfabeto interno
più ricco, disposto in modo arbitrario (e diverso per ogni coppia di utenti), per costruire il crittogramma

Cifrario di Alberti

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

Chiave: A-S

Messaggio: NON FIDARTI DI EVE

m = N O N F I D A 2 R T I D I E V E

c = U N U J R K S Q

qui la chiave diventa A-Q

Cifrario di Alberti

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

Chiave: A-Q

Messaggio: NON FIDARTI DI EVE

m = N O N F I D A 2 R T I D I E V E

c = U N U J R K S Q

qui la chiave diventa A-Q

Cifrario di Alberti

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

Chiave: A–Q

Messaggio: NON FIDARTI DI EVE

m = N O N F I D A 2 R T I D I E V E

c = U N U J R K S Q U Y B M B S P S

qui la chiave diventa A–Q

Metodo "indice mobile"

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

m:	I	L	D	*2*	E	L	*P*	F	I	N	O
c:	P	D	C	S	W	D	O	O	I	R	J

Il numero 2, ottenuto decifrando S, indica che dopo due caratteri la chiave verrà cambiata

O, decifrato in P, indica la nuova chiave A-P

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

Cifrario di Alberti

si cambia chiave ogni volta che si incontra un carattere speciale

inserendo spesso i caratteri speciali (scartati nel messaggio ricostruito) il cifrario è difficile da attaccare

il continuo cambio di chiave rende inutili gli attacchi basati sulla frequenza dei caratteri

La Macchina Enigma
(Germania, 1918)

Estensione elettromeccanica del cifrario di Alberti

Sull'idea di Alberti lavorò de Vigenère (1586)

La chiave è corta e ripetuta ciclicamente.

Ogni lettera della chiave indica una traslazione della corrispondente lettera del testo.

chiave:	C	H	I	A	V	E
traslazione:	2	7	8	0	24	4

N	O	N	F	I	D	A	R	T	I	D	I	E	V	E
2	7	8	0	24	4	2	7	8	0	24	4	2	7	8
↓														
P														

Sull'idea di Alberti lavorò de Vigenère (1586)

La chiave è corta e ripetuta ciclicamente.

Ogni lettera della chiave indica una traslazione della corrispondente lettera del testo.

chiave:	C	H	I	A	V	E
traslazione:	2	7	8	0	24	4

N	O	N	F	I	D	A	R	T	I	D	I	E	V	E
2	7	8	0	24	4	2	7	8	0	24	4	2	7	8
↓	↓													
P	V													

Sull'idea di Alberti lavorò de Vigenère (1586)

La chiave è corta e ripetuta ciclicamente.

Ogni lettera della chiave indica una traslazione della corrispondente lettera del testo.

chiave:	C	H	I	A	V	E
traslazione:	2	7	8	0	24	4

N	O	N	F	I	D	A	R	T	I	D	I	E	V	E
2	7	8	0	24	4	2	7	8	0	24	4	2	7	8
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
P	V	V	F	G	H	C	Y	B	I	B	M	G	C	M

Cifrario di Vigenère

Tabella T, 26 × 26, nota a tutti

Riga i-esima

alfabeto di 26 lettere rotato verso sinistra di i-1 posizioni

A	B	C	...	X	Y	Z
B	C	D	...	Y	Z	A
C	D	E	...	Z	A	B
...	...	...	...	...	...	...
X	Y	Z	...	U	V	W
Y	Z	A	...	V	W	X
Z	A	B	...	W	X	Y

Cifrario di Vigenère

Chiave: parola segreta k

Cifratura di un messaggio m

si dispongono m e k su due righe adiacenti, allineando le lettere in verticale (se k è più corta di m, la chiave si ricopia più volte)

Ogni lettera X del messaggio in chiaro risulta allineata ad una lettera Y della chiave

La X viene sostituita nel crittogramma con la lettera che si trova nella cella di T all'incrocio tra la riga che inizia con X e la colonna che inizia con Y

Esempio

m = IL DELFINO

k = ABRA

I	L		D	E	L	F	I	N	O
A	B		R	A	A	B	R	A	A
↓	↓		↓	↓	↓	↓	↓	↓	↓
I	M		U	E	L	G	Z	N	O

Esempio

Le lettere del messaggio allineate con la lettera A della chiave non subiscono alcuna modifica

Quelle allineate con B sono traslate di una posizione in avanti

Quelle allineate con R sono traslate di 17 posizioni in avanti; etc.

Una stessa lettera in chiaro viene cifrata in modi diversi, a seconda della lettera della chiave a cui è allineata

Per la decifrazione si segue il procedimento inverso

Sicurezza

La sicurezza del metodo è influenzata dalla lunghezza della chiave

Se la chiave contiene **h** caratteri, le apparizioni della stessa lettera distanti un multiplo di **h** nel messaggio si sovrappongono alla stessa lettera della chiave,

quindi sono trasformate nella stessa lettera cifrata

Sicurezza

Per ogni intero positivo $i \leq h$

- si costruisce un sottomessaggio m[i] formato dalle lettere di m che occupano le posizioni i, i + h, i + 2h, ...
- In ciascuno di tali sottomessaggi tutte le lettere sono allineate con la stessa lettera della chiave
- Il messaggio è decomposto in h sottomessaggi, ciascuno dei quali è di fatto cifrato con un metodo monoalfabetico

I cifrari polialfabetici non sono dunque tanto più potenti dei monoalfabetici se le chiavi non sono molto lunghe

One-Time Pad (1917)

Se estendiamo il metodo di Vigenère impiegando una chiave lunga come il testo, casuale e non riutilizzabile, il cifrario diviene inattaccabile!

Non può essere decifrato senza conoscere la chiave

È il caso di One-Time Pad (1917) che impiega un codice binario per messaggi e chiavi

Fu usato nella Hot Line per le comunicazioni tra la Casa Bianca e il Cremlino a partire dal 1967

Cifrari a trasposizione

Idea di base: eliminare qualsiasi struttura linguistica presente nel crittogramma

- permutando le lettere del messaggio in chiaro
- e inserendone eventualmente altre che vengono ignorate nella decifrazione

Cifrario a permutazione semplice

Chiave:

intero h; permutazione π degli interi {1, 2, ..., h}

Cifratura:

- si suddivide il messaggio m in blocchi di h lettere
- si permutano le lettere di ciascun blocco secondo π

Osservazione:

se la lunghezza di m non è divisibile per h, si aggiungono alla fine delle lettere qualsiasi (padding)

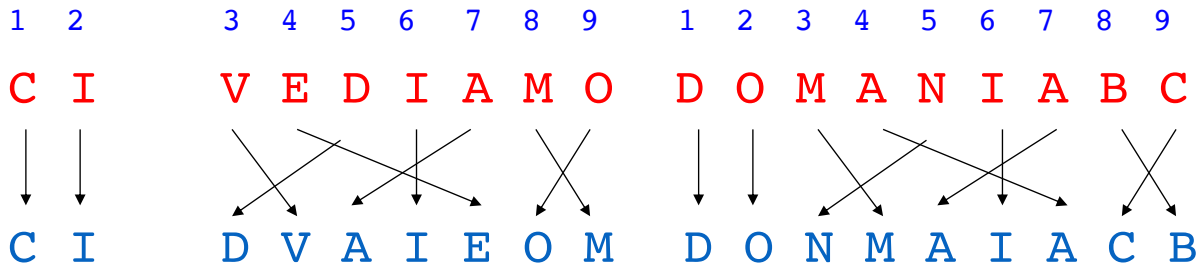
- che partecipano alla trasposizione
- ma sono ignorate dal destinatario perché la decifrazione le riporta alla fine del messaggio

Cifrario a permutazione semplice

ESEMPIO

h = 9

π = {1 2 5 3 7 6 4 9 8}



Cifrario a permutazione semplice

Numero delle chiavi

$$h! - 1$$

h non è fissato a priori

tanto maggiore è h, tanto più difficile è impostare un attacco esauriente

Al crescere di h cresce anche la difficoltà di ricordare la chiave π

Cifrario a permutazione di colonne

$k = < c, r, \pi >$

- c e r denotano il numero di colonne e di righe di una tabella di lavoro T
- π: permutazione degli interi {1, 2,..., c}

messaggio m:

- decomposto in blocchi $m_1, m_2, \ldots$ di $c \times r$ caratteri ciascuno

Cifrario a permutazione di colonne

Cifratura del blocco m_i

- I caratteri sono distribuiti tra le celle di T in modo regolare, scrivendoli per righe dall'alto verso il basso

Esempio

$c = 6, r = 3, \pi = \{2, 1, 5, 3, 4, 6\}$

m = NON SONO IL COLPEVOLE

N	O	N	S	O	N
O	I	L	C	O	L
P	E	V	O	L	E

Cifrario a permutazione di colonne

Le colonne di T sono permutate secondo π

Esempio: $\pi = \{2, 1, 5, 3, 4, 6\}$

1	2	3	4	5	6
N	O	N	S	O	N
O	I	L	C	O	L
P	E	V	O	L	E

T

2	1	5	3	4	6
O	N	O	N	S	N
I	O	O	L	C	L
E	P	L	V	O	E

T permutata

c = | OIE | NOP | OOL | NLV | SCO | NLE |

Cifrario a permutazione di colonne

Cifratura del blocco m_{i+1}

T viene azzerata e il procedimento si ripete.

Numero di chiavi

Teoricamente esponenziale nella lunghezza del messaggio, non essendoci vincoli sulla scelta di r e c.

Cifrario a griglia

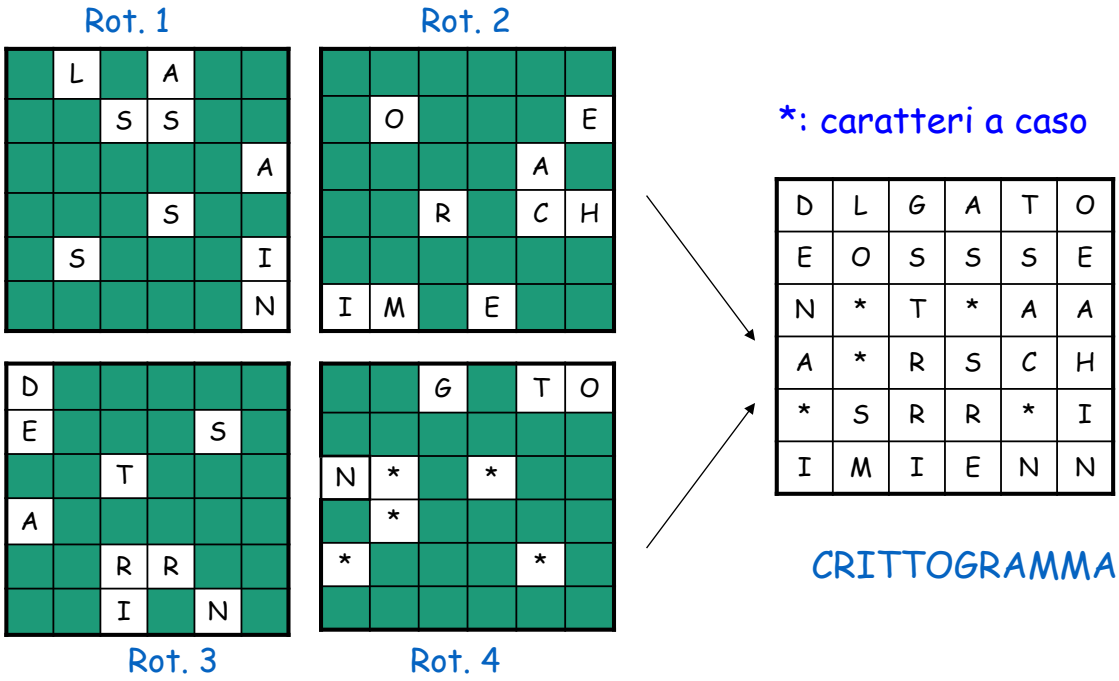
Progenitore: cifrario di Richelieu

- Il crittogramma può essere celato in un libro qualsiasi
- la chiave è data da una scheda perforata e dall'indicazione di una pagina del libro
- La decifrazione consiste nel sovrapporre la scheda alla pagina: le lettere visibili attraverso la perforazione costituiscono il messaggio in chiaro

Variante

- La chiave segreta è una griglia quadrata, di dimensioni $q \times q$, con q pari
- $s = q^2/4$ celle della griglia (un quarto del totale) sono trasparenti, le altre opache
- Si scrivono i primi s caratteri del messaggio, nelle posizioni corrispondenti alle celle trasparenti
- La griglia viene rotata tre volte di 90 gradi in senso orario, e si ripete per ogni rotazione l'operazione di scrittura di tre successivi gruppi di s caratteri

Esempio: q = 6, s = 9,
m = L'ASSASSINO È ARCHIMEDES TARRINGTON



Variante

- La griglia deve essere scelta in modo che le posizioni corrispondenti alle celle trasparenti non si sovrappongano mai nelle quattro rotazioni
- Se la lunghezza del messaggio è minore di 4s, le posizioni della pagina P rimaste vuote si riempiono con caratteri scelti a caso.
- Se la lunghezza del messaggio è maggiore di 4s, il messaggio viene decomposto in blocchi di 4s caratteri ciascuno, e ogni blocco è cifrato indipendentemente dagli altri
- La decifrazione di P è eseguita sovrapponendovi quattro volte la griglia

Chiavi

Vi sono $G = 4^s$ griglie, i.e., chiavi segrete, possibili

Per $q = 6$, $G = 4^9 \approx 260\,000$

Per $q = 12$, $G = 4^{36}$

numero sufficiente a porre il cifrario al riparo da un attacco esauriente

Crittoanalisi statistica

La sicurezza di un cifrario è legata alla dimensione dello spazio delle chiavi

Altri metodi di attacco

I cifrari storici sono stati violati con un attacco statistico di tipo *cipher text* (il crittoanalista ha a disposizione solo il crittogramma)

L' impiego del metodo si fa risalire in Europa alla metà del XIX secolo, quando si scoprì come violare il cifrario di Vigenère, considerato assolutamente sicuro da 300 anni

Crittoanalisi statistica: ipotesi

Informazioni note al crittoanalista

- metodo impiegato per la cifratura/decifrazione
- linguaggio naturale in cui è scritto il messaggio
- si ammette che il messaggio sia sufficientemente lungo per poter rilevare alcuni dati statistici sui caratteri che compongono il crittogramma

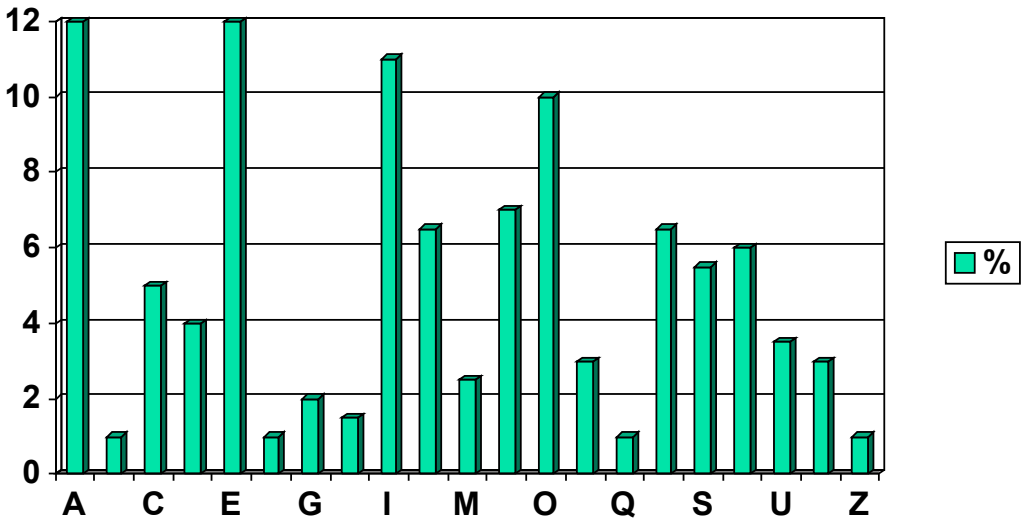
Crittoanalisi statistica: attacco

La frequenza con cui appaiono in media le varie lettere dell'alfabeto è ben studiata in ogni lingua

Dati simili sono noti per le frequenze di

- ***digrammi*** (gruppi di due lettere consecutive)
- ***trigrammi*** (gruppi di tre lettere consecutive)
- e così via (***q-grammi***)

Frequenza in % delle lettere dell' italiano



Crittoanalisi statistica: attacco

Se un crittogramma è stato generato per sostituzione monoalfabetica

- y nel crittogramma corrisponda a x nel messaggio
- frequenza(y) ≈ frequenza(x)

Si confrontano le frequenze delle lettere

si provano alcune permutazioni tra lettere con frequenze assai prossime

→ ipotesi di prima decifrazione

Decifrazione del cifrario di Cesare

È sufficiente scoprire la corrispondenza di una sola coppia <x,y> per svelare l' intero messaggio

Decifrazione di cifrari affini

È sufficiente individuare due coppie di lettere corrispondenti con cui impostare un sistema di due equazioni nelle due incognite a e b che formano la chiave segreta

La risoluzione del sistema è sempre possibile perché a è invertibile

Decifrazione di cifrari completi

Si associano le lettere in base alle frequenze

Esempio

se le lettere E, R e U appaiono nel crittogramma con frequenze comprese tra 6/100 e 7/100, rappresentano con ogni probabilità le lettere L, N e R del messaggio

si provano le possibili associazioni

le associazioni si possono raffinare controllando i digrammi più frequenti

in genere a questo punto il cifrario è completamente svelato; altrimenti si passa ai trigrammi, e così via

Cifrari a sostituzione polialfabetica

La decifrazione è più difficile

Cifrario di Vigenère:

ogni lettera y del crittogramma dipende da una coppia di lettere <x,k> provenienti dal messaggio e dalla chiave (si altera la frequenza delle lettere del crittogramma)

DEBOLEZZA: chiave unica ripetuta più volte

Cifrari a sostituzione polialfabetica

Chiave di h caratteri

il crittogramma si decompone in h sottosequenze, ciascuna ottenuta per sostituzione monoalfabetica

Problema: scoprire il valore di h

- per scomporre il crittogramma
- e continuare la decifrazione con il metodo monoalfabetico

Valore di *h* (q-grammi)

Il messaggio contiene quasi sicuramente gruppi di lettere adiacenti ripetuti più volte (trigrammi più frequenti nella lingua; parole cui il testo si riferisce)

Apparizioni della stessa sottosequenza allineate con la stessa porzione della chiave sono trasformate nel crittogramma in sottosequenze identiche

Si cercano nel crittogramma coppie di posizioni p_1, p_2 in cui iniziano sottosequenze identiche

La distanza $d = p_2 - p_1$ è probabilmente uguale alla lunghezza h della chiave, o a un suo multiplo

Cifrario di Alberti

Immune da questi attacchi se la chiave viene cambiata spesso evitando pattern ripetitivi

Mantenere a lungo una chiave mette a rischio il cifrario perché in quel tratto la sostituzione è monoalfabetica

Cifrari a trasposizione

Le lettere nel crittogramma sono le stesse del messaggio in chiaro, quindi non ha senso condurre un attacco statistico basato sulle frequenze

Un aiuto viene dallo studio dei q-grammi

Cifrari a permutazione semplice

Se si conosce la lunghezza h della chiave

- si divide il crittogramma in porzioni di lunghezza h
- in ciascuna si cercano i gruppi di q lettere che formano i q-grammi più diffusi nel linguaggio (non saranno adiacenti)
- se un gruppo deriva effettivamente da un q-gramma, si scopre parte della permutazione
  Es. QU

Conclusione

La rilevazione delle frequenze delle singole lettere del crittogramma è un potente indizio per discernere tra i vari tipi di cifrario

nei cifrari a trasposizione l' istogramma delle frequenze coincide approssimativamente con quello proprio del linguaggio

nei cifrari a sostituzione monoalfabetica i due istogrammi coincidono a meno di una permutazione delle lettere

nei cifrari a sostituzione polialfabetica, l'istogramma del crittogramma è assai più appiattito di quello del linguaggio (le frequenze delle lettere variano assai meno tra loro)

La macchina ENIGMA

Prima evoluzione verso sistemi automatizzati

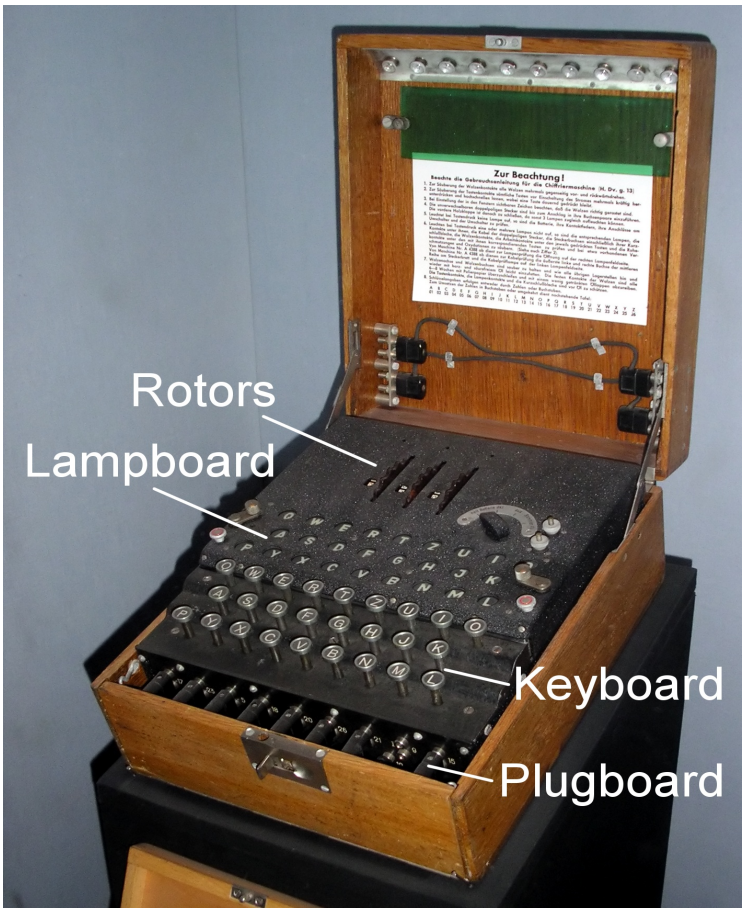
Ruolo fondamentale nella storia recente (II guerra mondiale)

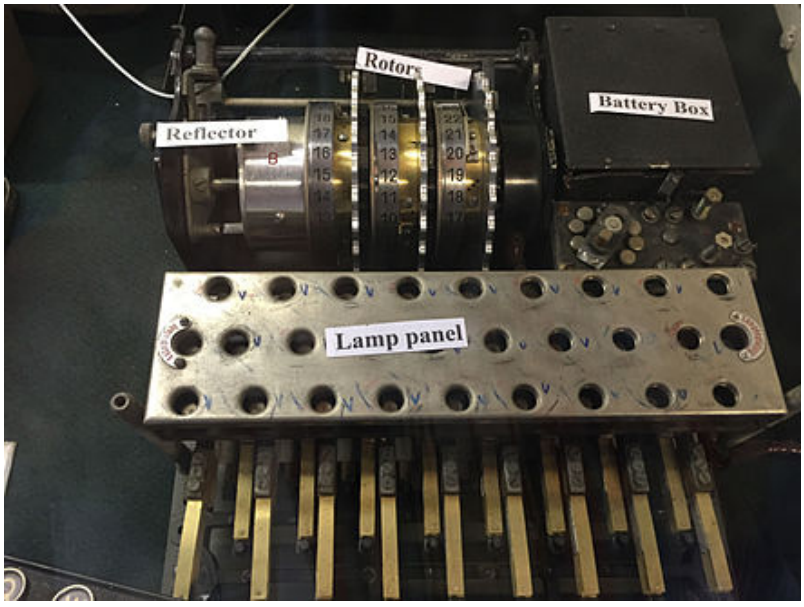
Molti studi dedicati a comprometterne la sicurezza

Fondamenti della nascita dei calcolatori odierni

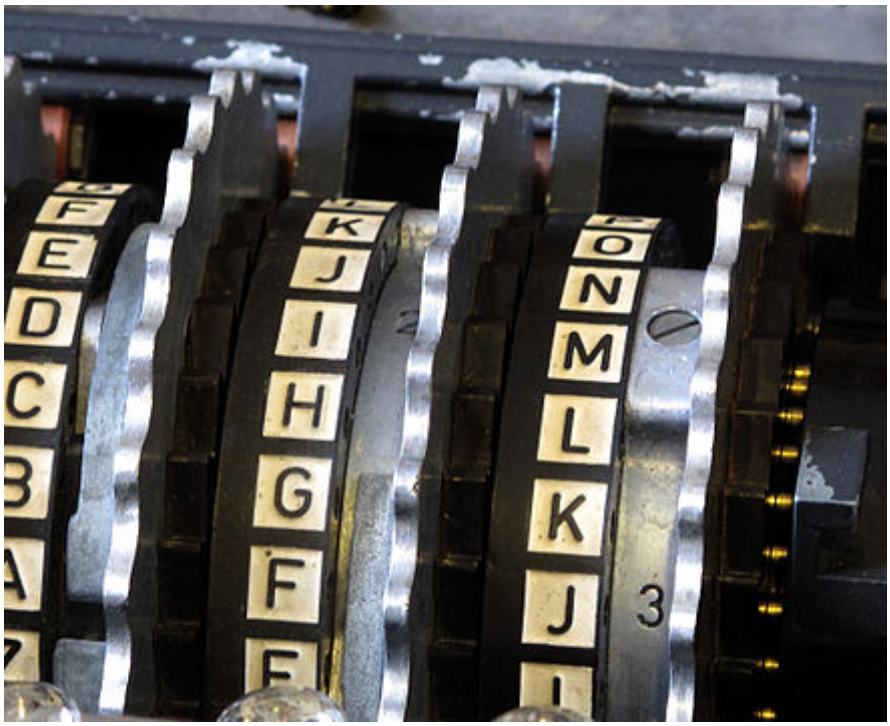
La macchina ENIGMA

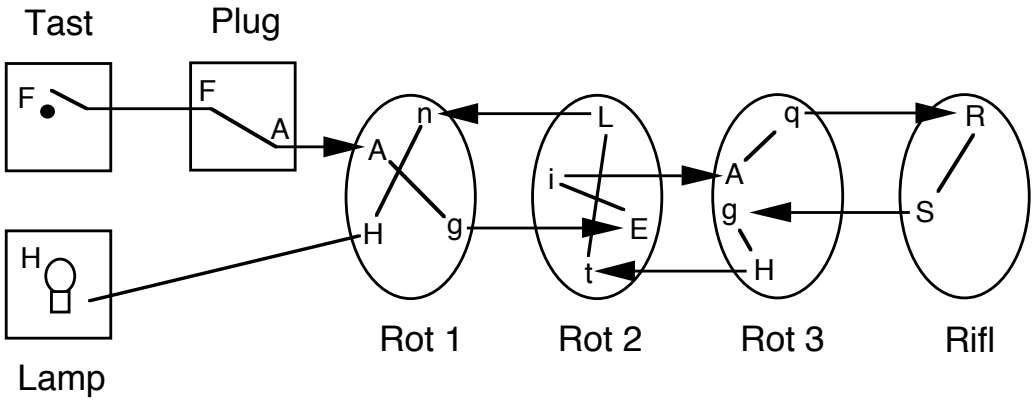
- Germania (1918) per applicazioni commerciali
- Estensione elettromeccanica del cifrario di Alberti


Zur Beachtung!
Rotors
Lampboard
Keyboard
Plugboard


Rotors
Battery Box
Reflector
Lamp panel


Nur Glühlampen mit 12 mm Durchmesser verwenden


FEDCBA
KJIHGF
NMLKJ
3


Tast
Plug
F
F
A
H
H
Lamp
n
A
g
L
i
E
t
q
A
g
H
R
S
Rot 1
Rot 2
Rot 3
Rifl

Movimento dei rotori

- I rotori non mantenevano la stessa posizione reciproca durante la cifratura
- Per ogni lettera battuta sulla tastiera
  - Il primo rotore avanzava di un passo
  - Dopo 26 passi il rotore era tornato sulla posizione iniziale, e avanzava di un passo il secondo rotore
  - Dopo la rotazione completa del secondo rotore, avanzava di un passo il terzo rotore
- La corrispondenza tra caratteri cambiava ad ogni passo (la chiave cambia a ogni passo)

Numero di permutazioni

- 26 con le rotazioni del primo rotore rispetto al secondo
- 26 con le rotazioni del secondo rotore rispetto al terzo
- 26 con le rotazioni del terzo rotore rispetto al riflettore
- 26 x 26 x 26 = 17576 chiavi diverse

Debolezza

- Rotori immutabili
- 26^3 permutazioni sono sempre le stesse, applicate nello stesso ordine
- Note a tutti i proprietari di una macchina Enigma
  - Alberti aveva previsto, per ogni coppia di utenti, una coppia di dischi diversa da tutte le altre

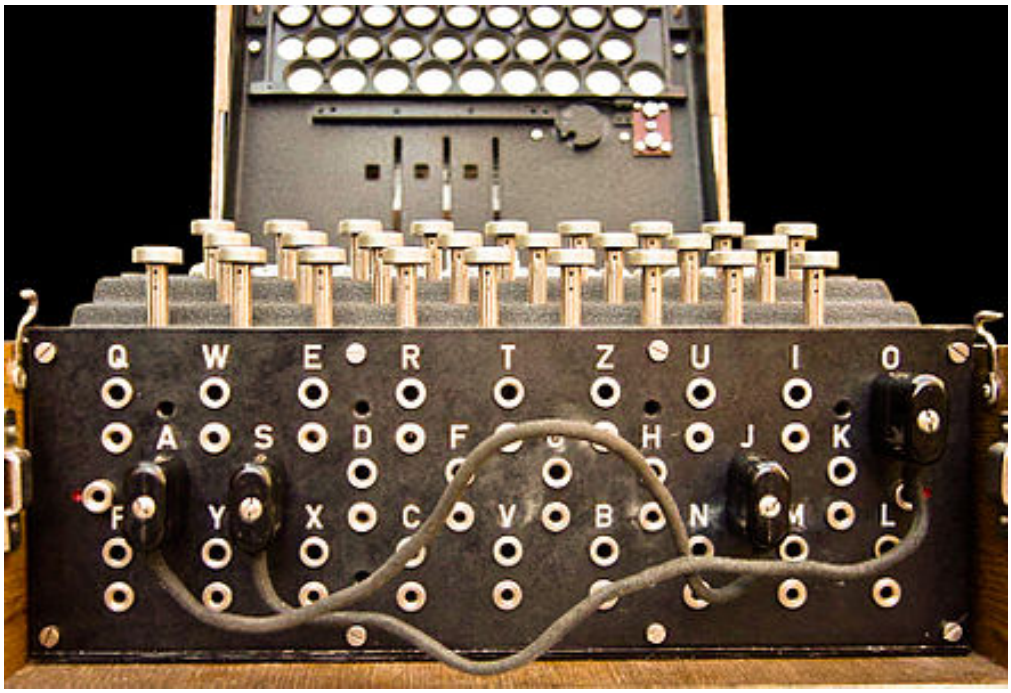
Modifiche

- Possibilità di permutare tra loro i tre rotori:

  # permutazioni: $(3!) \times 26^3 > 10^5$

- Aggiunta del plugboard tra tastiera e primo rotore

  Consente di scambiare tra loro i caratteri di 6 coppie scelte arbitrariamente in ogni trasmissione



Modifiche

- Ogni cablaggio è descritto da una sequenza di 12 caratteri (le 6 coppie da scambiare)
- Combinazioni possibili: $\binom{26}{12} \sim 10^7$
- Ogni gruppo di 12 caratteri si può presentare in 12! permutazioni diverse, ma non tutte producono effetti diversi:

  AB CD EF GH IJ KL

  CD AB EF GH IJ KL

  producono lo stesso effetto, e con queste anche tutte le 6! permutazione delle 6 coppie

Modifiche

Infine si devono considerare i possibili scambi tra gli elementi delle coppie, che producono lo stesso effetto

AB CD EF GH IJ KL
BA CD EF HG IJ KL

Dobbiamo dividere per un ulteriore fattore $2^6 = 64$

Numero delle chiavi

Il numero di chiavi dei rotori ($> 10^5$) si moltiplica per un fattore

$$\binom{26}{12}\frac{12!}{6!\cdot 64} > 10^{11}$$

per un totale di più di 10^{16} chiavi

(10 milioni di miliardi di combinazioni possibili)

Conteggio alternativo

Si scelgono 6 coppie di variabili, in

$$\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2}=\frac{26!}{2^6\,14!}=\binom{26}{12}\frac{12!}{2^6}$$

modi, e poi si divide per le 6! permutazioni tra le coppie:

$$\binom{26}{12}\frac{12!}{6!\cdot 64}$$

II guerra mondiale

- 8 rotori in dotazione, da cui sceglierne 3
- aumentarono da 6 a 10 le coppie scambiabili nel plugboard

II guerra mondiale

Elenco di chiavi giornaliere in dotazione ai reparti militari

- assetto iniziale della macchina per quel giorno

Con l' assetto iniziale si trasmetteva una nuova chiave di messaggio

- indicava l'assetto da usare in quella particolare trasmissione

Storia di ENIGMA

Standard militare tedesco durante la II guerra mondiale

Matematici polacchi e inglesi studiarono come rompere il cifrario

- centro di Bletchley Park

Storia di ENIGMA

Difficoltà

necessità di rapida decifrazione, sistema continuamente variato

- Costruzione di un simulatore di Enigma, per studiarne il comportamento sotto possibili variazioni (Alan Turing et al.)
- macchina COLOSSUS (1944)
- prototipo embrionale dei successivi calcolatori elettronici