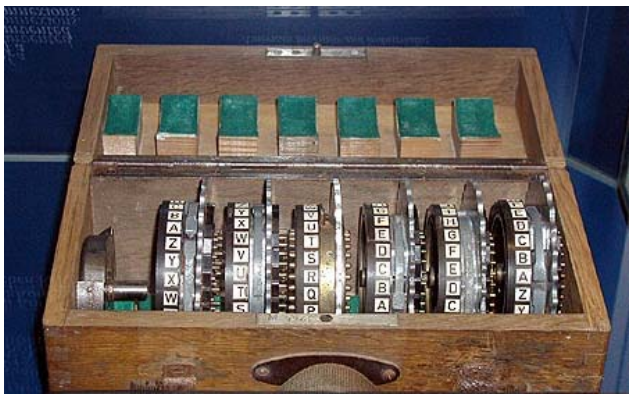
Cenni storici della macchina Enigma

Nella prima metà del XX secolo cominciarono a diffondersi macchine cifranti a rotori, utilizzate, poi, fino all'introduzione dei cifrari elettronici e microelettronici, che hanno sconvolto il mondo della cittrografia.



La più celebre è ***Enigma***, inventata nel 1916 dal tedesco Arthur Scherbiuse, poi modificata secondo varie versioni.

Egli creò a Berlino una società per produrre tale dispositivo e la prima versione commerciale fu venduta nel 1923.

Diversi esemplari furono acquistati dalla Marina Militare tedesca nel 1926, poi, nel 1929, la macchina fu acquisita dall'Esercito, da ogni organizzazione militare tedesca e dalla maggior parte della gerarchia nazista.

Versioni di ***Enigma*** furono usate, durante la II guerra mondiale, per quasi tutte le comunicazioni militari.

***Enigma*** è un dispositivo elettromeccanico per cifrare e decifrare messaggi; è una macchina simmetrica, nel senso che se la lettera A è cifrata con la G in una certa posizione del testo, allora nella stessa posizione la G sarà cifrata con la A.

E' questa una grossa comodità operativa, ma anche una debolezza e un limite crittografico.

La macchina ha al suo interno un certo numero di rotori collegati elettricamente e liberi di ruotare; quando l'operatore preme un tasto un segnale elettrico passa da rotore a rotore fino a quello finale, detto *riflettore*, e quindi torna indietro a mostrare una lettera che si illumina e rappresenta il carattere cifrato.

Non esiste, però, possibilità di stampa e, dunque, l'operatore deve copiare a mano, carattere per carattere, il messaggio cifrato da trasmettere.

La chiave dell'***Enigma*** è la disposizione iniziale dei rotori, tale chiave veniva cambiata ogni 24 ore secondo una regola prestabilita e quindi questa regola era la vera chiave segreta.

I rotori si potevano scambiare tra loro; pertanto, se essi erano *n*, le disposizioni possibili erano *n! (n fattoriale = n! = 1 · 2 · … · n)*.

I tedeschi erano convinti che l'***Enigma*** fosse inattaccabile.

Ma già nei primi anni '30 i matematici polacchi Rejewski, Zigalski e Rozicki erano riusciti a ricostruire la struttura dei rotori e a decrittare i messaggi, sfruttando le debolezze intrinseche del dispositivo, tra le quali il fatto che nessuna lettera poteva

mai comparire nel testo cifrato come se stessa, e alcune ingenuità degli stessi cifratori.
I tedeschi però cambiarono il funzionamento di ***Enigma*** introducendo un set di cinque rotori, di cui ne venivano usati tre diversi ogni giorno: ciò moltiplicava per 60 le combinazioni possibili, rendendo vani gli sforzi dei matematici polacchi.
Il 25 luglio 1939, nell'imminenza dell'attacco tedesco alla Polonia, si tenne a Varsavia una riunione tra gli uffici cifra polacchi, francesi ed inglesi, nella quale i polacchi misero a disposizione degli alleati i loro metodi per forzare ***Enigma***.
Nello stesso anno gli inglesi avevano trasferito nel villaggio di Bletchley Park, a metà strada tra Oxford e Cambridge, la sede del loro servizio di decrittazione , noto con il nome di *Ultra*. Partecipava attivamente alle ricerche, per conto del governo inglese, Alan Turing.


Noto come padre dell'informatica teorica, egli è stato autore di ricerche estremamente raffinate e molto profonde sul concetto logico – matematico di *calcolabilità*; lo strumento che concretizzò tali ricerche è noto oggi come *macchina di Turing*. Essa non possiede valvole, transistor o circuiti integrati, ma è una struttura *astratta* e meramente ideale.
Turing ideò, per la decrittazione, nuove e più efficienti *bombe crittologiche*, i *Colossi*, cosicché ***Enigma*** venne sistematicamente forzata: nel 1942 si arrivò a decrittare più di 8000 messaggi cifrati tedeschi al mese.