La Macchina Enigma

di Marco Cipriani

La Macchina Enigma

- Inventata nel 1918 da Arthur Scherbius (Berlino)
- Usata dalle forze militari tedesche durante la Seconda Guerra Mondiale
- Macchina cifrante a rotori
- Cifrario a sostituzione con shift di Cesare

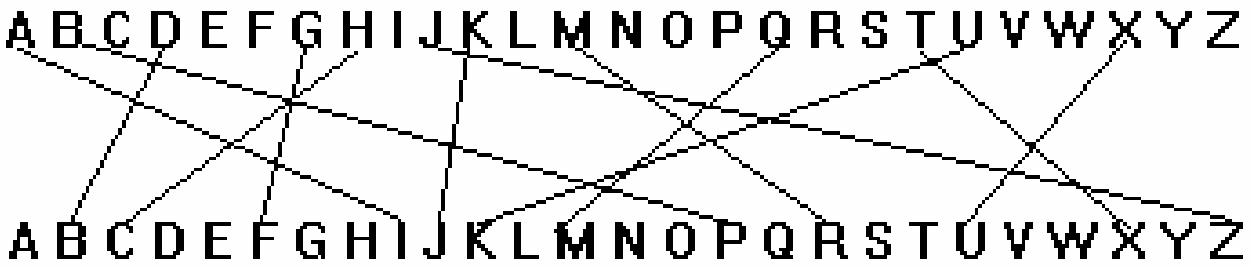
La Macchina Enigma

La macchina Enigma è composta da:

- Tastiera
- 3 Rotori
- Riflettore
- Entry disc
- Stecker (o plugboard)
- Lampadine di output

La Macchina Enigma

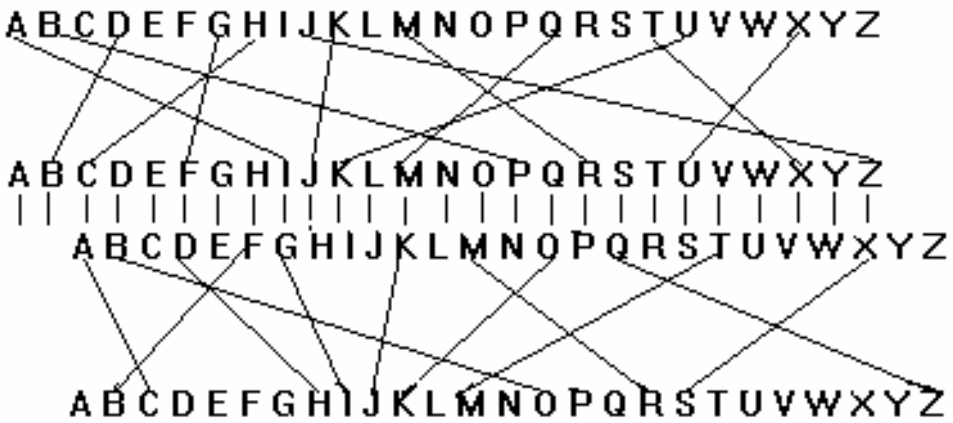
- Cifrario a sostituzione: ogni simbolo è cifrato in un altro secondo una qualche regola
- Utilizzo di connessioni elettriche per cifrare
- Un esempio di codice a sostituzione semplice:



Equivale ad una permutazione: (AI) (BP) (DB) (GF) …

La Macchina Enigma

Esempio di cifrario a sostituzione con sostituzioni a cascata:



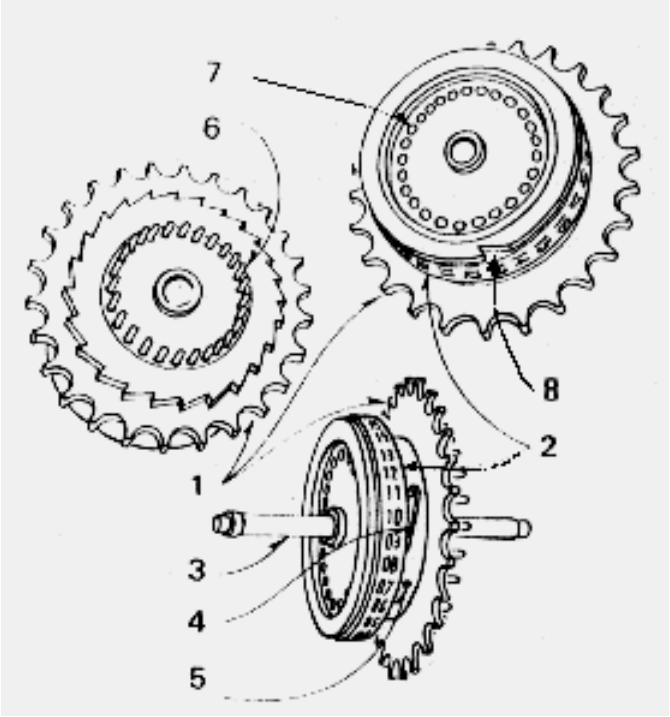
- Equivale alla composizione di permutazioni su coppie di simboli
- Idea di Scherbius: utilizzare uno shift di Cesare diverso per ogni lettera cifrata
- Permette l'utilizzo di 26 diversi alfabeti di cifratura
- Sistema implementato con "rotori"

I rotori

- Tre rotori all'interno della macchina
- Successivamente ampliata la scelta a 5
- Eseguono 7 cifrature a sostituzione
- La posizione inziale e la loro scelta rappresenta la chiave del sistema:

- Variabili da cui dipende la chiave:
  - scelta di 3 rotori su cinque $\Rightarrow$ 60 possibili posizioni
  - 26 possibili posizioni iniziali $\Rightarrow$ 17576 posizioni degli alfabeti

I rotori



1. Dentellature usate per posizionare il rotore
2. Anello dell'alfabeto
3. Asse di rotazione
4. Gancio che blocca l'anello al nucleo (5)
5. Nucleo contenente i collegamenti elettrici tra contatti (6) e dischi(7)
6. Contatti elettrici
7. Dischi di contatto tra rotori successivi
8. Gancio di CARRY per ruotare l'anello dell'alfabeto

Il reflettore

- Inventato da Willi Korn
- Implementa una serie di scambi tra coppie di lettere
- Ridireziona l'output ai rotori

Vantaggi:

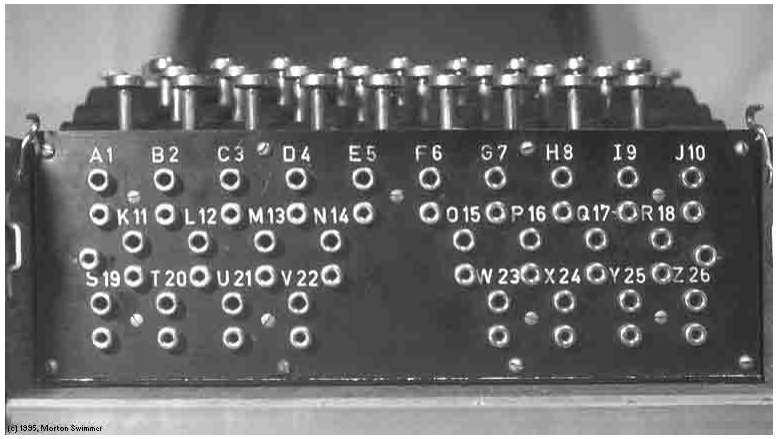
- Disponibili 17576 diversi alfabeti
- Stessa macchina per cifrare e decifrare

Svantaggi:

- Enigma diventa un sistema *reciproco*
- Introduce una debolezza che verrà sfruttata in futuro per la crittoanalisi:

Impossibilità di cifrare una lettera in se stessa

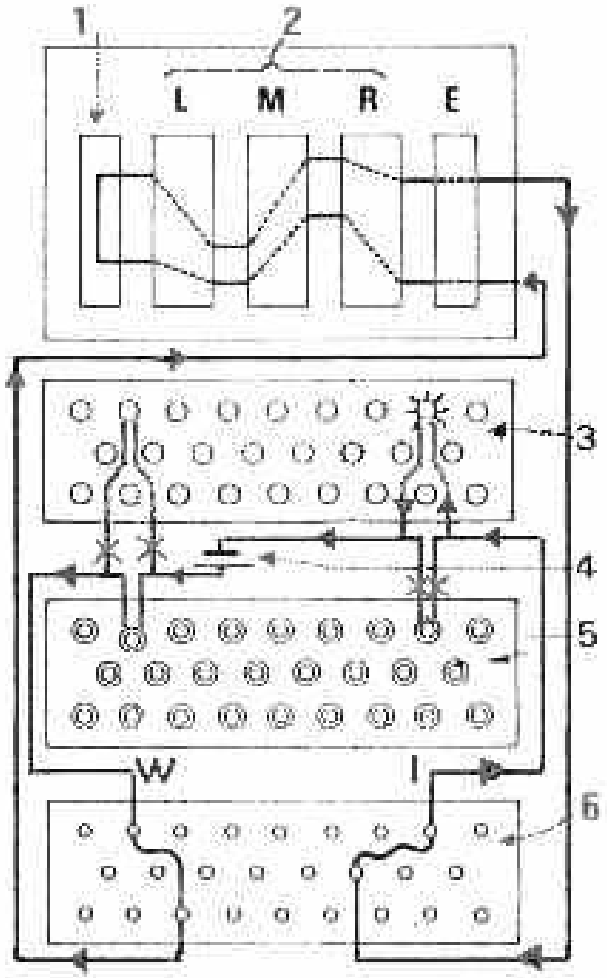
Lo Stecker (o plugboard)



- Veniva settato dall'operatore secondo una regola che fa parte della chiave del messaggio -

- Introduce un'ulteriore permutazione iniziale:
  1. Tra la tastiera e l'entry disc
  2. Tra l'entry disc e le lampadine
- Usate 10 connessioni in tempi di guerra
- Inalterata la proprietà di simmetria
- 150.738.274.937.250 possibili combinazioni

Il funzionamento



1. Reflettore
2. Rotori
3. Lampadine
4. Batteria
5. Tastiera
6. Plugboard

Disposizione dei simboli:

Q W E R T Z U I O

A S D F G H J K

P Y X C V B N M L

Esempio di cifratura

Rotori

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

Reflettore

reflector B	(AY) (BR) (CU) (DH) (EQ) (FS) (GL) (IP) (JX) (KN) (MO) (TZ) (VW)
reflector C	(AF) (BV) (CP) (DJ) (EI) (GO) (HY) (KR) (LZ) (MX) (NW) (TQ) (SU)

Setting dello Stecker: (AR) (BD) (CO) (EJ) (FN) (GT) (HK) (IV) (LM) (PW)

La chiave del Sistema

- Rotori scelti e loro ordine di assemblaggio
- Posizione iniziale
- Settaggio dello Stecker

Variazioni a scadenza giornaliera

La trasmissione dei messaggi

Geheim!

Sonder-Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppe
31.	I V III	06 20 24	UA PF RQ SO NI EY BG HL TX ZJ	jeu nyq aqm
30.	V II III	01 07 12	GF KV JM IB UW LX TD QS NA 2H	azs zds kck
29.	IV I V	11 17 26	CI OK PV ZL HX NB AW DJ FE ST	kap gwh lyx

INVIO

- Setting della macchina secondo schema giornaliero
- Scelta della posizione iniziale dei rotori (chiave)
  - Preambolo del messaggio
- Cifratura della chiave (due volte)

(continua…)

La trasmissione dei messaggi

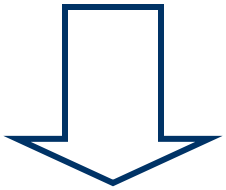
- Re-setting della posizione iniziale
- Cifratura del messaggio
- Invio del cifrato con preambolo

RICEZIONE

- Settaggio secondo regole giornailiere e preambolo
- Cifratura della chiave
- Ri-settaggio dei rotori
- Decifratura messaggio

Complessità

- Cardinalità dell'insieme delle chiavi:
  - Posizionamento di 3 rotori scelti su 5: 60 possibili scelte
  - Posizionamento degli anelli dell'alfabeto: 576 scelte influenti
  - Scelta iniziale dei 3 indicatori: 17576 possibili scelte
  - Settaggio della plugboard: 150.738.274.937.250 possibili scelte



Chiavi esistenti: 107.458.687.327.250.619.360.000

(~$2^{76.5}$ ma molte di meno considerando gli errori dei tedeschi)