

# Crittografia classica



# Introduzione alla crittografia

- La crittografia è il processo di trasformazione di un messaggio in modo da renderlo incomprensibile per tutti, tranne che per il legittimo destinatario
- A differenza di quanto accade per le tecniche steganografiche, non si vuole nascondere il messaggio, ma solo renderlo indecifrabile

VFHPRFKLOHJJH !

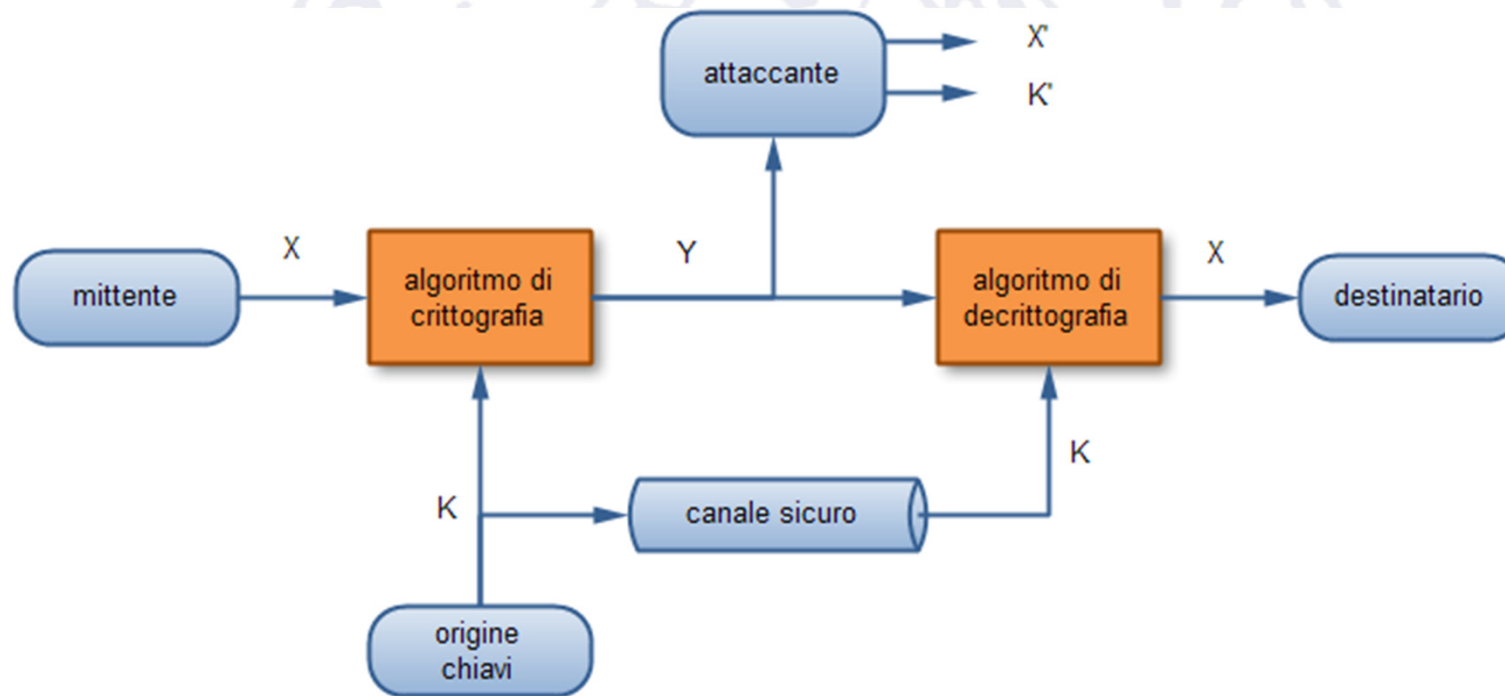
- In questa lezione studieremo alcune tecniche di crittografia classiche, usate fino alla seconda metà del XX secolo. Tutte queste tecniche sono dette a “cifatura simmetrica” (per distinguerle dalla più recente cifatura asimmetrica, che sarà oggetto delle prossime lezioni)

## Modello di cifratura simmetrico

- **Testo in chiaro:** il messaggio originale (si parla comunemente di *testo* composto da *lettere*, ma non è necessariamente un documento testuale! Ad esempio il testo in chiaro potrebbe essere un file, e le lettere che lo compongono sono i singoli byte)
- **Algoritmo di cifratura (cifrario):** il procedimento che, tramite una chiave segreta, permette di trasformare il testo in chiaro in un...
- **Testo cifrato:** il messaggio codificato, incomprensibile. Detto anche crittogramma
- **Chiave segreta:** un dato (ad es. una password) conosciuto solo da mittente e destinatario, che permette al mittente di creare il testo cifrato e al destinatario di decifrarlo
- **Algoritmo di decifratura:** esegue il procedimento inverso dell'algoritmo di crittografia

## Modello di cifratura simmetrico / 2

- Più nel dettaglio...



X: messaggio in chiaro, Y: messaggio crittato, K: chiave.

X', K': stime di X e K da parte di un attaccante

## Modello di cifratura simmetrico / 3

- Principio di **Kerckhoffs**: un attaccante non deve essere in grado di decifrare il testo cifrato o indovinare la chiave, anche se conosce l'algoritmo usato
- La sicurezza della comunicazione dipende quindi esclusivamente dalla sicurezza della chiave, che va trasmessa tramite un **canale sicuro**

# Classificazione dei sistemi crittografici

- ***In base all'algoritmo usato:*** cifratura a trasposizione vs. cifratura a sostituzione
- ***In base al numero di chiavi usate:*** cifratura simmetrica (a chiave singola) vs. cifratura asimmetrica (a chiave pubblica/privata)
- ***In base al modo in cui il testo viene elaborato:*** cifratura a blocchi / cifratura a flusso

## Crittanalisi

Studia come forzare i sistemi di crittazione

- ***Attacchi a forza bruta:*** si prova ogni chiave possibile, fino a trovare quella corretta
- ***Analisi crittografica:*** si sfruttano informazioni sull'algoritmo, le caratteristiche dei testi in chiaro, o l'analisi di coppie note di testo in chiaro/testo cifrato



## Sicurezza dei cifrari (contro attacchi passivi)

- **Sicurezza incondizionata:** è impossibile decifrare il testo senza sapere la chiave, indipendentemente dal tempo e dalla quantità di dati disponibili
- **Sicurezza computazionale:**
  - il costo di violazione supera il valore delle informazioni crittografate
  - il tempo di violazione supera la vita utile delle informazioni crittografate

*Nota: di tutti gli algoritmi che vedremo, solo OTP è incondizionatamente sicuro. Tuttavia è anche inutilizzabile ai fini pratici.*



## Cifrari a trasposizione

- Le lettere del testo in chiaro non cambiano (come invece vedremo accadere per le tecniche a sostituzione), ma ne viene alterata la posizione
- Il testo cifrato è quindi una permutazione del testo in chiaro
- La chiave è la permutazione stessa. Un attacco a forza bruta dovrebbe quindi tentare tutte le permutazioni possibili (ovvero  $n!$ , con  $n$  lunghezza del messaggio)

## Cifrari a trasposizione / 2

- Esempio dall'antichità: la scitale spartana (V sec. a.C.)



- La scitale non è altro che un caso particolare della tecnica di crittografia a trasposizione detta “rail fence” (a staccionata)

## Crittografia rail fence

- Si scrive il testo per righe in una matrice, e poi lo si trasmette per colonne (chiave: dimensione della matrice)

v	e	d	i	a	m
o	c	i	d	o	m
a	n	i	m	a	t
t	i	n	a	a	l
l	e	n	o	v	e



voatlecniediin  
nidmaoaoaav  
mmtle

- Può essere resa più complessa dall'inserimento di una permutazione delle colonne (la permutazione diventa la chiave)
- Crittanalisi: i messaggi cifrati a trasposizione sono facili da riconoscere perché preservano le frequenze delle lettere (vedi crittanalisi dei cifrari a sostituzione)

## Cifrari a sostituzione

- Le tecniche di sostituzione sostituiscono le lettere del testo in chiaro con altre lettere (o numeri, o simboli...)
- Una delle più semplici e famose è la cifratura di Cesare
- Caio Giulio Cesare usava diverse tecniche crittografiche per le sue comunicazioni, tant'è che Valerio Probo scrisse sull'argomento un intero trattato, purtroppo andato perso
- Quella che va oggi sotto il nome di “cifratura di Cesare” è descritta da Svetonio nella sua “Vita dei Cesari”

## Cifratura di Cesare

- L'alfabeto cifrante è traslato di tre lettere rispetto all'alfabeto in chiaro

Chiaro (C):	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato (E):	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

O, più formalmente,  $E[x] = C[(x+3) \bmod 26]$

- Convenzione: l'alfabeto in chiaro è scritto in minuscolo, quello cifrante in maiuscolo

veni, vidi, vici  
YHQL, YLGL, YLFL

*(ma sarebbe meglio  
rimuovere spazi e  
punteggiatura per  
non dare troppi indizi  
ai crittanalisti)*

## Violare il cifrario di Cesare

- Il cifrario di Cesare non utilizza nessuna chiave, la semplice conoscenza dell'algoritmo permette di violarne la cifratura (tecnicamente, non è un cifrario)
- E' un classico esempio di cifrario che non rispetta il principio di Kerckhoffs

## Cifratura di Cesare / 2

- Più generico: traslare l'alfabeto cifrante di un numero arbitrario  $k$  di lettere:  $E[x] = C[(x+k) \bmod 26]$
- La chiave in questo caso è lo shift  $k$
- Solo 25 chiavi possibili  $\Rightarrow$  è possibile un attacco a forza bruta! (ammesso che il testo in chiaro sia comprensibile)

Esercizio: decifrare questo messaggio:

UYIWXSIVEJEGMPI

Un aiuto: <http://critto.liceofoscarini.it/critto/caesar.htm>



## Cifratura a sostituzione monoalfabetica

- Il cifrario di Cesare è un caso particolare di cifratura monoalfabetica
- L'alfabeto cifrante non è solo traslato, ma permutato (“mischiato”) in maniera casuale

Chiario:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato:	C	N	T	K	L	B	S	I	V	M	A	W	G	H	U	Y	R	J	E	O	D	Z	X	Q	F	P

venividivici  
ZLHVZVKVZVTV

$$E[x] = C[\pi(x)]$$

con  $\pi$  permutazione

*Curiosità: una delle descrizioni più antiche della cifratura monoalfabetica si può trovare nel Kama Sutra (IV sec. d.C.), in cui la crittografia viene elencata tra le 64 arti che una donna deve studiare*


## Crittanalisi della cifratura monoalfabetica

- La chiave consiste nella permutazione usata come alfabeto cifrante
- Quante permutazioni si possono ottenere con 26 lettere?
- Risposta:  $26! = \text{circa } 4 \times 10^{26}$
- Il numero di chiavi è molto elevato, impossibile usare attacchi a forza bruta

## Crittanalisi della cifratura monoalfabetica / 2

- Tempo richiesto per un attacco a forza bruta, ipotizzando di valutare  $10^6$  permutazioni al secondo...
- $3.6 \times 10^9$  chiavi all'ora
- $8.64 \times 10^{10}$  chiavi al giorno
- $3.15 \times 10^{13}$  chiavi all'anno...
- servirebbero circa  $10^{13}$  anni per completare la ricerca (si consideri che l'età universo è di circa  $1.3 \times 10^{10}$  anni)
- Questo significa che la cifratura monoalfabetica è sicura?  
Assolutamente no...

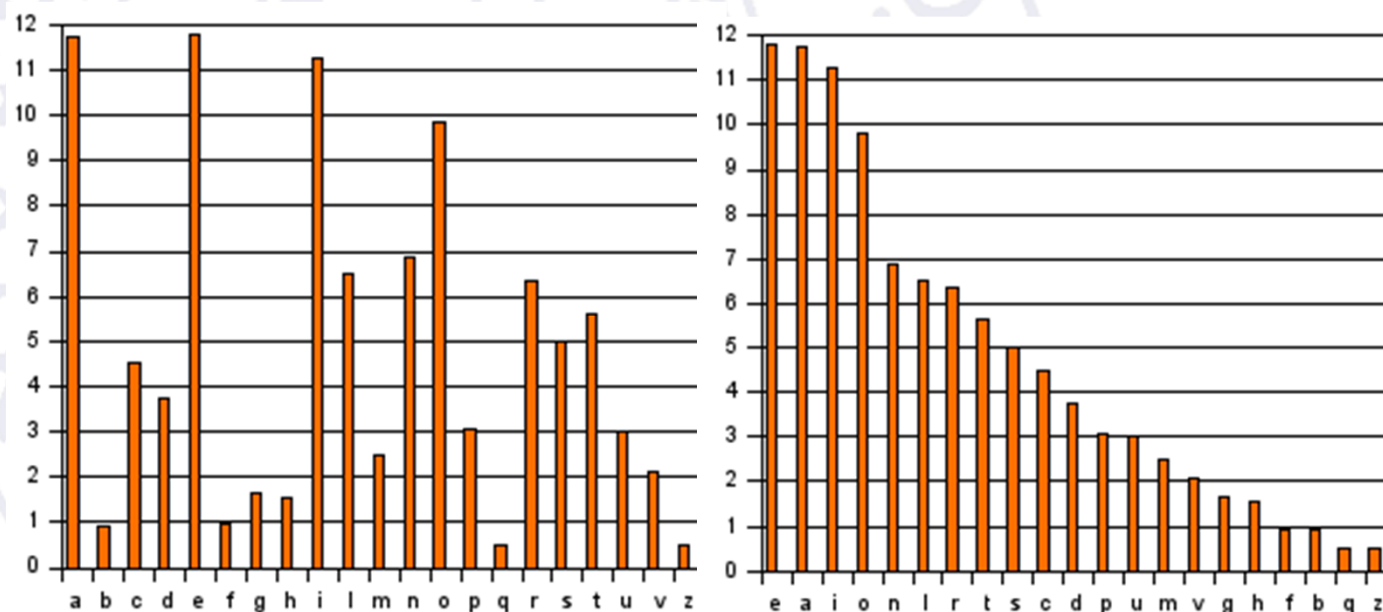
## Crittanalisi della cifratura monoalfabetica / 2

- Ancora oggi si usa la tecnica descritta nel IX secolo dallo studioso arabo Abu Yusuf Ibn Ishaq Al-Kindi, basata sull'*analisi delle frequenze*
- IDEA (per i documenti testuali): in ogni lingua ciascuna lettera dell'alfabeto ha una sua frequenza caratteristica. Questa frequenza non viene alterata nel messaggio cifrato, per cui è un ottimo indizio!
- Ad esempio, in italiano la lettera 'a' ha una frequenza di utilizzo dell'11.74%  se nel testo crittato compare un carattere con una frequenza simile, probabilmente è una 'a'

## Crittanalisi della cifratura monoalfabetica / 3

- Tabella delle frequenze per la lingua italiana:

Lettera	Frequenza
a	11.74%
b	0.92%
c	4.50%
d	3.73%
e	11.79%
f	0.95%
g	1.64%
h	1.54%
i	11.28%
l	6.51%
m	2.51%
n	6.88%
o	9.83%
p	3.05%
q	0.51%
r	6.37%
s	4.98%
t	5.62%
u	3.01%
v	2.10%
z	0.49%



(fonte: [http://it.wikipedia.org/wiki/Analisi\\_delle\\_frequenze](http://it.wikipedia.org/wiki/Analisi_delle_frequenze))

## Crittanalisi della cifratura monoalfabetica / 4

- Esercizio per casa: decrittare il seguente messaggio

<http://avires.dimi.uniud.it/claudio/teach/sicurezza2010/mono.txt>

IPBZOSMVRBZZSCVRDQVMVQABUVZCBSMBKKVCDVOLVYOSRPBQSYBLBLVLDLY  
BOOVYYBRDMVLYDYPYYVSJBLDBSCVZHDSJBQVLRSRBZZVJFVOCBOBBRBZODBL  
YOSOB RDIPBZZDUDBLIPSJDSPLYOSYYVSODJYODLCBOJDBSFOBLRBOQVOJBH  
DCPOS RDHDPMBYOSPLFOVMVLYVODVSRBJYOSBPLSMFDSQVJYDBOSRSZZSZY  
OSFSOYBBDZ FVLYBQABDUDQVLC DPLCBZBRPBODUBFSOQABOBLRSSLQVOFDPJ  
BLJDEDZBSZZVQQADVIPBJYSYOSJHVOMSKDVLBBJBCLDDZFPLYVDLQPDDZZSCV  
QBJJSBZSRRSODQVMDLQDSFBOODFDCZDSOFVDLVMBRDZSCVRVUBZBODUBSZ  
ZVLYSLSLRVJDRDLPVUVZSJQDSLZSQIPSRDJYBLRBOJDBOSZZBLYSOJDDL LPVUD  
CVZHDBDLLPVUDJBLD

- Aiutarsi con tool disponibili online, come  
<http://ganzua.sourceforge.net/>

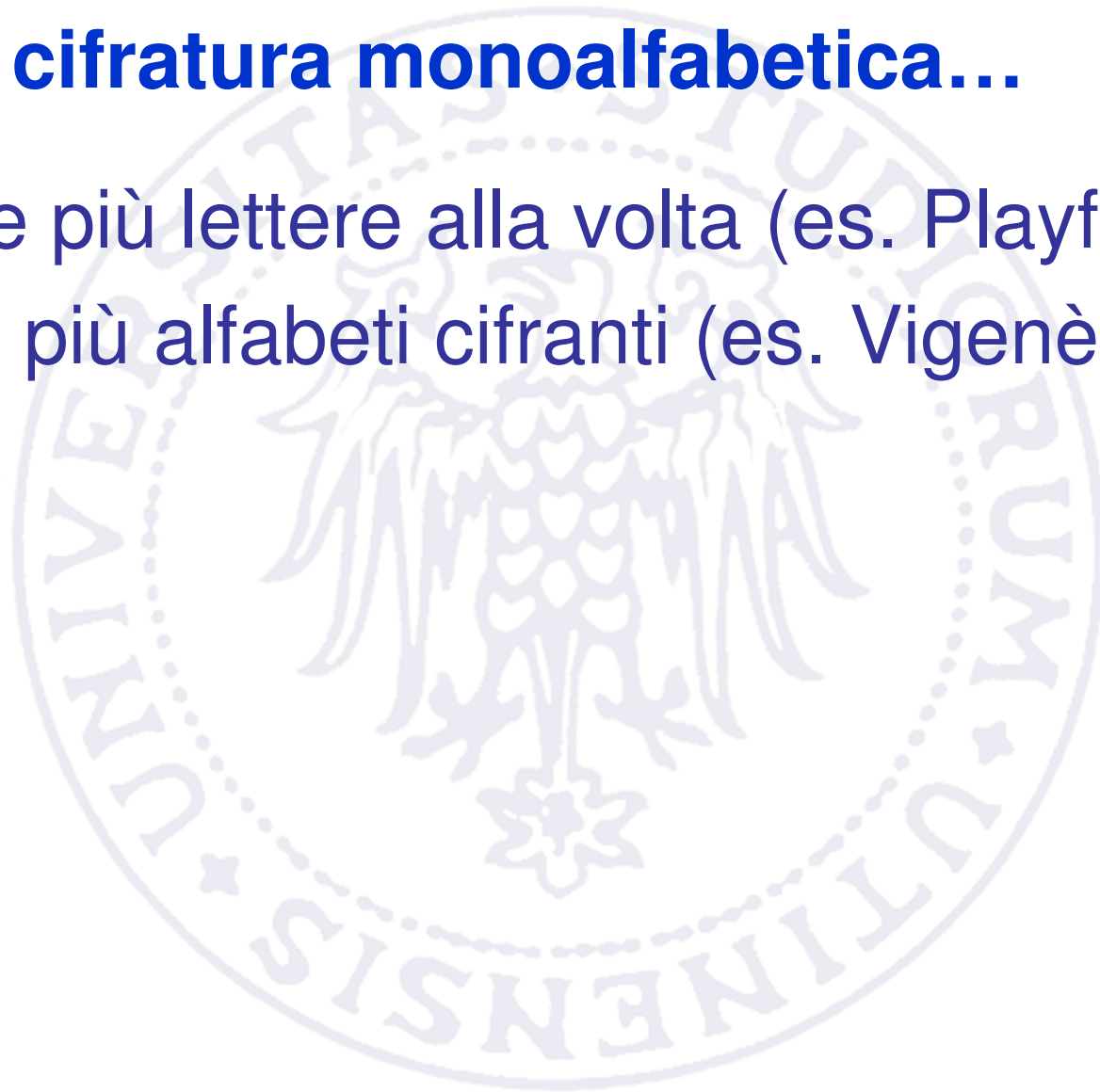
## Crittanalisi della cifratura monoalfabetica / 5

- Altre considerazioni che possono tornare utili durante la fase di analisi:
  - Se una lettera compare “doppia” (es. KK) è probabilmente una consonante
  - Se due lettere compaiono sempre assieme, potrebbe essere il digramma ‘qu’
  - Più in generale, l’analisi delle frequenze si può applicare anche a digrammi e trigrammi



## Oltre la cifratura monoalfabetica...

- Cifrare più lettere alla volta (es. Playfair)
- Usare più alfabeti cifranti (es. Vigenère)



## Cifratura Playfair

- Idea: usare i digrammi (gruppi di due lettere) come elemento base per la cifratura
- 1) creare una griglia 5x5
- 2) scrivere nelle prime caselle la parola chiave, *omettendo le lettere duplicate*
- 3) completare la tabella con le lettere mancanti (I e J occupano la stessa casella)

*(usata durante la prima guerra mondiale dall'esercito britannico)*

## Cifratura Playfair / 2

- Esempio: parola chiave: LOCOMOTIVA
- Parola chiave senza duplicati: LOCMTIVA
- Griglia finale:

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

## Cifratura Playfair / 3

- Dividere il testo in chiaro in digrammi. Se un digramma contiene due volte la stessa lettera, inserire un carattere di riempimento (ad es 'x').
- Esempio:

attaccare immediatamente



at ta cx ca re im me di at am en te

## Cifratura Playfair / 4

- Per ogni digramma, si considerino le due lettere che lo compongono
- Se appartengono alla stessa riga della tabella, ognuna va sostituita dalla lettera alla propria destra (in modo circolare)
- Se appartengono alla stessa colonna, ognuna va sostituita dalla lettera sottostante (in modo circolare)
- In tutti gli altri casi, ogni lettera va sostituita con quella appartenente alla stessa riga, ma sulla colonna dell'altra lettera del digramma

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

Esempi:

ad → BI  
 of → VP  
 ex → GU

E	F	G
N	P	Q
U	W	X

## Cifratura Playfair / 5

- Esempio:

at ta cx ca re im me di at am en te

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

DC CD AC AG NH BL LH IV DC BC NU LK

- Per decifrare, applicare il procedimento inverso

## Cifratura Playfair / 6

- Vantaggio rispetto alla cifratura monoalfabetica: ogni lettera può essere cifrata in diversi modi, a seconda dell'altra lettera nel digramma
- Debolezza: è ancora possibile un attacco statistico basato sui digrammi (anche se è più difficile: esistono infatti  $25 \times 24 = 600$  digrammi diversi possibili)



## La cifratura polialfabetica

- Idea: usare più alfabeti cifranti monoalfabetici, cambiando l'alfabeto man mano che si procede con la crittazione
- Elementi fondamentali:
  - Un insieme di alfabeti cifranti monoalfabetici
  - Una chiave che determina, ad ogni passo, quale alfabeto cifrante deve essere usato
- Esempio: il cifrario di Vigenère

## Il cifrario di Vigenère

- Ideato dal diplomatico francese Blaise de Vigenère nel XVI secolo
- Per secoli è stato considerato inviolabile, al punto da guadagnarsi il nome di “*chiffre indéchiffable*”
- In realtà fu violato, in maniera indipendente, da Babbage e Kasiski nel XIX secolo



## Il cifrario di Vigenère / 3

- Esempio:  
 plutoplutoplu (chiave)  
 attaccareoggi (testo in chiaro)

		PLAIN TEXT																									
KEY		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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	

Riga P, colonna A → P

Riga L, colonna T → E

Riga U, colonna T → N

...

Riga U, colonna I → C



PENTQRLXCVR



## Violare il cifrario di Vigenère

- Metodo di Babbage / Kasiski
- La debolezza sta nella ripetizione della chiave: si supponga di usare una chiave di lunghezza 5, come “pluto”


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	26	27	28	29	30	
p l u t				o p l u t				o p l u t				o p l u t				o p l u t				o p l u t				o p l u t				o ..		

- Osservate come ogni lettera del testo in chiaro in posizione 1,6,11,16... ( $1+5n$ ) venga crittata dalla stessa lettera della chiave ‘p’, e quindi dallo stesso cifrario monoalfabetico!
- La stessa cosa vale per le altre lettere
- Se si conosce la lunghezza della chiave  $n$ , è quindi sufficiente violare  $n$  cifrari monoalfabetici (ad es. con un attacco basato sulle frequenze)

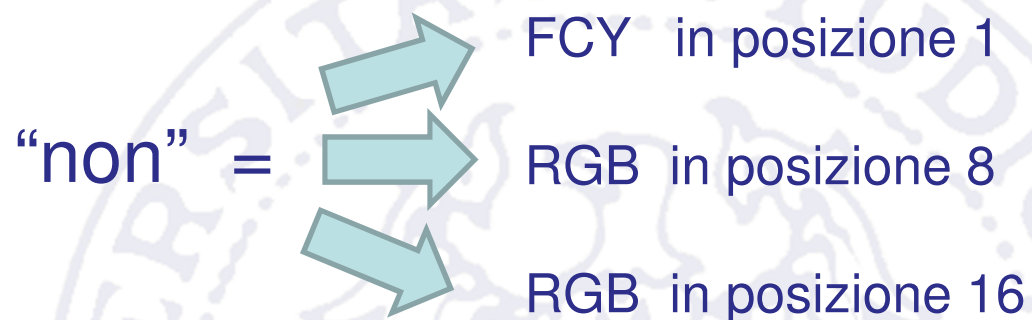
## Stimare la lunghezza della chiave

- Si ipotizza che nel testo in chiaro esistano gruppi di lettere ripetuti, a distanze pari a multipli di  $n$ . Questi gruppi verranno cifrati sempre nello stesso modo!
- Esempio

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

“non” =  FCY in posizione 1  
RGB in posizione 8  
RGB in posizione 16

## Stimare la lunghezza della chiave / 2



- Poiché esiste una ripetizione a distanza 8, si può ipotizzare che la lunghezza della chiave sia un divisore di 8 (ad es. 2, 4 oppure 8)
- Cercando altre ripetizioni si può arrivare ad una stima ragionevolmente sicura della lunghezza della chiave
- Naturalmente esistono anche ripetizioni casuali, che non sono dovute a ripetizioni nel testo in chiaro. Per questo la stima non è sicura al 100%



## Stimare la lunghezza della chiave / 3

- Esercizio: qual è probabilmente la lunghezza della chiave con cui è stato cifrato il seguente testo?

xwlotmovqp  
copbafgwhcjwhcj  
vezdturkxibvwdwdu  
tgtiqgligvirsnisgw

mvcnivcxwloxwfsnqcs  
rquwpilhqlczuwlsglabewrorqugw  
uebvzewnuobfwpcvpwcvogrirwxi  
lcpbabqtauiqu  
ipimiuqcofwlqgaucpivouwlhcvtermrag

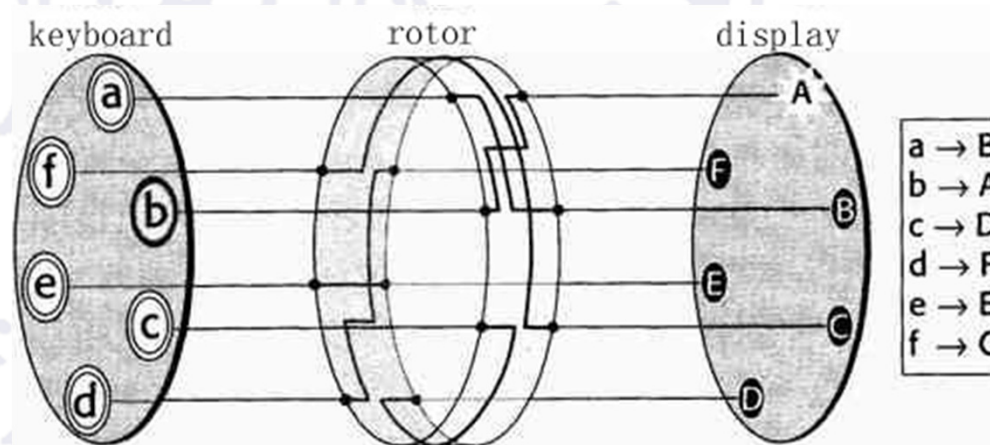
# La macchina Enigma

- La macchina Enigma era un dispositivo usato dai nazisti durante la seconda guerra mondiale per cifrare e decifrare messaggi



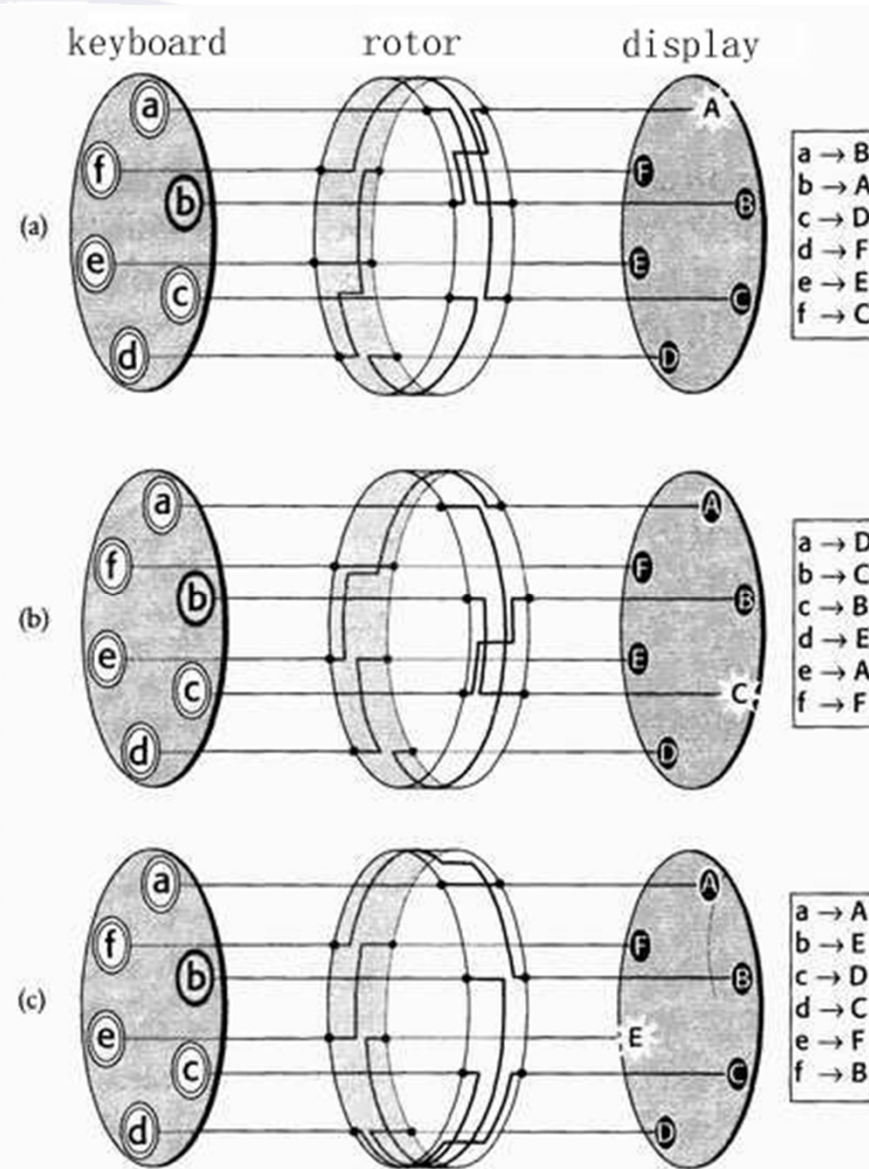
## I rotori

- L'elemento base di Enigma è il *rotore* (o *scambiatore*), una ruota dentata con 26 contatti elettrici su un lato, collegati in maniera casuale ad altri 26 contatti elettrici in uscita
- In altre parole, implementa in hardware una crittazione monoalfabetica!



## I rotori / 2

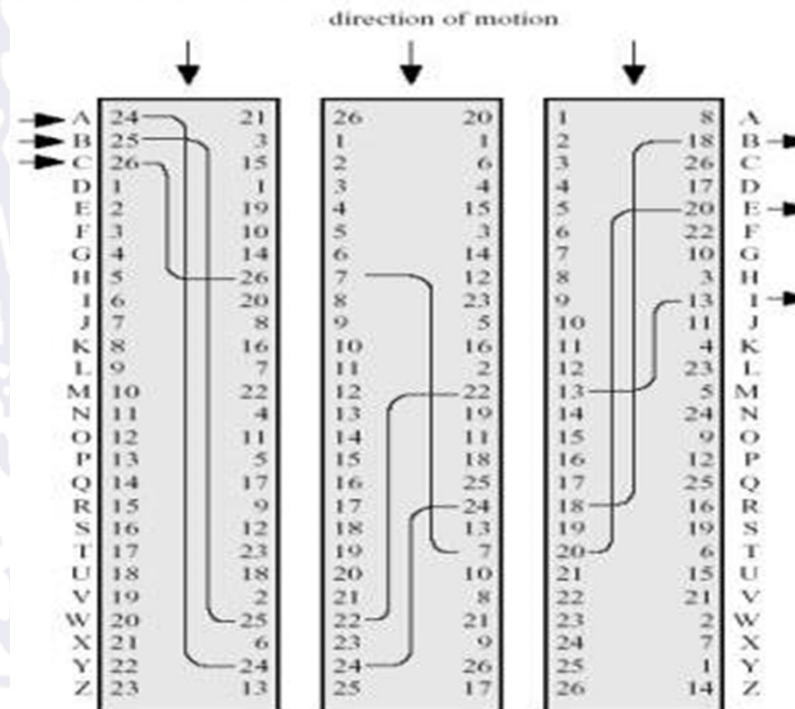
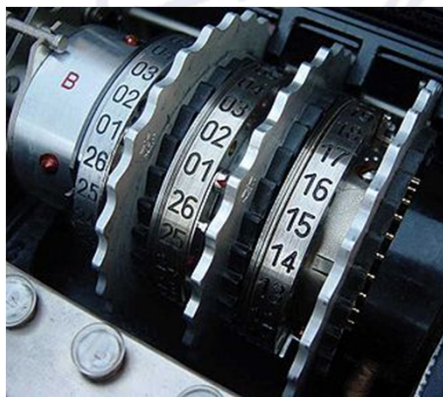
- Un rotore può ruotare (da cui il nome) attorno ad un perno: in questo modo con un singolo rotore si possono ottenere 26 cifrature monoalfabetiche diverse, a seconda della posizione del rotore.
- Se il rotore ruota ad ogni carattere cifrato, allora implementa una cifratura polialfabetica con 26 alfabeti diversi





## I rotori / 3

- La macchina Enigma era dotata di tre rotori in cascata: il primo ruotava avanzando di una posizione ad ogni carattere cifrato, il secondo avanzava di una posizione ad ogni giro completo del primo, e il terzo avanzava di una posizione ad ogni giro completo del secondo (come un contachilometri!)



## I rotori / 3

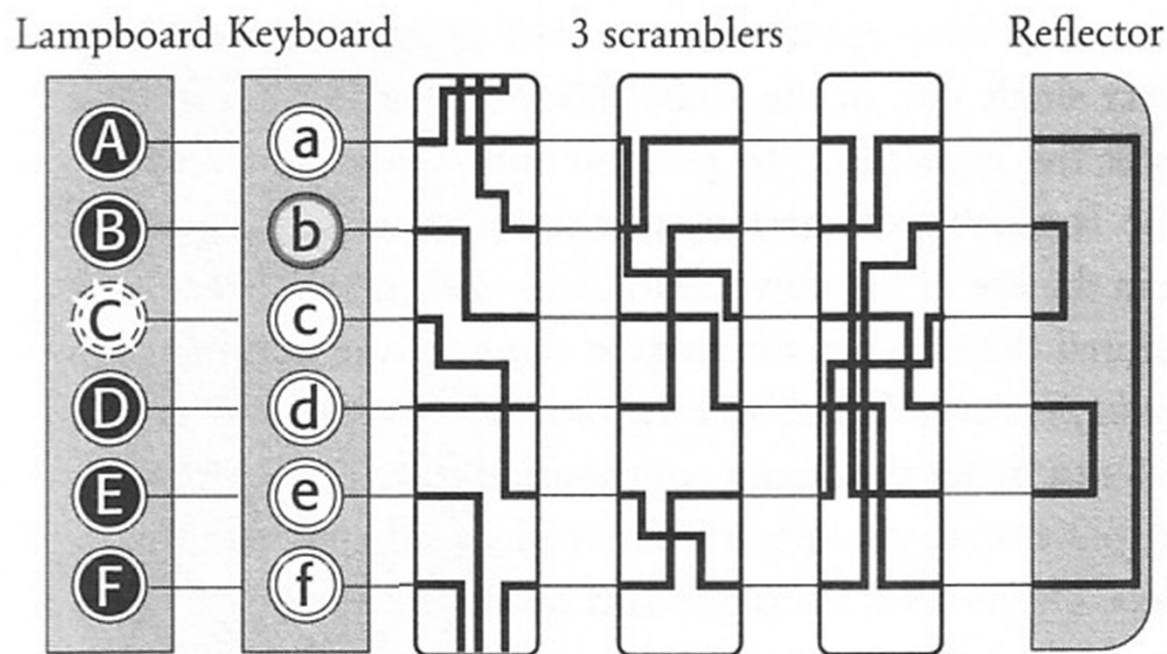
- La macchina Enigma usa 3 rotori in cascata, ognuno dei quali può assumere 26 posizioni diverse



- Realizza una cifratura polialfabetica basata sull'uso di  $26 \times 26 \times 26 = 17576$  alfabeti cifranti

## Il riflettore

- Per far sì che la macchina possa essere usata anche per decrittare i messaggi, viene introdotto il *riflettore*:



In questa configurazione, premendo il tasto A si ottiene la lettera crittata C  
Ma anche, premendo il tasto C si ottiene la corrispondente lettera decrittata A !

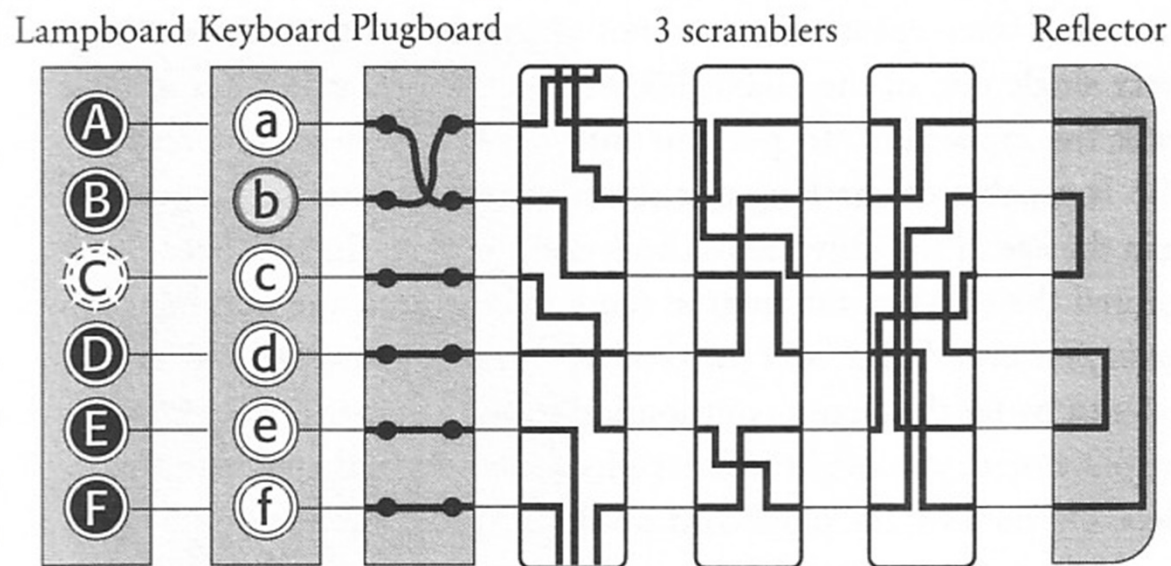


## Il riflettore / 2

- Il riflettore quindi non aumenta la robustezza della cifratura di Enigma, in quanto è un elemento fisso (non ruota come i rotori). Il numero di alfabeti cifranti rimane  $26^3$
- Tuttavia ha un'utilità pratica: mittente e destinatario possono usare lo stesso dispositivo sia per cifrare che per decifrare, ammesso che utilizzino entrambi la stessa configurazione di partenza dei rotori (che è quindi la *chiave* del messaggio)

## Il pannello a prese multiple

- Infine, la macchina Enigma era dotata di un pannello a prese multiple che, mediante l'utilizzo di 6 cavi, permetteva di scambiare tra loro 6 coppie di lettere, aggiungendo quindi un ulteriore livello di cifratura a sostituzione



## Il pannello a prese multiple / 2

- La configurazione delle connessioni sul pannello non cambia durante la cifratura del messaggio, quindi è assimilabile ad una cifratura monoalfabetica
- Tuttavia il numero di combinazioni possibili è molto alto: usando 6 cavi si possono ottenere 100.391.791.500 configurazioni differenti

Dettagli su come calcolare il numero totale di combinazioni possibili:

<http://www.codesandciphers.org.uk/enigma/steckercount.htm>

## Robustezza di Enigma

Un attacco a forza bruta richiederebbe di testare tutte le possibili configurazioni:

$$\begin{array}{rcl} 17.576 & \text{(disposizioni possibili dei rotori, } 26^3\text{)} & \\ \times & & \\ 100.391.791.500 & \text{(configurazioni possibili del pannello)} & \\ = & & \\ 1.764.486.127.404.000 & \text{configurazioni possibili totali} & \end{array}$$

*(Nota: in questa lezione si è presentato un modello semplificato di Enigma. Le macchine effettivamente utilizzate dall'esercito nazista adottavano ulteriori accorgimenti che aumentavano ulteriormente il numero di configurazioni possibili)*

## Robustezza di Enigma / 2

- La macchina Enigma si basa quindi sulla combinazione di...

**Un pannello a prese multiple**, che realizza una semplice cifratura monoalfabetica, ma aumenta drasticamente il numero di combinazioni possibili da provare in un attacco a forza bruta

**Tre rotori collegati in cascata**, che hanno un numero totale di combinazioni limitato ( $26^3$ ) ma che realizzano una cifratura polialfabetica, poiché la loro posizione cambia ad ogni carattere cifrato

## Fare breccia in Enigma

- La cifratura di Enigma venne violata grazie allo sforzo congiunto dei migliori matematici dell'epoca
- I primi a trovare delle vulnerabilità nel sistema furono dei crittanalisti polacchi
- Alan Turing, uno dei padri dell'informatica moderna, costruì delle macchine per la decifratura automatica di Enigma



## Fare breccia in Enigma / 2

- I crittanalisti si basarono sull'ipotesi che alcuni testi cifrati contenessero delle parole note in posizioni specifiche
- Ad esempio, era noto che i tedeschi trasmettessero ogni giorno dei bollettini meteorologici, i quali contenevano invariabilmente la parola “wetter” (=tempo atmosferico) in una determinata posizione



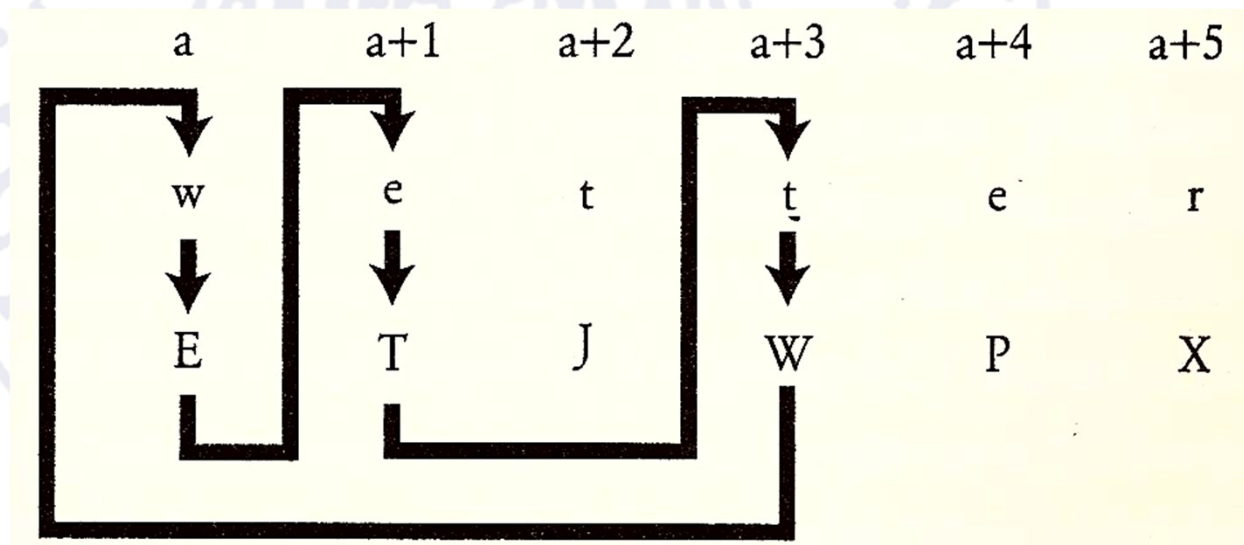
## Fare breccia in Enigma / 3

- Ci si concentrò sulla ricerca dei cosiddetti *crib*, delle concatenazioni circolari di lettere in chiaro / lettere cifrate

Assetto di Enigma

Testo in chiaro  
ipotizzato

Testo cifrato noto



Concatenazione individuata:  $W \rightarrow E \rightarrow T \rightarrow W$  (lunghezza: 3 passi)

## Fare breccia in Enigma / 4

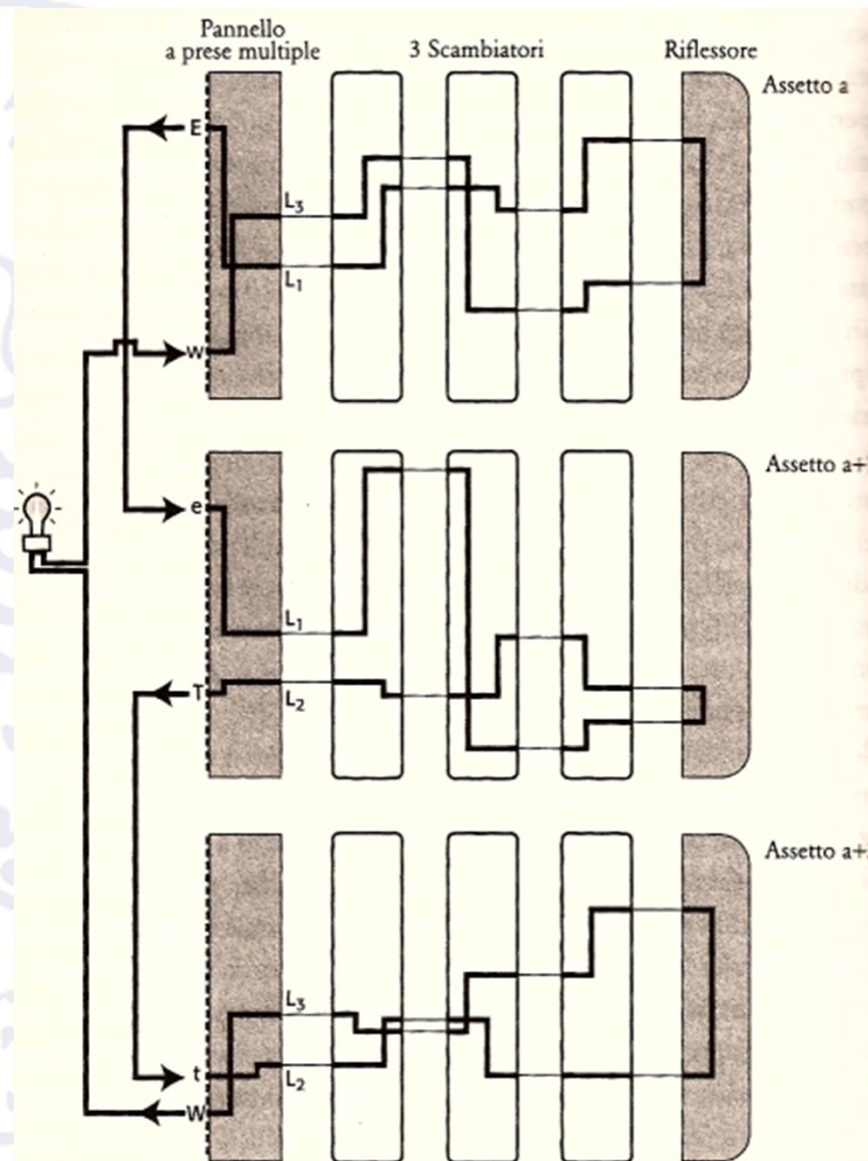
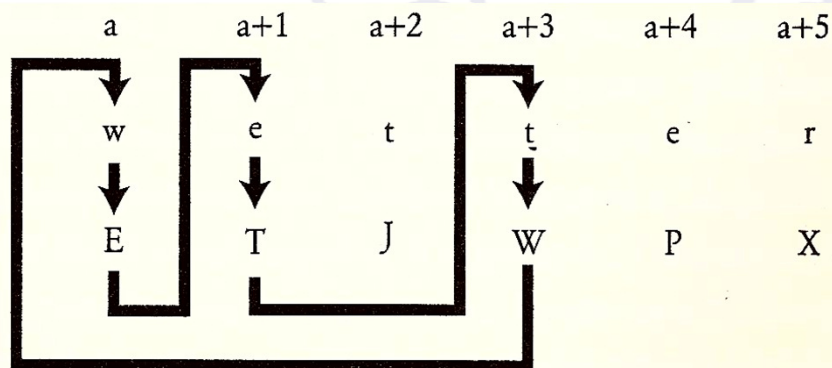
- Apparentemente i crib non hanno alcuna utilità...
- In realtà sono una “firma caratteristica”, una sorta di “impronta digitale” di una data configurazione della macchina
- Se, durante un attacco a forza bruta, si trova una configurazione con dei crib della stessa lunghezza di quelli identificati nel testo cifrato, probabilmente è la configurazione cercata!
- La cosa non sembra per ora avere alcun vantaggio, poiché il numero di configurazioni da provare rimane altissimo...

## Fare breccia in Enigma / 5

- Idea fondamentale: in realtà la lunghezza dei crib *non dipende dal pannello a prese multiple*, ma solo dalla disposizione dei rotori (vedi slide successiva)
- In un attacco a forza bruta basato sulla ricerca di crib, non occorre quindi testare tutte le 1.764.486.127.404.000 configurazioni possibili, ma solo le 17.576 configurazioni dovute alle diverse disposizioni dei rotori.

## Sicurezza nelle applicazioni multimediali: lezione 2, crittografia classica

La lunghezza di un crib è indipendente dalla configurazione del pannello a prese multiple. Nell'immagine qui a lato, tre macchine Enigma sono state collegate in serie per identificare la presenza del crib  $W \rightarrow E \rightarrow T \rightarrow W$ . Si noti come lo schema rimarrebbe lo stesso anche se il carattere L1 della prima macchina fosse collegato direttamente al carattere L1 della seconda (analogamente per L2 ed L3), "scavalcando" così il pannello a prese multiple. Cambiando la configurazione del pannello si cambierebbero le lettere coinvolte nel crib, ma la sua lunghezza rimarrebbe invariata.



## Fare breccia in Enigma / 6

- Una volta trovata la giusta configurazione dei rotori, decifrare la crittazione monoalfabetica del pannello a prese multiple è relativamente semplice
- Ad esempio, se il testo decrittato contiene la parola “tewwer”, è probabile si tratti in realtà di “wetter”, con le lettere ‘t’ e ‘w’ scambiate dal pannello

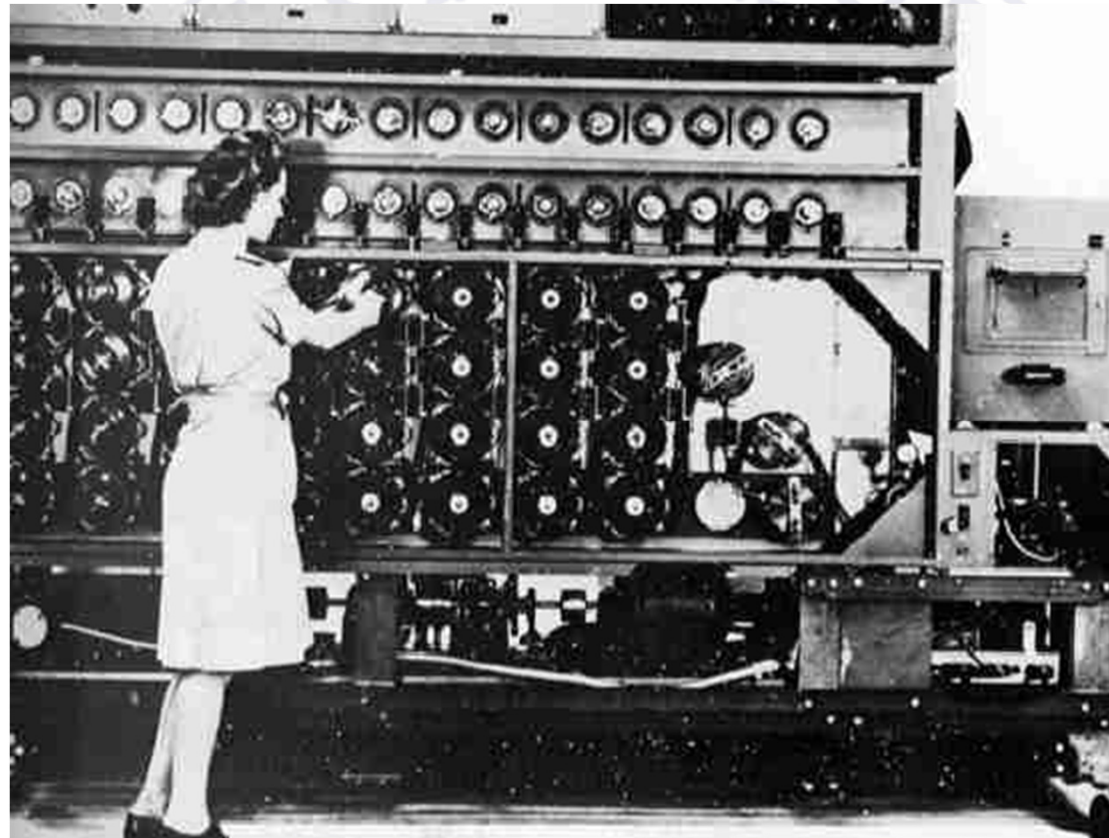
Si riuscì quindi a fare breccia in Enigma scomponendo un problema complesso in due problemi più semplici ed indipendenti:

- trovare la configurazione dei rotori mediante i crib
- decifrare la crittazione introdotta dal pannello a prese multiple.

Questo permise di costruire delle macchine (chiamate *bombe*) che automatizzavano la maggior parte del processo di decrittazione, che poteva così essere interamente svolto nell’arco di poche ore.



## Fare breccia in Enigma / 7



Una delle “bombe” di Turing