pagina Q hmr Quattro chiacchiere sul calcolo, senza fare conti

# The Imagination Game, cap. 4
# Le altre macchine

*N. 36, 22 marzo 2015*
*di Giovanni A. Cignoni*

Dell'Enigma e di come è stata battuta abbiamo detto. E poi? Solo i Tedeschi crittavano e solo gli Inglesi a Bletchley Park decrittavano? E quel *Colossus* ricordato spesso quando si parla di Bletchley Park cos'era e cosa faceva? E il *Christopher* del film era "una macchina" di Turing o era "la Macchina" di Turing? E quali erano le macchine di Turing? E, a proposito, cosa fa una Macchina di Turing?

Una cosa per volta. Ovviamente, anche gli Alleati avevano i loro sistemi crittografici e, altrettanto ovviamente, i Tedeschi si davano da fare per violarli. Da questo lato della barricata però è mancata una protagonista dal nome enigmatico e nessuno probabilmente ci farà mai un film.

Gli Americani avevano una macchinetta sfiziosissima che però si perde fra troppe asettiche sigle: *C-38* per il produttore, *M-209* e *M-210* le due versioni adottate dall'US Army, *CSP-1500* quella dell'US-Navy. Era stata progettata da Boris Hagelin uno dei tanti svedesi maghi della meccanica di precisione – al Museo trovate nella storia delle calcolatrici diversi connazionali: Odhner, Sundstrand, Friden. La C-38 era completamente meccanica, non aveva bisogno di alimentazione elettrica (un bel vantaggio) e il cifrato (o il decifrato) usciva comodamente stampato su un nastrino di carta. Come l'Enigma era usata per le comunicazioni tattiche. E stava in un tascapane.

L'Enigma americana, la piccola di Hagelin

Per le comunicazioni strategiche gli Americani usavano invece la *SIGABA*, il cui brutto nome non è neanche un acronimo, ma una parola costruita a caso per rendere il più possibile anonimo il progetto, ottimo ai fini della riservatezza, pessimo per suscitare l'interesse di scrittori e sceneggiatori. La SIGABA era probabilmente la più sofisticata delle macchine del tempo, fra tutte l'unica che, a quanto risulta, non è mai stata violata. Segretissima, era usata ai massimi livelli, inclusa la corrispondenza fra Roosevelt e Churchill, ma a Londra era usata da personale americano e agli Inglesi non fu mai fatta vedere. La *National Security Agency* ha concesso la liberatoria per brevettare la SIGABA, rendendone pubblico il funzionamento, solo nel 2001.

Fra gli Inglesi la macchina più usata era la *TypeX*. Derivata dall'Enigma commerciale, intorno al 1937 fu adottata dalla Royal Air Force e designata "RAF Enigma with Type X attachments". A Bletchley Park, una volta scoperte le impostazioni giornaliere dell'Enigma, i messaggi intercettati venivano decodificati al volo dalle Wrens usando proprio le TypeX.

Una TypeX di Bletchley Park, modificata per essere usata come una Enigma

Sul fronte dell'Asse decrittavano, ma non ci furono clamorosi successi né strutture organizzate e complesse come Bletchley Park. I Tedeschi avevano i loro criptoanalisti, ma erano sparpagliati qua e là; Wehrmacht, Luftwaffe, Kriegsmarine, Abwehr, Reichspost: ognuno aveva il suo servizio alla faccia della proverbiale organizzazione teutonica. In qualche occasione però riuscirono a violare le comunicazioni tattiche degli Alleati: durante la Battaglia dell'Atlantico il *B-Dienst* della Kriegsmarine leggeva con frequenza le comunicazioni dei mercantili alleati. E bucarono diverse volte anche la piccola C-38.

Veniamo al *Colossus*. È una macchina importante di Bletchley Park, ma non è citata dal film. Plauso agli sceneggiatori che hanno resistito alla tentazione di mettere in scena "Colossus vs Enigma", un match di grande richiamo a partire dai nomi, già sfruttato in molte rivisitazioni fantasiose della storia di Bletchley Park, ma storicamente falso: Colossus vs Enigma non è mai stato disputato. Né poteva esserlo: pesi diversi. Con l'Enigma combatterono, in più riprese, solo le *Bombe*. Il Colossus c'era (anzi ce ne erano una decina), ma con la *Tunny Machine* e *Heath Robinson* fu il campione della squadra di macchine che Bletchley Park mise in campo per combattere nella categoria "comunicazioni strategiche". Il campione teutonico contro cui combatté Colossus era un'altra macchina cifrante: la *Lorenz SZ 40/42*, in pratica l'analoga tedesca della SIGABA americana. Per la cronaca, grazie principalmente a Max Newman, Ralf Tester, Bill Tutte e Tommy Flowers, la squadra di Bletchley Park vinse ancora una volta. Il buon Alan fu coinvolto, il suo contributo fu un metodo per abbattere il numero di impostazioni della Lorenz da far provare ai Colossi.

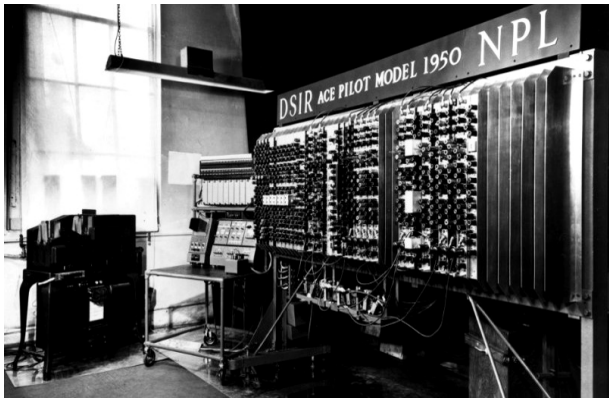
Abbiamo citato le Bombe, inventate dai Polacchi, riprogettate da Turing, Welchman e Keen, poi migliorate ancora dagli Americani. Abbiamo già detto che ce

ne erano parecchie: a fine guerra se ne contavano 209 in Inghilterra e 160 in USA. Nel film se ne vede una, Christopher. Licenza poetica e numeri a parte, ci preme dire che le Bombe non erano calcolatori. Neanche il Colossus e le altre macchine di Bletchley Park erano calcolatori. Né lo erano le varie macchine cifranti. Non lo erano perché erano macchine specializzate: facevano una cosa sola, mentre i calcolatori fanno cose diverse in funzione del programma che eseguono.

Il Turing del film con la v. 2.0 di Christopher, fantasiosamente homemade

Insomma, in tutta la storia di Bletchley Park non c'è un calcolatore (no computer, se preferite l'inglese). I calcolatori verranno dopo. Poco dopo, ma dopo.

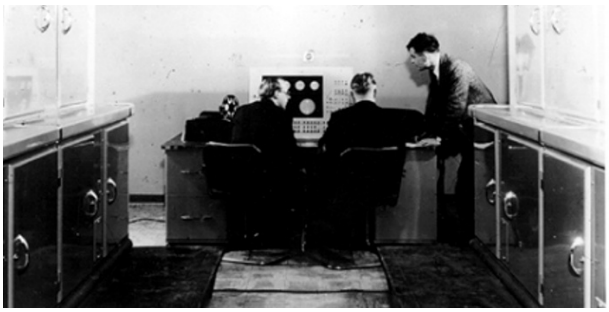
In Inghilterra i primi a muoversi furono l'Università di Cambridge, l'Università di Manchester e il National Physical Laboratory. Turing lo troviamo in due su tre. Il calcolatore *ACE* del NPL lo progetta proprio lui nel 1946, ma ci sono difficoltà tecnologiche ed economiche per realizzarlo: lo completeranno solo nel 1950, senza Turing e in una versione ridotta, il *Pilot ACE*.




Il Pilot ACE progettato da Turing all'NPL e lì costruito, ma senza di lui

Un po' scontento di come va all'NPL, Alan nel '48 si sposta a Manchester dall'amico Newman (sì, quello del Colossus). Lì sono un pezzo avanti: Frederic Williams e Tom Kilburn hanno messo a punto una buona soluzione per realizzare la memoria, l'hanno appena sperimentata con successo sulla *Small Scale Experimental Machine*, detta "Baby", e stanno costruendo un secondo calcolatore full optional: la Manchester Automatic Digital Machine, detta "Mad'm". Turing lavorerà alla programmazione della macchina.

Quindi pensando a calcolatori veri, con valvole e cavi, ACE e Mad'm sono macchine che a buon titolo possono essere considerate "di Turing", ma non li costruì in casa e, soprattutto, non fece tutto da solo: uno lo progettò e se ne andò prima che lo costruissero, un altro lo trovò fatto e lo programmò (ma non solo lui).



Turing alla consolle del calcolatore di Manchester

La *macchina di Turing* invece non ha né valvole né cavi. È un modello concettuale che Turing usò per dimostrare che l'*Entscheidungproblem* di Hilbert non può essere risolto. Succedeva nel 1936 e, di nuovo, Turing non era solo: poco prima Alonso Church aveva fatto lo stesso, ma con il *λ-calcolo* come modello concettuale.

Aver dato una risposta (per quanto negativa) al problema di Hilbert è un bel risultato, ma diventarono altrettanto importanti gli strumenti usati.

Turing andò a fare il dottorato con Church e i due, con Stephen Kleene e qualche altro, arrivarono a stabilire che la macchina di Turing (o il λ-calcolo) sono ottimi modelli per definire l'insieme dei calcoli effettivamente... calcolabili.

Per calcolo non si intende solo un'operazione aritmetica, ma qualsiasi procedimento che da un po' di simboli in ingresso produce un po' di simboli in uscita che, per noi, significano la soluzione di un problema.

La calcolatrice che fa 2+2=4 fa un calcolo, cifre e segni di operazione sono i simboli in gioco. L'Enigma, la SIGABA e simili cifrando i caratteri (altri simboli) di un messaggio fanno un calcolo, la Bombe e il Colossus cercando pezzi di testo noti nei messaggi cifrati fanno un calcolo, Google mostrandoci tutte le pagine web che contengono la parola che ci interessa fa un calcolo, il pc che impagina il testo che sto scrivendo fa un calcolo, la playstation fa un calcolo. Sono calcoli diversi, ovviamente, parecchio complicati anche, ma per ognuno di essi c'è sempre una particolare macchina di Turing (o una particolare formula in λ-calcolo) che fa proprio quel calcolo.

Fra i tanti calcoli ce ne è uno davvero interessante: è quello capace di leggere la descrizione di una qualsiasi macchina di Turing ed eseguire il calcolo ad essa associato. Come tutti i calcoli, anche questo interessante calcolo può essere espresso da una particolare macchina di Turing: la *Macchina di Turing Universale*. Che, con la 'M' maiuscola, è un buon modello dell'idea di *calcolatore programmabile*, capace cioè di eseguire (purché opportunamente istruito) tutti i calcoli effettivamente calcolabili. Una potenza.

Quindi, il primo Christopher, la Bombe, non era la Macchina di Turing, perché facendo solo il calcolo della Bombe non è universale e non merita la maiuscola. Ma esiste una macchina di Turing Christopher. E, si può istruire la Macchina di Turing affinché si comporti proprio come Christopher.

Se siete arrivati fin qua, Cinzia paga da bere :)