# La macchina ENIGMA

## Accenni di Storia

La storia dell' Enigma inizia intorno al 1915, con l'invenzione della macchina basata sul rotore cifrario. Come di consueto nella storia, la macchina a rotore è stata inventata più o meno contemporaneamente in diverse parti del mondo. Nel 1917 ci furono invenzioni da Edward Hebern negli S.U.A., Arvid Damm in Svezia, Hugo Koch in Olanda e Arthur Scherbius in Germania.



Ufficialmente, però, la macchina Enigma è stata inventata da Arthur Scherbius nel 1918, proprio alla fine della prima guerra mondiale. Dopo diversi anni di migliorare della sua invenzione, la prima macchina vide la luce nel 1923. Appena un anno prima, aveva assicurato i diritti di brevetto NL10700 l' inventore olandese Hugo Koch.

Più tardi: Chiffriermaschinen AG, anche di Berlino. Questa macchina sarebbe diventata nota come l' Enigma A.

C'erano un sacco di problemi con l' Enigma A. Ha avuto problemi di affidabilità ed è stata sostituita un anno più tardi da Enigma B (1924).

Scherbius ha sviluppato una macchina che riproduce l'uscita su un pannello di lampade, piuttosto che su carta. Il primo modello era l' Enigma C che è stato introdotto in 1924. Era anche conosciuto come Gluhlampenmaschine (macchina lampada incandescenza).

Di norma Enigma C ha 26 tasti (A-Z) per le lampade di input e 26 (A-Z) per l'output. Il testo è criptato tramite tre rotori cifrario che sporgono dal coperchio superiore. Ogni rotore cifrario ha 26 contatti ai lati. Sono state prodotte diverse varianti dell'Enigma C, come il cosiddetto Funkschlüssel C (per la Marina tedesca) e una variante svedese, entrambi con 28 tasti

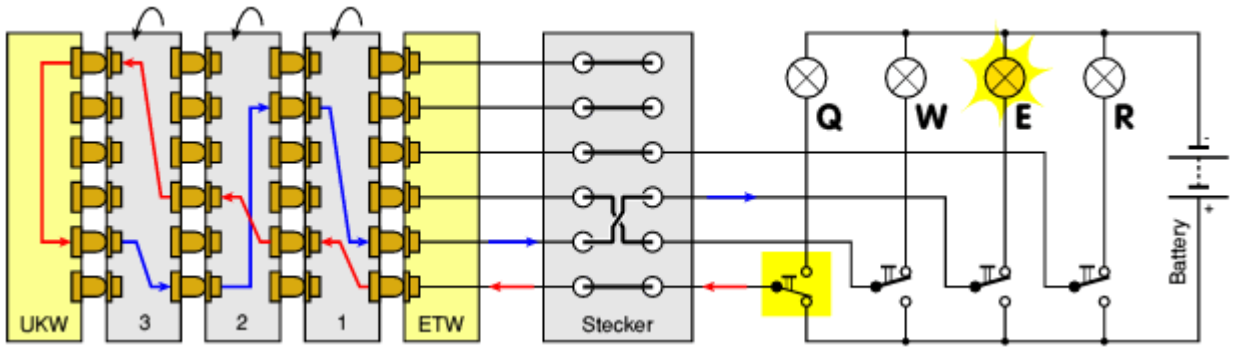
Nel 1926 è stata introdotta l'Enigma per uso commerciale.

Nel 1926, il progetto dell'Enigma a lampada incandescenza è stato drasticamente migliorato. E' stato introdotto il riflettore (UKW) che può essere impostato su 26 posizioni differenti. Esso è stato montato a sinistra delle tre rotori cifrario, motivo per cui questa macchina a volte si pensa che sia una Enigma a 4 rotori.
La macchina è stata riconosciuta Enigma D. Come la C, ha avuto diverse migliorie.

Una lampada si accende quando viene pressato un tasto. L'Enigma D divenne la base per la maggior parte delle macchine successive.
Prima della seconda guerra mondiale, furono sviluppate e costruite diverse tipi di macchine Enigma. Più tardi il tedesco Wehemacht progetta il modello che sarà la base di tutte le macchine Enigma dell'Esercito tedesco: ha tre rotori mobili un riflettore fisso (Umkehrwalze, UKW) e un pannello di connessioni (Steckerbrett).

**Principio di funzionamento**
Qui di seguito si cercherà di spiegare, in modo più semplice possibile, il funzionamento dell'Enigma. Bisogna seguire il diagramma del circuito e seguire la corrente elettrica dalla tastiera, attraverso i rotori e al pannello delle lampade. In seguito si spiegherà il movimento dei rotori e la configurazione del pannello delle connessioni (Stecker). Conseguentemente il numero delle impostazioni possibili.

Schema Elettrico:




Lo schema, semplificato, si riferisce ad una macchina Enigma con tre rotori. Bisogna considerare che in realtà ci sono molte diverse varianti di macchine. Alcune differenze rendono impossibile decrittografare un messaggio codificato su un altro modello.
Le lettere sono "criptate" da un set di rotori ciascuno di 26 lettere con 26 contatti su entrambi i lati. Ogni contatto su un lato è collegato (via filo) a un contatto sul lato opposto in qualche modo casuale. Ogni volta che viene premuto un tasto, il rotore di destra ruota di un passo, con il risultato di una diversa mappatura dei fili interni. Di conseguenza, ogni volta una nuova lettera è codificata in modo diverso. Ogni rotore avanza di una tacca e deve percorrere tutto il suo perimetro di 26 tacche per fare spostare la prima tacca del successivo rotore.
La tastiera ha 26 tasti che segna **A÷Z.** Ogni volta che viene premuto un tasto, per esempio **Q,** il rotore viene spostato in una nuova posizione e un contatto si chiude, di conseguenza una corrente fluirà. I fili da 26 tasti sono collegati ad una ruota statica (Statore –ETW). L'ordine in cui i tasti sono collegati ai 26 contatti sulla ETW varia tra i diversi modelli di Enigma.
La corrente passando per ETW entra nel rotore 1 tramite uno dei contatti al suo lato destro. Il cablaggio interno di quel rotore lo mette in contatto con il lato sinistro e da li la corrente passa ad altro rotore e così via. A sinistra dei rotori c'è il **riflettore** (Umkehrwalze – UKW). Questo invia la corrente nuovamente dentro i rotori, ma questa volta la corrente scorre da sinistra a

destra fino a raggiungere nuovamente la ETW. Da li la corrente va alla scheda delle lampade dove si accenderà la lettera corrispondente **E.** Da questo grafico si deduce che non si potrà mai ottenere la stessa lettera che si pigia sulla tastiera.
Prima di iniziare il processo di codifica, l' Enigma deve essere configurata in un modo noto a entrambi i lati del collegamento. Questo significa che l'ordine dei rotori (Walzenlage) deve essere noto pure la posizione di partenza di ogni rotore (Grundstellung). Per complicare le cose ulteriormente, ogni rotore ha un anello indice impostabile che sposta i contatti indipendenti dell'alfabeto del rotore. Questo è chiamato impostazione di anello (Ringstellung).
Per complicare maggiormente le cose, le macchine dedicate alle attività militari, erano equipaggiate con un pannello di connessioni (Steckerbrett), che permette di scambiare coppie di lettere. Qualsiasi numero di cavi da 1 a 13 può essere collegato al pannello. Significa che le coppie di lettere possono essere scambiate tra 0 e 13 lettere. Se una lettera non è mappata (cioè nessun stecher è usato per quella lettera), la lettera è conosciuta per essere **Self-Steckered.**

*Vista esplosa del rotore*

Macchia Enigma con tre rotori.
Le macchine Enigma per la marina erano a quattro rotori e avevano la possibilità di poter scegliere tra otto rotori I II III IV V VI VII VIII

Nel campo militare, l'uso del pannello delle connessioni, potenziava di parecchio le combinazioni che si potevano ottenere. Dalla tabella seguente le combinazioni che si potevano ottenere in relazione al numero di cavi di collegamento.

| Cavi (n) | Possibili combinazioni | |
|---|---|---|
| 0 | 1 | |
| 1 | 325 | |
| 2 | 44.850 | |
| 3 | 3.453.450 | |
| 4 | 164,038,875 | |
| 5 | 5,019,589,575 | |
| 6 | 100,391,791,500 | |
| 7 | 1,305,093,290,000 | |
| 8 | 10,767,019,640,000 | |
| 9 | 53,835,098,190,000 | |
| **10** | **150,738,274,900,000** | < - standard numero di cavi |
| 11 | 205,552,193,100,000 | |
| 12 | 102,776,096,500,000 | |
| 13 | 7,905,853,580,550 | |
| **Totale** | **532,985,208,200,000** | |

**La macchina elettronica che simula qualsiasi tipo di ENIGMA**

Presso il museo **Jan Corver** (cryptomuseum.com) in Olanda si trova una simulazione elettronica della Enigma in scatola di montaggio ideata da due radioamatori: Paul Reuvers e Marc Simons. Qui di seguito la macchina montata:

Come si può notare è molto simile a quella originale, con il vantaggio che può simulare qualsiasi tipo di macchina ENIGMA
Per collaudare la macchina simulata elettronica, sono andato a Fidenza dal titolare del museo Rover Joe, Campanini il quale mi ha messo a disposizione una macchina Enigma originale. I risultati sono stati stupefacenti a condizione che si rispettassero tutte le varianti che dovevano essere uguali per le due macchine; cioè, dovevano essere rispettate tutte queste varianti. Dovevano esser uguali:

i 3 rotori installati con lo stesso ordine (per es. I IV III Walznlage)
la posizione iniziale dei rotori (Grundstellung);
la regolazione dell'anello (Ringstellung)
la posizione del riflettore (Umkehrwalze)

Per le macchine a tre rotori si usano cinque rotori e precisamente individuati con: I II III IV V.
In questo modo si è potuto mandare i messaggi cifrati e le dovute decifrature. Qui di seguito i modelli copiati da quelli originali Tedeschi per l'avvenuto scambio dei messaggi

**NOTTE EUROPEA DEI RICERCATORI - 26 set 2014**

**Sede** ARI Fidenza NOTTE EUROPEA DEI RICERCATORI

Rotori I II IV | Posiz iniz. ZIN | TX A II1ENG ORE T2005

RX da II1ENG | ore T2000

Operatore I4CQO

| Mess. Codificato | | | | | | | | | | Mess. Decodificato | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| H | D | V | Z | K | U | K | X | N | I | L | E | | M | I | E | | I | N | V | E | N |
| Q | G | W | O | F | X | I | V | I | J | Z | I | O | N | I | | S | O | N | O | | |
| R | V | P | O | B | T | Y | X | L | W | P | E | R | | S | A | L | V | A | R | E | |
| E | G | H | L | M | P | O | T | S | V | L | A | | U | M | A | N | I | T | A | | |
| P | E | P | Y | H | B | K | Q | M | T | N | O | N | | P | E | R | | D | I | S | T |
| C | L | Y | K | W | M | D | V | P | W | R | U | G | G | E | R | L | A | | N | U | M |
| M | D | T | O | M | | | | | | | Q | S | O | | I | N | T | | | | |
| fine enigma | | | | | | | | | | | | | | | | | | | | | |

E' sempre utile sapere quale era la esattezza delle comunicazioni. Durante il mio servizio in MM, spesso ho fatto esercitazioni NATO e fra le varie nazioni partecipanti ci si scambiava messaggi tipo telegrammi codificati. Erano messaggi composti di gruppi di cinque lettere che potevano raggiungere il numero di 200 e dovendo dare ricevuto relativo a 200 gruppi, non era facile. Si ricorreva al collegamento duplex, avevamo una frequenza per trasmettere e una per ricevere. Quando si riceveva, alla prima perdita di una lettera, si trasmetteva una serie di punti, chi trasmetteva interrompeva la trasmissione passando in ascolto. Chi riceveva trasmetteva la lettera di inizio dell'ultimo gruppo ricevuto bene. Da li in poi si riprendeva a trasmettere. Cosi si aveva le certezza di aver ricevuto tutto dando il ricevuto immediatamente. L'unica cosa che

si controllava era il numero dei gruppi che doveva corrispondere al numero contenuto nel preambolo del messaggio. Ma anche qui c'era una agevolazione: per la ricezione si usavano modelli che contenevano degli spazi numerati dove andavano scritti i gruppi di lettere, quindi il controllo era immediato.
Per i messaggi codificati con la macchina Enigma, si dovevano rispettare delle regole. Per esempio: dato che i messaggi codificati diventavano gruppi di 5 lettere si doveva mandare un segnale per far capire quando finiva la parola decodificata. Quel segnale da codificare era la X.
Quando si dovevano trasmettere dei numeri si dovevano adoperare i numeri romani. Il punto interrogativo era trasmesso con UD, la virgola con Y ecc. ecc. Qui sotto la postazione di Fidenza.

Da I4CQO Giacomo IN 112