



il mistero di
ALAN TURING
l'uomo
che svelò
l'Enigma

— StO —

DALLA MACCHINA UNIVERSALE ALL'INTELLIGENZA ARTIFICIALE

ALAIN CHARBONNIER

Un matematico eclettico aveva contribuito alla vittoria degli Alleati nella Seconda guerra mondiale, decifrando i messaggi trasmessi con la macchina 'Enigma'. Aveva posto le basi teoriche di una Macchina Universale capace di risolvere qualunque problema, oltre ai principi di quella che sarà chiamata 'intelligenza artificiale'. Alan Turing è considerato il 'padre della cibernetica', ma quando scomparve, nel 1954, sui giornali apparvero poche righe e per i successivi vent'anni su di lui scese il silenzio, come del resto era calato su tutto ciò che durante la guerra era stato inventato a Bletchley Park.

Quando Eliza Clayton giunse a casa Turing, a Wilmslow, il pomeriggio dell'8 giugno 1954, non trovò traccia del padrone di casa. La luce era accesa in camera da letto, bussò alla porta e, non ricevendo risposta, vi entrò. Sul letto, immobile, esanime, con le coperte tirate fino al collo giaceva Alan Turing. «Aveva una leggera schiuma biancastra sulle labbra e un sottile odore di mandorle amare aleggiava nell'aria. L'orologio da polso era sul comodino accanto a una mela sbocconcellata, come era sua consuetudine fare prima di addormentarsi», si leggerà nel rapporto del sergente Cottrell, redatto durante il sopralluogo. In una stanza attigua c'era un recipiente collegato a una presa elettrica con liquido ancora caldo, dal quale si spandeva un odore di mandorle amare. In un barattolo erano visibili sali di cianuro di potassio. Il medico legale stabilì che la morte risaliva alla notte precedente. Il magistrato chiuse l'inchiesta in due giorni, senza neppure verificare se la mela mangiucchiata fosse imbevuta di veleno. Il verdetto fu: «suicidio da squilibrio mentale»; una tesi fortemente contestata dalla madre Ethel, dal fratello e da amici del mondo accademico.

I giornali diedero la notizia della tragica morte di Turing in poche righe, senza riferimenti alla sua pregressa condanna per omosessualità. Il 12 giugno il cadavere fu cremato a Woking, nel Surrey, e così di Alan Mathison Turing, matematico, pioniere della cibernetica, restavano soltanto le sue opere, i suoi studi, le sue teorie su quella che negli anni successivi sarebbe stata chiamata 'intelligenza artificiale'.

Un episodio della sua vita, però, deve far riflettere.

Anni prima Turing era rimasto affascinato dalla scena del film *Biancaneve*, in cui la strega, con una mela attaccata a un filo, sospesa sul calderone nel quale ribolliva la mistura velenosa, borbottava la filastrocca: «Metti, metti la mela nell'intruglio, che s'imbeva del sonno della morte». Alan continuò a canticchiarla per giorni e, probabilmente, sedici anni dopo la mise in atto.

Nel 1954, al momento della sua morte, la cortina di riservatezza avvolgeva ancora il lavoro di Turing, si era in piena Guerra fredda e, secondo un'ipotesi suggestiva e mai riscontrata, i Servizi segreti avrebbero avuto l'interesse a eliminare un protagonista, scomodo e ricattabile del periodo di Bletchley Park.

Nel 1955, la Royal Society pubblicò una biografia di Turing, ma non v'era cenno alla sua opera di crittoanalista. L'unico riferimento recitava: «Fu insignito dell'ordine dell'Impero britannico per il lavoro svolto per il Foreign Office».

Vent'anni dopo, nel libro *The Ultra secret*, Frederick Winterbotham raccontò i misteri di Bletchley Park e la violazione di Enigma, senza tuttavia parlare di Turing. L'anno successivo Anthony Cave Brown pubblicò *Bodyguard of lies: The vital role of deceptive strategy in World War II*, che, nella versione italiana, assunse il titolo *Una cortina di bugie*. Finalmente veniva citato il nome di Alan Turing e le sue 'Bombe'. Il segreto su Bletchley Park, peraltro, era stato rimosso negli anni successivi alla fine della guerra. A Turing potevano essere ora dedicate targhe e steli, aule, libri, film, tra cui l'ultimo, *The Imitation Game*, proiettato di recente e a distanza di sessant'anni dalla sua scomparsa. Eppure Alan Turing aveva affrontato e vinto la sfida con l'infernale macchina cifrante che tutti, i tedeschi per primi, ritenevano inviolabile. Una presunzione che non teneva conto dell'intelligenza e della passione di un giovane scienziato, che il suo insegnante di matematica aveva così descritto: «Non va molto bene. Sembra perdere molto del suo tempo in ricerche di matematica superiore a scapito dello studio di quella elementare. Un buon lavoro di base è essenziale in ogni materia. Gli elaborati sono sporchi e disordinati».

Nato nel 1912, quando erano tornati in India – dove il padre Julius era funzionario amministrativo e magistrato della provincia di Madras – i genitori preferirono non portare con loro Alan, che aveva appena nove mesi e soffriva di rachitismo. Lo affidarono, insieme con il fratello John, alla famiglia Ward, ad Hastings. Prima ancora di imparare a leggere, cosa che inizialmente apprendeva con una certa difficoltà, Alan Turing già s'interessava ai numeri, inventava parole nuove. Nel 1921 la madre si ritrovò alle prese con un figlio chiuso e trasognato, a tratti antipatico, che non amava i giochi di squadra, preferiva dedicarsi agli scacchi, alle lunghe corse in bicicletta e a piedi, alla costruzione di strani marchingegni, a esperimenti di chimica. Gli insegnanti lo consideravano pigro e insolente, ma Alan si lamentava che la professoressa di algebra «trasmetteva un'idea sbagliata di cosa si intenda veramente con la X».

A 15 anni Turing scrisse un compendio della *Teoria della relatività* di Einstein appena pubblicata per spiegarla alla madre; l'anno dopo, per fare impressione sull'amico Christopher Morcom, calcolò il valore del 'p greco' fino a trentasei cifre decimali. Ammesso a

Cambridge con una borsa per il King's, si laureò con lode nel 1934, ottenendo una borsa di studio di 200 sterline annue. Da quel momento Alan si dedicò alla soluzione di problemi apparentemente non risolvibili. Nell'estate del 1935, sdraiato in un campo di periferia di Grantchester, rifletteva sull'*Entscheidungsproblem* (problema della decisione), posto dal matematico tedesco David Hilbert. In quel momento Turing ebbe chiarissima la percezione che, per stabilire se un problema fosse risolvibile o meno, non restava che tentare di risolverlo, ponendolo sotto forma di equazione. La soluzione passava attraverso un algoritmo. Ergo, dedusse Turing, se era possibile dimostrare che un certo algoritmo dava un risultato definitivo, allora il problema era risolvibile. Turing immaginò così una macchina capace di definire tutti i problemi e dimostrò che alcuni di essi non potevano essere risolti con nessuna tabella di regole, contrariamente a quanto sostenuto da Hilbert. Tuttavia, la macchina era in grado di calcolare qualsiasi cosa fosse calcolabile e, con una singola tabella di regole, di risolvere tutti i problemi risolvibili. Era nata la 'Macchina Universale' o 'Macchina di Turing', congegno astratto, mai realizzata concretamente, ma di fatto antesignana dei moderni computer.

L'anno dopo, la pubblicazione dei risultati ottenuti sulla rivista «Proceedings of the London Mathematical Society» gli aprì la strada per Princeton, quando Max Newman lo segnalò al matematico americano Alonzo Church per un dottorato di ricerca. Nella prestigiosa università americana entrò in contatto con Albert Einstein e John von Neumann, che ne apprezzarono la capacità. Ma Turing era già orientato verso un altro obiettivo: un codice o un sistema di cifratura generale, con corollario di numerosi codici singolari, impossibile da decifrare senza una chiave e molto rapido da criptare.

Spiravano venti di guerra, Turing era tornato in Inghilterra con un prototipo di moltiplicatore elettrico per la cifratura di messaggi, sostituendo le lettere con numeri poi, a loro volta, moltiplicati per un numero chiave segreto. A Cambridge aveva parlato di codici e cifrari e uno dei suoi uditori, presumibilmente uno degli anziani di Cambridge, lo segnalò ad Alastair Denniston, capo del Government Code and Cypher School (Gc&Cs), l'unità governativa di crittoanalisi.

Nell'estate del 1938 Alan fu iscritto a un corso di preparazione tenuto dal Gc&Cs, già oltremodo sotto pressione per l'impossibilità di penetrare le comunicazioni tedesche codificate con la complessa macchina cifrante Enigma. Seguì un ulteriore periodo di addestramento in cui si ritrovò a lavorare con Dillwyn 'Dilly' Knox sulla cifrante tedesca. Giunse poi a Bletchley Park il 4 settembre 1939, insieme al matematico Gordon Welchman. Durante il corso, Turing era riuscito a decifrare il materiale di cinque giorni di intercettazioni di Enigma, ma nessuno aveva violato ancora il traffico corrente per leggere in tempo reale le comunicazioni con i sommergibili.

La macchina cifrante inventata da Arthur Scherbius, in realtà, era già stata violata da tre matematici polacchi, Marian Rejewski, Henryk Zygalski e Jerzy Różycki attraverso la 'Bomba crittologica', capace di individuare la configurazione iniziale dei tre rotori, senza però decifrare il codice. Allo scoppio della guerra non avevano fatto passi avanti. Turing rimase molto impressionato dai risultati dei polacchi e si mise al lavoro con Wel-

chmann. Era convinto che la sua Macchina Universale sarebbe stata in grado di violare Enigma e ogni altro linguaggio cifrato, se non fosse rimasta allo stadio di teoria. In compenso era possibile aumentare la velocità della 'Bomba', mettendola in grado di affrontare Enigma a sei rotori.

L'incontro di Turing con l'ingegnere Harold 'Doc' Keen, della British Tabulating Machine Company (Btm), ebbe come risultato una macchina di due metri per due e profonda 60 centimetri, pesante più di una tonnellata, con 36 decodificatori che emulavano Enigma mentre 108 tamburi selezionavano le possibili configurazioni chiave. Ogni volta, però, che i tedeschi cambiavano la configurazione iniziale bisognava ricominciare. Finché Welchmann non inventò la cosiddetta 'scheda diagonale', che consentiva di eseguire la scansione simultanea di tutte e 26 le configurazioni iniziali. Era l'estate del 1940, la *drôle de guerre* era finita, i tedeschi avevano occupato Olanda, Danimarca, Belgio, Norvegia, Francia e adesso puntavano alla Gran Bretagna. A Bletchley Park, 'Dilly' Knox, Turing e tutti i componenti del Gc&Cs erano sotto pressione. Ciononostante misero a punto una seconda 'Bomba' con cui riuscirono a violare i codici dell'aviazione tedesca, volgendo a proprio favore gli esiti della Battaglia d'Inghilterra. Rimanevano ancora oscuri i sistemi in uso alla marina nazista, su cui Turing si applicò affermando: «è una sfida interessante, so che posso farcela». Più difficile che mai, visto che la marina tedesca utilizzava una Enigma a otto rotori, il che comportava un aumento esponenziale delle possibili combinazioni. L'opportunità di studiare il prototipo originale di Enigma fu offerta dalla cattura da parte della Marina inglese, nel mare d'Islanda, di un U-Boot 110 tedesco, in cui venne rinvenuto un esemplare della macchina, unitamente ai codici segreti e al manuale d'istruzione.

Alla fine del 1941, nel quadro di una collaborazione con i crittoanalisti americani, Turing raggiunse gli Stati Uniti dove contribuì a realizzare la loro prima 'Bomba anti Enigma', a penetrare il codice italiano Hag, grazie alla macchina *Nightingale* (Usignolo), nonché a decifrare il codice JN-25 della marina giapponese, facilitando la vittoria americana nella battaglia del Mar dei Coralli.

Tornato in patria fu trasferito al Research Center ove cominciò a lavorare sui messaggi inviati con la cifrante Lorenz, denominata *Tunny*. Ripristinato in poco tempo il funzionamento della macchina, elaborò un metodo per violare il codice. Fu chiamato 'Turingery' e da quel momento a Bletchley Park i messaggi cifrati non

ebbero più segreti. Unitosi al gruppo, il matematico inglese Max Newman ipotizzò che i calcoli per stabilire il funzionamento di Tunny potessero essere svolti con una macchina elettronica. Il prototipo, chiamato 'Robinson', fu esaminato da Turing e sottoposto all'attenzione dell'ingegnere telefonico Tommy Flowers, che aveva perfezionato la 'Bomba'. Flowers capì che la macchina di Newman non avrebbe funzionato senza l'utilizzo di valvole termoioniche, e infatti 'Robinson' in tre mesi decifrò appena venti intercettazioni. Nei laboratori telefonici di Dollis Hill, a nord di Londra, Flowers costruì un nuovo prototipo in dieci mesi. Grande come una stanza, del peso di una tonnellata, 'Colossus' cominciò a lavorare per rilevare le posizioni dei rotori di Tunny all'inizio di ogni messaggio. Per lavorare aveva bisogno di 1.500 valvole tenute sempre accese con corrente a bassa tensione. In poco tempo furono costruiti altri esemplari di 'Colossus', gli ultimi con capacità di elaborazione di 25.000 caratteri al secondo. La realizzazione di 'Colossus' è attribuita a Turing, anche se in verità fu opera di Flowers. Le sue possibilità di programmazione, tuttavia, si fondavano su concetti chiave sviluppati da Turing.

Quando la guerra finì, quest'ultimo aveva contribuito a realizzare due macchine per criptare le conversazioni: una enorme, detta 'Sig-saly', utilizzata nei colloqui fra Churchill e Roosevelt; l'altra, portatile, detta 'Delilah', basata sui sistemi di codifica delle Tunny.

Chiunque avesse lavorato a Bletchley Park aveva firmato sotto giuramento l'*Official Secrets Act* e si era impegnato a mantenere per sempre il riserbo assoluto sul lavoro dell'unità di crittoanalisi. Turing onorò questo impegno anche quando cominciò a collaborare per la realizzazione dei primi rudimentali 'cervelli elettronici' Eniac, Univac, Ferranti Mark I. Il matematico inglese passava da un progetto all'altro senza sceglierne nessuno, seppur suggerendo soluzioni per tutti. Si interessava di programmare una macchina, pensava a una macchina intelligente, cercava l'intelligenza artificiale, punto d'arrivo della sua 'Macchina Universale', nella convinzione che ci sarebbero voluti 100 anni. La sua profezia non si è ancora avverata, i 100 anni non sono trascorsi



BIBLIOGRAFIA MINIMA

- S. BUDIANSKY, *La guerra dei codici*, Garzanti, Milano 2002.
 N. CAWTHORNE, *L'enigma di un genio*, Newton Compton, Roma 2014.
 A. HODGES, *Alan Turing. Storia di un enigma*, Bollati Boringhieri, Torino 2014.