La Macchina Cifrante Enigma

Introduzione storica

Il 23 Febbraio del 1918, l'ingegnere tedesco Arthur Scherbius brevettò una macchina cifrante che utilizzava rotori. Nacque così la versione commerciale dell'Enigma: una macchina elettromeccanica per cifrare e decifrare messaggi.
Diverse copie dell'Enigma commerciale furono acquistate dalla Marina tedesca e dall' esercito che, con il tempo, introdussero diverse modifiche alla macchina originaria, incrementandone la sicurezza. Videro la luce così la versione M3 del 1934 che possedeva 3 rotori e la M4 che ne possedeva 4 e veniva utilizzata dai sottomarini.
Anche altre nazioni utilizzarono macchine Enigma. La Marina italiana adottò la versione commerciale come anche gli Spagnoli che se ne servirono durante la guerra civile del 1936.
Gli Svizzeri impiegarono un modello da loro modificato per scopi militari e diplomatici, mentre i Giapponesi crearono il modello T con nome in codice Tirpiz.
E' stato stimato che sono state costruite 100.000 macchine Enigma, 40.000 delle quali durante la Seconda Guerra Mondiale.
In pratica le sorti della Seconda Guerra Mondiale furono decise, crittograficamente parlando, dalla relativa impenetrabilità delle macchine a rotore.
Secondo alcuni storici, alcune vittorie sono state possibile grazie alla superiorità crittografica nel decifrare messaggi segreti cifrati da macchine a rotori.
Alcuni esempi possono essere:

- **Sbarco in Normandia**: Eisenhower e Montgomery erano in grado di leggere tutti i messaggi degli alti comandi tedeschi; ebbero così conferma che Hitler aveva creduto alla falsa notizia di un imminente sbarco alleato nei pressi di Calais, e aveva concentrato le sue migliori truppe in quella zona. Poterono quindi ordinare lo sbarco in Normandia sicuri che avrebbe incontrato ben poca resistenza.
- **Pearl Harbour**: gli Americani sapevano in anticipo dell'attacco di Pearl Harbour e decisero di non impedirlo, avevano infatti bisogno di un motivo forte per convincere la riluttante opinione pubblica americana della necessità di entrare in guerra e quell'attacco a tradimento dei Giapponesi fu ideale per questo scopo. Una teoria più prudente sostiene che gli Americani sapevano che il Giappone stava per attaccare, ma non sapevano dove. Certo è che al momento dell'attacco nella baia di Pearl Harbour non c'era nemmeno una portaerei e in definitiva furono affondate solo alcune navi vecchie e di importanza non fondamentale per la guerra.

Funzionamento

Il modello base dell' Enigma ha l'aspetto di una macchina da scrivere, con la differenza che possiede **due tastiere**. Una tastiera serve per scrivere lettera per lettera il messaggio da cifrare, l'altra è composta da una serie di lettere che si illuminano. Ogni volta che si immette nella prima tastiera una lettera da cifrare, per esempio "**A**", verrà illuminata la lettera corrispondente cifrata, ad esempio "**C**", nella seconda tastiera.

Immagine A.

Nell' Immagine A, (1) rappresenta la tastiera in cui si immette il testo, (2) rappresenta la tastiera che si illumina.

A determinare la chiave di cifratura tramite la quale avviene la traformazione di "**A**" in "**C**" è la disposizione dei **rotori**.

I rotori fisicamente sono dei dischi cablati che possiedono 26 contatti (corrispondenti alle lettere dell'alfabeto) su ogni faccia. Le 26 lettere ordinate dell'alfabeto di una faccia sono collegate elettricamente con 26 lettere non ordinate dell'altra faccia, questi collegamenti variano da rotore a rotore.
Ad esempio un rotore si può rappresentare come una coppia di alfabeti:

Faccia 1: `EKMFLGDQVZNTOWYHXUSPAIBRCJ`
Faccia 2: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

La lettera "**A**" sarà collegata con "**E**" e così via.
Nel corso della trattazione si utilizzeranno esempi con rotori collegati così:

Rotore 1
`BDFHJLCPRTXVZNYEIWGAKMUSQO`
`ABCDEFGHIJKLMNOPQRSTUVWXYZ`

Rotore 2
`AJDKSIRUXBLHWTMCQGZNPYFVOE`
`ABCDEFGHIJKLMNOPQRSTUVWXYZ`

Rotore 3
`EKMFLGDQVZNTOWYHXUSPAIBRCJ`
`ABCDEFGHIJKLMNOPQRSTUVWXYZ`

I rotori sono imperniati su un medesimo asse ed è possibile cambiare l'ordine di disposizione dei tre dischi.

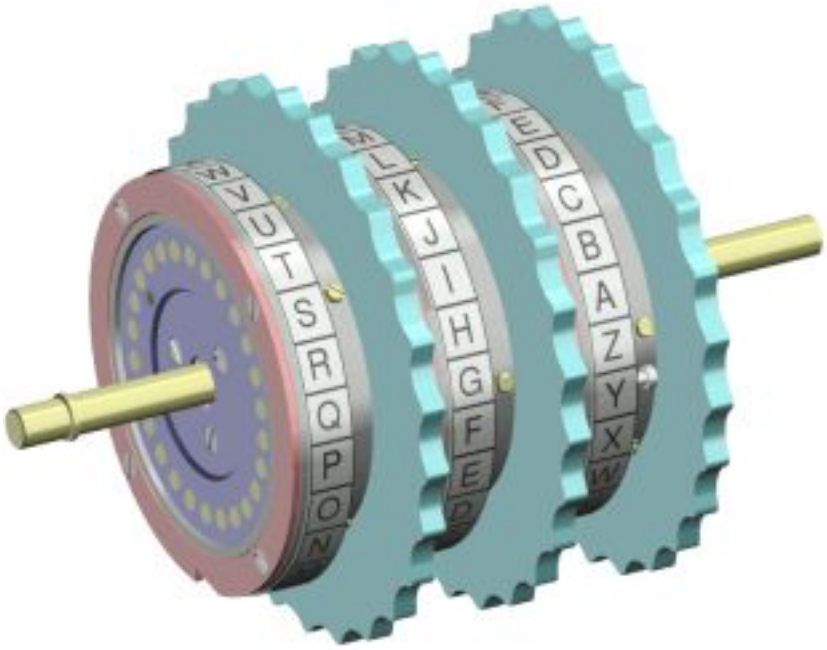


Immagine B.

Come si può vedere nell'immagine B, sono state stampate sui dischi le lettere dell'alfabeto ordinato, queste serviranno all'operatore che vuole utilizzare la macchina per determinare la chiave di cifratura ruotando ogni singolo disco. Nell'immagine A punto (3), e nell'immagine C si osserva come appaiono i rotori esternamente, in quest'ultima immagine la chiave è "**BDKP**".

Immagine C.

I rotori, man mano che l'operatore scrive le lettere del messaggio da cifrare, si muovono autonomamente con un meccanismo simile a quello di un odometro (meccanismo interno a contachilometri e tassametri, che permette di misurare la distanza percorsa da un veicolo). Alla pressione di un tasto, il rotore più a sinistra (Rotore 1) ruota verso l'alto, di una posizione.
Facciamo un esempio, tenendo conto che il movimento dei rotori sarà fatto lateralmente e non dal basso verso l'alto, per facilitarne la comprensione.

La chiave è "**AAA**" infatti come si può vedere nei vari rotori, l'alfabeto ordinato inizia sempre con la "**A**".

Rotore 1
BDFHJLCPRTXVZNYEIWGAKMUSQO
ABCDEFGHIJKLMNOPQRSTU**V**WXYZ

Rotore 2
AJDKSIRUXBLHWTMCQGZNPYFVOE
ABCD**E**FGHIJKLMNOPQRSTUVWXYZ

Rotore 3
EKMFLGDQVZNTOWYHXUSPAIBRCJ
ABCDEFGHIJKLMNOP**Q**RSTUVWXYZ

Quando viene premuto un tasto, il Rotore 1 si sposterà di una posizione verso sinistra, la lettera "A" e il suo rispettivo collegamento lasceranno il posto alle lettere successive e si posizioneranno al fondo dell'alfabeto così:

Rotore 1
DFHJLCPRTXVZNYEIWGAKMUSQOB
BCDEFGHIJKLMNOPQRSTU**V**WXYZ**A**

Mentre gli altri rotori 2 e 3 rimarranno invariati.

Quando il Rotore 1 avrà raggiunto una determinata posizione (che varia da rotore a rotore) determinerà lo spostamento del rotore adiacente (Rotore 2) di una posizione.
Le posizioni che determinano lo spostamento del rotore adiacente sono rispettivamente le lettere:
- "**V**" per il Rotore 1
- "**E**" per il Rotore 2
- "**Q**" per il Rotore 3

Facendo sempre riferimento alle lettere dell'alfabeto ordinato.

Ad esempio se la chaive è "**AAV**" i rotori saranno disposti così:

Rotore 1
MUSQOBDFHJLCPRTXVZNYEIWGAK
VWXYZABCDEFGHIJKLMNOPQRSTU

Rotore 2
AJDKSIRUXBLHWTMCQGZNPYFVOE
ABCD**E**FGHIJKLMNOPQRSTUVWXYZ

Rotore 3
EKMFLGDQVZNTOWYHXUSPAIBRCJ
ABCDEFGHIJKLMNOP**Q**RSTUVWXYZ

Quando viene premuto un tasto, il Rotore 1 si muoverà di una posizione, ma poichè prima della rotazione esso iniziava con la posizione "**V**", allora ruoterà anche il Rotore 2 di una posizione:

Rotore 1
USQOBDFHJLCPRTXVZNYEIWGAKM
WXYZABCDEFGHIJKLMNOPQRSTUV

Rotore 2
JDKSIRUXBLHWTMCQGZNPYFVOEA
BCDEFGHIJKLMNOPQRSTUVWXYZA

Rotore 3
EKMFLGDQVZNTOWYHXUSPAIBRCJ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Ovviamente anche quando il Rotore 2 avrà raggiunto la posizione "**E**", farà muovere il Rotore 3.

Un esempio che merita di essere visto è il caso in cui la chiave è "**EDV**":

Rotore 1
MUSQOBDFHJLCPRTXVZNYEIWGAK
VWXYZABCDEFGHIJKLMNOPQRSTU

Rotore 2
KSIRUXBLHWTMCQGZNPYFVOEAJD
DEFGHIJKLMNOPQRSTUVWXYZABC

Rotore 3
LGDQVZNTOWYHXUSPAIBRCJEKMF
EFGHIJKLMNOPQRSTUVWXYZABCD

Quando viene premuto un tasto, si avrà uno spostamento del Rotore 1 e 2:

Rotore 1
USQOBDFHJLCPRTXVZNYEIWGAKM
WXYZABCDEFGHIJKLMNOPQRSTUV

Rotore 2
SIRUXBLHWTMCQGZNPYFVOEAJDK
EFGHIJKLMNOPQRSTUVWXYZABCD

Rotore 3
LGDQVZNTOWYHXUSPAIBRCJEKMF
EFGHIJKLMNOPQRSTUVWXYZABCD

Successivamente quando viene premuto un secondo tasto, si avrà uno spostamento di tutte e tre i rotori.

Rotore 1
SQOBDFHJLCPRTXVZNYEIWGAKMU
XYZABCDEFGHIJKLMNOPQRSTUVW

Rotore 2
IRUXBLHWTMCQGZNPYFVOEAJDKS
FGHIJKLMNOPQRSTUVWXYZABCDE

Rotore 3
GDQVZNTOWYHXUSPAIBRCJEKMFL
FGHIJKLMNOPQRSTUVWXYZABCDE

L'ultimo componente dell'Enigma è il **riflettore**, esso può essere rappresentato come un alfabeto speciale in cui sono presenti lettere che si ripetono:

Riflettore
ABCDEFGDIJKGMKMIEBFTCVVJAT

La sua funzione sarà più chiara in seguito.

Esempio concreto

Supponiamo di avere i nostri tre rotori di prima, imperniati sull'asse nel solito ordine **1,2,3** (***wheel order***) e come chiave "**ABC**" (***indicators***) .
Il testo da cifrare (***plaintext***) è : "**TEST**".

I rotori quindi sono disposti così:

Rotore 1
FHJLCPRTXVZNYEIWGAKMUSQOBD
CDEFGHIJKLMNOPQRSTUVWXYZAB

Rotore 2
JDKSIRUXBLHWTMCQGZNPYFVOEA
BCDEFGHIJKLMNOPQRSTUVWXYZA

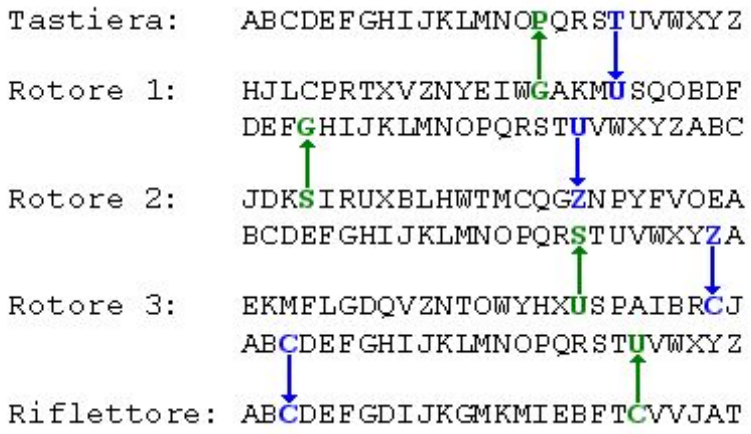
Rotore 3
EKMFLGDQVZNTOWYHXUSPAIBRCJ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Prima di tutto bisogna premettere che i movimenti dei rotori avvengono prima che inizi la codifica, subito dopo la pressione dei tasti.
Quindi, una volta premuta la lettera "**T**", il Rotore 1 si muoverà di una posizione, così:

Rotore 1
HJLCPRTXVZNYEIWGAKMUSQOBDF
DEFGHIJKLMNOPQRSTUVWXYZABC

Gli altri rotori rimarranno invariati poichè non si è giunti in nessuna posizione che faccia scattare i rotori adiacenti.

Si può ora rappresentare l'Enigma in questo modo:



Ora seguiamo le lettere colorate di blu dall'alto verso il basso: sulla tastiera schiacciamo la "**T**", sotto la "**T**" troviamo nel Rotore 1 una "**U**". Ora cerchiamo la "**U**" nel secondo alfabeto del Rotore 1. Ora sotto quest'ultima "**U**" troviamo nel Rotore 2 una "**Z**", cerchiamo questa lettera nel secondo alfabeto del Rotore 2. Sotto di essa troviamo una "**C**" del Rotore 3, cerchiamo questa lettera nel secondo alfabeto del Rotore 3.
Giunti a questo punto entra in gioco il riflettore: esso semplicemente inverte il flusso di sostituzioni facendolo andare dal basso verso l'alto.
Sotto l'ultima "**C**" del Rotore 3, troviamo un'altra "**C**" del riflettore. Ora cerchiamo un'altra "**C**" nell'alfabeto del riflettore. Bisogna quindi procedere da qui in poi nell'altro senso. Seguiamo le lettere colorate di verde. Sopra la "**C**" del riflettore troviamo una "**U**" nel Rotore 3, cerchiamo questa lettera nel primo alfabeto del Rotore 3. Sopra di essa troviamo una "**S**" del Rotore 2, cerchiamo questa lettera nel primo alfabeto del Rotore 2. Sopra di essa troviamo una "**G**", cerchiamo questa lettera nel primo alfabeto del Rotore 1. Sopra di essa troviamo una "**P**".
Quest'ultima "**P**" è la lettera che nell'Enigma reale si accende nella seconda tastiera poichè corrisponde alla nostra lettera "**T**" iniziale: è la sua versione cifrata.

Ora bisogna procedere in questo modo per cifrare le altre tre lettere del nostro messaggio("**TEST**"). Poichè si è capito il procedimento non analizzeremo come cifrare le altre lettere, se si vuole vedere come si sarebbe dovuto continuare basta utilizzare il programma allegato, settando questi parametri:

Wheel Order: 1 2 3
Indicators: A B C
Plaintext: TEST

Schiacciare il tasto "Save", dare un nome al file di output ed infine premere il tasto "Encrypt/Decrypt". Il file creato conterrà i passaggi di cifratura effettuati su ogni singola lettera del messaggio originale. (Se non si specifica nessun file di output il programma si limiterà a mostrare il messaggio cifrato nella apposita sezione nominata **ciphertext**).

Conclusioni

Come si è potuto capire l'Enigma essenzialmente cifra messaggi basandosi su un sistema di permutazioni dell'alfabeto.
Non si è ancora parlato di come funzioni la fase di decriptazione, cioè di come sia possibile risalire al messaggio originale partendo da quello cifrato, conoscendo la chiave. Basti sapere che il procedimento è lo stesso attuato per cifrare, poichè l'Enigma è una macchina simmetrica. Quindi, se come messaggio da cifrare si usa uno già cifrato, si arriva al messaggio originale.

La macchina Enigma rispetta il principio di Kerckhoff ovvero “La robustezza di un crittosistema non deve dipendere dalla segretezza dell'algoritmo”.
Il punto debole di questo crittosistema è però il fatto che nessuna lettera può comparire nel testo cifrato come se stessa.

Allegato a questo testo c'è una simulazione, scritta appositamente da me, per il sistema operativo Windows (tutte le versioni). Il codice relativo alla crittazione/decriptazione è stato scritto in C rispettando lo standard ISO 9899:1999 , in questo modo il sorgente è portabile al 100% su tutti i sistemi. L'interfaccia garfica è stata scritta in C utilizzando le sole api di Windows, senza l'ausilio di framework come l'MFC, rendendo così il programma finale veloce e di soli 19.456 bytes (di cui ben 9.270 costituiscono il logo dell'Enigma [206 x 88 x 4 BPP] in formato Bitmap).

Luca Boasso