La Matematica della macchina Enigma

Settimana della Scienza

2025 - La Crittografia: segreti, enigmi e codici da decifrare

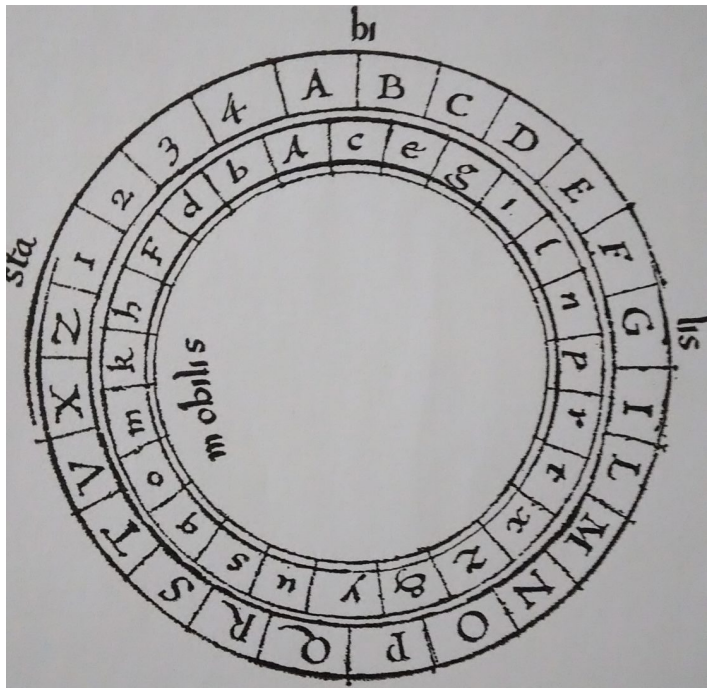
Marco Antonio Pellegrini

Università Cattolica del Sacro Cuore

23 ottobre 2025

La macchina Enigma

Nel 1918 l'inventore tedesco Arthur Scherbius ottenne il brevetto per un dispositivo elettromeccanico che, ispirandosi al disco cifrante di Leon Battista Alberti, permetteva di cifrare (e decifrare) messaggi in modo estremamente veloce e sicuro.



La prima versione era contenuta in una scatola $34 \times 28 \times 15$ cm e pesava 12 kg.

La macchina Enigma

Scherbius cercò di vendere la sua macchina a uomini d'affari, diplomatici e militari. L'alta cifra richiesta per ognuna di esse (più di 40 000 euro attuali) ne limitò la vendita.

L'esercito tedesco però si rese conto che Enigma poteva essere la soluzione ai fiaschi crittografici della Prima Guerra Mondiale. A partire dal 1925 le forze armate tedesche acquistarono più di 30 000 macchine Enigma (i cui circuiti erano differenti rispetto a quelli della versione commerciale), facendone la protagonista dei loro protocolli crittografici.

Scherbius non riuscì a godere dei guadagni della sua invenzione: morì per le ferite riportate in un incidente col suo calesse il 13 maggio 1929.

Le componenti di Enigma

Una macchina Enigma disponeva di due tastiere: su quella inferiore si componeva il testo in chiaro, quella superiore si illuminava in corrispondenza del testo cifrato. Battendo il testo in chiaro si otteneva quello cifrato e battendo il testo cifrato si otteneva il testo in chiaro.

Nella sua versione standard Enigma consisteva di cinque componenti variabili:

(1) un pannello di controllo dove erano presenti 26 doppi fori, etichettati dalle lettere dell'alfabeto;

(2) tre rotori, ordinati da sinistra a destra, che collegavano 26 punti di contatto in ingresso con 26 punti di contatto in uscita, posti sulla faccia opposta;

(3) 26 dentellature poste sul bordo di ciascun rotore, per poterne specificare la posizione iniziale;

(4) un anello mobile per ognuno dei rotori che modifica la posizione dell'anello alfabetico rispetto al cablaggio interno;

(5) un riflettore (un mezzo rotore che in realtà non ruota) che rimandava all'ultimo rotore il segnale ricevuto dal rotore stesso.

Il tutto alimentato tramite una batteria.

Le componenti di Enigma

L'operatore di una macchina Enigma doveva solo configurare la sua macchina e digitare il testo in chiaro per ottenere quello cifrato o viceversa. Non erano richiesti conti o problemi da risolvere, Enigma si occupava di tutto.

La crittografia basata su Enigma era considerata dai tedeschi estremamente sicura. In effetti, i calcoli matematici che effettueremo sembrano confermare questa impressione.

Cerchiamo allora di calcolare quante erano le possibili configurazioni di una macchina Enigma. Ci affidiamo quindi a quella parte della Matematica, la Combinatoria, che si occupa proprio di contare gli oggetti.

Pillole di Combinatoria

Principio di moltiplicazione

Se dobbiamo prendere varie decisioni, il numero totale di scelte sarà il prodotto del numero di scelte possibili per ogni decisione.

Esempio

Supponiamo di avere nel nostro armadio 3 magliette $\{A, B, C\}$ e 2 paia di pantaloni $\{X, Y\}$. In quanti modi potremo vestirci? Abbiamo tre scelte per la maglietta e due scelte per i pantaloni: $3 \cdot 2 = 6$.

$$(A, X), \quad (B, X), \quad (C, X), \quad (A, Y), \quad (B, Y), \quad (C, Y).$$

A volte le scelte che facciamo sono tra loro indipendenti, a volte una scelta dipende da ciò che abbiamo fatto prima.

Pillole di Combinatoria

Esempio

Supponiamo ora di avere 4 oggetti $\{A, B, C, D\}$ e di volerli disporre in una fila ordinata: quante possibilità avremo?

$$(A,B,C,D),\ (A,B,D,C),\ (A,C,B,D),\ (A,C,D,B),\ (A,D,B,C),\ (A,D,C,B)$$

$$(B,A,C,D),\ (B,A,D,C),\ (B,C,A,D),\ (B,C,D,A),\ (B,D,A,C),\ (B,D,C,A)$$

$$(C,B,A,D),\ (C,B,D,A),\ (C,A,B,D),\ (C,A,D,B),\ (C,D,B,A),\ (C,D,A,B)$$

$$(D,B,C,A),\ (D,B,A,C),\ (D,C,B,A),\ (D,C,A,B),\ (D,A,B,C),\ (D,A,C,B)$$

Abbiamo così $4 \cdot 3 \cdot 2 \cdot 1 = 24$ scelte.

Definizione

Dato un intero positivo n, definiamo $n!$ (fattoriale) come il prodotto

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n.$$

Poniamo anche $0! = 1$.

Pillole di Combinatoria

Esempio

Vogliamo ora mettere in fila 3 persone, scelte da un gruppo $\{A, B, C, D, E, F, G\}$ di 7 persone.
Abbiamo allora 7 scelte possibili per la prima persona della fila. Fatta questa scelta, abbiamo 6 scelte per la seconda persona. Fatta questa seconda scelta, abbiamo 5 possibilità per la terza persona:

$$7 \cdot 6 \cdot 5 = \frac{7!}{4!} = 210.$$

In generale, se dobbiamo disporre in una fila ordinata k oggetti scelti tra gli n a nostra disposizione, avremo

$$n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}$$

possibilità.

Pillole di Combinatoria

Esempio

Vogliamo ora scegliere 3 oggetti da un insieme $\{A, B, C, D, E\}$ di 5 oggetti. Questa volta non ci interessa l'ordine, stiamo scegliendo i nostri oggetti nello stesso momento.
Per calcolare quante possibilità abbiamo, pensiamo di mettere in fila 3 oggetti tra i 5 a disposizione, ottenendo $5 \cdot 4 \cdot 3 = \frac{5!}{2!}$ possibilità. Ora però non ci interessa l'ordine di questi 3 oggetti, per cui dividiamo per 3! (il numero di modi in cui possiamo disporre in fila tre oggetti):

$$\frac{5!}{2!} \cdot \frac{1}{3!} = \frac{5!}{2!\,3!} = 10.$$

$$\{A, B, C\},\ \{A, B, D\},\ \{A, B, E\},\ \{A, C, D\},\ \{A, C, E\},$$
$$\{A, D, E\},\ \{B, C, D\},\ \{B, C, E\},\ \{B, D, E\},\ \{C, D, E\}.$$

$$\{A, B, C\} = \{A, C, B\} = \{B, A, C\} = \{B, C, A\} = \{C, A, B\} = \{C, B, A\}.$$

Pillole di Combinatoria

In generale, se abbiamo n oggetti e ne vogliamo selezionare k in modo che l'ordine non sia importante, allora lo potremo fare in

$$\frac{n!}{k!\,(n-k)!}$$

modi diversi. Poniamo

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} \qquad \text{(coefficiente binomiale)}.$$

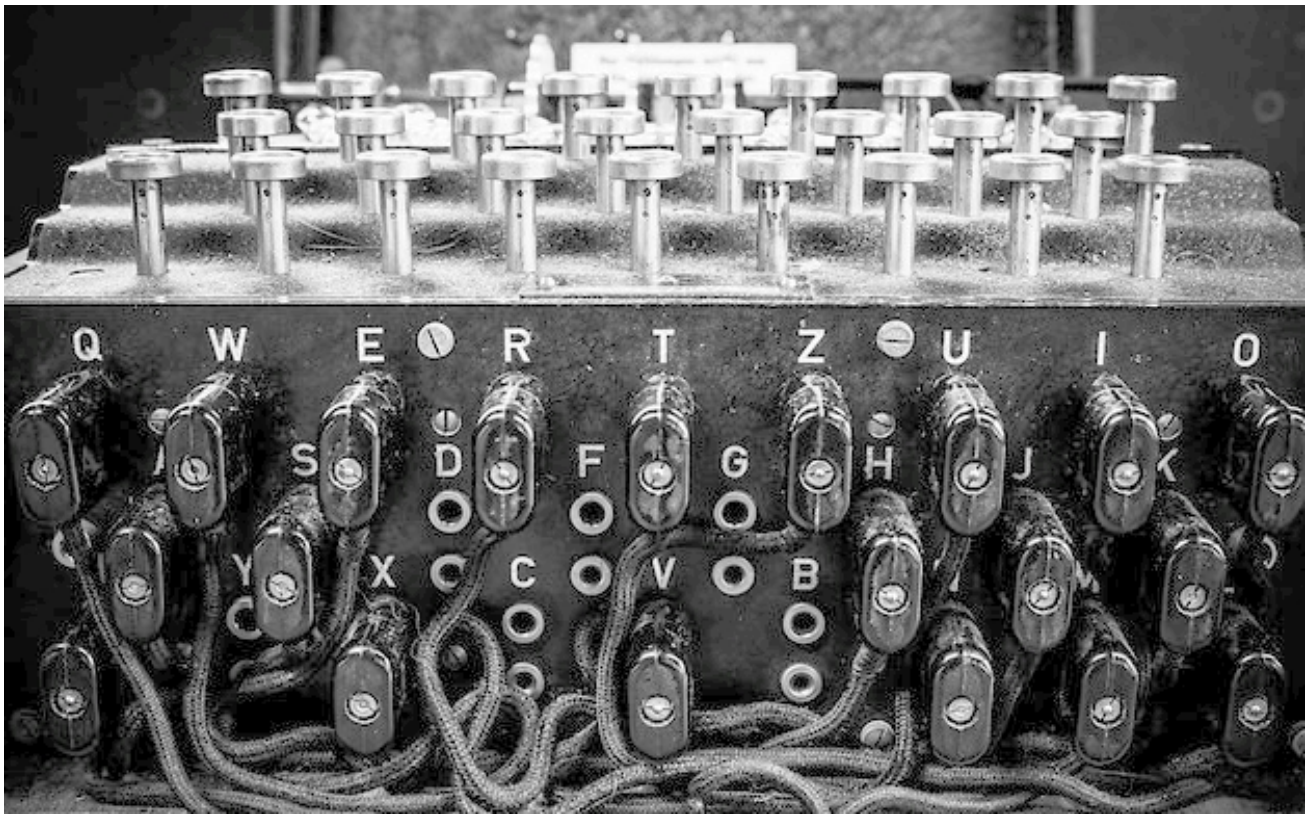
Abbiamo

$$\binom{n}{n} = \binom{n}{0} = 1 \quad \text{e} \quad \binom{n}{1} = n.$$

Torniamo alla macchina Enigma.

Il pannello di controllo

Il primo elemento che analizziamo è il Pannello di controllo in cui sono presenti 26 (doppi) fori, che potevano essere collegati tramite un massimo di 13 cavi connettori.
L'operatore, seguendo le indicazioni ricevute, poteva connettere due differenti fori con l'effetto di scambiare gli output delle lettere corrispondenti.

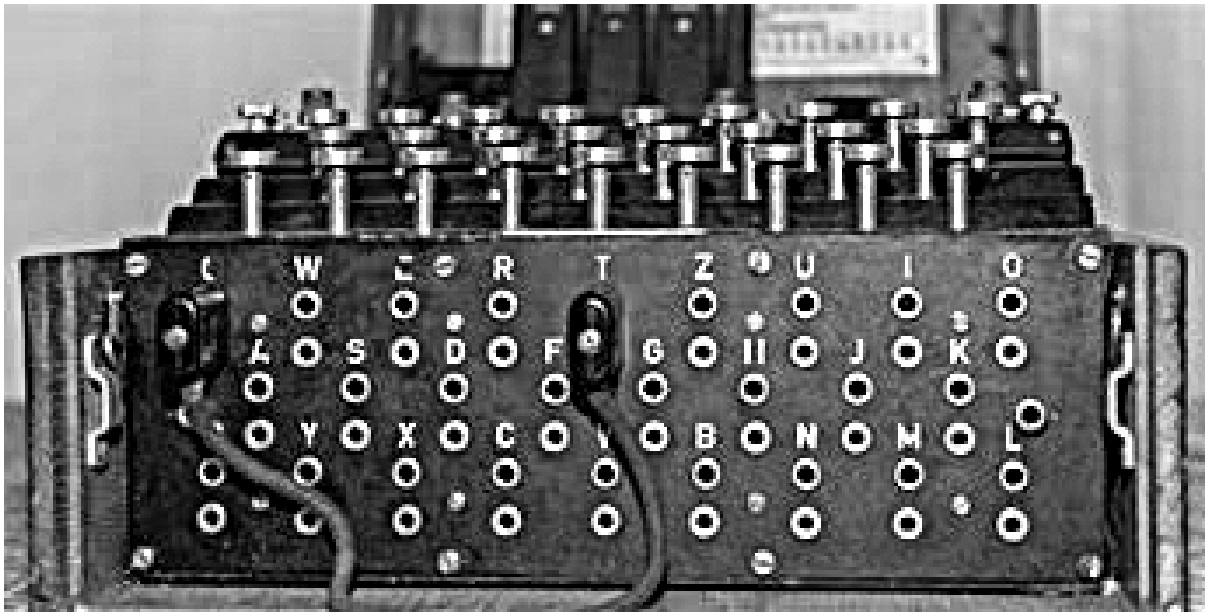


Il pannello di controllo

Esempio

Supponiamo che l'operatore connetta i fori corrispondenti alle lettere `Q` e `T`. Digitando sulla tastiera la parola `QUANTISTICO`, si otterrà una parola in cui le due lettere sono state scambiate:

$$\texttt{QUANTISTICO} \to \texttt{TUANQISQICO}$$



Il pannello di controllo

Esempio

Se ora l'operatore connette anche i fori corrispondenti alle lettere `I` e `P`, digitando sulla tastiera ancora la parola `QUANTISTICO`, questa volta si scambieranno tra loro le lettere `Q` e `T` e le lettere `I` e `P`:

$$\texttt{QUANTISTICO} \rightarrow \texttt{TUANQPSQPCO}$$

Attenzione: l'operatore non potrà connettere, ad esempio, le lettere `Q` e `P`, avendo già collegato i fori delle lettere `Q` e `T`.

Il pannello di controllo

Esempio

Se ora l'operatore connette anche i fori corrispondenti alle lettere I e P, digitando sulla tastiera ancora la parola QUANTISTICO, questa volta si scambieranno tra loro le lettere Q e T e le lettere I e P:

$$\texttt{QUANTISTICO} \rightarrow \texttt{TUANQPSQPCO}$$

Attenzione: l'operatore non potrà connettere, ad esempio, le lettere Q e P, avendo già collegato i fori delle lettere Q e T.

L'operatore può utilizzare da 0 a 13 cavi, connettendo solo coppie di lettere distinte: un cavo non può connettere una lettera con se stessa e due cavi non possono essere attaccati allo stesso foro. Quante sono le possibilità?

Il pannello di controllo

Se l'operatore utilizza 0 cavi, allora ha un solo modo per farlo.

Il pannello di controllo

Se l'operatore utilizza 0 cavi, allora ha un solo modo per farlo.

Se utilizza 1 cavo, allora stiamo scegliendo 2 lettere da un insieme di 26 lettere (l'ordine non è importante). Abbiamo così $\binom{26}{2}$ possibilità.

Il pannello di controllo

Se l'operatore utilizza 0 cavi, allora ha un solo modo per farlo.

Se utilizza 1 cavo, allora stiamo scegliendo 2 lettere da un insieme di 26 lettere (l'ordine non è importante). Abbiamo così $\binom{26}{2}$ possibilità.

E se utilizza 2 cavi? Avendo due cavi, possiamo connettere due coppie di lettere.

Esempio

In quanti modi possiamo connettere a coppie le quattro lettere `I`, `P`, `Q`, `T`?

{I,P} e {Q,T}, {I,Q} e {P,T}, {I,T} e {P,Q}.

Il pannello di controllo

(1) Abbiamo quindi scelto 4 delle 26 lettere a disposizione: $\binom{26}{4}$;

(2) in seguito, abbiamo scelto 2 di queste 4 lettere: $\binom{4}{2}$;

(3) infine, abbiamo scelto 2 delle 2 rimanenti lettere: $\binom{2}{2}$.

Non importa però l'ordine in cui scegliamo le nostre due coppie:

scegliere {I,P} e {Q,T} equivale a scegliere {Q,T} e {I,P}.

Otteniamo così:

$$\binom{26}{4}\binom{4}{2}\binom{2}{2}\frac{1}{2!} = \binom{26}{4} \cdot 3 = 44850$$

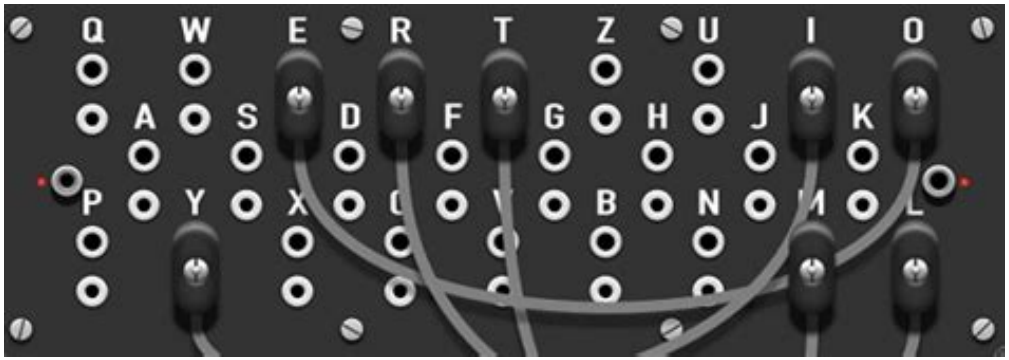
possibilità.

Il pannello di controllo

Quante possibilità abbiamo se si utilizzano 4 cavi?

Dobbiamo quindi scegliere 8 lettere e formare quattro coppie:

$$\binom{26}{8}\binom{8}{2}\binom{6}{2}\binom{4}{2}\binom{2}{2}\frac{1}{4!}$$



Osserviamo che

$$\begin{aligned}\binom{8}{2}\binom{6}{2}\binom{4}{2}\binom{2}{2}\frac{1}{4!} &= \frac{8!}{2!\,6!}\cdot\frac{6!}{2!\,4!}\cdot\frac{4!}{2!\,2!}\cdot\frac{2!}{2!\,0!}\cdot\frac{1}{4!}\\ &= \frac{8\cdot 7}{2}\cdot\frac{6\cdot 5}{2}\cdot\frac{4\cdot 3}{2}\,\frac{1}{4\cdot 3\cdot 2\cdot 1}\\ &= 7\cdot 5\cdot 3\cdot 1\end{aligned}$$

Il pannello di controllo

Conviene così introdurre una nuova notazione.

Definizione

Per ogni intero positivo n, scriveremo $n!!$ (doppio fattoriale) per indicare il seguente prodotto:

$$n!! = \begin{cases} n(n-2)\cdots 2 & \text{se } n \text{ è pari,} \\ n(n-2)\cdots 1 & \text{se } n \text{ è dispari.} \end{cases}$$

Esempio

Abbiamo

$$8!! = 8 \cdot 6 \cdot 4 \cdot 2$$

e

$$7!! = 7 \cdot 5 \cdot 3 \cdot 1.$$

Poniamo anche

$$(-1)!! = 1.$$

Il pannello di controllo

Possiamo così riscrivere

$$\binom{4}{2}\binom{2}{2}\frac{1}{2!} = 3 \cdot 1 = 3!! \quad \text{e} \quad \binom{8}{2}\binom{6}{2}\binom{4}{2}\binom{2}{2}\frac{1}{4!} = 7 \cdot 5 \cdot 3 \cdot 1 = 7!!$$

Il pannello di controllo

Possiamo così riscrivere

$$\binom{4}{2}\binom{2}{2}\frac{1}{2!} = 3\cdot 1 = 3!! \quad \text{e} \quad \binom{8}{2}\binom{6}{2}\binom{4}{2}\binom{2}{2}\frac{1}{4!} = 7\cdot 5\cdot 3\cdot 1 = 7!!$$

Quindi, potendo usare da 0 a 13 cavi, quante possibilità abbiamo?

$$\binom{26}{0}(-1)!! + \binom{26}{2}1!! + \binom{26}{4}3!! + \binom{26}{6}5!! + \binom{26}{8}7!! + \cdots + \binom{26}{26}25!!$$

In altre parole, abbiamo 532 985 208 200 576 possibilità (più di $5\cdot 10^{14}$).

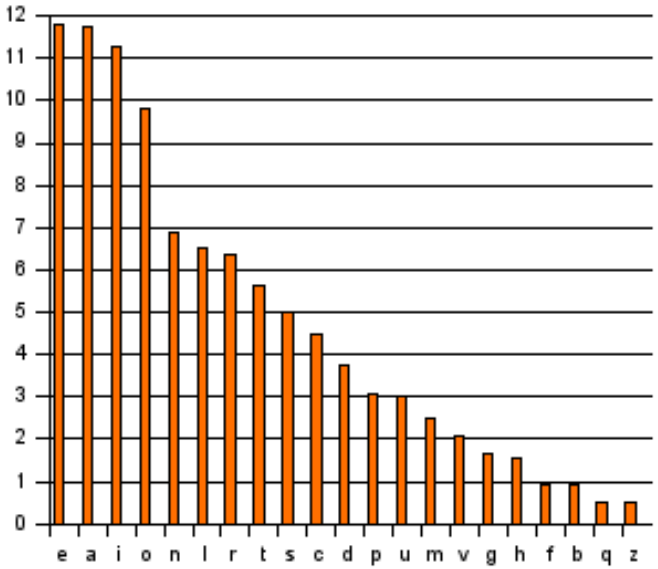
Per dare un'idea, la probabilità di fare 6 al SuperEnalotto è pari a 1 su

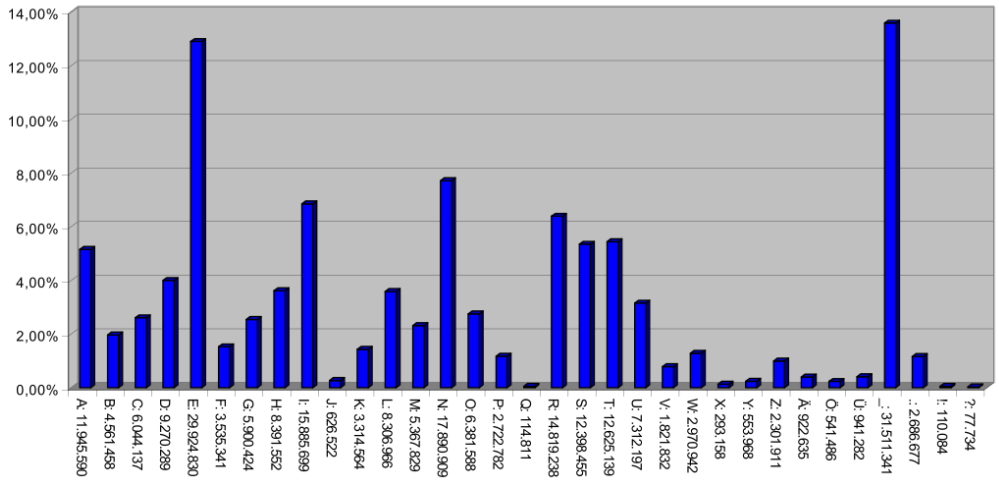
622 614 630.

Il pannello di controllo

Nonostante questo numero enorme di combinazioni, la sola presenza del pannello di controllo non garantisce una grande sicurezza.

Ogni lingua possiede infatti delle lettere che appaiono in un testo con maggior frequenza rispetto ad altre.





Il pannello di controllo

Se il testo è abbastanza lungo, o se si riescono a capire come sono cifrate alcune lettere, diventa allora facile decifrare l'intero testo.

3219. PAROLE CROCIATE CRITTOGRAFATE

1	2	3	4	5	■	4	5	4	3	■	4	6
6	7	8	3	■	4	1	■	9	■	10	5	7
11	9	7	■	12	7	12	12	13	4	7	9	3
5	■	6	4	7	14	14	7	12	5	8	11	1
■	6	14	5	4	3	7	15	3	6	11	7	■
16	1	9	16	5	11	11	7	9	3	5	■	■
■	9	3	16	15	5	11	11	5	9	6	3	■
2	5	9	3	15	15	3	1	■	7 A	4 C	9 R	5 E
1	15	5	■	1	15	■	■	2	■	1	3	15
6	15	■	3	■	3	8	10	3	7	■	10	3
6	7	13	8	7	■	2	7	6	3	15	5	7

I rotori

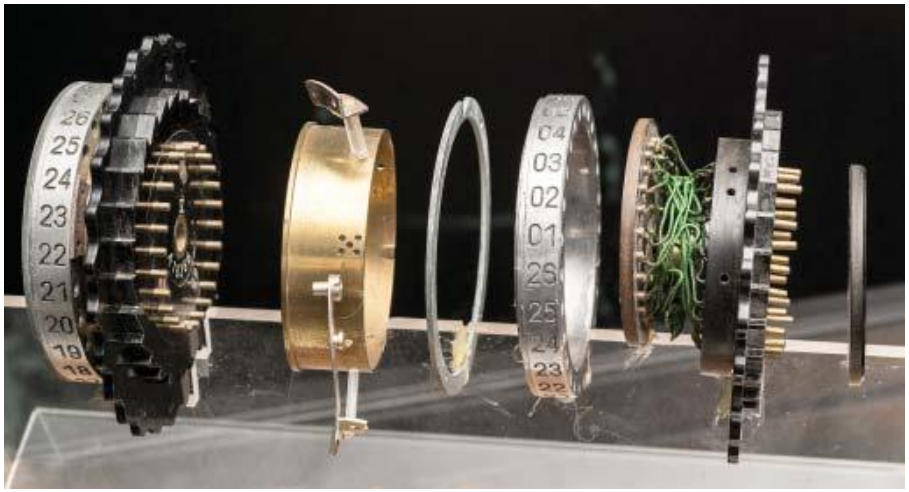
I rotori sono la seconda componente che contribuisce alla forza di Enigma. Ognuno di esso corrisponde a una permutazione delle 26 lettere dell'alfabeto, cioè a un loro riordino.

Esempio

A	B	C	D	E	F	G	H	I	J	K	L	M
O	U	N	D	K	T	I	Z	A	X	W	V	E

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	S	C	R	F	H	J	P	M	G	B	Y	Q

Ogni rotore realizza così uno qualsiasi dei $26!$ possibili riordinamenti delle lettere dell'alfabeto.

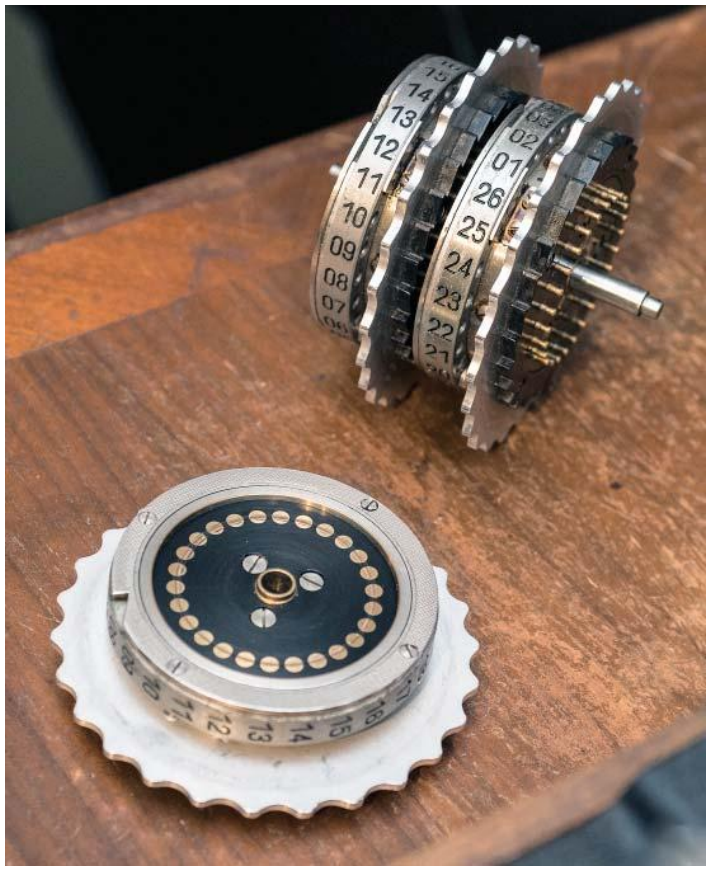


I rotori

Una macchina Enigma standard possedeva 3 rotori: abbiamo allora $(26!)^3$ possibili scelte. Tuttavia, i tedeschi utilizzavano sempre tre rotori distinti. Abbiamo così

$$(26!)(26! - 1)(26! - 2)$$

scelte possibili per i tre rotori distinti.



I rotori

Ora però dobbiamo posizionare i tre rotori nella macchina Enigma. L'operatore poteva ruotare i tre rotori scegliendo per ognuno di essi la posizione iniziale desiderata. Abbiamo così

$$26^3$$

possibilità.

Riassumendo, abbiamo finora ottenuto

$$(26!)(26! - 1)(26! - 2) \cdot (26^3)$$

possibili scelte per i tre rotori e le loro posizioni iniziali.

I rotori

Ogni volta che si preme un tasto, il rotore di destra ruota di una posizione. Ogni intera rotazione di questo rotore (sono stati quindi premuti i tasti 26 volte) forza la rotazione del rotore centrale. In modo simile, un'intera rotazione del rotore centrale forza la rotazione del rotore di sinistra (cioè il rotore di sinistra ruota di una posizione dopo che son stati premuti i tasti $26 \cdot 26 = 676$ volte). Questa rotazione avviene grazie a una tacca che però è posizionata in modo differente a seconda del rotore.

Senza le tacche, lettere uguali verrebbero cifrate in lettere uguali, permettendo così ancora un attacco tramite l'Analisi delle Frequenze.

Esempio

Nel rotore di tipo I, la tacca è posizionata in corrispondenza della lettera Q: se il rotore passa dalla lettera Q alla lettera R, il rotore posto alla sua sinistra, avanzerà di una posizione.

I rotori

Esempio

Se quindi la posizione iniziale del rotore I è alla lettera A, il rotore alla sua sinistra ruoterà di una posizione dopo 17 battute; se è posizionato alla lettera P, il rotore a sinistra ruoterà dopo 2 battute.

La tacca, in linea teorica, può essere posizionata in corrispondenza di una qualsiasi delle 26 lettere. Quella sul terzo rotore non ha alcun effetto. Pertanto, abbiamo 26^2 possibili scelte per le posizioni delle tacche sui primi due rotori.

Possiamo così concludere che i tre rotori distinti permettono, in linea teorica, le seguenti possibili scelte:

$$(26!)(26!-1)(26!-2)\cdot(26^5) =$$

$$779\,334\,352\,896\,580\,066\,161\,554\,254\,878\,325\,424\,489\,829\,948\,685\,613\,287\,168\,631\,295\,693\,655\,561\,016\,967\,168\,000\,000,$$

cioè più di $7 \cdot 10^{86}$ scelte.

Il riflettore

Il riflettore funziona come un pannello di controllo con 13 cavi inseriti. Ogni lettera è connessa con un'altra lettera tramite un cavo, causando uno scambio tra queste coppie di lettere. La differenza col pannello di controllo iniziale è che il riflettore non veniva cambiato. Abbiamo così

$$\binom{26}{26}(26-1)!! = 7\,905\,853\,580\,625$$

possibilità

Quante sono le possibili configurazioni?

Riassumendo, per recuperare un messaggio cifrato tramite Enigma dobbiamo essere in grado di capire

(1) quanti cavi sono stati utilizzati nel pannello di controllo;

(2) quali sono i tre rotori inseriti;

(3) quale è la posizione iniziale di ciascuno di questi tre rotori;

(4) come sono collocate le tacche sul primo e sul secondo rotore;

(5) la configurazione del riflettore.

Quante sono le possibili configurazioni?

Dobbiamo così comprendere quale sia la configurazione della macchina tra tutte le possibili

$$\left(\binom{26}{0}(-1)!! + \binom{26}{2}1!! + \binom{26}{4}3!! + \cdots + \binom{26}{26}25!!\right)$$

$$\cdot \left(26!(26! - 1)(26! - 2)(26^5)\right) \cdot (25!!) =$$

3 283 883 513 796 974 198 700 882 069 882 752 878 379 955 261 095 623 685 444 055 315 226 006 433 615 627 409 666 933 182 371 154 802 769 920 000 000 000

configurazioni; abbiamo cioè 1 su più di $3 \cdot 10^{114}$ (l'età dell'universo sarebbe di circa $3{,}2 \cdot 10^{22}$ secondi).

Se i tedeschi potevano configurare la loro macchina Enigma in più di 10^{114} modi diversi, come riuscirono allora gli Alleati a violare Enigma?

Hans-Thilo Schmidt

I primi che cercarono di capire il funzionamento di Enigma furono i polacchi che nel 1926 si accorsero come i tedeschi avessero cambiato i loro protocolli crittografici, rendendoli molto più sicuri.

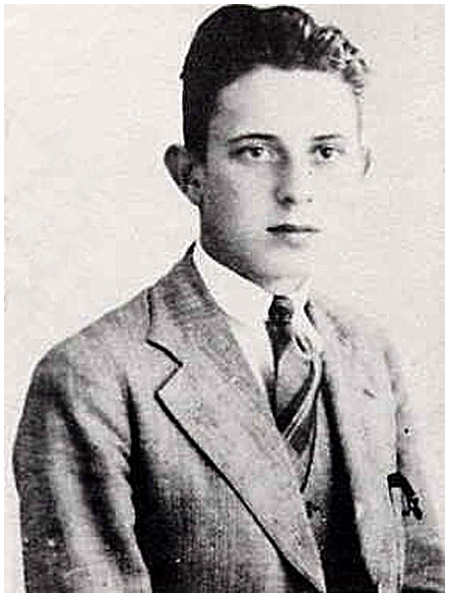
Poiché la versione commerciale di Enigma era molto diversa da quella usata dai tedeschi, i polacchi cercarono di capire come erano configurati i tre rotori.

Il primo vero passo avanti si ottenne quando Hans-Thilo Schmidt, fratello del responsabile della sicurezza delle comunicazioni tedesche, nel 1931 si incontrò in Belgio con un agente francese e per la cifra di 10 000 marchi permise all'agente di fotografare due manuali di istruzioni sull'uso di Enigma, senza però fornire particolari sui circuiti dei rotori.

Marian Rejewski

I francesi, ritenendo che Enigma fosse impenetrabile, abbandonarono la sfida. I polacchi invece, sentendosi minacciati da Russia e Germania, capirono che violare Enigma sarebbe stato fondamentale in un eventuale conflitto.

A tale scopo furono assunti nel 1932 tre matematici: Marian Rejewski (1905–1980), Jerzy Rozycki (1909–1942) e Henryk Zygalski (1908–1978).


Le chiavi di Enigma

Grazie alle varie informazioni raccolte, al suo lavoro e a un po' di fortuna, Rejevski riuscì a costruire una replica della macchina usata dai militari tedeschi: questo però non bastava per decifrare i messaggi senza possedere la chiave di cifratura.

Grazie ai documenti di Schmidt, i polacchi sapevano che ogni mese gli operatori di Enigma ricevevano un nuovo cifrario con le chiavi da usare di giorno in giorno, senza modificare l'assetto dei rotori.

Fino al 1938, un operatore di Enigma aveva a disposizione solo 6 cavi per il pannello di controllo e 3 rotori.

L'anello mobile

Per aumentare le possibilità offerte dai soli tre rotori, su ciascuno di essi vi è un anello mobile che ne modificava la posizione dell'anello alfabetico rispetto al cablaggio interno.

Esempio

Consideriamo ancora un rotore di tipo I. Posizionando l'anello in corrispondenza della lettera A, otteniamo

A	B	C	D	...	X	Y	Z
E	K	M	F	...	R	C	J

Posizionando invece l'anello sulla lettera B, il tutto verrà shiftato di una posizione:

B	C	D	E	...	Y	Z	A
F	L	N	G	...	S	D	K

Le chiavi di Enigma

Esempio

Il primo giorno del mese il cifrario poteva indicare:

Assetto del pannello di controllo:	A/L, P/R, T/D, B/W, C/U, O/Y
Disposizione dei rotori:	II, III, I
Posizione degli anelli:	U, A, Y;
Posizione iniziale dei rotori:	Q, C, W.

Chiaramente, usare la stessa chiave per tutti i messaggi di una stessa giornata rendeva Enigma meno sicura. Per aumentare la sicurezza delle loro comunicazioni, i tedeschi decisero di usare la chiave giornaliera non per trasmettere un messaggio completo, ma per trasmettere solo una seconda chiave (detta chiave di messaggio), diversa di volta in volta, da utilizzare per decifrare il resto del messaggio.

Le chiavi di messaggio utilizzavano gli stessi collegamenti del pannello di controllo e lo stesso ordine dei rotori, cambiava solo la posizione iniziale di questi ultimi.

La chiave di messaggio non si trovava nel cifrario, che elencava solo le chiavi giornaliere, ma andava comunicata di volta in volta al destinatario.

Rompere Enigma

Il procedimento era il seguente:

(1) il mittente regolava Enigma in base alla chiave giornaliera, compresa la posizione iniziale dei rotori:

Esempio

Assetto del pannello di controllo:	
Disposizione dei rotori:	II, III, I
Posizione degli anelli:	U, A, Y;
Posizione iniziale dei rotori:	Q, C, W.

(2) Decideva quindi la posizione iniziale dei rotori per la codifica vera e propria del messaggio (supponiamo PGH).

(3) L'operatore cifrava quindi il testo del messaggio PGH con i rotori ancora regolati su QCW.

Tuttavia, per garantire che la chiave di messaggio fosse ricevuta correttamente, la trasmetteva due volte: cifrava quindi PGHPGH. Il messaggio cifrato poteva essere del tipo IYWGDU: lettere uguali erano cifrate in lettere diverse, per sfuggire all'Analisi delle Frequenze.

Le chiavi di Enigma

Una volta regolati i rotori su PGH, l'operatore inviava il resto del messaggio. Il destinatario del messaggio aveva già Enigma regolata sulla chiave giornaliera e batteva il messaggio IYWGDU ottenendo PGHPGH. Regolava quindi i rotori su PGH e decifrava il resto del messaggio.

Questa procedura sembra molto sicura: usare la chiave di messaggio evitava che varie pagine di testo venissero cifrate tutte con la stessa chiave. Non avevano però fatto i conti con Rejewski e la sua squadra!

La strategia del matematico polacco si basava sul fatto che la ripetizione è nemica della sicurezza perché crea degli schemi. In particolare, in Enigma la ripetizione delle tre lettere della chiave di messaggio si rivelò essere un grave errore.

Ogni giorno Rejewski riceveva un pacco di messaggi intercettati, tutti con la doppia chiave di messaggio cifrata usando la chiave giornaliera.

Le chiavi di Enigma

Esempio

Per esempi poteva ricevere quattro messaggi del tipo

I	Y	W	G	D	U
D	I	T	Y	S	A
G	E	R	A	N	V
L	N	T	K	Q	A

Nel primo messaggio la stessa lettera era cifrata prima come I e poi come G. L'assetto della macchina doveva perciò essere tale da cifrare una lettera della chiave giornaliera come I e, dopo 3 scatti, come G.

Guardando solo i quattro messaggi, scopriamo così che:

1^a lettera	A	B	C	D	E	F	G	H	I	J	K	L	M
4^a lettera				Y			A		G			K	
1^a lettera	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4^a lettera													

Le chiavi di Enigma

Se in una giornata venivano intercettati abbastanza messaggi, Rejewski poteva completare la tabella.

Esempio

Ad esempio, poteva ottenere

1^a lettera	A	B	C	D	E	F	G	H	I	J	K	L	M
4^a lettera	I	X	V	Y	M	Q	A	P	G	F	U	K	J
1^a lettera	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4^a lettera	N	H	O	S	R	T	B	W	L	Z	E	C	D

Per determinare la chiave giornaliera, Rejewski iniziò a cercare regolarità:

Esempio

$$
\begin{aligned}
&\mathtt{A} \to \mathtt{I} \to \mathtt{G} \to \mathtt{A}\\
&\mathtt{B} \to \mathtt{X} \to \mathtt{E} \to \mathtt{M} \to \mathtt{J} \to \mathtt{F} \to \mathtt{Q} \to \mathtt{S} \to \mathtt{T} \to \mathtt{B}\\
&\mathtt{C} \to \mathtt{V} \to \mathtt{L} \to \mathtt{K} \to \mathtt{U} \to \mathtt{W} \to \mathtt{Z} \to \mathtt{D} \to \mathtt{Y} \to \mathtt{C}\\
&\mathtt{H} \to \mathtt{P} \to \mathtt{O} \to \mathtt{H}\\
&\mathtt{N} \to \mathtt{N}\\
&\mathtt{R} \to \mathtt{R}
\end{aligned}
$$

Le chiavi di Enigma

Fin qui abbiamo tenuto conto solo della prima e della quarta lettera. Il tutto però si ripeteva considerando la seconda e quinta lettera, e la terza e sesta lettera.

Rejewski si accorse che le concatenazioni cambiavano ogni giorno, a volte erano brevi a volte più lunghe: dipendevano dalla chiave giornaliera.

Capì anche che la lunghezza delle concatenazioni non dipendeva dal pannello di controllo.

Le chiavi di Enigma

Esempio

Se aggiungiamo il cavo HN:

$$
\begin{aligned}
&\mathtt{A} \to \mathtt{I} \to \mathtt{G} \to \mathtt{A}\\
&\mathtt{B} \to \mathtt{X} \to \mathtt{E} \to \mathtt{M} \to \mathtt{J} \to \mathtt{F} \to \mathtt{Q} \to \mathtt{S} \to \mathtt{T} \to \mathtt{B}\\
&\mathtt{C} \to \mathtt{V} \to \mathtt{L} \to \mathtt{K} \to \mathtt{U} \to \mathtt{W} \to \mathtt{Z} \to \mathtt{D} \to \mathtt{Y} \to \mathtt{C}\\
&\mathtt{H} \to \mathtt{P} \to \mathtt{O} \to \mathtt{H}\\
&\mathtt{N} \to \mathtt{N}\\
&\mathtt{R} \to \mathtt{R}
\end{aligned}
$$

diventa

$$
\begin{aligned}
&\mathtt{A} \to \mathtt{I} \to \mathtt{G} \to \mathtt{A}\\
&\mathtt{B} \to \mathtt{X} \to \mathtt{E} \to \mathtt{M} \to \mathtt{J} \to \mathtt{F} \to \mathtt{Q} \to \mathtt{S} \to \mathtt{T} \to \mathtt{B}\\
&\mathtt{C} \to \mathtt{V} \to \mathtt{L} \to \mathtt{K} \to \mathtt{U} \to \mathtt{W} \to \mathtt{Z} \to \mathtt{D} \to \mathtt{Y} \to \mathtt{C}\\
&\mathtt{N} \to \mathtt{P} \to \mathtt{O} \to \mathtt{N}\\
&\mathtt{H} \to \mathtt{H}\\
&\mathtt{R} \to \mathtt{R}
\end{aligned}
$$

Le chiavi di Enigma

Rejewski aveva pertanto trovato degli invarianti: il numero e la lunghezza delle concatenazioni.

Utilizzando le repliche di Enigma che avevano realizzato grazie al tradimento di Schmidt, i membri della squadra di Rejewski si divisero il compito di controllare quali concatenazioni si realizzavano per ogni possibile assetto di Enigma: fu un lavoro che richiese un intero anno.

Così facendo però Rejewski poteva controllare quali fossero i possibili assetti compatibili con la chiave giornaliera.

La presenza del pannello di controllo non rappresentava un ostacolo troppo difficile, poiché spesso si poteva desumere il senso del messaggio da una parziale decifrazione.

Rejewski realizzò un adattamento di Enigma in grado di controllare automaticamente e rapidamente i vari assetti dei rotori fino a trovare una corrispondenza con i dati forniti. Queste unità di calcolo, che lavoravano in parallelo, erano dette bombe.

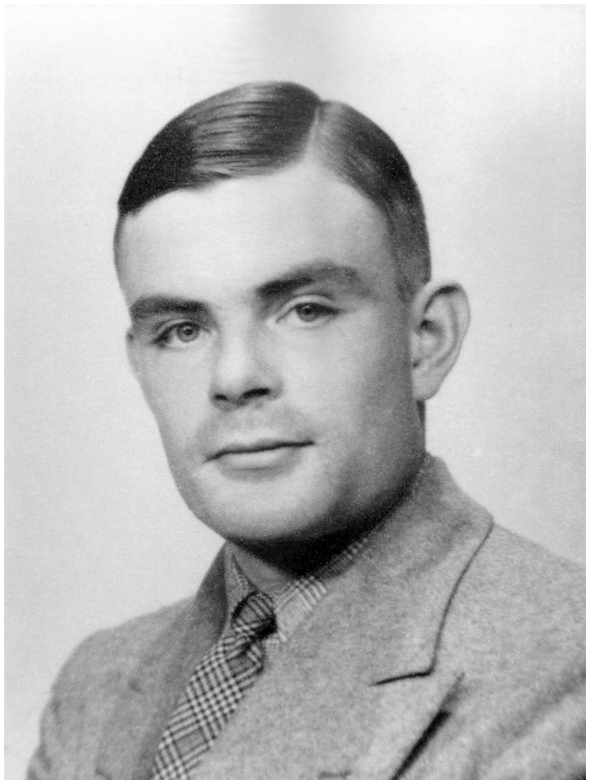
Enigma diventa più sicura

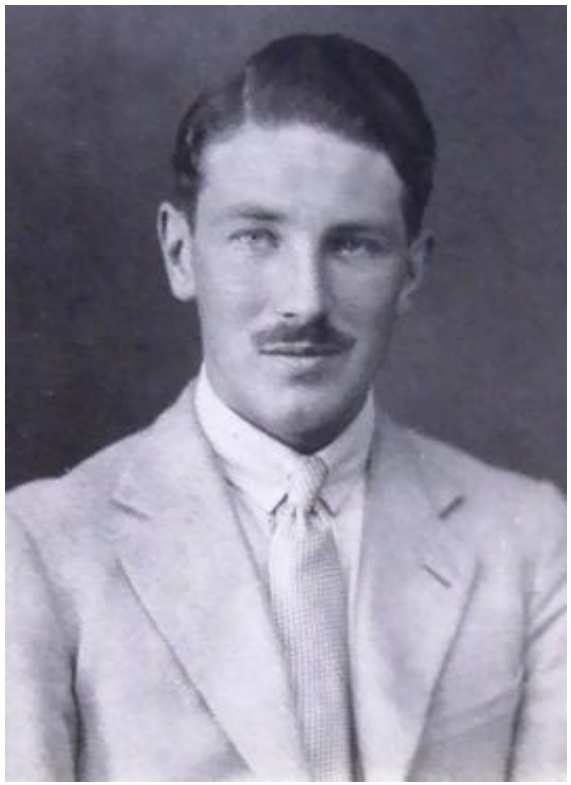
A partire dal dicembre 1938 i tedeschi aumentarono la sicurezza di Enigma: un operatore poteva ora scegliere 3 rotori tra i 5 a disposizione (la Marina ne aveva 8 a disposizione) e venivano utilizzati 10 cavi. Questo fece aumentare drasticamente il numero di possibilità.

Essendo ormai chiaro che la Germania avrebbe invaso la Polonia, il 30 giugno 1939 il responsabile del Biuru Szyfrów polacco contattò i colleghi francesi e britannici per metterli al corrente di come per circa 10 anni erano riusciti a violare Enigma, donando loro due riproduzioni di Enigma e i progetti di costruzione delle bombe di Rejewski.

Bletchley Park

Assimilata la strategia dei polacchi, i britannici assunsero vari matematici, tra cui Alan Turing (1912–1954) e Gordon Welchman (1906–1985). Nella nuova sede di Bletchley Park (dove lavoravano più di 8 000 persone), gli analisti britannici cominciarono a trovare nuove scorciatoie per scoprire le chiavi di Enigma, nonostante i tedeschi avessero abbandonato l'usanza di ripetere due volte la chiave di messaggio.





Cillies and Cribs

Per esempio, i britannici notarono che, invece di utilizzare come chiave una sequenza casuale di tre lettere, gli operatori Enigma tendevano a battere sequenze come `QWE` o `BNM`. In particolare, un operatore usava spesso le iniziali della fidanzata `CIL`: queste sequenze non casuali vennero così chiamate Cillies.

Turing e i suoi compagni svilupparono inoltre un nuovo metodo che sfruttava la presenza di quelle che sono note come crib. Un *crib* è una parola di cui si sospetta la presenza nel testo in chiaro.

Per esempio, uno dei crib più utilizzati dai britannici è la parola wetter (tempo atmosferico). Intercettando un messaggio proveniente da una stazione meteorologica, era molto probabile che il messaggio contenesse la parola wetter.

Crib

Questa volta, invece di cercare concatenazioni, Turing voleva trovare legami tra il testo in chiaro e quello cifrato.

Esempio

Supponiamo di sapere che la parola wetter sia stata cifrata come `ETJWPX`:

a	$a+1$	$a+2$	$a+3$	$a+4$	$a+5$
W	E	T	T	E	R
E	T	J	W	P	X

Osserviamo che la `W` viene cifrata come `E` e che la `E` viene cifrata come `T`. Quest'ultima viene cifrata come `W`, creando così un ciclo

$$\texttt{W} \to \texttt{E} \to \texttt{T} \to \texttt{W}$$

Si cercano quindi quali assetti dei rotori producano un tale ciclo.

Bletchley Park

Grazie a Alan Turing, i britannici realizzarono bombe che vagliavano le possibili configurazioni di Enigma. Ci vollero mesi per progettare queste macchine. Tuttavia, se all'inizio servivano sei settimane per realizzare una bomba, in seguito i britannici riuscirono a costruirne una alla settimana.

Qualche storico stima che il lavoro di Turing e degli altri analisti di Bletchley Park "accorciò" la Seconda Guerra Mondiale di due anni.

Fonti

- Simon Singh, Codici & Segreti, Rizzoli, 1999.
- Margaret Cozzens, Steven J. Miller, The Mathematics of Encryption, American Mathematical Society, 2013.
- A. Ray Miller, The Cryptographic Mathematics of Enigma, Center for Cryptologic History National Security Agency, 2019. `https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/CryptoMathEnigma_Miller.pdf`
- Jennifer Wilcox, Solving the Enigma: History of the Cryptanalytic Bombe, Center for Cryptologic History National Security Agency, 2006. `https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/solving_enigma.pdf`
- Immagini prese da Internet.

Grazie per l'attenzione!