



**procedimento
e programma di rottura**

Struttura

- *“Si è partiti dal presupposto, nel giudicare la sicurezza del crittosistema, che il nemico abbia a disposizione il congegno”*
- Componenti collegati da fili elettrici:
 - Visore che indica il testo cifrato
 - Tastiera in cui digitare il testo in chiaro
 - Tre scambiatori (rotori) che collegano la tastiera e il visore: qui avviene la cifratura
 - Riflettore

Rotori

- Primo rotore:
 - Avanzamento ad ogni digitazione
 - evita trasformazioni monoalfabetiche
 - Cifratura polialfabetica
 - ripetizione dell'alfabeto ogni 26 battute
- Secondo rotore:
 - Rotazione parziale ogni volta che il primo rotore completa un giro
 - $26 \times 26 = 676$ alfabeti cifranti

Rotori

- Terzo rotore:
 - Inserito per maggiore sicurezza
- La chiave di cifratura dipende dalla configurazione iniziale dei 3 rotori



Riflessore

- Sorta di rotore statico
- I fili elettrici escono dallo stesso lato di entrata del riflessore
 - l'impulso riattraversa i rotori e accende una lettera diversa
- Biunivocità della cifratura
 - Digitando testo in chiaro si ottiene testo cifrato e viceversa

Irrobustimenti a Enigma

- 5 rotori removibili e sostituibili
- Pannello a prese multiple tra tastiera e primo rotore
 - Utilizzo di cavi con spinotti per scambiare 2 lettere prima dell'immissione nel rotore
 - Scambio di massimo 6 coppie di lettere
 - Sostituzioni inalterate durante la cifratura

Numero di chiavi

- Rotori:
 - $26 \times 26 \times 26 = 17.576$ assetti
- Unità cifratrice:
 - $3! = 6$ posizioni dei rotor
- Pannello a prese multiple:
 - 100.391.791.500 combinazioni

Circa *10 milioni di miliardi* di configurazioni

Cifratura del messaggio

- Distribuito un blocco contenenti le chiavi giornaliere indicanti l'assetto iniziale
 - Assetto del pannello a prese multiple
 - Disposizione degli scambiatori
 - Orientamento degli scambiatori
- Stessa chiave per lo scambio di centinaia di messaggi
 - creazione di una “chiave di messaggio” di 3 lettere (= n. rotori)

Cifratura del messaggio

- Il mittente regola l'assetto dei rotori come richiesto dal cifrario
- Definisce la chiave di messaggio
- Cifra la chiave di messaggio (ripetuta 2 volte) con la chiave giornaliera
- Modifica l'assetto della macchina secondo la seconda chiave e cifra il messaggio

Breccia nel sistema (1)

- Basata sullo studio della ripetizione della chiave di messaggio
- Legame tra assetto iniziale e lettera 4
 - ricerca dell'assetto che inizia con L1 e dopo 3 avanzamenti porta la medesima lettera in L2
- Tabella degli abbinamenti tra L1 e L2
- Controllo delle concatenazioni di lettere
 - num. di collegamenti in una concatenazione indipendente dalle prese multiple

Breccia nel sistema (1)

- Creazione di un “database” delle lunghezze delle concatenazioni (uniche) e dei relativi assetti
- Controllo sul testo decrittato delle lettere scambiate

Rottura del sistema (2)

- Successivamente ad un irrobustimento di Enigma da parte dei tedeschi
 - 4 rotori a scelta su un set di 8 (Enigma navale)
 - 2 riflessori
 - 14 prese multiple
 - chiave di messaggio inviata una sola volta
- Ad opera dei crittografi inglesi di Bletchley Park
 - A. Turing

Rottura del sistema (2)

- Basato sulla debolezza che nessuna lettera può comparire nel testo cifrato come se stessa
- Ricerca di cribs per ottenere la chiave
 - porzioni di testo in chiaro interpretato in base a considerazione non crittoanalitiche
 - messaggi meteo
- Ratto dei cifrari dagli U-boot tedeschi

Principali errori

- Cifratura anche dei messaggi che non necessitano di essere occultati
- Grande mole di dati cifrati ogni giorno

Bibliografia

- “Codici & Segreti”, Simon Singh, 1999.
- Wikipedia

