LA STORIA MAI RACCONTATA

Alan Turing – il padre dell'Informatica

Alan Mathison Turing (Paddington, Londra, 23 giugno 1912 – Wilmslow, 7 giugno 1954), personaggio strano e misterioso come tutti i grandi geni, è stato uno dei pionieri della logica dei computer. Turing fu uno dei più grandi matematici del Novecento, logico, analista britannico, crittoanalista che riuscì a decifrare i messaggi scambiati fra i diplomatici e militari delle Potenze dell'Asse durante la seconda guerra mondiale. Per violare i cifrari tedeschi utilizzò il metodo della bomba, una macchina elettromeccanica in grado di decodificare i codici generati da una macchina tedesca chiamata Enigma.
Considerato il padre dell'informatica teorica e del computer, Turing, applicò il concetto di algoritmo ai calcolatori digitali e fu uno dei precursori del legame fra macchina e natura da cui nacque l'Intelligenza Artificiale. A lui si deve la "Macchina di Turing" e il "Test di Turing".
In suo onore la Association for Computing Machinery (ACM) ha creato nel 1966 il Turing Award, la massima riconoscenza nel campo dell'informatica, dei sistemi intelligenti e dell'intelligenza artificiale. Lo A.M. Turing Award viene assegnato annualmente ad una personalità che eccelle per contributi di natura tecnica/informatica. Spesso questa riconoscenza viene chiamata "premio Nobel del calcolo automatico".

Figura 1 - Alan Mathison Turing

Il padre di Alan, Julius Turing, era un funzionario britannico amministrativo dell'Indian Civil Service. I genitori di Alan, secondo di due figli, essendo costretti a lunghi periodi di permanenza in India (allora colonia britannica), non avevano molto tempo da dedicare ai propri figli. Per questo motivo Alan e suo fratello John furono spediti in un convitto inglese all'età di 9 anni dalla madre che giudicava l'ambiente scolastico coloniale inadatto all'educazione dei figli. Così trascorsero la loro infanzia in case-famiglie, visitati sporadicamente dai loro genitori, nei periodi della licenza dal lavoro di suo padre.
Turing era un bambino solitario; all'età di 5 anni imparò da solo a leggere in tre settimane, e manifestò fin da piccolo attitudini alla matematica: spesso si fermava davanti ai pali della luce per leggerne il numero di serie impresso.
Fin da piccolo gli piaceva inventare e sperimentare su se stesso le sostanze chimiche, a tal punto che la madre disse, quando morì, che si trattava di un esperimento andato male.

I genitori, pur non essendo benestanti, non badarono a spese per far istruire dignitosamente i propri figli; infatti, fecero prendere lezioni private a entrambi i figli al fine di poterli iscrivere in una scuola pubblica, una specie di liceo privato, al quale si poteva accedere solo attraverso un test d'ingresso.
A scuola Alan non era brillante anzi le sue pagelle erano pessime; l'insegnante di lettere delle medie, che lo considerava l'ultimo della classe, così lo descriveva: "*Io posso perdonare la sua calligrafia, sebbene sia la peggiore che abbia mai visto, e posso tentare di essere tollerante verso la sua eterna imprecisione, il suo lavoro trasandato, sporco, ma non posso perdonare la stupidità del suo atteggiamento verso una sana discussione sul nuovo testamento*". Al liceo, che si era diplomato a stento, il preside, in una lettera, aveva scritto alla madre: "*Alan è il tipo di ragazzo condannato a rappresentare un problema in ogni tipo di scuola o comunità*".
Turing, infatti, era poco interessato alle materie umanistiche e ad esse privilegiava le materie scientifiche come la matematica e la chimica, inventando esperimenti chimici e leggendo molto; la struttura rigida della scuola e la bassa considerazione nei college inglesi delle discipline scientifiche non gli permettevano di esprimersi nelle sue materie preferite. Non solo, nelle materie di suo interesse spesso usciva fuori dagli schemi, ricercando soluzioni alternative e originali a quelle proposte dagli altri scienziati e docenti.
In definitiva, Alan era il tipico ragazzo-alunno di cui non si capiva se era un genio o un idiota, dato che manifestava un'elevata attitudine alle discipline scientifiche, in particolare alla matematica, alla fisica e alla chimica; nello stesso tempo si rivelava un disastro nelle materie umanistiche come il latino considerandola una materia inutile. Questa sua intolleranza alle materie non scientifiche lo porterà nella sua carriera a scrivere un inglese grammaticamente pessimo.
La scuola inglese, sebbene era un antico sistema educativo, con regole ferree e spesso crudeli, non è stata in grado di formare un ragazzo con delle doti fuori dal comune come quelle di Alan. Un esempio di indottrinamento esagerato dei college inglesi era la punizione corporale, ufficialmente abolite da non molti anni.
Alan si trovò di fronte a due scelte alternative: piegarsi alle regole scolastiche e quindi diventare un alunno che si confondeva con il resto della massa incolore e che accettava tale sistema solo per sopravvivere oppure, come fece, isolarsi dal mondo, approfondendo esclusivamente le discipline di suo interesse, spesso senza farsi vedere, senza alcun aiuto nell'organizzare i suoi studi e preferendo un piano di studi proprio.
Gli anni della scuola pubblica segnarono l'inizio della sua carriera come matematico; ottenuto il diploma nel 1931, nello stesso anno venne ammesso ad una università prestigiosa di Cambridge, il King's College, dove approfondì i suoi studi sulla meccanica quantistica, la logica e la teoria della probabilità (dimostrò in modo del tutto autonomo il teorema del limite centrale già descritto precedentemente dal matematico Lindeberg). Il giovane Turing riuscì a destreggiarsi anche nelle materie in cui non eccelleva e riuscì a trasformarsi grazie alla grandissima amicizia con Christopher Morcom conosciuto nel secondo anno di corso, apparentemente molto più promettente di lui e molto più stabile. L'amico, sebbene morì di tubercolosi due anni dopo l'incontro, gli trasmise un sostegno morale e un incitamento che lo segnò profondamente a tal punto da ricercare e trovare dentro di sé la determinazione

necessaria per continuare con successo gli studi e la ricerca, sviluppandone le sue immense potenzialità.
Turing iniziò a studiare la struttura della mente umana, al rapporto tra la mente e la materia e a come la mente si separa dal corpo al momento della morte. Cercava, nella fisica del Novecento e nella meccanica quantistica, la risposta al grande problema filosofico del rapporto tra mente e corpo.
Anche al college Turing veniva considerato un tipo strano, scorbutico e maleducato. Era sportivo, praticava la maratona, il ciclismo, il canottaggio, in una università dove l'attività fisica veniva disprezzata. Nello stesso tempo era trasandato nel vestire, infatti, compariva spesso in facoltà con le unghie sporche o la barba incolta, avvolte indossava la giacca del pigiama al posto della camicia, altre volte arrivava al college con la maschera antigas per difendersi dalle allergie, oppure giocava a tennis con un impermeabile sotto il quale non indossava nulla. Talvolta si presentava agli studenti con i pantaloni legati con una fune al posto della cintura. Queste ed altre stranezze lo portavano all'isolamento dagli altri studenti e se si trovava nel mezzo di una discussione che non gli sembrava interessante se ne andava di scatto senza apparente motivo, lasciando allibiti i colleghi. Alan era un autodidatta incorreggibile, studiava poco e male, ma a volte era in grado di riscoprire da solo importanti teoremi della logica matematica o del calcolo della probabilità.
Nel 1934, Alan si laureò brillantemente in matematica con il massimo dei voti, ottenendo l'anno successivo una borsa di studio e nel 1936 il premio Smith, riconoscimento che veniva assegnato ai due migliori studenti ricercatori in Fisica e Matematica presso l'Università di Cambridge.
Da questo momento Alan si cimenterà nello studio delle macchine che imparano da sole, quella scienza che oggi chiamiamo Intelligenza Artificiale.
Sempre nel 1936, Alan pubblicò un articolo dal titolo "*On Computable Numbers with an Application to the Entscheidungsproblem*", caposaldo storico dell'umanità. Durante una serie di conferenze cui aveva assistito qualche mese addietro, Alan era venuto a conoscenza dell'Entscheidungsproblem, il cosiddetto "problema decidibilità" formulato da David Hilbert, grande matematico tedesco e teorizzatore del "formalismo", e giacente ancora senza soluzione: "Può esistere, almeno in linea di principio, un metodo meccanico attraverso il quale, data una qualsiasi proposizione matematica, si possa decidere se essa sia dimostrabile o meno?

Capitò così che in un pomeriggio, sui prati di Grant Chester, Alan intuì che poteva essere idealizzata una macchina universale che potesse riprodurre questo ragionamento. Una macchina che poteva occuparsi di un qualunque tipo di operazione logica o matematica, e che una successione di un numero finito di istruzioni potesse essere descritta tramite un algoritmo. Turing, quindi, dimostrò che si poteva creare una macchina teoricamente in grado di calcolare qualsiasi funzione matematica, ma capì anche che la macchina, pur potendo risolvere infiniti problemi matematici, ne avrebbe incontrati alcuni che l'avrebbero costretta a calcolare all'infinito senza poter provare una soluzione. A partire da queste intuizioni, Turing riuscì a dare una risposta negativa al quesito di Hilbert.

Nei secoli precedenti molti scienziati avevano immaginato macchine calcolatrici, ma Turing andò oltre e intuì che una macchina poteva fare molto di più, e che un giorno forse le macchine avrebbero potuto compiere azioni intelligenti.
La sua risposta al problema di Hilbert non fu l'unica; poco prima di Turing, un logico matematico americano, Alonzo Church, aveva già pubblicato un articolo in cui descriveva la soluzione al problema di Hilbert; ma Church riconobbe pubblicamente che Alan era riuscito nello stesso intento in maniera indipendente e meno elaborata. Nel settembre del 1936 Church invitò Turing a Princeston, la famosa università americana, dove vi rimase per studiare due anni ottenendo il dottorato - Ph.D (Doctor of Philosophy) – in matematica. Il Ph.D è un titolo accademico riconosciuto internazionalmente (l'equivalente del dottorato di ricerca italiano), il più alto titolo accademico riconosciuto. A Princeston vi lavoravano alcuni fra i maggiori scienziati del mondo, fisici del calibro di Albert Einstein, logici come Kurt Godel, fisici matematici come von Neumann, un altro fra i grandi pionieri della "Computer Science". Von Neumann si accorse delle capacità del matematico inglese, e gli offrì di lavorare con lui. Molti scienziati avrebbero fatto carte false per una tale occasione, ma Turing rifiutò. Fu a Princeton che Alan iniziò a pensare all'idea di costruire una macchina simile a quelle che noi oggi definiamo computer. Turing, però, l'unica cosa che desiderava era tornare in Europa prima che scoppiasse la guerra e così nel 1938 ritornò a Londra.

L'Europa era sotto l'incubo nazista. Alan era preoccupato da mesi, pensava sempre più alle sue macchine logiche. "*Se possono risolvere ogni problema affrontabile dall'uomo armato di carta e penna, tali macchine possono aiutare anche contro il nazismo*", disse Alan. Già negli anni della prima guerra mondiale il governo inglese aveva creato, all'interno del ministero della difesa, un dipartimento per lo studio dei codici segreti. Negli anni '20 questo dipartimento venne aggiornato ed ebbe il compito di studiare i metodi di comunicazione in cifra usati dalle potenze straniere, ed esprimere pareri in ordine alla sicurezza dei codici e cifrari britannici. Durante la seconda guerra mondiale, l'esercito tedesco aveva messo a punto la famosa macchina Enigma. Macchina assai complessa che permetteva la cifratura e la decifratura dei messaggi in maniera tale che se non si avevano doppie o tripli chiavi non si riusciva a entrare nel messaggio. Per affrontare la crittografia geniale di Enigma ci voleva un grande matematico, quale Alan Turing. Dal suo ritorno in Inghilterra, Turing era ufficialmente un borsista del King's College e in segreto l'ufficio governativo che si occupava di decodificare i messaggi era diventato un elle forze armate tedesche (GCCS – Government Code and Cypher School) lo assunse (solo dopo aver frequentato un corso di formazione) nel 1939, allo scoppio della guerra, come responsabile di questo gruppo che aveva il compito di decifrare i codici segreti tedeschi. Al GCCS, che fino a quel momento era costituito da circa 400 persone appartenenti solo alle categorie letterarie, furono reclutati anche matematici, ingegneri e logici dei Paesi Alleati per arrivare a circa 30.000 persone alla fine della guerra. Il gruppo era ospitato a Bletchley Park, un paesino di campagna, in una villa vittoriana, controllata giorno e notte da agenti in borghese. I servizi segreti avevano recuperato alcune macchine enigma catturate in territorio tedesco e le avevano smontate. Ma capire come funzionava la macchina non era sufficiente per risolvere il problema. Turing, allora, analizzò il problema

dal punto di vista matematico; pensò, inoltre, che per poter risolvere il problema non era sufficiente la sola matematica ma ci voleva una macchina. Iniziarono a costruire colossali calcolatori elettro-meccanici; il più grande di questi era Colossus. Queste macchine erano capaci di scoprire velocemente le chiavi generate da Enigma, che cambiavano quotidianamente. Nel primo anno di guerra, gli affondamenti da parte dei sommergibili tedeschi, misero a nudo la fragilità della flotta mercantile britannica. Era necessaria, quindi, un azione più efficace contro i sottomarini tedeschi U-boot che infestavano i mari. Decodificare i messaggi cifrati della marina tedesca era di importanza vitale per l'Inghilterra. La decifrazione di Enigma sarebbe rimasta un segreto militare fino agli anni '60. Nel 1946, Turing, pur non essendo mai stato al fronte, fu insignito della "medaglia all'Ordine dell'Impero Britannico". Qualche anno prima, lo stesso Churchill, aveva elogiato il gruppo di Bletchley Park, primo fra tutti Alan Turing. Di questi onori pochi però sapevano i motivi e Turing non poté parlarne a nessuno fino alla morte. Durante e dopo la guerra, negli Stati Uniti vennero costruiti i primi grandi calcolatori elettronici programmabili come ENIAC o Edvac. Gli inglesi non vollero restare indietro e progettarono un computer battezzato ACE (Automatic Computing Engine - Asso), uno dei primi tentativi di creare un vero computer digitale. Turing partecipò al progetto (finanziato dal National Physical Laboratory), ma era già stanco di progettare grandi macchine per calcoli numerici. Il suo sogno, ormai, era più ambizioso. Eterno sognatore, Turing, cominciò ad interessarsi alla biologia per esplorare le relazioni tra i computer e il mondo naturale. Iniziava a circolare il concetto di Intelligenza Artificiale. Ormai Alan non pensava ad altro che alla sua Macchina Universale, calcolatore che avrebbe non solo potuto riprodurre le facoltà del pensiero umano che potesse, ma che avrebbe potuto pensare se opportunamente programmata correttamente.

Nel 1947, Turing si chiedeva: "*È stato detto che le macchine calcolatrici possono effettuare solo ciò per cui vengono istruite. È vero che l'intenzione nel costruire tali macchine è quella di trattarle come schiavi, di dare loro solo compiti che sono stati pensati in dettagli, e tali che l'utente della macchina sappia in ogni istante cosa sta succedendo. Fino ad oggi le macchine sono state impiegate in questo senso ma è necessario che sia sempre così?"*. Nel 1950, per rispondere a coloro che ritenevano impossibile che una macchina potesse pensare, Turing pubblicò sulla rivista Mind un articolo in cui immaginava una macchina capace di ingannare, di fingersi un essere umano, un bambino elettronico bugiardo. Turing si chiedeva: "*Se avessimo una macchina tanto sofisticata da reagire in tutto e per tutto come una persona non dovremmo ammettere che essa pensa?*". Turing dichiarando che l'intelligenza e la mente non potevano esistere se non connessi a un corpo, pensò che i computer del futuro dovevano essere in grado di comunicare con l'esterno. Immaginò di dotarli di occhi, orecchi, mani, gambe, per permettergli di esplorare il mondo e sviluppare coì la coscienza e l'iniziativa. Turing stava inventando l'Intelligenza Artificiale. Scrisse: "*Credo che per la fine del secolo l'uso delle parole e l'opinione comune della gente colta saranno mutate a tal punto che si potrà parlare di macchine pensanti senza temere* di venire contraddetti".

Nell'ultima parte della sua vita Turing lasciò il National Physical Laboratory per collaborare, all'università di Manchester al progetto del Manchester Automatic Digital Machine (MADAM) sperando di realizzare, seppure a lunga scadenza, il sogno dell'intelligenza artificiale.

Turing nel marzo del 1952 confessò alla polizia di aver avuto una relazione omosessuale con un ragazzo che si era introdotto in casa sua assieme ad altri ladruncoli. I due amanti furono arrestati il 21 marzo imputati del crimine di atti osceni gravi e Turing fu condannato a un anno di carcere. Il 7 giugno 1954, il quarantaduenne scapolo Alan Turing, venne trovato morto, riverso sul letto della sua stanza con accanto una mela intrisa di cianuro. Il medico legale scrisse sul rapporto: "*causa del decesso: cianuro di potassio autosomministrato in un momento di squilibrio cerebrale*". Il genio incompreso, l'uomo simbolo di tutti quei progetti ignoti al mondo, corteggiato dagli scienziati e dai militari, e poi trattato come un criminale, pedinato dai servizi segreti, costretto ad un anno di tortura chimica, si è spento in un silenzio misterioso. Turing muore come in una favola avvelenato con una mela; e così scompare uno degli scienziati più innovativi e geniali della storia dell'informatica, sconfitto dall'assurde ideologie di alcuni uomini. Solo due anni dopo la sua morte, nell'agosto del 1956, venne coniato il termine di "Intelligenza Artificiale". Oggi non sappiamo ancora cosa sarà del sogno di Alan Turing, del sogno di quel ragazzo che guardando le nuvole si chiedeva: "*può una macchina pensare?*".

Il Colossus di Turing (1943) sconfigge Enigma (1923)

Uno dei fronti su cui si combatté la seconda guerra mondiale fra i due schieramenti opposti fu quello dell'intelligence, o più volgarmente spionaggio. Lo spionaggio si serviva di tutti gli strumenti e mezzi standard, ma anche di tecnologie sofisticate al fine di produrre delle armi segrete. L'arma più importante dello spionaggio fu sicuramente la crittografia, cioè l'uso di macchine in grado di codificare i messaggi. L'arma più importante del contro-spionaggio fu la decrittazione, ossia la decifratura dei messaggi segreti.

La novità della seconda guerra mondiale, fu che entrambe queste attività iniziavano ad essere svolte mediante dei rudimentali calcolatori elettro-meccanici.

Gli agenti degli alleati, infatti, erano alle prese con un problema apparentemente irrisolvibile: decodificare i messaggi criptati generati dalla macchina tedesca Enigma.

Enigma era un calcolatore elettro-meccanico portatile: era costituito da una parte meccanica e da una parte, meno importante, elettrica. La parte meccanica era costituita da meccanismi ad orologeria (la parte software del calcolatore), da una serie di tamburi rotanti (rotoli) utilizzati per la codifica e da commutatori elettrici. I rotoli si muovevano in continuazione con una meccanica estremamente complessa e, immesso un messaggio, questo veniva codificato in modo da essere incomprensibile per chi lo leggeva. La parte elettrica, costituita da una pila elettrica, serviva per far ruotare i tamburi e per evidenziare attraverso delle luci il funzionamento della macchina codificatrice.

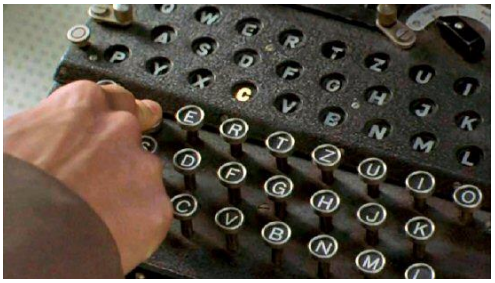

Figura 2 - La tastiera di "Enigma"

Enigma era la macchina usata per crittografare messaggi segreti dai tedeschi, sviluppata a partire dal 1919 dal ingegnere tedesco Arthur Scherbius (1878-1929). Egli creò una società a Berlino per produrre tale macchina che, a dispetto di quanto si potrebbe credere, non era nata per scopi militari ma per usi commerciali al fine di soddisfare le esigenze dei grandi industriali dell'epoca che, subito dopo la fine della prima guerra mondiale, si videro costretti a fronteggiare il nuovo fenomeno dello spionaggio industriale. La prima macchina fu esposta al congresso internazionale dell'Unione Postale del 1923 e poi fu messa in commercio suscitando l'interesse di acquirenti inaspettati, come gli stati maggiori degli eserciti di Germania, Giappone, Polonia e Stati Uniti.
Successivamente, diversi esemplari furono venduti dalla Marina Militare tedesca nel 1926, e nel 1929 venne acquistato dall'Esercito. Da allora, Enigma fu praticamente utilizzata da ogni organizzazione militare tedesca e dalla maggior parte della gerarchia nazista. Diverse versioni di Enigma furono impiegate per quasi tutte le comunicazioni radio codificate tedesche, spesso anche per quelle telegrafiche, durante la seconda guerra mondiale, e perfino per i bollettini meteorologici cifrati tedeschi.
La marina da guerra tedesca (kriegsmarine), soprattutto per l'uso sui sommergibili, ne possedeva una variante particolarmente sicura costituita da ben 8 rotori (di cui 3 operativi, a scelta) che permetteva un numero elevatissimo di configurazioni differenti: miliardi di miliardi, 10^{114}.
Non solo i tedeschi ma anche gli spagnoli, durante la Guerra Civile (1936-1939), e gli italiani, durante la seconda guerra mondiale, utilizzarono Enigma, o meglio una versione commerciale non modificata per le comunicazioni militari: questo portò a pesanti sconfitte spagnole e italiane dato che gli inglesi avevano già violato tale versione di Enigma.

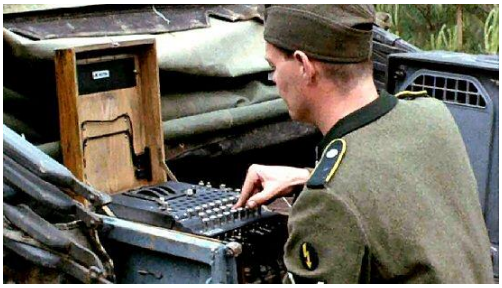

Figura 3 - Enigma sul campo di battaglia

Enigma fu usata anche dopo la fine della guerra: gli Alleati vendettero le macchine Enigma catturate ai servizi di spionaggio di molte nazioni del terzo mondo. Le verità su Enigma e la Bomba furono rese pubbliche solo dopo il 1970.
Enigma fu ampiamente utilizzata dal servizio delle forze armate tedesche durante il periodo nazista e durante la seconda guerra mondiale per trasmettere messaggi codificati e indecifrabili.
Enigma era così sofisticata che nessuno credeva possibile la decrittazione dei suoi messaggi: il modello iniziale possedeva 3 rotori (poi diventeranno 5 e più) e già si arrivava a circa 150 trilioni (cioè 150 milioni di milioni di milioni) di possibili combinazioni differenti.
Nonostante Enigma fosse stata migliorata e potenziata nell'arco del suo tempo di utilizzo, molti decriptatori esperti si impegnarono a lungo per violarla. I primi che riuscirono a decifrare i messaggi

codificati generati da Enigma furono i servizi segreti polacchi con il matematico e crittografo Marian Adam Rejewski (1905-1980), prima del 1938, grazie all'unico difetto (bug) del sistema cifrante: nessuna lettera poteva mai comparire nel testo cifrato come se stessa. L'intelligence polacco progettò una macchina apposita, chiamata Bomba, per estrarre da un messaggio enigma le chiavi di regolazione della macchina che lo aveva cifrato e quindi poterlo cifrare a loro volta. Il nome Bomba deriva dal ticchettio continuo, un sibilo che la macchina emetteva quando tutti i suoi rotori giravano alla massima velocità. La macchina era costituita da moduli grande come un grosso armadio; ogni modulo faceva girare 108 rotori (più 3 di controllo), in gruppi di 12 per fila.

Figura 4 - I moduli della Bomba

I tedeschi, però, cambiarono il funzionamento della macchina, introducendo un set di 5 rotori, di cui ne venivano usati 3 diversi ogni giorno: le combinazioni possibili diventavano 60 volte più elevate. I polacchi non furono più in grado di risolvere questo aumento della complessità della macchina Enigma; allora, il progetto Bomba, alla vigilia dell'invasione della Polonia, nel 1939 fu trasferito in Inghilterra. Gli inglesi riprogettarono Bomba, rendendola più veloce e efficace, organizzarono un'attività di intercettazione e di decifratura su vasta scala delle comunicazioni radio tedesche a Bletchley Park, una piccola cittadina a nord di Londra, nella contea di Buckingam (Buckinghamshiere), con uno snodo ferroviario.

Figura 5 - Marian Adam Rejewski

Gli analisti tedeschi, infatti, erano convinti che per decifrare uno dei 15.576 codici sarebbe occorso a un gruppo di matematici almeno un mese di tempo. Per questo motivo, Churcill incaricò Turing di organizzare e dirigere il centro sulla comunicazione cifrata di Bletchley Park, formato da centinaia di menti brillanti e originali. Era giunto il momento che Bletchley Park diventasse famosa con il proprio nome in codice: la Stazione X.

In una villa di stile vittoriano si è svolta una parte importante della storia dal 1938 fino alla fine della seconda guerra mondiale.

Figura 6 - La residenza di Bletchley Park

Tale gruppo, che raggiunse nel 1944 circa settemila persone, era composto da specialisti inglesi e americani, da civili e militari, archeologi e uomini d'affari, giornalisti e cartografi, crittoanalisti e scienziati, linguisti e geni della matematica, crittografi e musicisti, enigmisti e diplomatici, esperti navali e scacchisti, giocatori d'azzardo ed eminenti docenti di Oxford e Cambridge. Una piccola comunità di brillanti persone riuniti per tentare di decodificare Enigma.

Grazie a alla macchina Bomba fu possibile leggere tutto il traffico segreto della Luftwaffe, l'aviazione tedesca. Quello della marina era ancora inespugnabile.

Nel 1940 furono decrittati, con l'aiuto di Bomba, solo 178 messaggi. Ma i risultati furono comunque importanti, tanto che negli anni successivi si continuò a migliorare la macchina decodificatrice e a costruirne di nuove, fino ad averne ben 211 operative nel maggio del 1945, con 2000 tecnici che le gestivano.

Molte Bombe furono distrutte dopo la fine della guerra, ma sembra che alcune siano poi state sviluppate ed utilizzate ancora negli anni della "guerra fredda" contro i russi ed il blocco orientale.

Oggi, tutta le crittografia e decrittazione si fa con apparati elettronici, senza alcuna parte in movimento, e quindi senza il sibilo della Bomba. Il numero delle configurazioni non è invece particolarmente aumentato: sono passate dal fattore 114 al fattore 128.

Il sistema Bomba era, quindi, ormai diventato inefficiente; allora, Turing non si arrese e riuscì a risolvere il problema sviluppando un enorme sistema di calcolo: il Colossus Mark I, la prima macchina calcolatrice elettromeccanica britannica in grado di decifrare il codice segreto tedesco, ad enorme velocità.

Colossus fu ideato da Max H.A. Newman e progettato nel 1943 nella Post Office Research Station a Dollis Hill, quartiere nord-ovest di Londra, da due ingegneri, della British Telecom, Tommy H.Flowers e S.W. Bradhurst. Nel febbraio del 1944 fu assemblato e messo in funzione il prototipo Mark I a Bletchley Park. In nove mesi, Flowers riuscì a realizzare un calcolatore a valvole in grado di effettuare calcoli matematici ad una velocità impensaible per quei tempi.

Il migliorato Mark II venne installato nel giugno del 1944, e dieci altri Colossus vennero costruiti prima della fine della guerra.
Il Colossus fu sviluppato per forzare i messaggi codificati con il Lorenz SZ 40/42: il tempo per decodificare i messaggi cifrati si ridusse da settimane a ore.
La macchina effettuava delle comparazioni fra due flussi di dati: il primo era il messaggio da decifrare, il secondo era generato dalla macchina stessa che cerca di individuare la chiave di codifica attraverso prove ripetute e confrontando i risultati ottenuti. Se una simulazione dimostra un grado di accuratezza superiore a una specificata soglia, il risultato veniva stampato tramite una macchina da scrivere elettrica. Si stima che sviluppasse circa 5000 operazioni al secondo e quindi tra il 1943 e il 1946 fu il più potente calcolatore del pianeta (surclassata da ENIAC nel 1946).
I Colossus erano macchina che ancora si programmavano con rotori, switch e cavi. Continuarono la loro attività fino al 1960 quando furono smantellati e bruciati tutti i documenti tecnici e gli schemi. La loro esistenza rimase segrete ancora ben oltre gli anni ‘70.
La macchina era molto veloce a tal punto che gli alleati riuscirono a ricevere i messaggi durante la guerra in nord Africa, molto prima del comando tedesco.
Grazie a questa macchina gli alleati dal ‘43 potevano sapere in anticipo le mosse del nemico tedesco: la guerra era vinta: la decrittazione del codice di Enigma costò alla marina italiana tre incrociatori pesanti e due cacciatorpediniere e nella battaglia di Capo Matapan del 28 marzo 1941, in cui persero la vita 2000 marinai. La sconfitta della marina italiana in questa battaglia è da imputare alla capacità degli inglesi di saper decifrare fin dall’inizio le strategie e i movimenti della nostra flotta.
Colossus, la prima macchina ad impiegare le valvole al posto dei relè, era fornito di 1.500 valvole e pesava più di una tonnellata. Sebbene non disponeva di memoria e non poteva essere programmato, Colossus era in grado di trattare 5.000 caratteri al secondo e di decifrare ogni giorno, dopo avere scardinato il sistema crittografico di Enigma, più di 4.000 messaggi segreti tedeschi e altrettanti giapponesi e italiani.

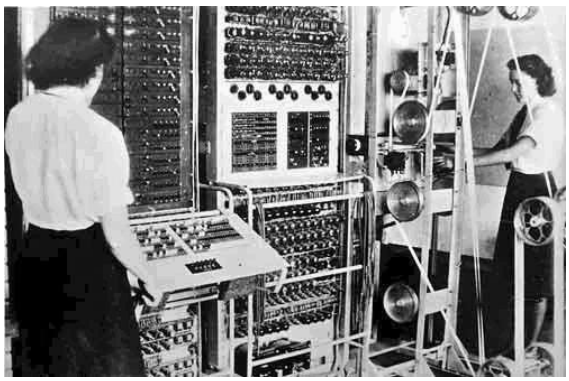

Figura 7 - Il Colossus Mark II: il pannello di controllo a sinistra è il controllore dei settaggi del decodificatore di Lorenz. A destra i nastri con i dati

Churcill, però, non si rese conto fino in fondo delle enormi possibilità date dai calcolatori e dalle teorie di Turing. Dopo la guerra, ordinò di smontare e distruggere tutti i modelli di Colossus utilizzati per sconfiggere i nazisti.
Al termine della guerra Turing venne insignito di un'onorificenza militare dal governo britannico; tuttavia la sua impresa rimase segreta per oltre trent'anni.
Dopo la guerra Turing continuò a dedicarsi allo studio dell'intelligenza artificiale e all'ideazione di nuovi calcolatori elettronici.
Ipersensibile, incompreso, circondato dallo scetticismo e dall'ostilità dell'ambiente scientifico, il matematico inglese si suicidò il 7 giugno del 1954, mangiando una mela al cianuro di potassio, per motivi mai chiariti. Due anni prima era stato coinvolto in uno scandalo per una relazione omosessuale (all'epoca considerata un reato in Gran Bretagna) e condannato a seguire una terapia ormonale che lo aveva reso impotente. Solo nel 2009 vi furono le scuse ufficiali da parte del governo britannico, formulate dall'allora primo ministro Gordon Brown, e solo dopo una petizione e una campagna Internet. Brown riconobbe che Alan Turing fu oggetto di un terribile trattamento omofobico:
«*Per quelli fra noi che sono nati dopo il 1945, in un'Europa unita, democratica e in pace, è difficile immaginare che il nostro continente fu un tempo teatro del momento più buio dell'umanità. È difficile credere che in tempi ancora alla portata della memoria di chi è ancora vivo oggi, la gente potesse essere così consumata dall'odio - dall'antisemitismo, dall'omofobia, dalla xenofobia e da altri pregiudizi assassini - da far sì che le camere a gas e i crematori diventassero parte del paesaggio europeo tanto quanto le gallerie d'arte e le università e le sale da concerto che avevano contraddistinto la civiltà europea per secoli. [...] Così, per conto del governo britannico, e di tutti coloro che vivono liberi grazie al lavoro di Alan, sono orgoglioso di dire: ci dispiace, avresti meritato di meglio.* »
Questa è la risposta di Gordon Brown alla petizione.

La cifratrice tedesca Lorenz e il sistema Ultra di decifratura

http://critto.liceofoscarini.it/critto/lorenz.html (da storia della crittografia)
Nonostante Enigma sia stata la macchina cifrante più famosa, durante la seconda guerra mondiale fu utilizzata anche un'altra macchina: la Lorenz SZ40/42. La Lorenz, molto diversa da Enigma, veniva utilizzata come telescrivente per la comunicazione di informazioni importanti, coperte da segreto, fra gli alti gradi del regime Nazista.
La Lorenz era una macchina cifratrice telescrivente inventata dalla ditta tedesca Standard Elektrik Lorenz AG su richiesta delle autorità militari del Terzo Reich come plugin alla macchina cifratrice Enigma.
Il funzionamento di questa macchina era il seguente:

- utilizzava un set di 32 caratteri;
- ogni lettera, del testo in chiaro, veniva codificata in un numero binario di 5 bit, secondo il codice Baudot (precursore del codice ASCII);

- ogni carattere della chiave di cifratura veniva codificata mediante la macchina Enigma al fine di generare la chiave pseudocasuale: questo metodo di generazione pesudocasuale si basava sul cifrario di Vernam;
- ogni lettera in chiaro codificata veniva messa in XOR (operatore booleano di somma logica negata) con ogni lettera della chiave codificata con Enigma.

Il vantaggio di questa macchina era che il mittente inseriva il testo in chiaro ed il destinatario lo riceveva anche lui in chiaro. Tuttavia, esso era troppo grande e pesante per rimpiazzare completamente Enigma, e quindi fu utilizzato solo per il traffico radio fra i più alti livelli gerarchici tedeschi.
La sicurezza del codice era ottenuta grazie all'utilizzo di chiavi lunghe e casuali. Ciò comportava due grandi problemi: mantenere segreta la chiave e trovare un algoritmo per renderla casuale.
Per ovviare a questo secondo problema, i tedeschi utilizzarono la macchina Enigma per generare un codice pseudo-casuale. La forzatura di Enigma, unita al fatto che le chiavi usate erano difficilmente di lunghezza maggiore rispetto al messaggio, consentì ai crittoanalisti di rompere il codice ottenuto tramite la macchina di Lorenz.
La struttura della macchina era del tutto simile a quella di Enigma, ovvero presentava una tastiera per l'immissione del testo in chiaro, di un unità elettronica in grado di compiere l'operazione di XOR, e di un telex, che trasmetteva e stampava una copia del messaggio cifrato. La macchina di Lorenz, naturalmente, riusciva anche a decriptare i messaggi ricevuti.

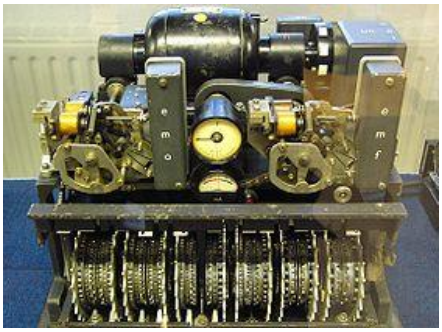

Figura 8 - Macchina di Lorenz

Ultra era il nome che i britannici davano alle informazioni derivate dalla decifratura delle comunicazioni tedesche generate dalla Lorenz. Il nome deriva dal fatto che i successi crittoanalitici erano considerati più importanti del più alto livello di segretezza disponibile e perciò fu conferita la denominazione di ultra segreto.
I crittanalisti inglese del progetto Ultra a Bletchley Park dopo aver forzato la macchina Enigma riuscirono a forzare anche la macchina Lorenz, ancora utilizzando la macchina Colossus. Queste intercettazioni erano sicuramente più importanti in quanto la macchina Lorenz veniva utilizzata dagli alti comandi tedeschi.