Il funzionamento della macchina Enigma

- Dettagli tecnici –

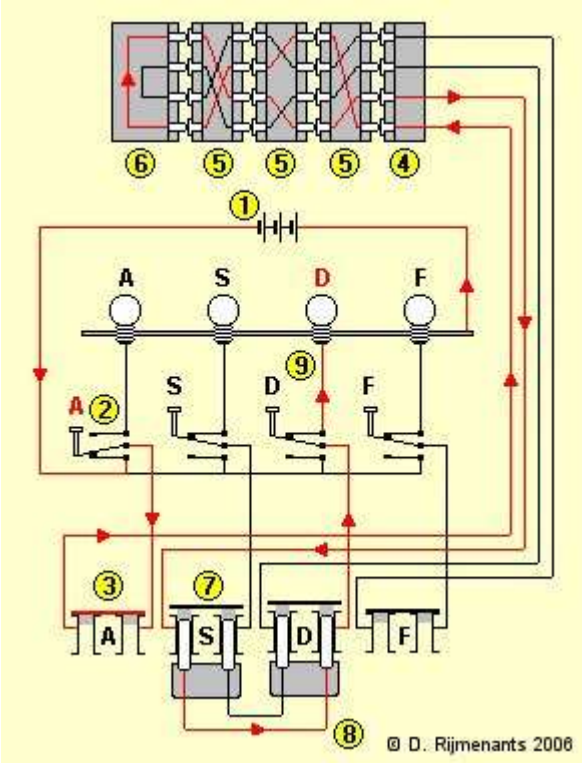
Enigma della Wehrmacht

Enigma M4

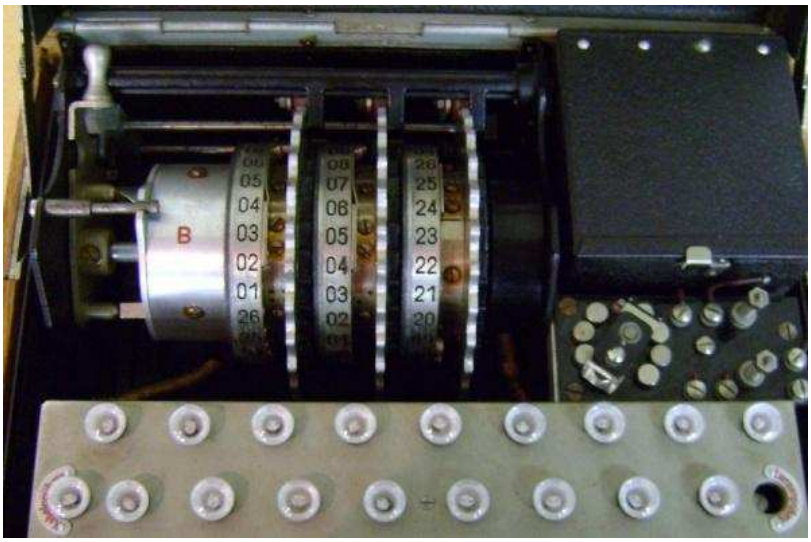
Traduzione italiana: Silvio Coccaro
www.silcosoft.it

Questa pagina presenta i dettagli tecnici della macchina Enigma della Wehrmacht, di quella della Luftwaffe e di quella M4 della Kriegsmarine.

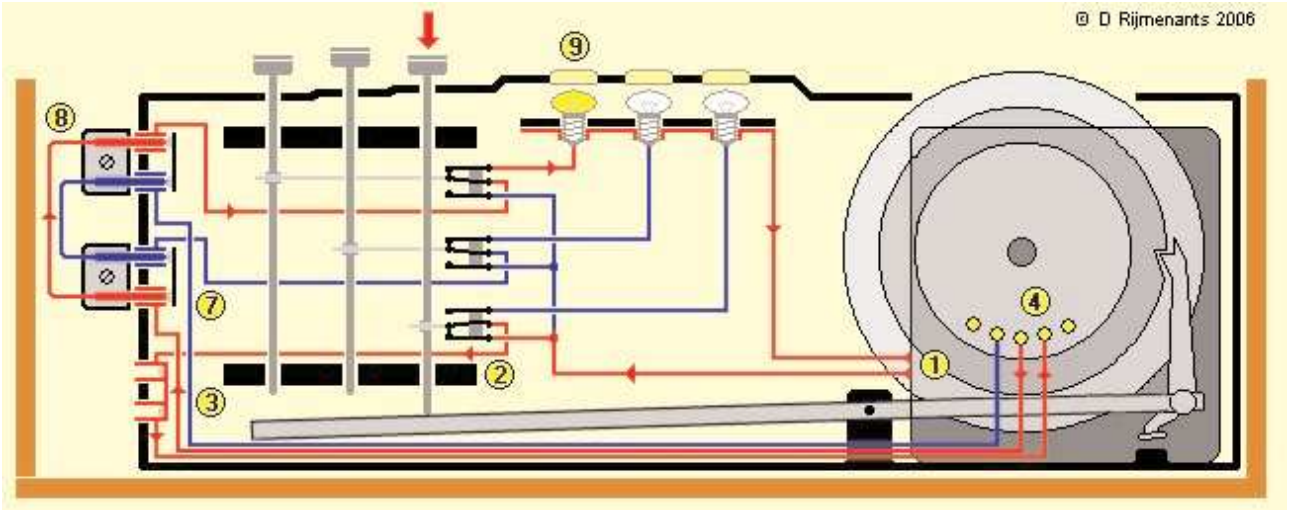
- Il diagramma dei cablaggi
- I rotori
- Il riflettore
- Le tabelle dei cablaggi dei rotori
- Il processo di cifratura a rotore
- Il meccanismo di avanzamento
- Il pannello a spine multiple
- Gli accessori
- La sua sicurezza matematica

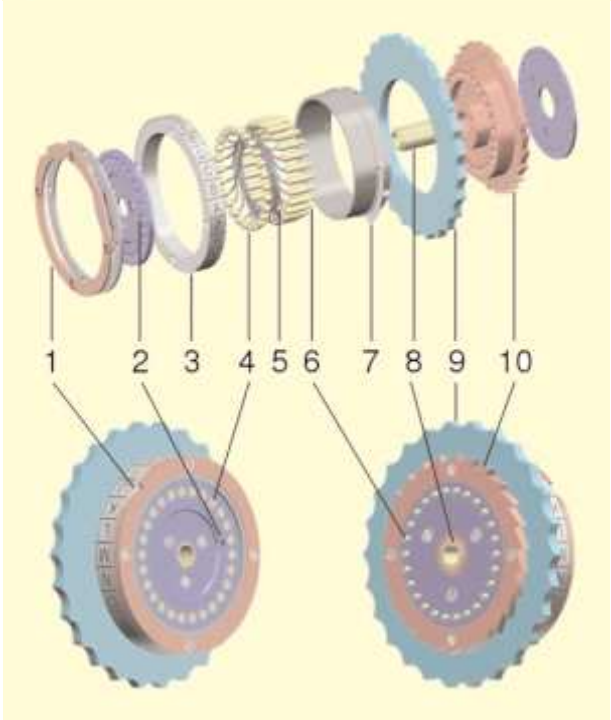


La macchina Enigma è un dispositivo elettromeccanico costituito da una tastiera (nel formato tedesco QWERTZ), un pannello di lampade, che rappresenta l'alfabeto e tre o quattro rotori. I rotori compiono uno scatto ogni qual volta un tasto viene premuto. La pressione di un tasto, tramite i rotori ed il pannello a spine multiple, fa accendere una lampadina, che rappresenta la lettera cifrata. È presente nella macchina un piccolo comparto per una batteria a 4 volt ed una spina per alimentare la macchina con una corrente elettrica esterna o con un trasformatore di CA.
Il disegno qui a lato mostra i cablaggi. Per rendere l'esempio più semplice, sono mostrati solo quattro componenti di ogni tipo. In realtà, le lampade, i tasti, le spine multiple e le connessioni all'interno di ogni rotore sono 26. La corrente fluisce dalla batteria [1], attraversa l'interruttore bidirezionale corrispondente alla lettera premuta [2] e raggiunge il pannello a spine multiple [3]. Questo pannello consente la modifica del cablaggio tra la tastiera [2] e lo statore [4]. Quindi, la corrente prosegue attraverso la presa inutilizzata [3] che è chiusa e raggiunge lo statore [4] per percorrere poi i cablaggi di tre rotori [5] (nell'Enigma della Wehrmacht) o di 4 rotori [5] (nell'Enigma M4 della Kriegsmarine) e raggiungere il riflettore [6]. Il riflettore inverte il senso della corrente, lungo un percorso diverso, che le fa attraversare di nuovo i rotori [5] e lo statore [4] e raggiungere ancora una volta il pannello a spine multiple, poi attraversa la spina "S" connessa con un cavo [8] alla spina "D" ed un altro interruttore bidirezionale [9] e quindi accende la lampada. Notare che la pressione di un tasto per prima cosa fa avanzare i rotori e poi invia la corrente a loro ed al bulbo della lampadina. Quando il tasto viene rilasciato la lampadina si spegne. Tuttavia, quando nessun tasto è più premuto, si può vedere sul rotore la lettera che è stata appena cifrata!
Il disegno della pagina successiva mostra la meccanica di Enigma, vista dal lato destro, con un diagramma dei cablaggi più o meno identico a quello del disegno precedente.



Una macchina Enigma della Wehrmacht con il coperchio sollevato. Da sinistra a destra: il riflettore B, i tre rotori, il rotore di ingresso (nero) ed il vano della batteria. A destra e sotto il vano della batteria vi sono i contatti dell'interruttore di alimentazione. Nella seconda riga di lampadine sul lato sinistro vi è una lampadina di ricambio ed il foro a destra serve a provarla.





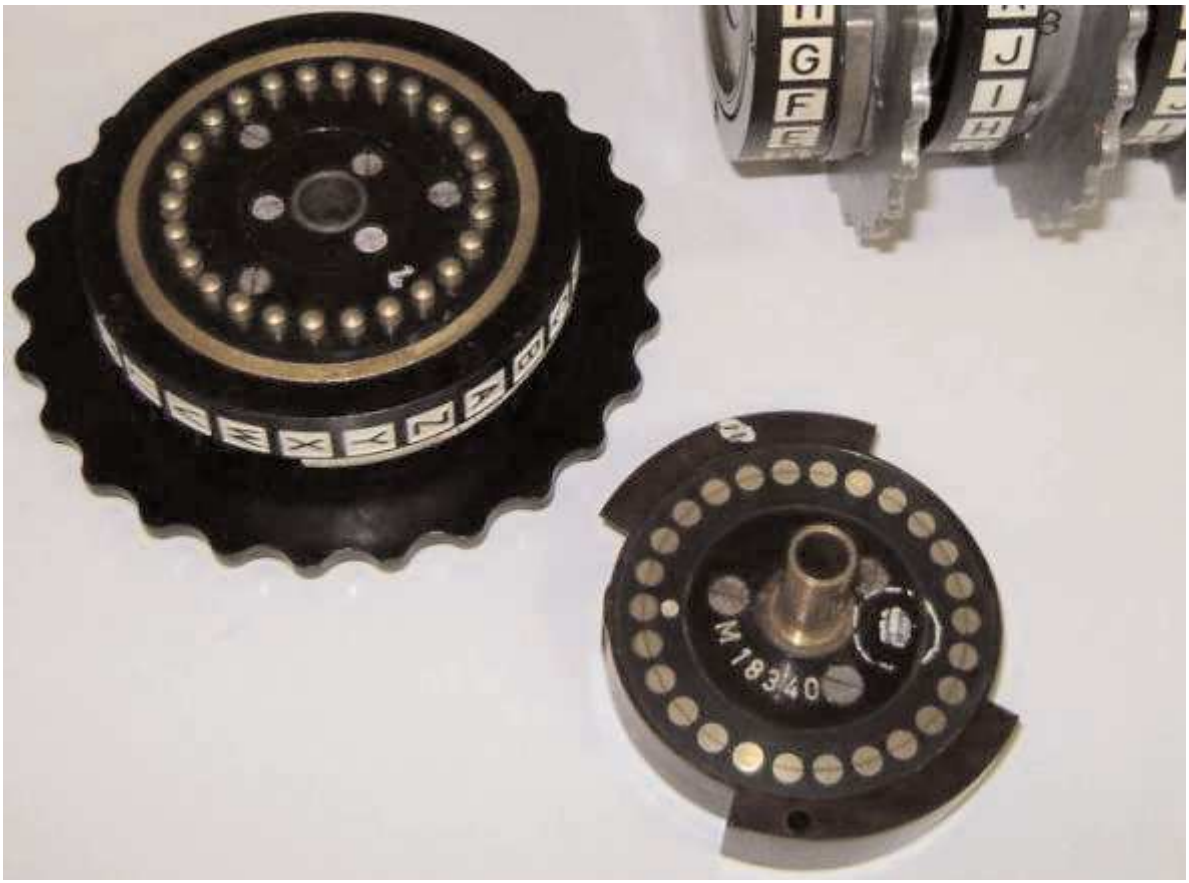
I rotori (Walzen in tedesco) sono gli elementi più importanti della macchina. Essi sono dei dischi circolari [9], approssimativamente di 10 cm di diametro, di metallo o di bakelite che nella parte centrale possiedono 26 contatti a molla [6] sul lato destro e 26 cablaggi cifrati [5] connessi ai 26 contatti piatti [4] sul lato sinistro ed asse cavo centrale [8]. All'esterno dei cablaggi cifrati è montato un anello mobile [3] con 26 numeri o lettere ed una tacca [1]. Questo anello è mobile ma può essere bloccato in una posizione qualsiasi dell'alfabeto con uno spinotto a molla (Wehrmacht) [7] o due archetti a molla (Kriegsmarine). Facendo compiere all'anello una rotazione si produrrà un cambiamento nella posizione della tacca e dell'alfabeto, in relazione al cablaggio interno. Questa impostazione prende il nome di regolazione dell'anello o Ringstellung e la sua posizione è resa visibile da un punto di marcatura [2]. Ogni rotore possiede alla sua sinistra una tacca

[1] mentre a destra è presente una ruota a denti di sega [10] che permettono al rotore di avanzare a scatti unidirezionali. Il cablaggio interno è diverso per ogni tipo di rotore e costituisce una cifratura per sostituzione. Il ricorso a diversi rotori, che mutano continuamente le loro posizioni relative, rende la cifratura tanto complicata.
Inizialmente, Enigma utilizzava tre rotori. Nel 1939, questi rotori venivano scelti da un insieme di cinque rotori, contrassegnati da numeri romani I, II, III, IV e V, ma tutti avevano solo una tacca. La Kriegsmarine portò l'insieme dei rotori ad otto, chiamando VI, VII ed VIII i nuovi rotori, tutti con due tacche. Nel 1942, l'Enigma M4 della Kriegsmarine introdusse un quarto rotore. A causa di questa modifica, i più spessi riflettori B o C della versione a tre rotori furono sostituiti dai riflettori B o C sottili, per far posto allo speciale rotore di tipo quarto. Questi rotori erano di due tipi, chiamati Beta e Gamma, con contatti a molla su entrambe le loro facce. Essi erano incompatibili con gli altri otto rotori. Il quarto rotore era immobile poiché la M4 utilizzava lo stesso meccanismo della versione a tre rotori e perciò non aveva un quarto nottolino che facesse avanzare il rotore. Tuttavia l'operatore poteva regolare manualmente il rotore in una posizione qualsiasi dell'alfabeto.

Il riflettore B dell'Enigma della Wehrmacht

Il riflettore, in tedesco Umkehrwalze o UKW, è una caratteristica unica di Enigma. Nel cablaggio interno dei rotori mobili, ogni lettera può essere connessa ad un'altra qualsiasi. La "A" può venir connessa alla "F" e la "F" a sua volta alla "K". Nel riflettore, le connessioni avvengono per coppie. Infatti, se la "A" è connessa alla "F" ne consegue che la "F" è sua volta connessa con la "A", risultandone una cifratura reciproca. Il vantaggio che ne deriva per l'operatore è evidente. La cifratura e la decifrazione sono entrambe possibili mantenendo le stesse impostazioni e gli stessi cablaggi della macchina. Sfortunatamente, una lettera non può mai cifrare se stessa e questo fatto aprì la strada alla crittanalisi, rendendo più facile il lavoro dei crittanalisti. Nell'arco della Seconda Guerra Mondiale furono utilizzati due tipi di riflettori, il B e il C. La macchina Enigma a 4 rotori della Kriegsmarine utilizzava degli speciali riflettori sottili, chiamati allo stesso modo B e C, il cui cablaggio interno differiva da quello degli analoghi riflettori della Wehrmacht e della Luftwaffe.

Tuttavia, se il riflettore sottile B della Kriegsmarine veniva utilizzato assieme al quarto rotore Beta in posizione A e con l'anello in posizione A o con il riflettore C ed il rotore gamma, questi riflettori diventavano compatibili con le versioni a tre rotori, consentendo la comunicazione tra tipi diversi di macchine. I riflettori sottili avevano contatti piatti ed erano impiegati in combinazione con i rotori speciali Beta e Gamma (rotori di tipo quarto) con contatti a molla su entrambe le facce. Negli ultimi giorni di guerra, fu introdotto il riflettore speciale di tipo D. Era un riflettore regolabile a 12 connessioni e a 24 spine. La 13ª connessione era una connessione fissa.



Il rotore navale beta ed il riflettore sottile

Per poter comprendere perché il cablaggio interno dei rotori operi come un sistema cifrante a sostituzione semplice, occorre analizzare il rotore di tipo I senza alcuna regolazione dell'anello. L'input è sul suo lato destro, guardando la macchina Enigma frontalmente! Si vede facilmente che una "A" è cifrata con una "E", una "B" da una "K" e che "K" è codificata con "N". Si noti che ogni lettera è codificata in un'altra. Si noti anche che quando la corrente torna dal riflettore all'indietro, essa attraversa nuovamente tutti i rotori ma secondo un percorso diverso da quello di andata.
Regolare l'anello o Ringstellung significa regolare la posizione del cablaggio interno rispetto all'alfabeto ed alla tacca. Infatti, un rotore è formato da due parti principali. La prima è costituita dall'anello esterno con l'alfabeto e la tacca. La seconda è formata da un nucleo centrale coi cablaggi interni, la parte cifrante vera e propria. Perciò modificare la regolazione dell'anello significa modificare la posizione dei cablaggi interni rispetto al punto di rotazione ed alla posizione visibile del rotore. Mentre il rotore I nella posizione "A" cifra in condizioni normali la "A" con

la “E”, con una regolazione di scostamento “B” (02) dell’anello, i cablaggi si spostano di una posizione (verso sinistra nella tabella) ed allora la “A” verrà cifrata con la “K”. Sul rotore, la “regolazione dell’anello” è contrassegnata da un punto sito sulla parte centrale dei cablaggi rotanti. Quando la regolazione dell’anello viene avanzata di una posizione, il punto di svolta del rotore corrisponderà sempre alla stessa lettera del rotore, poiché la tacca è fissa rispetto all’anello dell’alfabeto. La cifratura, invece, subisce uno scostamento di una posizione.

```
Input = ABCDEFGHIJKLMNOPQRSTUVWXYZ (lato destro del rotore)
        ||||||||||||||||||||||||||
I     = EKMFLGDQVZNTOWYHXUSPAIBRCJ
II    = AJDKSIRUXBLHWTMCQGZNPYFVOE
III   = BDFHJLCPRTXVZNYEIWGAKMUSQO
IV    = ESOVPZJAYQUIRHXLNFTGKDCMWB
V     = VZBRGITYUPSDNHLXAWMJQOFECK
```

Rotori standard della Wehrmacht, della Luftwaffe e della Kriegsmarine.

```
Input = ABCDEFGHIJKLMNOPQRSTUVWXYZ (lato destro del rotore)
        ||||||||||||||||||||||||||
VI    = JPGVOUMFYQBENHZRDKASXLICTW
VII   = NZJHGRCXMYSWBOUFAIVLPEKQDT
VIII  = FKQHTLXOCBJSPDZRAMEWNIUYGV
```

Altri rotori M3 e rotori M4 utilizzati dalla Kriegsmarine.

```
Input = ABCDEFGHIJKLMNOPQRSTUVWXYZ (lato destro del rotore)
        ||||||||||||||||||||||||||
Beta  = LEYJVCNIXWPBQMDRTAKZGFUHOS
Gamma = FSOKANUERHMBTIYCWLQPZXVGJD
```

I rotori speciali di tipo quarto, detti anche Zusatzwalzen o rotori greci.
Usati nel rotore M4 della Kriegsmarine soltanto con i riflettori sottili.

Nella tabella dei cablaggi del riflettore possiamo vedere che nel riflettore largo B una “A” ritorna una “Y” e che una “Y” ritorna una “A”. Notare che il cablaggio è mantenuto costante nel tempo come un’ansa tra due lettere.

```
Contatti      = ABCDEFGHIJKLMNOPQRSTUVWXYZ
                ||||||||||||||||||||||||||
Riflettore B  = YRUHQSLDPXNGOKMIEBFZCWVJAT
Riflettore C  = FVPJIAOYEDRZXWGCTKUQSBNMHL
```

Cablaggi standard dei riflettori larghi della Wehrmacht e della Luftwaffe.

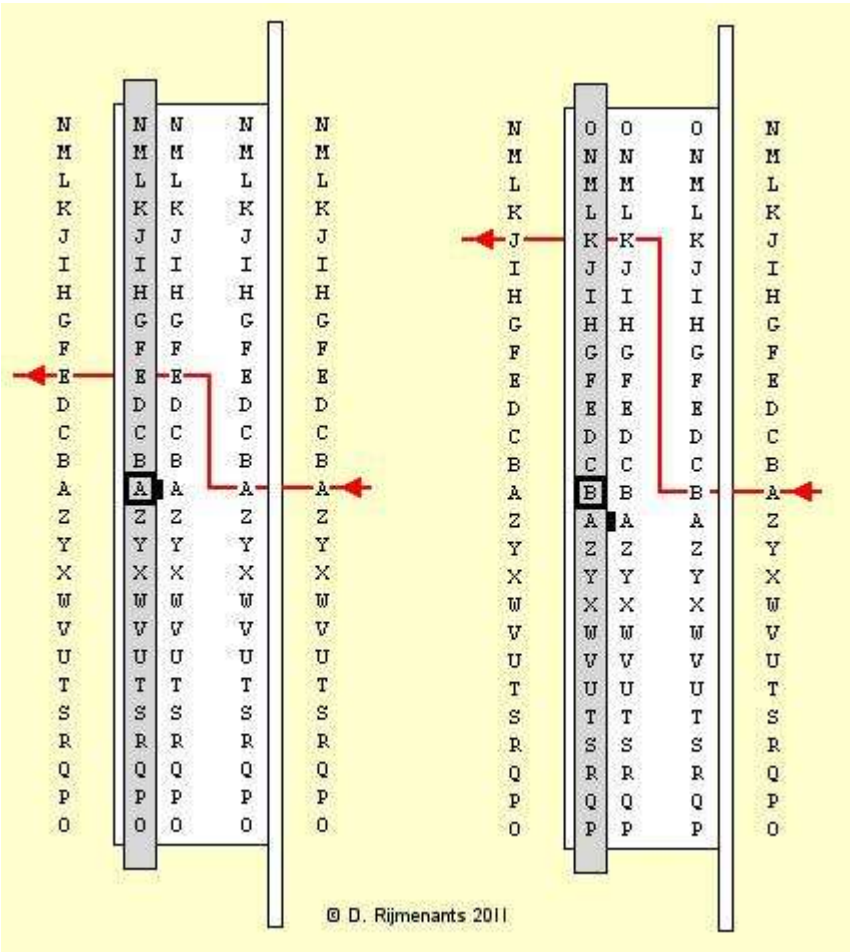
```
                Contatti = ABCDEFGHIJKLMNOPQRSTUVWXYZ
                           ||||||||||||||||||||||||||
Riflettore B sottile = ENKQAUYWJICOPBLMDXZVFTHRGS
Riflettore B sottile = RDOBJNTKVEHMLFCWZAXGYIPSUQ
```

Riflettori sottili, solo per la Kriegsmarine M4.

I cablaggi qui descritti si riferiscono unicamente ai rotori della Wehrmacht, della Lufwaffe e della Kriegsmarine. I rotori di altre versioni di Enigma avevano altri cablaggi interni.

Il processo di cifratura mediante i rotori

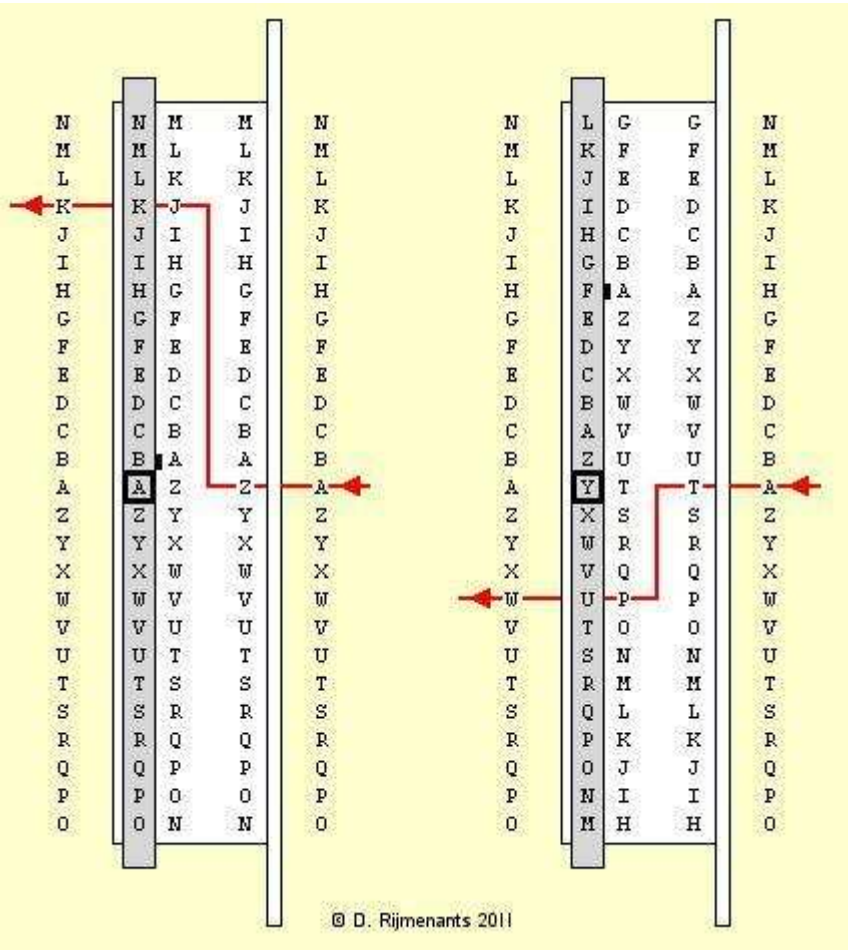
Un rotore consta di due parti principali. In primo luogo, abbiamo l'anello mobile esterno che reca l'alfabeto (visibile nella finestrella) e la tacca (responsabile dello scatto di avanzamento). In secondo luogo, la parte centrale con il cablaggio interno (la cifratura vera e propria) ed i suoi 2 X 26 contatti. Questa parte centrale è fissata ad una grande rotella che si utilizza per regolare manualmente la posizione del rotore. Il cambio della posizione dell'anello esterno viene chiamato regolazione dell'anello o 'Ringstellung' e con esso si cambia la posizione dell'alfabeto sull'anello e la sua tacca (punto di rotazione), relativo alla parte cablata interna.



Nei disegni che seguono noi usiamo il rotore di Enigma di tipo I (uno romano). L'anello mobile è rappresentato dal campo verticale grigio. Il nucleo cablato e la rotella fissata ad esso sono di colore bianco (nella realtà il campo bianco non ha lettere). La posizione del rotore è indicata dalla lettera nella cornice nera (la finestrella nel coperchio della macchina). Il piccolo campo nero alla destra dell'anello è lo spinottino di fermo, per bloccare la posizione dell'anello ed indica la regolazione dell'anello.

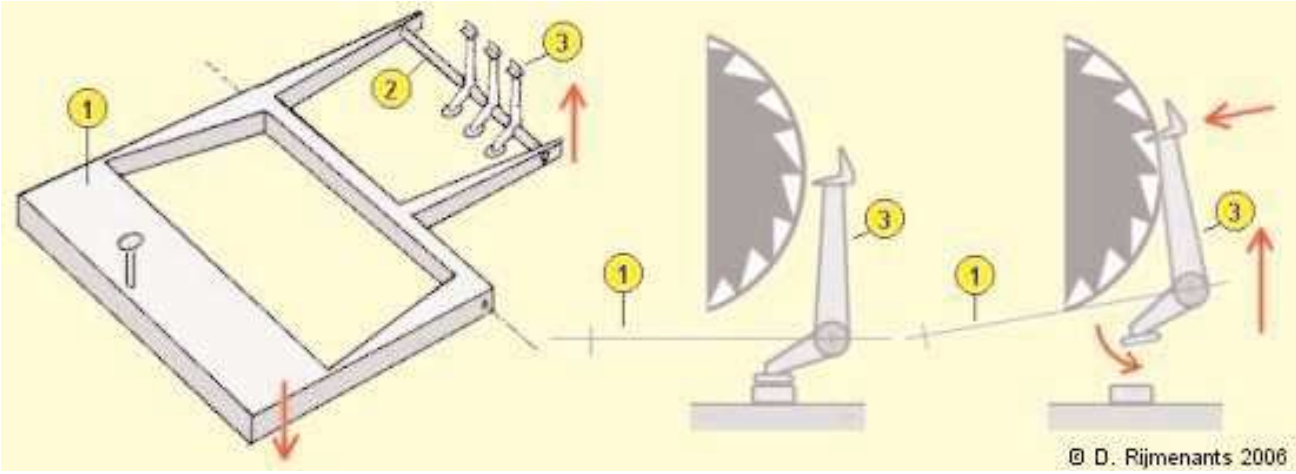
Il primo esempio mostra come il rotore I (con regolazione A – 01) dell'anello cifra due pressioni successive del tasto A. A sinistra puoi vedere il rotore I nella posizione A (visibile nella finestrella). Il segnale, pro-

veniente dal tasto A che è stato premuto, arriva alla posizione A, entra sul contatto A ed esce sul contatto E alla posizione E.
A destra, il rotore è avanzato nella posizione B. Il segnale arriva di nuovo alla posizione A, ma adesso entra al contatto B ed esce sul contatto K. Poiché l'intero rotore è avanzato di una posizione, il contatto K adesso è nella posizione J e perciò il segnale esce dalla posizione J verso il rotore successivo.
Sui rotori, il 'Ringstellung' è contrassegnato dallo spinotto di blocco (Wehrmacht) o da un punto sul nucleo dei cablaggi (Kriegsmarine) che contraddistingue la locazione del primo contatto (A o 01) del nucleo dei cablaggi. La regolazione dell'anello su F o 06 allineerà la lettera F o la cifra 06 dell'anello esterno col primo contatto del rotore, contrassegnato dallo spinotto o dal punto. Se cambiamo di una posizione l'anello, la cifratura slitta di una posizione (il punto di rotazione del rotore resta sulla medesima lettera, perché la tacca si trova sull'anello dell'alfabeto). La regolazione dell'anello non deve essere confusa con la posizione del rotore, che corrisponde alla lettera dell'anello dell'alfabeto, visibile nella finestrella del coperchio della macchina.
Seguono due esempi per spiegare la regolazione dell'anello. A sinistra, il rotore I ha per regolazione dell'anello B – 02 (spinotto o punto su B) ed il rotore è nella posizione A (la A è visibile nella finestrella). Il segnale arriva alla posizione A, entra nel contatto Z ed esce dal contatto J. A causa della regolazione dell'anello, il nucleo di cablaggio ha uno scostamento di una posizione e così pure i contatti di uscita. Perciò, il contatto di uscita J è adesso nella posizione K ed il segnale esce dalla posizione K in direzione del rotore successivo.



A destra, abbiamo lo stesso rotore I con regolazione dell'anello su F – 06 ed il rotore nella posizione Y. Il segnale giunge alla posizione A, entra nel contatto T ed esce dal contatto P. Tuttavia, la combinazione della posizione del rotore e la regolazione del suo anello determinano uno scostamento di sette posizioni dei contatti di uscita. Con il contatto di uscita P nella posizione W, il segnale esce dal rotore nella posizione W verso il rotore successivo.
Ricorda che, alla pressione di un tasto, i rotori avanzano **prima** che il segnale elettrico scorra attraverso i rotori. Perciò, per esaminare il flusso di corrente attraverso il ro-

tore più a destra ed in posizione A, il rotore deve essere disposto nella posizione Z prima della pressione del tasto (questo vale anche per gli altri rotori se questi devono compiere un avanzamento a scatto). Negli esempi di cui sopra, non risulta collegato al pannello a spine multiple nessuno spinotto ed il segnale scorre direttamente dal tasto A, mediante il rotore di ingresso, al rotore I.
Il flusso di segnale, come sopra descritto, va da destra a sinistra. Provenendo dal pannello a spine multiple arriva al rotore di ingresso (situato sul lato destro dell'alloggiamento dei rotori) e procede, da destra verso sinistra, attraverso il rotore più a destra, poi a quello centrale ed infine a quello di sinistra. Una volta che il segnale ha attraversato tutti i tre o i quattro rotori, il riflettore ritorna indietro questo segnale attraverso il rotore sinistro, centrale e destro secondo un altro percorso, determinando una seconda e completamente differente trasformazione del segnale. È ovvio che la combinazione del cablaggio del rotore, la posizione del rotore e lo scostamento dell'anello creano una cifratura complicata. Uno scatto singolo di un solo rotore produrrà un percorso completamente differente in tutti e tre i rotori.

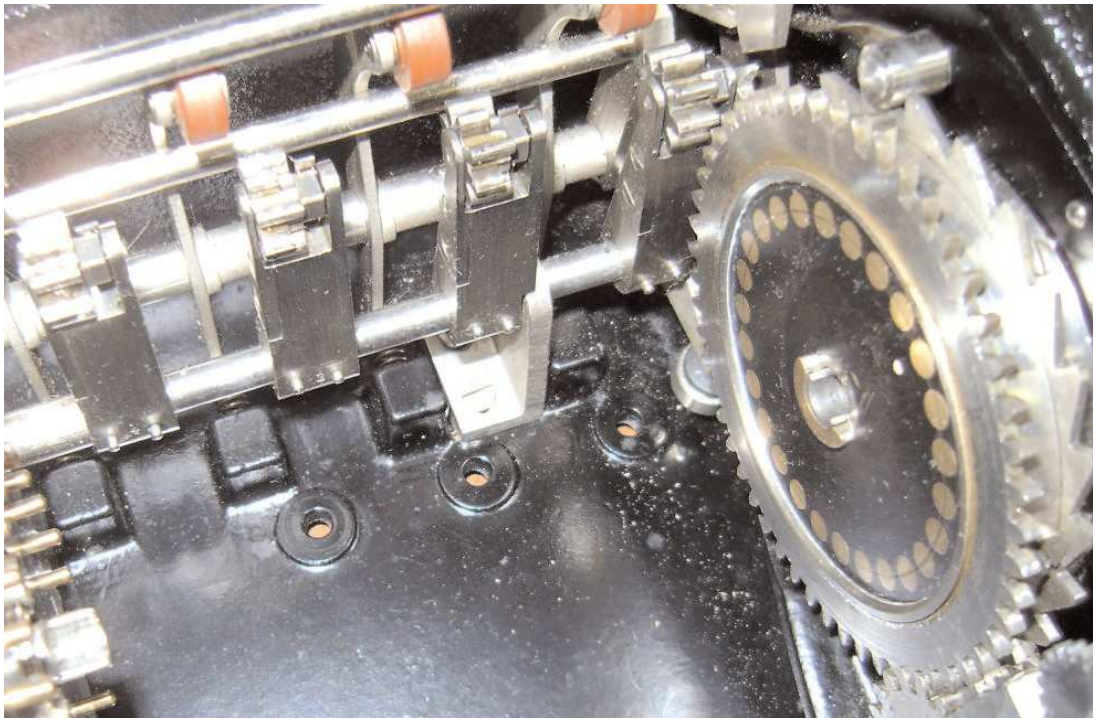


Il meccanismo di avanzamento a scatti

La posizione dei rotori cambia ogniqualvolta un tasto viene premuto. Perciò si realizza ogni volta una cifratura per sostituzione, di volta in volta differente, per una medesima lettera. Il primo rotore, posizionato alla destra della macchina, compie uno scatto ad ogni pressione di un tasto. Il rotore di centro avanza ogni 26 scatti del rotore di destra. Il terzo rotore, il più lento, avanza ogni 26 scatti del rotore centrale.
La pressione su di un tasto spinge verso il basso la barra di avanzamento [1] e l'asse dei nottolini e verso l'alto i tre nottolini azionati a spinta [3]. Quando l'asse dei nottolini [2] viene sollevato i nottolini fanno scattare i rotori in avanti. Ogni nottolino è in relazione sia con la tacca dell'anello del rotore alla sua destra che con la ruota a denti di sega alla sua sinistra. Se un rotore si trova nella posizione di impegno della tacca, il suo nottolino può incunearsi in essa e spingere la ruota dentata del rotore alla sua sinistra, facendo scattare il rotore di una posizione in avanti. Se il rotore alla sua destra non si trova nella posizione di impegno della tacca, il nottolino slitta sull'anello della tacca del rotore alla sua destra e non può più impegnarsi nella ruota dentata. Poiché non ci sono altri rotori alla destra del primo rotore, il nottolino più a destra si impegna nel primo rotore ad ogni depressione di un tasto.

Rotore	Tacca	Finestrella	il rotore a sinistra avanza quando il rotore scatta da -> a
I	Y	Q	Q -> R
II	M	E	E -> F
III	D	V	V -> W
IV	R	J	J -> K
V	H	Z	Z -> A
VI VII VIII	H + U	Z e M	Z -> A e M -> N

Se non è stato premuto nessun tasto, l'asse dei nottolini [2] forza i nottolini stessi [3] contro il piano alla base della macchina, allontanando i nottolini dai rotori. Ciò consente all'operatore di ruotare manualmente i rotori in entrambe le direzioni. La posizione della tacca è diversa per ogni tipo di rotore. Nella tabella soprastante si può vedere come il rotore I abbia la tacca sulla lettera Y. Se questa tacca viene posizionata di fronte al nottolino, allora nella finestrella è visibile la lettera Q. Inoltre, il rotore alla sinistra del rotore I avanzerà di una posizione se il rotore I avanza da Q a R (i crittanalisti usavano la frase mnemonica **R**oyal **F**lags **W**ave **K**ings **A**bove per ricordare le posizioni dei rotori dopo lo scatto). Si noti che i rotori della Kriegsmarine VI, VII e VIII avevano due tacche. Questo fatto faceva avanzare il rotore alla loro sinistra con velocità doppia rispetto agli altri rotori. Sebbene il meccanismo di avanzamento dei rotori sembri funzionare proprio come un normale odometro, non di meno, c'è una differenza fondamentale tra i due. Il rotore centrale avanza non solo quando il rotore di destra raggiunge la posizione d'impegno della tacca, ma anche quando anch'esso ha raggiunto l'analoga posizione di impegno della propria tacca.



Ecco il meccanismo di avanzamento a scatola di ingranaggi del raro precursore dell'Enigma G. Si noti la collocazione standard dei contatti del rotore rispetto a quella delle versioni successive dell'Enigma G a contatti speciali posizionati a zigzag.

Ecco una sequenza esemplificativa di scatto doppio: KDO, KDP, KER, LFS, LFT (i rotori utilizzati sono, da sinistra a destra: III, II e I). Questo avanzamento doppio fa sì che i rotori funzionino in modo diverso dall'odometro.
L'avanzamento doppio si verifica in questo modo: il primo (destro) rotore raggiunge la posizione di impegno della tacca e la pressione su di un tasto fa avanzare il secondo (centrale) rotore di una posizione. Se con questo avanzamento il secondo rotore raggiunge la propria posizione di impegno della tacca, il terzo nottolino al passo successivo si impegna nella ruota dentata del terzo (sinistro) rotore. Con questo avanzamento ulteriore, il terzo nottolino spinge la ruota dentata del terzo (sinistro) rotore e la fa avanzare, ma si impegna anche nella tacca del secondo rotore imprimendogli una spinta che fa avanzare ancora una volta il secondo rotore.
Il meccanismo di avanzamento che abbiamo appena descritto riguarda le macchine Enigma della Wehrmacht e della Kriegsmarine. L'Enigma M4 a 4 rotori della Kriegsmarine deriva dalla versione a tre rotori senza alcuna modifica al meccanismo di avanzamento dei rotori e senza l'aggiunta di un altro nottolino. Perciò il quarto rotore non può muoversi e può essere regolato solo manualmente.
L'EnigmaG dell'Abwehr (il Servizio segreto tedesco) possiede un meccanismo diverso alla cui base c'è un riflettore rotante e tre rotori con più tacche, azionati da una scatola di ingranaggi.

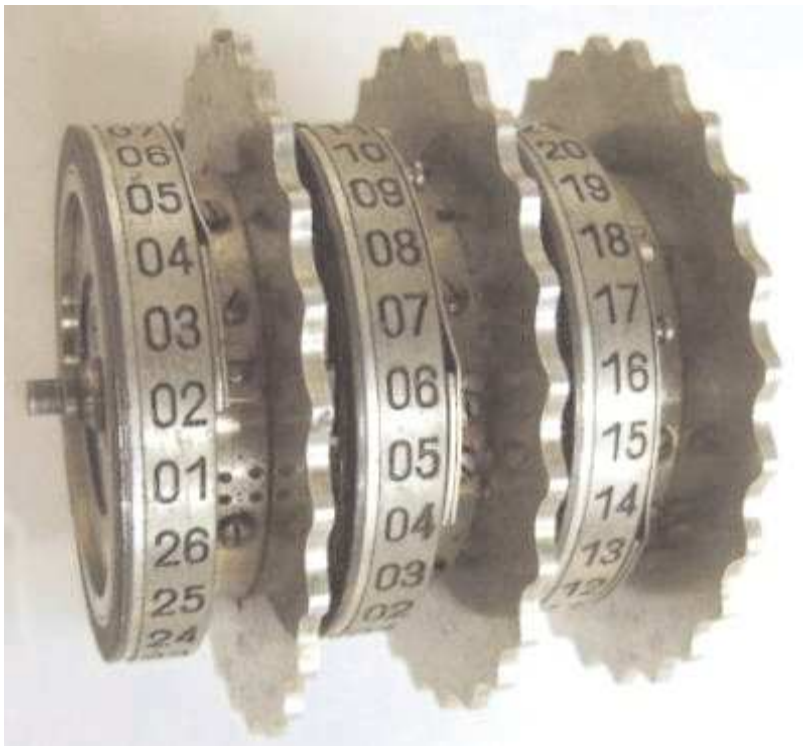
Il pannello a spine multiple della macchina Enigma

Nel 1930 fu introdotto sulla prima versione di Enigma per la Wehrmacht il pannello a spine multiple o Steckerbrett. Tale pannello è situato di fronte alla macchina. Se non si è inserita alcuna spina, la corrente fluisce dagli interruttori, sotto controllo della tastiera, direttamente allo statore. Con l'inserimento di una spina si ottiene lo scambio delle due lettere implicate prima che la corrente raggiunga lo statore.
Ogni macchina era equipaggiata di serie con un set di dieci cavi. Il pannello a spine multiple ha costituito un incremento importante della potenza cifrante di queste macchine. Ogni lettera ha due jack. Con l'inserimento di una spina si ha la disconnessione del jack superiore, connesso alla tastiera, dal jack inferiore, connesso allo statore. L'altra estremità del cavo di scambio deve essere inserita nel jack di un'altra lettera, determinando così lo scambio delle connessioni fra le due lettere. La corrente fluisce dal pannello a spine multiple una volta verso i rotori ed un'altra volta verso i bulbi delle lampadine.

Gli accessori

L'Uhr ed i suoi cavi che sostituiscono i cavi standard.

Un accessorio utile, utilizzato sull'Enigma della Kriegsmarine era la Schreibmax. Questa piccola stampante poteva imprimere i messaggi su un piccolo nastro di carta. Ciò rendeva inutile la presenza di un secondo operatore che leggesse le lampadine e ne scrivesse le lettere. La Schreibmax si collocava sulla parte alta della macchina Enigma ed era connessa al pannello di lampadine; per installarla il coperchio delle lampadine e tutte le lampadine dovevano essere rimosse.
Un altro accessorio era costituito dal pannello remoto di lampadine. Se la macchina era equipaggiata con un pannello extra, la custodia di legno della macchina Enigma doveva essere ingrandita per poterlo contenere. È stata costruita una versione con pannello a lampadine che poteva essere connesso in un secondo tempo ma richiedeva, proprio come la Schreibmax, la rimozione del pannello delle lampadine e delle lampadine stesse. Il pannello remoto rendeva possibile ad una persona la lettura del testo decifrato, senza consentirla all'operatore.
Nel 1944, la Luftwaffe introdusse un interruttore extra a spine multiple, detto Uhr (orologio). L'Uhr era costituito da una piccola scatola che conteneva un interruttore a 40 posizioni. Questo dispositivo sostituiva i cavi a spinotto standard. Dopo aver connesso gli spinotti, secondo le indicazioni dei fogli quotidiani delle chiavi, l'operatore poteva ruotare l'interruttore su una delle sue 40 posizioni, ciascuna delle quali cablava gli spinotti in modo differente. Quasi tutte queste connessioni cablate erano, diversamente dai cavi standard, disaccoppiate.

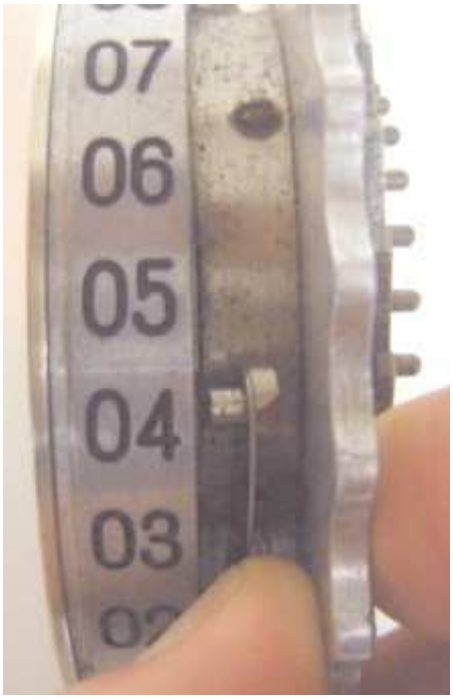


I tre rotori montati sul loro asse

Veduta da sinistra di un rotore con la sua tacca (a sinistra)

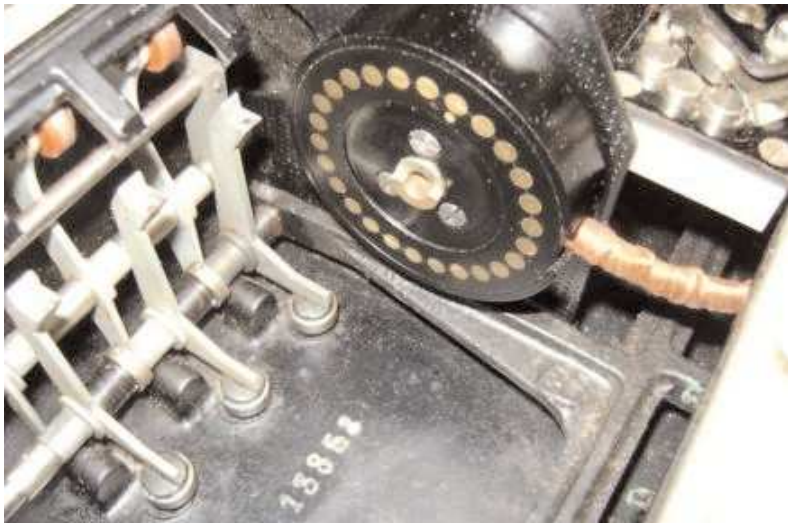
Lato destro di un rotore con la sua ruota a denti di sega

Rotore della Kriegsmarine con due tacche



Blocco dell'anello con uno spinotto (Wehrmacht)

Blocco dell'anello con due archi (Kriegsmarine)



I tre nottolini sul loro asse, a riposo sui piedini. L'asse dei nottolini è fissato sulla barra di avanzamento (la forma ad L di color argento). Alla destra dei nottolini si può vedere lo statore.

La sua sicurezza matematica

Per calcolare la sua sicurezza matematica dobbiamo trovare tutte le possibile impostazioni differenti della macchina. Inoltre, dobbiamo analizzare tutte le proprietà della macchina di seguito elencate: la selezione e l'ordine dei rotori, il loro cablaggio, la regolazione dell'anello di ogni rotore, la posizione di partenza di questi rotori all'inizio del messaggio, le impostazioni del riflettore e del pannello a spine multiple. Adesso, esistono diversi modi per calcolare il numero totale di queste combinazioni. In una pubblicazione della NSA, sono state incluse tutte le variazioni possibili dei cablaggi di ogni rotore e di ogni riflettore. Ciò conduce alla cifra astronomica di 3×10^{114}. Tuttavia, questa cifra fuorviante rappresenta tutte le variazioni della macchina teoricamente possibili.
Sfortunatamente per i tedeschi, i solutori di codici alleati conoscevano la macchina, i rotori ed il loro cablaggio interno. Inoltre, essi dovevano prendere in considerazione soltanto i possibili modi concreti in cui era possibile configurare la macchina, cioè l'impostazione realistica delle chiavi o spazio delle chiavi. Questo è quanto prende il nome di sicurezza pratica, che è molto lontana dalla sicurezza teorica nel caso di Enigma. Per i crittologi tedeschi, un singolo rotore poteva essere cablato in 4×10^{26} modi differenti. La combinazione di tre rotori e del riflettore porta rapidamente alle cifre astronomiche di cui sopra. Ma per i solutori di codici alleati, che conoscevano i cablaggi dei rotori, esistevano soltanto 26 varianti per ogni rotore, cioè, le 26 posizioni che esso poteva assumere nella macchina.
Essi non dovevano esplorare il numero immenso di cablaggi possibili. I crittologi tedeschi commisero un errore critico ignorando la legge di Auguste Kerckhoffs che la sicurezza di un dispositivo non deve mai dipendere dalla segretezza del sistema (ad es. il cablaggio dei rotori, il progetto), che in qualche modo può prima o dopo essere compromessa, ma soltanto sulla segretezza della chiave (ad es. la scelta del rotore, le connessioni del pannello a spine multiple). Nell'interessante articolo di R. A. Ratcliff per Cryptologia viene spiegato quanto sia pericoloso adagiarsi sulla sicurezza teorica.
Diamo adesso un'occhiata alle cose che realisticamente si possono regolare nella macchina e che sono sconosciute ai solutori di codici. Nel nostro esempio, noi prendiamo la macchina Enigma della Wehrmacht a tre rotori col riflettore standard B ed un insieme di cinque rotori. Utilizziamo 10 cavi con spinotti sul pannello a spine multiple, il numero predefinito di cavi, che accompagnano la macchina (non chiedetemi perché non venivano forniti 11 cavi, il che avrebbe fornito un numero molto più elevato di combinazioni). Selezionare tre rotori da un insieme possibile di cinque fornisce 60 combinazioni (5 x 4 x 3). Ciascun rotore, in altre parole il suo cablaggio interno, può essere regolato in 26 posizioni diverse. Perciò, con tre rotori si hanno 17.576 diverse posizioni del rotore (26 x 26 x 26). L'anello di ogni rotore espone una lettera (di cui qui non ci occupiamo) ed una tacca che influisce sull'avanzamento del rotore adiacente a sinistra. Ogni anello può a sua volta assumere una regolazione qualsiasi delle 26 possibili. Poiché non ci sono altri rotori a sinistra del terzo rotore (il rotore più a sinistra di tutti), soltanto gli anelli del rotore dell'estrema destra e del centro devono essere presi in considerazione per il calcolo. Ciò fornisce altre 676 combinazioni (26 x 26), conseguenti alla regolazione dell'anello. Con 10 cavi si può cablare il pannello a spine multiple in 150.738.274.937.250 modi diversi. Il totale di tutte queste possibilità è: 60 x 17.576 x 676 x 150.738.274.937.250 = **107.458.687.327.250.619.360.000** o **$1{,}07 \times 10^{23}$**.

Pertanto, nella vita reale, la macchina Enigma della Wehrmacht può essere regolata in 1,07 x 10^{23} modi diversi, il che è paragonabile ad una chiave di 77 bit. A proposito di questo numero dobbiamo fare alcune considerazioni. In realtà, il periodo massimo dei rotori – cioè il numero dei passi che la macchina deve compiere prima di tornare al punto di partenza – è leggermente minore di 17.576. Questo a causa del fenomeno dello scatto doppio. Il periodo effettivo dipende dal tipo di rotore. I tre rotori navali a doppia tacca hanno un periodismo ancora minore di quello dei rotori della Wehrmacht poiché il loro rotore centrale va incontro ad un numero doppio di scatti doppi. Tuttavia il periodo massimo non incide sulle regolazioni effettuabili e perciò non influenza lo spazio delle chiavi. La macchina della Wehmacht può essere equipaggiata col riflettore B o con quello C. In generale, le reti radio ricorrevano sempre allo stesso riflettore, poiché l'impiego di riflettori differenti creava problemi logistici, procedurali e pratici. Tuttavia, anche considerando ciò, la scelta del riflettore B o di quello C avrebbe soltanto raddoppiato lo spazio delle chiavi.
L'aggiunta del quarto rotore alla macchina Enigma Navale M4 per migliorarne la sicurezza fu una cosa bella ma inutile. Il quarto rotore, privo di movimento, rese la macchina più complicata solo per un fattore 26 ed, unitamente al riflettore sottile, lo si potrebbe considerare un riflettore regolabile a 26 posizioni, di cui gli Alleati trovarono ben presto i cablaggi (dopo 10 mesi di panico). L'introduzione di 8 rotori nell'Enigma navale M3 e successivamente in quella a quattro rotori M4 fu un approccio molto migliore. Ciò portò il numero delle combinazioni dei rotori da 60 a 336 ed aggiunse un'ulteriore complessità con i tre rotori VI, VII e VIII a tacche multiple.
Adesso calcoliamo la grandezza pratica delle chiavi dell'Enigma della Kriegsmarine M4. Questa macchina usava 3 rotori normali, scelti da un insieme di 8 (di cui 3 con tacche doppie). Il numero delle combinazioni possibili dei rotori è pari a 336 (8 x 7 x 6). L'M4 ha anche un rotore speciale, il quarto, detto Beta o Gamma (senza l'anello), che ci consente due scelte. Questi non sono compatibili con gli altri rotori e sono disponibili soltanto come quarti rotori (all'estrema sinistra). I 4 rotori possono essere regolati in una posizione qualsiasi tra 456.976 (26 x 26 x 26 x 26) posizioni. La M4 aveva un riflettore B o C più piccolo, per consentire l'alloggiamento del quarto rotore. Non prendiamo in considerazione il riflettore poiché esso, generalmente, non veniva mai cambiato. Di nuovo, erano implicati solo due anelli, poiché il terzo rotore non poteva far avanzare il quarto rotore, che non era mobile.
Anche la M4 era equipaggiata con 10 cavi. In totale, abbiamo: 336 x 456.976 x 676 x 150.738.274.937.250 = 31.291.969.749.695.380.357.632.000 o 3,1 x 10^{25} paragonabile ad una chiave di 84 bit. Questa chiave è circa 291 volte più forte di quella della macchina della Wehrmacht.La ragione di ciò si trova nel numero maggiore di rotori tra cui operare la scelta (già disponibile nella M3 prima della guerra) e dal numero delle possibili posizioni iniziali di 4 rotori anziché di 3. Tuttavia, sebbene il quarto rotore aumentasse la grandezza della chiave, esso non fu capace di potenziare la complessità della cifratura, poiché non era mobile in corso di essa. Una soluzione migliore sarebbe stata quella di ricablare regolarmente alcuni rotori. Il cablaggio variabile di un singolo rotore avrebbe moltiplicato lo spazio delle chiavi di un fattore non minore di 4 x 10^{26}, che è di gran lunga maggiore di quello di un riflettore regolabile con le sue 7,8 x 10^{12} possibili variazioni. Un singolo rotore, cambiato quotidianamente, ricablabile, che possiede praticamente 4 x 10^{26} possibili regolazioni, sarebbe stato molto più sicuro rispetto alle sovra-

stimate regolazioni del pannello a spine multiple, immobili e non regolabili quotidianamente con solo 2 x 10^{14} variazioni (il pannello a spine multiple funziona sempre a coppie).
L'impiego di un tale rotore, congiuntamente ad un riflettore sottile similM4 e a due rotori normali scelti tra quattro possibili, sarebbe stato un vero disastro per i solutori di codici. Tuttavia, l'introduzione di rotori ricablabili nel corso della guerra sarebbe stato scomodo e sarebbe stato un incubo logistico e finanziario, proprio come dimostrò di esserlo il riflettore D ricablabile. Troppo poco, troppo tardi. Il riflettore D, inizialmente, spaventò i solutori di codici, fino a quando essi capirono che il riflettore D veniva usato simultaneamente agli altri riflettori standard nelle stesse reti radio, per ragioni di ordine pratico. Questo uso doppio rese possibile la sua violazione anche manualmente. Ulteriori notizie sul riflettore D ed altro si possono trovare nella pagina della Storia di Enigma. Anche un esperto qualsiasi di crittologia risolverebbe le 17.576 combinazioni dell'anello. Anche con impostazioni completamente errate dell'anello, si può cominciare con un testo chiaro corretto. Non appena il testo diventa confuso, si aggiusti l'anello del rotore più a destra (si ha diritto alla probabilità di 1/26) e se si è fortunati non si hanno altri problemi per i successivi 676 caratteri. Se si è meno fortunati, si deve regolare l'anello del rotore centrale dopo 26 lettere. C'è voluto un attimo. Sfortunatamente per i tedeschi, l'ingegnoso progetto della bomba di Turing, con pacchi a specchio di rotori identici, scongiurò la necessità di ricercare nel numero immenso di regolazioni del pannello a spine multiple, riducendo di un fattore 2 x 10^{14} la lunghezza dei loro crib (pezzi noti di testi chiari e cifrati) per una certa regolazione di un rotore.
Non di meno, la violazione di Enigma era ancora una sfida immane con regolazioni della chiave che erano straordinarie per l'elettromeccanica di quei giorni. Con uno spazio pratico delle chiavi di 1,07 x 10^{23}, una ricerca esaustiva era impossibile nel 1940 e la sua chiave, paragonabile ad una moderna di 77 bit, è ancora enorme per gli standard odierni dei computer. Per aver un'idea della grandezza di questo numero, con 1,07 x 10^{23} fogli di carta (di 0,0099 cm di spessore ognuno) si potrebbero costruire 70.000.000 di cataste di carta, con base sulla Terra e vertice nel Sole. Oppure, 1,07 x 10^{23} equivale a 288.500 anni luce. Un numero straordinariamente grande! I tedeschi erano nel giusto nel ritenere che Enigma fosse teoricamente inviolabile. Tuttavia, la soluzione dei codici va oltre lo spazio delle chiavi ed i numeri, oltre la sicurezza teorica e oltre la ricerca della giusta combinazione. Ulteriori notizie su come gli Alleati violarono Enigma sono su questa pagina.

dell’autore. Per favore, contattare l’autore mediante l’indirizzo email sottostante per avere le autorizzazioni necessarie o per ulteriori informazioni.
dr.defcom@telenet.be