Le altre macchine, The Imagination Game, capitolo 4

Author : Redazione

Date : 22 marzo 2015

Dell'Enigma e di come è stata battuta abbiamo detto. E poi? Solo i Tedeschi crittavano e solo a Bletchley Park decrittavano? E cosa faceva quel *Colossus* ricordato spesso quando si parla di Bletchley Park? 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 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 faccenda però manca 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 sigle: *C-38* per il produttore, *M-209* per l'US Army e *CSP-1500* per l'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* non aveva bisogno di alimentazione elettrica e il cifrato usciva comodamente stampato su un nastrino di carta. Come l'Enigma era usata per le comunicazioni tattiche. E stava in un tascapane.

Per le comunicazioni strategiche gli Americani usavano invece la *SIGABA*, il cui brutto nome non è neanche un acronimo, ma una parola in codice costruita a caso. Era probabilmente la più sofisticata macchina del periodo e non risulta sia mai stata violata. Segretissima era usata ai massimi livelli, inclusa la corrispondenza fra Roosevelt e Churchill, ma a Londra c'era personale americano e agli Inglesi non fu mai fatta vedere. La NSA ha concesso di brevettarla solo nel 2001.

Fra gli Inglesi la macchina più usata era la *TypeX*. Derivata dall'Enigma commerciale, fu adottata inizialmente dalla Royal Air Force intorno al 1937 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.

Sull'altro fronte mancano anche clamorosi successi e organizzazioni complesse come Bletchley Park. I criptoanalisti tedeschi 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, ma storicamente falso. Il match Colossus vs Enigma non è mai stato disputato: pesi diversi, con l'Enigma combatterono, in più riprese, solo le Bombe.

Il Colossus a BP c'era (anzi ce ne erano una decina), ma insieme alla *Tunny Machine* e a *Heath Robinson* fu il campione della squadra di macchine messe in campo a BP per combattere, nella categoria "comunicazioni strategiche" un'altra macchina cifrante tedesca: 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 BP vinse ancora una volta. Il buon Alan fu coinvolto e ovviamente dette il suo contributo con uno dei metodi per abbattere il numero di impostazioni da far verificare ai Colossi.

Le Bombe, Christopher nel film, non erano calcolatori. Neanche il Colossus e le altre macchine di BP erano calcolatori. Né lo erano le varie macchine cifranti. Insomma, in tutta questa non c'è un calcolatore (*no computer*, se preferite l'inglese). I calcolatori verranno dopo. Poco 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 e in una versione ridotta, il *Pilot ACE*.

Un po' scontento di come va all'NPL, Alan nel '48 si sposta a Manchester dall'amico Newman. Lì sono avanti: Frederic Williams e Tom Kilburn hanno messo a punto una buona soluzione per la memoria, l'hanno appena sperimentata sulla Small Scale Experimental Machine, detta *Baby*, e stanno lavorando a un secondo calcolatore la Manchester Automatic Digital Machine, detta *Mad'm*. Turing sarà coinvolto nella 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 da solo.

La *macchina di Turing*, è invece un'altra cosa e non ha valvole e cavi. È un modello concettuale che Turing usò per dimostrare che l'*Entscheidungproblem* di Hilbert non può essere risolto. Nella storia della Matematica è un risultato importante. In più la macchina di Turing può essere usata per modellare tutti i calcoli effettivamente... calcolabili.

Per calcolo non si intende solo un'operazione aritmetica, ma qualsiasi cosa che da un po' di simboli in ingresso produce un po' di simboli in uscita che, toh, risolvono un nostro problema.
La calcolatrice che fa 2+2=4, fa un calcolo. L'Enigma, la SIGABA e compagnia cifrando i caratteri di un messaggio fanno un calcolo, la Bombe e il Colossus cercando pezzi di testo noti nei messaggi cifrati fanno un calcolo, Google trovando le pagine web che contengono una parola fa un calcolo, il pc che mi impagina il testo che sto scrivendo fa un calcolo, la playstation fa un calcolo. Calcoli diversi, ovviamente, parecchio complicati anche, ma a ognuno corrisponde una particolare macchina di Turing capace di eseguirlo.

Fra i tanti calcoli ce ne è uno davvero interessante: è quello capace di eseguire il calcolo di una qualsiasi macchina di Turing. Può essere anche lui espresso da una 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 fare (opportunamente istruito) tutti i calcoli effettivamente calcolabili. Una potenza.
Quindi, Christopher 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.
Se siete arrivati fin qua, Cinzia paga da bere :)

Giovanni A. Cignoni

Il programma di “Un mese con Turing e l’Enigma”, con le presentazioni usate negli incontri
Gli altri articoli della serie “Quattro chiacchiere sul calcolo, senza fare conti”