pagina Q hmr Quattro chiacchiere sul calcolo, senza fare conti

# The Imagination Game, cap. 3 L'Enigma

*N. 35, 15 marzo 2015*
*di Giovanni A. Cignoni*

Dopo le persone e i luoghi tocca a lei, la macchina, indiscussa protagonista femminile della storia: l'*Enigma*. Non ce ne voglia la graziosa Keira, d'altra parte anche agli Academy Awards era stata nominata "solo" come supporting actress :)

L'Enigma è il nemico da battere, l'entrata in scena è degna di una dark lady, nera e misteriosa, "beautiful" mormora un rapito Turing. È una della più belle immagini del film, studiata nella fotografia e nel significato: lei al centro dell'inquadratura, intorno gli altri, tutti uomini, affascinati e spaventati.

La protagonista femminile del film: l'Enigma

Certo come problema Enigma faceva paura. Ma come macchina era un po' meno segreta e un po' meno unica di come viene presentata nel film. I brevetti erano depositati sin dal 1919, in Germania, ma poi anche in Olanda, Inghilterra, Francia, USA e Svizzera.

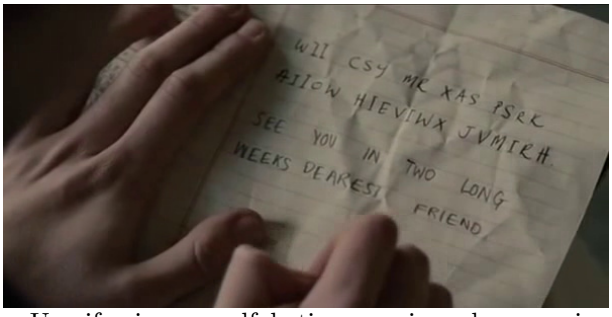
L'aveva progettata Arthur Scherbius, che aveva anche fondato la *Chiffriermaschinen AG* per produrla. Scherbius vide i primi successi commerciali della sua creatura, ma morì nel 1929 in un incidente di carrozza.

L'Enigma era sul mercato dal 1923, venduta a banche, finanzieri e industrie che la usavano per proteggere le loro comunicazioni quando dovevano affidarle ai servizi telegrafici.

I primi modelli di Enigma erano stampanti: il messaggio cifrato usciva comodamente su carta. Nel 1924 arriva l'Enigma C la prima con lo schermo luminoso. Il messaggio va trascritto a mano lettera per lettera via via che viene cifrato: noioso e fonte di possibili errori, ma così la macchina costa meno ed è portatile. Con il modello C l'Enigma acquista anche la sua forma inconfondibile, condivisa da tutte le versioni successive che sono distinguibili solo nei dettagli.

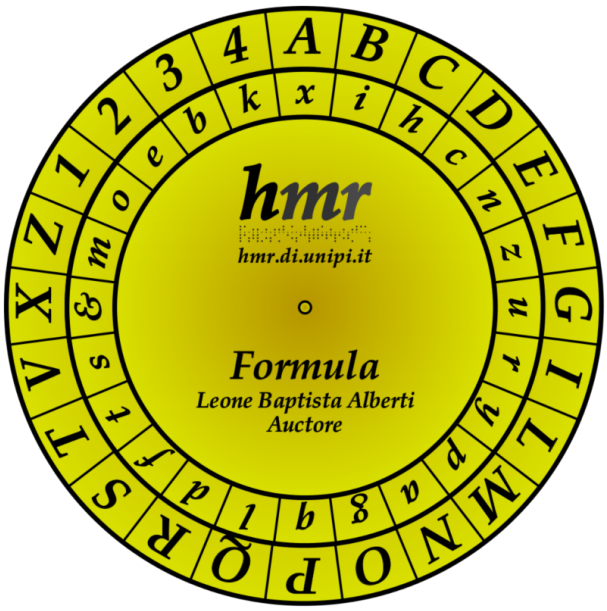
È l'Enigma D che attira le attenzioni dei militari tedeschi. Nel 1927 una sua versione, denominata progetto *Ch11a*, è la prima Enigma in uniforme. L'arruolamento definitivo è con l'*Enigma I* realizzata a partire dal 1932 e adottata dalla *Wehrmacht* (l'esercito) e dalla *Luftwaffe* (l'aviazione). Infine, nel 1934 anche la *Kriegsmarine* (la marina) vuole la sua. La marina sarà il cliente più esigente, con quattro modelli, prima *M1*, *M2*, e *M3* fra loro praticamente indistinguibili, e poi, dall'inizio del 1942, la *M4*, quella usata dagli *U-Boot*: questa Enigma tenne per un po' in scacco gli Alleati ed era la macchina da battere nel frammento della storia di Bletchley Park raccontato il film.

Il film, fra le righe, ci regala anche qualche lezione di crittografia. Il giovane Alan parte dalle basi e al college, con l'amato Christopher Morcom, usa un semplice *cifrario monoalfabetico*: ogni lettera viene sempre scambiata con la stessa lettera. Un sistema pratico, ma facilmente attaccabile sfruttando la frequenza delle lettere. Per esempio in Inglese la lettera più frequente è la 'e'. Nel cifrato di Morcom la lettera che compare più spesso è la 'I', ce ne sono ben sette. Secondo voi a cosa corrisponderà?




Un cifrario monoalfabetico, un gioco da ragazzi

Ancor più sottile e delizioso è l'accenno al cifrario usato da Cairncross. Lo cita Hugh Alexander quando dice ad Alan di sapere già che lui non è la spia russa perché usava un "troppo semplice" cifrario *Beale*. Il cifrario Beale esiste e cela le indicazioni per trovare un favoloso tesoro sepolto da qualche parte nella contea di Bedford in Virginia, ma non è mai stato decifrato, anche perché con ogni probabilità è una beffa. Ma molti continuano a provarci e altrettanti si aggirano dalle parti di Bedford con una vanga in mano.

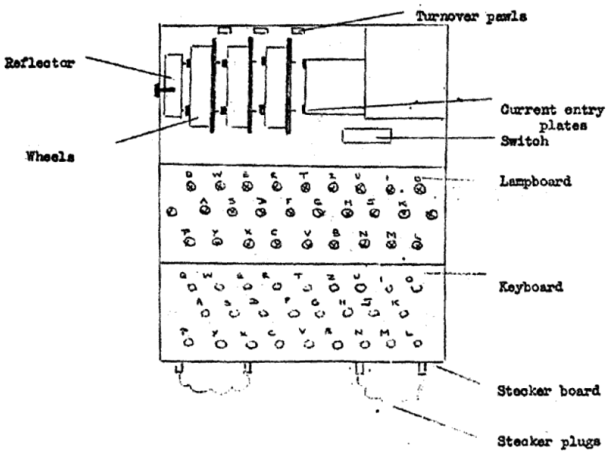



Il disco cifrante di Leon Battista Alberti, nella riproduzione da ritagliare di HMR

Fra il banale cifrario monoalfabetico, usato già da Giulio Cesare, e l'impossibile Beale, la storia della critto-

grafia è lunga. Nel mezzo, a partire dal Rinascimento, ci sono i cifrari *polialfabetici*. L'idea di base è sostituire occorrenze della stessa lettera con lettere diverse, così da vanificare i tentativi di decifrazione basati sulla frequenza delle lettere. Uno degli esempi più noti è la *Formula*, il disco cifrante di Leon Battista Alberti.

L'Enigma segue lo stesso principio del disco dell'Alberti: periodicamente cambia la corrispondenza fra le lettere in chiaro e le lettere cifrate. L'Alberti aveva pensato a un disco solo, le Macchine come Enigma per complicare la faccenda ne avevano più di uno, si chiamavano rotori e non c'era bisogno di girarli a mano.




L'Enigma I, in un disegno di Alexander, in alto i rotori (wheels) che cambiano le corrispondenze fra le lettere in chiaro e quelle cifrate

Battere l'enigma fu davvero una sfida, nel film sembra un round solo, giocato dalla squadra di Turing, ma ce ne furono molti, perché c'erano più modelli di Enigma, i modi di usarle erano diversi da comando a comando e venivano cambiati nel tempo – e solo i crucchi di Hollywood sono così tonti da mettere proprio il saluto al Fürher in coda a tutti i messaggi. E a lottare e a vincere non fu solo il gruppo di Turing, le Dilly's Filles per esempio le abbiamo già citate.

L'Hilton del film al lavoro con uno *Zygalski sheet*, anche se fra le righe, è un riconoscimento al contributo dei crittografi polacchi

Il primo round gli Alleati se lo aggiudicarono per merito dei Polacchi del *Biuro Szyfrów*. Marian Rejewski, Henryk Zygalski e Jerzy Rozycki furono i matematici che già prima della guerra leggevano con successo le comunicazioni tedesche crittografate con Enigma. A Bletchley Park partirono dai loro metodi e dalle loro macchine, aggiornandoli e migliorandoli per star dietro alle mutazioni di Lady Enigma. Nel film i Polacchi avrebbero meritato un po' di più di poche battute e qualche sottile indizio sulle scrivanie.

Per finire un numero. Vero, la promessa di questa serie di articoli è di parlare di calcolo senza fare conti, ma, giuro, mi fermo al numero, senza insistere tanto su come è ottenuto.

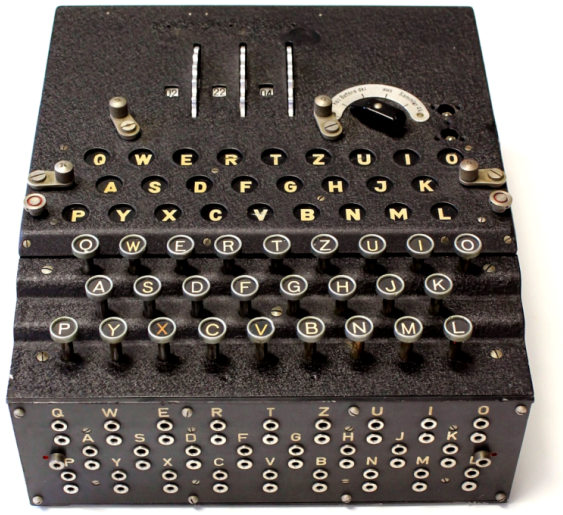
La forza di Enigma e degli altri sistemi crittografici simili non è nella macchina: Enigma era un prodotto commerciale, il suo funzionamento era noto. Le versioni militari erano un po' diverse, ma erano così capillarmente diffuse che molte furono catturate dagli Alleati in operazioni di guerra. La forza era nelle impostazioni che determinavano come la macchina cambiava la corrispondenza fra le lettere in chiaro e le lettere cifrate. Più sono le possibili impostazioni e più il sistema crittografico è sicuro perché più è il tempo che si impiega a trovare quella giusta. Il tempo di cui si parla non è molto: all'Enigma erano affidate comunicazioni tattiche che in poche ore perdevano ogni valore, e i Tedeschi cambiavano le impostazioni ogni giorno.

Il numero delle possibili impostazioni di Enigma ci dice quanto è grosso il pagliaio in cui, ogni giorno, a Bletchley Park cercavano l'ago che permetteva di bucare il sistema tedesco.

Nel film dicono *159 milioni di milioni di milioni*. È lo stesso di 159 miliardi di miliardi, ma, ovviamente, la tripla ripetizione fa più effetto.

Il numero è giusto per una Enigma I, quella che si vede nel film e che, grazie agli amici del Museo Storico della Comunicazione di Roma abbiamo al Museo in questi giorni. Non è facile calcolarlo, bisogna conoscere bene l'Enigma, diverse fonti, anche autorevoli, riportano cifre vicine, ma di fatto sbagliate. Quindi bravi gli sceneggiatori che hanno scelto proprio il numero giusto. Peccato abbiano sbagliato Enigma.

Contro l'Enigma I di Wehrmacht e Luftwaffe lavorava Hut 6, quello di Welchman. Il film è centrato sulle vicende dell'Hut 8 di Turing contro l'Enigma degli U-Boot, cioè la M4, il cui numero di impostazioni possibili era *46 milioni di milioni di miliardi*.



L'Enigma I oggi al Museo, come quella del film, ma non l'Enigma M4 usata dagli U-Boot