La crittologia da arte a scienza:
l'eredità di Shannon e Turing

Angelo Luvison

Sommario

Gli epocali contributi, sia teorici che pratici, di Claude Shannon – padre della teoria dell'informazione e della segretezza – e di Alan Turing – primo artefice della decrittazione dei messaggi della macchina Enigma – hanno trasformato la crittologia (crittografia + crittanalisi) da pratica artigianale a scienza rigorosa. Poiché le minacce alla sicurezza nel cyberspazio diventano sempre più subdole e tecnologicamente maliziose, la crittografia – oggi contemporaneamente arte e scienza – continuerà a svolgere un ruolo di protezione indispensabile nella sicurezza dei servizi informatici.

Abstract

The seminal contributions, both theoretical and practical, of Claude Shannon – father of the theory of information and secrecy – and Alan Turing – principal codebreaker of the Enigma machine – changed cryptology (cryptography + cryptanalysis) from a mainly hand-crafted work to a mathematical science. As security threats in cyberspace become more and more malicious and technologically smart, cryptography – being at the same time an art and a science – will play an increasing role to cope with high-level trust in digital service security.

Keywords: Milestones in cryptology, Shannon and Turing cryptologists, Enigma breaking, Cybersecurity

1. Introduzione

Strumento tecnico-scientifico fondamentale per la cybersicurezza è la crittologia – dal greco *kryptós* ("nascosto") e *logos* ("parola") – scienza che comprende due branche: la crittografia e la crittanalisi [1]. La prima propone nuovi metodi e algoritmi tanto per proteggere i dati e l'informazione quanto per garantire l'autenticità di un messaggio o la sua integrità; mentre la crittanalisi escogita metodi per forzare, illecitamente o a scopo di prova, uno schema cifrato. In realtà, con crittografia molti studiosi intendono sia la crittografia in senso stretto sia la crittanalisi. Il termine crittanalista è entrato nell'uso comune dopo la Seconda guerra mondiale, nel corso della quale la locuzione impiegata dagli anglo-americani era *codebraker* per indicare il solutore non autorizzato di codici cifrati (l'equivalente in italiano era "decrittatore").

Tuttavia, la crittografia non studia solo la segretezza dell'informazione ma si occupa egualmente dell'autenticità. I due obiettivi speculari, "segretezza" e "autenticità", spesso, non sono facili da distinguere. Solo recentemente i crittografi ne hanno apprezzato pienamente la differenza, caratterizzabile in questo modo sintetico: una tecnica fornisce "segretezza" se determina chi può "ricevere" il messaggio, fornisce "autenticità" se determina chi "ha inviato" il messaggio.

Il problema della cybersicurezza ha recentemente avuto un revival sotto il profilo sia economico (sicurezza del business) sia della responsabilità etica. Il primo aspetto, in realtà, ha sempre costituito un punto di attenzione per le aziende; il secondo, peraltro, è tornato in auge a causa di parecchie iniziative, non propriamente commendevoli dal punto di vista etico, del governo statunitense, perciò aspramente criticate da molti Paesi.

Oggi, "La crittografia è una questione di diritti umani", così il fondatore di Wikipedia, Jimmy Wales, ha commentato su Twitter l'annuncio che l'enciclopedia libera adotterà nel prossimo futuro il protocollo HTTPS – quello, per intenderci, usato dai sistemi di transazioni finanziarie e bancarie – per cifrare le comunicazioni da e per i server, rendendo teoricamente impossibile monitorare le abitudini di lettura degli utenti.

Il contrasto tra valori politici e valori etico-sociali non è certamente nuovo. Un gustoso episodio riguarda il Cypher Bureau statunitense, più noto come Black Chamber, che negli Anni Venti del secolo scorso fu l'ente di Signals Intelligence (SIGINT), precursore dell'attuale National Security Agency (NSA). Fondato subito dopo la prima guerra mondiale dal crittanalista Herbert Yardley, questo organismo venne chiuso nel 1929 da Henry Stimson, Segretario di Stato sotto il Presidente Edgar Hoover. L'aneddoto racconta che Stimson si fosse infuriato per la vanteria di Yardley di poter decrittare tutti i cablogrammi diplomatici, compresi quelli del Vaticano. Successivamente, nelle memorie, egli riassunse il suo punto di vista sulla crittografia con frase già allora demodé: "I gentiluomini non leggono la posta l'uno dell'altro" [2]. Questo modo garbato, quasi cavalleresco, corrispondeva ad accettare di buon grado la crittografia tanto nel settore governativo quanto in quello privato, mentre la prassi della crittanalisi era molto meno apprezzata. Il mondo di oggi, più scaltrito, guarda alla crittanalisi come a

un'attività politicamente corretta e prudenziale in ambito governativo, ma vicina allo spionaggio industriale nel privato. In questo secondo caso, essa può, tuttavia, svolgere un ruolo etico oltre che pratico: un crittanalista "amico" è certamente di ausilio per identificare impreviste debolezze di un sistema cifrante, che potrà essere ritirato dal servizio o adeguatamente re-ingegnerizzato.

L'attenzione alla cybersicurezza, o sicurezza nel cyberspazio, è oggi rivolta soprattutto alla difesa dei tradizionali sistemi informatici: PC, server, banche dati, software. Ma, per il continuo sviluppo delle nuove tecnologie – quali il cloud computing e le reti virtuali, l'Internet of Things (IoT) e l'Internet of Everything (IoE), i big data – occorre che la cybersicurezza sia costantemente perseguita e ampliata.

Stante la dipendenza della società da Internet e dalle comunicazioni, il cybercrimine è un problema globale di rilevanza crescente. Diversi studi e analisi valutano il suo costo annuale in circa mille miliardi di dollari: questo dato tiene conto del tempo perduto, delle occasioni mancate negli affari, dei costi per risolvere i problemi tecnici, del danno d'immagine. In parecchi settori dell'economia, si considera molto grave il problema della cybersicurezza e i continui cyberattacchi rafforzano per le imprese più accorte la necessità tanto di maggiori risorse dedicate alla ricerca sulla sicurezza quanto della formazione di figure professionali adeguate. Ogni volta che si usa una carta di credito, si accede a un conto bancario online o si invia un'email, gli algoritmi di cifratura lavorano dietro la scena: quindi, per assicurare la sicurezza dei dati e dell'informazione, nel cloud o nei server di rete, la crittografia svolge un ruolo fondamentale.

Poiché i computer diventano sempre più potenti, la velocità di comunicazione aumenta e la memoria dei dati cresce, i metodi attuali per proteggere l'informazione vengono minacciati o posti sotto attacco da malintenzionati. Per esempio, la capacità dei futuri sistemi di crittografia dovrà superare quella del pur valido Advanced Encryption Standard (AES) adottato dal governo USA nel 2001 per proteggere informazioni "classificate". I crittografi hanno, infatti, tre problemi principali da affrontare: oltre al costo e alla velocità, la sicurezza di lungo periodo.

In questo scenario, possiamo considerare, anche se in modo un po' schematico, Claude Shannon e Alan Turing i padri fondatori, rispettivamente, della crittografia e della crittanalisi contemporanee, per il loro ruolo di attori principali in eventi che hanno permesso l'evoluzione della crittologia da arte a scienza rigorosa, ma pur sempre creativa.

Il contributo di Shannon alla crittografia è la pubblicazione, nel 1949, di un solo ma fondamentale articolo, nel quale approfondisce concetti come "sicurezza teorica" e "pratica", "confusione" e "diffusione", che saranno incorporati in sistemi di cifratura standard.

L'apporto centrale di Turing come solutore di cifrari durante la Seconda guerra mondiale al quartier generale del Government Code and Cypher School (GC&CS) a Bletchley Park, località vicina a Londra, è stato la decrittazione di

Enigma, la formidabile macchina cifrante tedesca. Per decenni i lavori di decrittazione delle comunicazioni dell'Asse da parte di Turing sono stati vincolati al segreto di stato: questa è, quindi, un'occasione per riesaminarne il contributo alla nascita della crittanalisi contemporanea.

Figura 1
Frontespizio della terza edizione (1947) del Manuale di crittografia *di Luigi Sacco.*

Nel 1943, Shannon e Turing ebbero modo di incontrarsi sistematicamente alla mensa dei Bell Telephone Laboratories (BTL) dell'AT&T (American Telephone and Telegraph Corporation), ma – situazione davvero paradossale – non furono autorizzati a scambiarsi informazioni sui rispettivi lavori di intelligence, allora ritenuti assolutamente segreti per la sicurezza dei propri Paesi.

È giusto ricordare anche l'apporto italiano a questa importate disciplina. Infatti, la scienza dei codici e dei linguaggi segreti ha avuto fin dal passato eminenti cultori italiani, fra cui Leon Battista Alberti, Girolamo Cardano e Giovanni Battista della Porta. Ma anche più di recente il nostro Paese ha fornito contributi validi e significativi. Basti pensare al *Manuale di crittografia* (figura 1) del generale Luigi Sacco [3], pubblicato in quattro edizioni (l'ultima del 2014 è stata aggiornata da Paolo Bonavoglia, nipote di Sacco) e considerato da David Kahn nell'*opus magnum* [1][1] il migliore testo pubblicato – cioè non classificato – di crittografia classica (fino alla metà del Novecento). Il successo del *Manuale* fu notevole tant'è che nel 1941 sarebbe stato tradotto in inglese con il titolo *Manual of Cryptography* e nel 1951 in francese (*Manuel de cryptographie*). Anche in [4], Kahn ha parole di grande stima e rispetto per Sacco, che, dopo la battaglia di Caporetto della Prima guerra mondiale, riuscì a convincere gli alti comandi italiani ad abbandonare i vecchi cifrari, facilmente decrittati dagli austriaci [6], e di adottare nuovi sistemi fino allora rifiutati perché troppo complicati.

Il focus di questo lavoro è principalmente sui contributi di Shannon (paragrafo 3) e Turing (paragrafo 4) alla crittologia come disciplina scientifica. Nel seguito, si ripercorrono alcuni passaggi di fondamentale importanza prima di loro (nel paragrafo 2). Completano la rassegna le conclusioni nel paragrafo 5 e tre

[1] The Codebreakers *[1] è l'opera indispensabile per chiunque desideri penetrare i misteri della crittologia in una prospettiva storica. Tutti i successivi lavori di Kahn sono storicamente pregevoli e raccomandabili, in particolare [4]-[6]. Utile è il volume panoramico [7], purtroppo non esente da pecche o imprecisioni storiche e tecniche. Aggiornatissimo è il recente [8]. Un'encomiabile sintesi dell'intera disciplina si trova in [9], un saggio insolitamente penetrante per una voce enciclopedica (online).*

riquadri (curiosità e aneddoti; Shannon e Turing si incontrano ai BTL; misure dell'informazione e delle probabilità) di approfondimento su aspetti particolari appena menzionati nel testo.

La pur estesa bibliografia include solo una modesta parte della sempre più vasta documentazione disponibile in letteratura (o sul Web). Si ritiene, tuttavia, che essa possa risultare già abbastanza orientativa per il lettore desideroso di approfondire uno o più argomenti non sufficientemente dettagliati nel testo. Oggi la crittologia è una disciplina tecnico-scientifica matematicamente fondata e per il suo studio sono in circolazione molti validi manuali universitari, fra i quali gli eccellenti [10]-[13].

Il lessico della disciplina, non sempre uniforme nei lavori tanto scritti direttamente quanto tradotti in italiano, appare spesso ambiguo e incoerente (anche in Wikipedia). Perciò, per assicurare una terminologia con la precisione e la coerenza necessarie in un lavoro di rassegna su una rivista scientifica, si seguirà, con qualche modesto adattamento, quella impiegata in [13], uno dei migliori manuali universitari in italiano su teoria dell'informazione, codici, cifrari. In particolare, è opportuno prestare attenzione a uno dei cosiddetti *false friend* della lingua inglese: *decryption* non corrisponde a "decrittazione"; infatti, *to decrypt* significa decifrare – legittimamente poiché si conosce la chiave – il messaggio cifrato. È quindi, in senso stretto, un false friend giacché l'operazione di decrittazione – in italiano – è un'operazione di crittanalisi, cioè di recupero del messaggio originale in chiaro senza possedere la chiave, perciò sostanzialmente non autorizzato. Per questa ragione, la complessità computazionale del processo di decrittazione dovrebbe essere, almeno in linea di principio, significativamente maggiore di quella di decifrazione.

2. I precursori: due pietre miliari

In questo paragrafo si descrivono due importanti eventi – di rilevanza tanto tecnica quanto storica – che hanno caratterizzato le tecniche crittografiche nel passaggio dalla fase classica alla contemporaneità: il principio di Kerckoffs [14] e il cifrario di Vernam [15].

2.1 Il principio di Kerckhoffs

L'olandese Auguste Kerckhoffs in un articolo in due parti del 1883, *La cryptographie militaire* [14], enunciò una legge generale per i messaggi cifrati: "La sicurezza di un crittosistema dipende solo dalla capacità di tenerne celata la chiave". In base a questo principio, si dà per scontato che il "nemico" sia a conoscenza delle caratteristiche del cifrario o, per dirla in altri termini, che sia a conoscenza dell'algoritmo di cifratura.

Tuttavia, in molte applicazioni crittografiche, tradizionalmente in quelle militari e diplomatiche, il crittografo tende (o, piuttosto, tendeva) a difendere strenuamente la segretezza di tale algoritmo. Potrebbe sembrare, infatti, che il principio di Kerckhoffs sia controintuitivo, e che un progetto, di cui siano mantenute nascoste le specifiche, porti a un sistema intrinsecamente più sicuro: questa è l'idea della "sicurezza mediante oscurità".

Kerchhoff non sarebbe stato contrario all'oscurità di per sé, ma avrebbe ammonito il crittografo a non farvi troppo affidamento. L'esperienza e la storia militare hanno ripetutamente dimostrato che sistemi di questo tipo risultano troppo spesso deboli e che possono essere facilmente forzati non appena il progetto segreto sia stato abilmente "retroingegnerizzato", oppure carpito con altri mezzi più o meno leciti[2]. Un esempio: il Content Scrambling System (CSS) per la protezione del contenuto dei DVD è stato facilmente forzato dopo essere stato opportunamente retroingegnerizzato. Ecco perché uno schema crittografico deve rimanere sicuro anche nel caso in cui la sua completa descrizione sia disponibile a un opponente e perché risulta rischioso affidarsi alla speranza di salvaguardare il progetto della propria cifratura da intrusioni non autorizzate. Come vedremo nel paragrafo 4, anche l'opera di forzatura di Enigma può essere interpretata come un'azione di retroingegnerizzazione.

Il principio di Kerckhoff sarebbe stato riformulato decenni dopo (o, forse, formulato indipendentemente) da Shannon secondo l'enunciato: "Il nemico conosce il sistema", ossia, "Un sistema (di sicurezza) dovrebbe essere progettato assumendo che l'opponente sia in grado di acquisire rapidamente completa familiarità con esso". L'aurea massima di Shannon è oggi condivisa da tutti gli esperti di crittografia.

2.2 Il cifrario a blocco monouso (*one-time pad*) di Vernam

Nel 1926, Gilbert Vernam – ingegnere all'AT&T – pubblicò [15] un importante cifrario da usare con il classico codice Baudot sviluppato nel 1984 e successivamente impiegato nelle telescriventi. L'idea innovativa proposta da Vernam era di utilizzare la chiave una e una sola volta, cioè di cifrare ciascun bit del testo con un bit della chiave scelto in modo completamente casuale. Vernam riteneva – a ragione, sia pur senza dimostrarlo rigorosamente[3] – che il cifrario fosse resistente, cioè inviolabile (*unbreakable*), ed era pure consapevole che non sarebbe stato così se i bit della chiave fossero stati successivamente riutilizzati. Vernam nello stesso articolo [15] riferì di prove in campo, condotte dall'U.S. Army Signal Corps, che avrebbero provato l'inviolabilità del cifrario, un obiettivo, peraltro, che nessuna sperimentazione, per quanto estesa, può garantire con certezza assoluta. Il motivo per definire "prescientifica" la crittologia del periodo prima della Seconda guerra mondiale è che fino allora si procedeva per intuizioni e convinzioni non suffragate da dimostrazioni valide. Non fu che allo scoppio di questa guerra che la comunità crittologica comprese appieno il contributo che matematici e ingegneri – fra i quali Shannon e Turing – avrebbero potuto fornire in materia.

Anche se l'articolo è del 1926, già nel 1918 Vernam aveva costruito una macchina elettromeccanica – brevettata l'anno successivo – che automaticamente cifrava le comunicazioni effettuate con telescrivente. Il testo in chiaro alimentava il dispositivo con un nastro di carta, mentre un secondo nastro

---

[2] *"By hook or by crook" è l'icastica frase idiomatica in inglese.*

[3] *Anche se Vernam era nel giusto, la storia della crittografia è costellata di inventori che erroneamente credono e dichiarano che i loro cifrari siano inviolabili.*

in input forniva la chiave. Per la prima volta cifratura e trasmissione venivano automatizzate nello stesso apparato.

Il sistema crittografico di Vernam, oggi è più conosciuto con il nome di *one-time pad*, o blocco monouso, dalla modalità di utilizzazione da parte dello spionaggio internazionale prima, durante e dopo la Seconda guerra mondiale. Gli agenti segreti erano dotati di un blocco di carta contenente la chiave segreta, scelta casualmente e da utilizzare una e una sola volta, cioè monouso. Conseguenza molto importante di questo schema – ed è la ragione per cui la sua ideazione costituisce tuttora una pietra miliare in crittografia – è che fornisce l'unico tipo di crittosistema incondizionatamente sicuro. Ciò sarà, tuttavia, provato quasi trent'anni dopo da un altro ricercatore dell'AT&T: Claude Shannon.

Per completezza di informazione, si può aggiungere che Joseph Mauborgne (U.S. Army Signal Corps) è generalmente considerato co-inventore di Vernam del one-time pad, mentre si è ultimamente accertato [16] che il bancario Frank Miller è stato precursore di entrambi, avendo pubblicato nel 1882 la monografia *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*, in cui già allora proponeva l'uso di questo sistema di cifratura per il servizio telegrafico. Indubbiamente però, la sua prima realizzazione concreta va attribuita a Vernam.

3. Terza pietra miliare: l'articolo di Shannon

Esiste una ormai sterminata aneddotica sull'abitudine di Shannon di lavorare (o giocare) allo stesso tempo con problemi di tipo diverso (figura 2). Oltre a scrivere articoli fondamentali di teoria dell'informazione, Shannon – sempre curioso degli argomenti più eterogenei – ha dato inizio all'era della progettazione dei circuiti logici con la sua tesi di master discussa nel 1937, ha studiato la composizione ottimale di portafogli azionari (si veda, per esempio, [17]), ha coltivato un interesse durevole per le macchine che giocano a scacchi, ai BTL, al MIT, nel garage di casa propria. Tutti i suoi lavori principali sono reperibili in un unico volume pubblicato dall'IEEE Press [18].

Figura 2
Shannon gioca con il suo topo elettromeccanico

Shannon raggiunse i BTL nel 1941 per lavorare nel settore crittografico: i suoi contributi teorici sarebbero stati basilari per sviluppare il sistema SIGSALY del Progetto X, l'imponente apparato di scrambling vocale che avrebbe permesso a Churchill e Roosevelt di parlare da una stanzetta speciale mediante un sistema di codifica vocale d'avanguardia ancora oggi (cfr. § 4 e riquadro 2).

Con la pubblicazione, qualche anno dopo nell'ottobre 1949, del suo fondamentale articolo "Communication theory of secrecy systems" [19] ha definito i principi teorici delle comunicazioni segrete, inaugurando l'era della crittografia scientifica a chiave segreta[4].

Come anticipato, la versione di Shannon del principio di Kerckhoffs è nella forma "il nemico conosce il sistema". In altri termini, Shannon ipotizza implicitamente che "ogni aspetto progettuale del processo di cifratura sia noto al crittanalista opponente, tranne ovviamente i valori correnti, per esempio, del testo in chiaro e della chiave segreta del messaggio istanziato". In particolare, l'algoritmo di cifratura stesso *non* è segreto.

In una nota a piè di pagina, l'autore avverte che il contenuto dell'articolo [19] era già apparso nel 1945 come un memorandum confidenziale BTL, poi reso pubblico (*declassified*). L'articolo incomincia con la proposizione: "I problemi della crittografia e dei sistemi segreti forniscono un'interessante applicazione della teoria delle comunicazioni"; le comunicazioni segrete, indubbiamente, ne costituiscono l'intento principale.

Anche il titolo è di per sé molto significativo. Gli obiettivi delle tecniche crittografiche sono due: la segretezza e l'autenticazione. Shannon chiarisce che sta considerando solo la segretezza e precisa che vi sono due tipi di sistemi per la segretezza: quelli progettati in difesa da un attaccante ostile in possesso di risorse computazionali illimitate e quelli progettati per proteggersi da un attaccante con capacità computazionale finita. Shannon definisce la prima "segretezza teorica" e la seconda "segretezza pratica" – questi termini sono stati sostituiti nell'uso attuale da "sicurezza incondizionata" (o, talvolta, "sicurezza teorica dell'informazione") e "sicurezza computazionale"; il senso, peraltro, non cambia.

3.1 Sicurezza teorica o pratica

La discussione di Shannon sulla segretezza teorica è concettualmente molto ricca. Shannon fornisce per la prima volta la definizione di *unbreakabiltity* (inviolabilità o inattaccabilità) di un cifrario, dimostrando che lo schema di Vernam, il cifrario a blocco monouso, garantisce la "segretezza perfetta" – termine usato per denotare l'inviolabilità.

Più precisamente, Shannon dimostra che la segretezza perfetta richiede una chiave segreta la cui lunghezza in cifre binarie sia almeno pari al numero di bit di informazione del messaggio cifrato. Diventa con ciò chiaro che la sicurezza pratica è quanto di meglio si possa sperare in situazioni reali dove la chiave segreta è relativamente breve.

Benché i vari circoli di esperti ritenessero da tempo che questo schema di cifratura non potesse essere forzato, fu probabilmente Shannon a pubblicare per primo una conferma teoricamente convincente della congettura ipotizzata. La dimostrazione è molto semplice perché si basa unicamente sull'indipendenza statistica della somma modulo due $c = m \oplus k$ di due processi casuali tempo-discreti statisticamente indipendenti: c è il messaggio cifrato, i

[4] *Questa parte attinge principalmente dall'ottimo saggio [20] di James Massey.*

due processi *m* e *k* sono, rispettivamente, il messaggio originale in chiaro *m* e la chiave *k*.

È da notare che il blocco monouso assicura la segretezza perfetta, non importa quale sia la statistica del testo in chiaro. Proprietà questa molto importante perché non è desiderabile che il sistema di cifratura dipenda dalla statistica della sorgente dei messaggi. Ma il fatto che si richieda un bit di chiave segreta per ogni bit in chiaro rende il sistema poco utilizzabile in pratica – tranne nelle applicazioni dove l'esigenza di segretezza fa premio sul costo e la lunghezza del testo in chiaro è piuttosto limitata: viene subito in mente la "linea calda" tra i capi di stato di Paesi alleati.

3.2 Confusione e diffusione

Secondo Shannon vi sono due operazioni primarie con le quali si possono costruire algoritmi di cifratura robusti e resistenti agli attacchi:

1. **Confusione** è un'operazione di cifratura dove la relazione tra chiave e crittogramma è resa oscura. Un mezzo oggi comunemente impiegato per ottenere confusione è la sostituzione dei bit.
2. **Diffusione** è un'operazione di cifratura dove l'influenza di un solo simbolo del testo in chiaro è spalmata su molti simboli del testo cifrato con l'obiettivo di nascondere le proprietà statistiche del testo in chiaro. Un semplice elemento di diffusione è la permutazione dei bit.

Cifrari che realizzano solo confusione – un esempio è la macchina cifrante tedesca Enigma impiegata durante la Seconda guerra mondiale – non sono sicuri. Né lo sono cifrari basati esclusivamente sulla diffusione. Tuttavia, concatenando le due operazioni, si può costruire un sistema robusto: siamo ancora debitori a Shannon per l'idea di questo artificio. Tecniche di progettazione di sistemi cifranti, che ripetono sui dati le operazioni di "confusione" e "diffusione", sono oggi utilizzate in tutti gli algoritmi di crittografia a blocchi[5], quali il Data Encryption Standard (DES) e le sue alternative più recenti: il Triple DES (basato sulla ripetizione del DES per tre volte) e l'Advanced Encryption Standard (AES) [11], 12].

Le cifrature a blocchi moderne posseggono eccellenti proprietà di diffusione, questo significa rendere il testo cifrato (quasi) statisticamente indipendente dall'originale: requisito essenziale nella progettazione dei cifrari a blocchi [11].

4. La rivoluzione nella crittanalisi: Alan Turing

È opinione generalmente condivisa tra gli storici che l'ausilio della crittanalisi per intercettare e decifrare le comunicazioni dell'Asse da parte degli Alleati abbia permesso di abbreviare di almeno due anni la durata della Seconda guerra mondiale, risparmiando quindi milioni di vite umane – queste valutazioni sono di

[5] *Con cifrario a blocchi si intende un sistema che trasforma blocchi del messaggio (testo in chiaro) di lunghezza fissa (per esempio, di* n *bit) in blocchi di crittogramma della stessa lunghezza con il controllo di una chiave (di* m *bit).*

sir Harry Hinsley, lo storico ufficiale dell'intelligence britannica della Seconda guerra mondiale, presentate in varie occasioni e riassunte in [21].

Winston Churchill, forse esagerando, avrebbe detto a Giorgio VI, re del Regno Unito: "È grazie a Ultra[6] che abbiamo vinto la guerra". E inoltre: "Non direi che Turing ci abbia fatto vincere la guerra, ma oserei dire che l'avremmo perduta senza di lui", dichiarò esplicitamente Irving John (Jack) Gould, altro codebreaker di punta in tempo di guerra [22].

Incontrovertibile rimane il fatto che i crittanalisti alleati con la loro tecnologia abbiano sconfitto i crittografi tedeschi nonostante i loro pur sofisticatissimi sistemi.

4.1 La visione di Turing

Del film di successo *The Imitation Game*[7] del 2014 sulla vita – alquanto romanzata – di Alan Turing molti spettatori ricordano, sia pure a grandi linee, l'intuizione visionaria di Turing di costruire una macchina, la *Bombe*, che facesse il lavoro di centinaia di persone per decrittare Enigma, il sistema cifrante impiegato dalle forze armate tedesche. L'apparato Bombe permetteva ai britannici di confrontare un messaggio in chiaro con il messaggio cifrato intercettato e vedere se una qualsiasi configurazione dei rotori di Enigma potesse corrispondere a tale cifratura. Quando e qualora la coincidenza si fosse verificata, essa avrebbe fornito la chiave di decrittazione giornaliera consentendo ai britannici di leggere tutti gli altri messaggi intercettati nella stessa giornata.

A Bletchley Park (il centro era anche chiamato Station X [24]), non tutti erano convinti che Turing ce l'avrebbe fatta: circolava la voce che Alastair Denniston, il primo capo del centro, avesse dichiarato al responsabile della Sezione navale: "I tedeschi non hanno intenzione di farci leggere le loro cose, e dubito che possiate mai riuscirvi". Ma Turing e i suoi colleghi ci riuscirono. (In *The Imitation Game*, Denniston appare ancora più categorico: "Enigma non è difficile. È impossibile!").

Questo non fu l'unico grande contributo di Turing in crittanalisi; in effetti, Turing si prodigò anche per risolvere i messaggi tedeschi cifrati con telescrivente *ad hoc* – definita a Bletchley Park con il criptonimo "Tunny" – e negli USA lavorò sul

---

[6] Denominazione in codice (o, meglio, "criptonimo") per indicare il lavoro e i risultati di tutte le operazioni del servizio di SIGINT britannico nel periodo bellico, cioè di crittanalisi delle comunicazioni cifrate dell'Asse da parte degli Alleati. Ultra è il nome di un progetto complessivo: l'idea corrente che si riferisse solo a Enigma è imprecisa e parziale. Allo stesso modo, si dovrebbe ricordare – anche se qui non avremo modo di approfondire – che Enigma non fu l'unico sistema cifrato; la stessa Enigma ebbe numerose varianti e fu utilizzata in molti modi nelle reti dei diversi sevizi bellici tedeschi. Un altro criptonimo utilizzato, per un breve periodo, per occultare le fonti di informazione provenienti dai canali di intercettazione più disparati fu Boniface.

[7] Una delle cose migliori del film, diretto da Morten Tyldum, è, probabilmente, l'elogio insistito in ben tre scene della creatività progettuale: "A volte sono le persone che nessuno immagina possano fare certe cose, quelle che fanno cose che nessuno può immaginare", quasi un Leitmotiv *della sceneggiatura. In ogni caso, il film – liberamente ispiratosi dalla biografia di Alan Hodges su Turing [23] – è meritevole di plauso per le atmosfere evocative e suggestive del periodo.*

sistema SIGSALY di telefonia con voce cifrata. Quest'ultima realizzazione, unica nel suo genere, fu utilizzata regolarmente in importanti comunicazioni d'alto livello su operazioni strategiche, incluse le conversazioni segrete tra il presidente USA Franklin Delano Roosevelt (sostituito da Harry S. Truman prima della fine della guerra) e il premier britannico Winston Churchill (riquadro 2).

Figura 3
La residenza di Bletchley Park

Allo scoppio delle ostilità nel settembre 1939, Turing fu assegnato dal governo britannico al quartier generale del Government Code and Cypher School (GC&CS)[8] a Bletchley Park (figura 3), dove il suo brillante lavoro avrebbe avuto conseguenze di grande portata. I britannici avevano appena ricevuto i risultati dei tentativi effettuati dai crittanalisti polacchi, aiutati dai colleghi francesi, per forzare il cifrario Enigma (figura 4), in dotazione al settore comunicazioni radio dell'esercito tedesco. Già nel 1932, una piccola squadra di matematici polacchi, guidati da Marian Rejewski, era riuscita a ricostruire – ecco un formidabile esempio di retroingegnerizzazione – il cablaggio interno del modello della macchina Enigma allora in uso.

Nel 1938 i polacchi poi erano poi riusciti a sviluppare una macchina di crittoanalisi [25], dal nome in codice *Bomba* (probabilmente da un termine allora in uso in Polonia per un tipo di gelato). Per funzionare con successo Bomba dipendeva dalle norme operative dei tedeschi, quindi un cambiamento procedurale nel maggio 1940 rese Bomba praticamente inutilizzabile. Durante il 1939 e l'inizio del 1940, Turing con il suo staff progettò una macchina

[8] Nel 1946, alla fine della guerra, il GC&CS sarebbe diventato il GCHQ (Government Communications Headquarter).

crittanalitica completamente diversa denominata *Bombe*, alla francese e a imitazione dei polacchi (il nuovo termine, invero, indica un ipercalorico dessert inglese, sempre a base di gelato). Con l'ingegnosa macchina di Turing (figura 5), i crittanalisti di Bletchley Park all'inizio del 1942 furono in grado di intercettare e decifrare circa 39.000 messaggi al mese, numero che rapidamente crebbe fino a 84.000 e oltre. Poiché il suo contributo alla vittoria degli Alleati rimase per decenni coperto dal segreto di stato, l'unica onorificenza conferita a Turing fu l'Order of the British Empire, sia pure un riconoscimento di routine e non certo di rango eccezionale.

Figura 4
Una versione della macchina cifrante Enigma

Ovviamente, i contributi di Turing toccarono più discipline, in ognuna delle quali lo scienziato lasciò impronte memorabili – il titolo del basilare riferimento bibliografico [22]: *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life; Plus the Secrets of Enigma* è indicativo della reale vastità dei suoi interessi.

La descrizione dettagliata dei principi di funzionamento di Enigma, dell'architettura e della sua complicata meccanica a più rotori, non solo nelle numerose varianti, ma già nella versione-base, esula dagli scopi del presente lavoro. Parecchi testi o articoli citati in bibliografia, oltre a molti altri, riportano – con diversi gradi di approfondimento, accuratezza, precisione – i modi di funzionamento di Enigma nonché le tecniche per la sua decrittazione (la *Bomba* polacca, la *Bombe* anglo-americana, ecc.). Per un resoconto di interesse anche storico si rinvia alla fonte primaria [26].

È necessario ribadire un punto: le successive versioni della macchina Bombe britannica non costituivano solamente un miglioramento più veloce della Bomba polacca, molto più piccola e assai meno sofisticata. Bombe, rispetto a Bomba, trovava soluzioni all'Enigma con metodi radicalmente diversi che, infatti, coinvolgevano porzioni di testo in chiaro ed elaborazioni in parallelo nel provare le permutazioni delle possibili connessioni di Enigma. Entrambe però erano elettromeccaniche – solo il successivo (proto)computer Colossus [27] sarebbe stato elettronico.

Dell'esperienza di Turing con Enigma si possono evincere tre aspetti principali:

1. L'uso di tecniche probabilistiche, basate su una logica inferenziale bayesiana, e anticipatorie di quella che sarebbe diventata l'analisi statistica sequenziale di Abraham Wald [28] (v. il punto 4.3).
2. La rilevanza di processi *just in time*, cioè la necessità di trovare la chiave giornaliera entro le prime ore del mattino. Tempestività però che si concretizzava non solo nella rapidità ma anche nella perfezione ingegneristica.
3. L'importanza di condividere informazioni in team con competenze interdisciplinari. Benché Turing possedesse un'indole solitaria – "un introverso cronico" lo definì l'amico Max Newman – in realtà, a Bletchley Park non lavorava isolato: vi erano quasi 10.000 dipendenti fra tecnici e amministrativi, di cui circa 2.000 destinati al lavoro di crittanalisi. In tutti i sensi si trattò di un imponente lavoro collettivo, anche se a compartimenti stagni per ragioni di segretezza, durante il quale Turing fu affiancato da collaboratori validissimi.

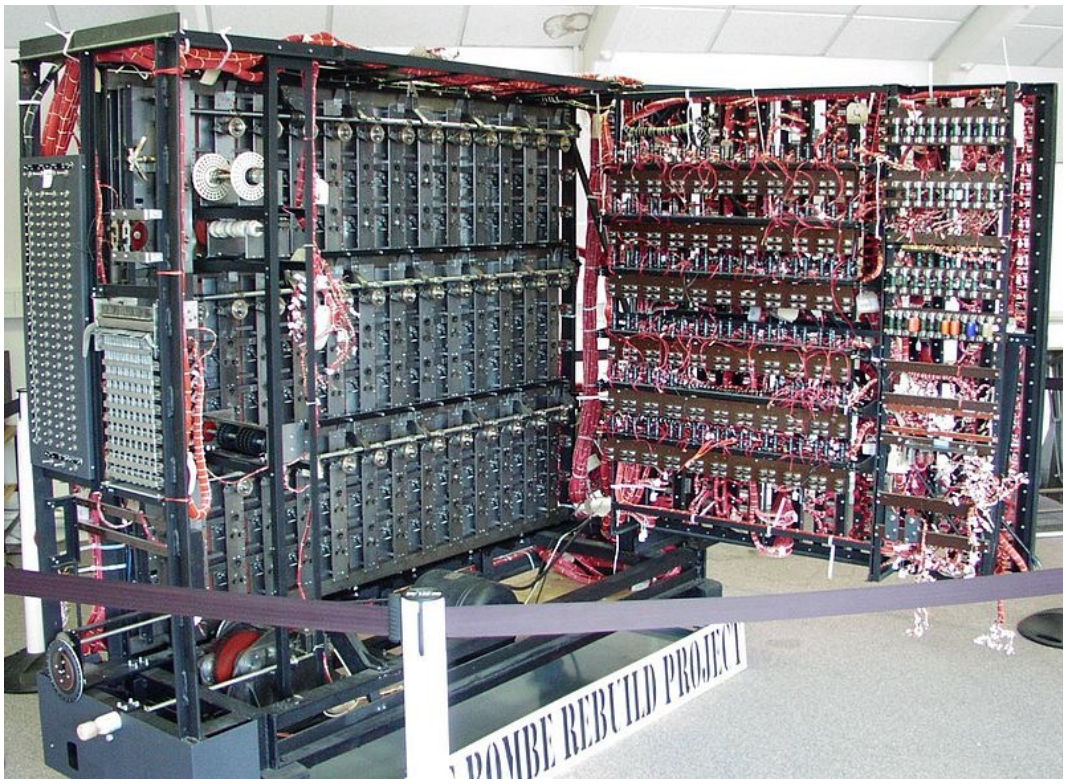

Figura 5
Replica completa e funzionante della macchina Bombe *realizzata da Turing a Bletchley Park*

4.2 L'illusione di Enigma e il successo di *Bombe*

Poiché l'unico modo per decrittare i messaggi intercettati di Enigma era di conoscerne il settaggio giornaliero (cioè una tra le 159.000.000.000.000.000.000 combinazioni possibili, come rivela un personaggio nel film citato) e, vista la necessità di cifrare i vari messaggi nel minor tempo possibile, Turing inventò diversi metodi per ridurre drasticamente il numero di settaggi possibili. (In verità, il numero esatto di combinazioni è 158.962.555.217.826.360.000). Per la variante navale di Enigma questo numero deve essere ulteriormente moltiplicato per un altro fattore di variabilità, cioè 26 x 26 = 676, il che porta a uno spazio di 1,07 x 10^{23} combinazioni da esplorare [29] (ma il film non lo dice). Come si chiarirà meglio qui di seguito, la sicurezza teorica (o matematica) era di gran lunga maggiore di questi valori numerici, di per sé già impressionanti.

Le tecniche utilizzate da Turing e colleghi furono: 1) i *crib*, 2) il "Banburismo" (*Banburismus*), 3) la meccanizzazione dell'intero processo di decrittazione di Enigma, inclusi i due punti precedenti, mediante le macchine Bombe[9].

L'individuazione dei crib e il Banburismo si basavano entrambi su una metrica logaritmica dell'informazione con logica bayesiana – come per Shannon – denominata "peso dell'evidenza" (riquadro 2). Uno degli assistenti principali di Turing a Bletchley Park, Jack Good, avrebbe sviluppato dopo la guerra il concetto di analisi statistica sequenziale in varie discipline applicative, restando però sempre molto riservato – almeno sino alla fine degli Anni 1970 – sui successi propri e di Turing in Ultra. Come ebbe a dire Good in svariate occasioni: "Il gioco del Banburismo comportava la capacità di mettere insieme un gran numero di pezzi di informazione probabilistica in qualche modo, come nella ricostruzione di sequenze di DNA. Il migliore giocatore, in un gruppetto di dieci, fu Hugh Alexander, il campione di scacchi britannico, che divenne capo della sezione Enigma navale quando Turing incominciò a lavorare sulla segretezza del linguaggio parlato" [28].

Per ridurre il tempo di calcolo necessario a trovare la soluzione di Enigma, i crittanalisti britannici fecero anche ricorso a debolezze pratiche, introdotte inconsapevolmente dai crittografi tedeschi nella fase di cifratura, quali breve frasi di routine che potevano dare origine a congetture sul possibile testo in chiaro, per esempio indicazioni sul tempo atmosferico o espressioni di saluto. Il termine per queste parole probabili era appunto "crib", la quale nel gergo inglese indica l'azione di scopiazzare da altri, azione ben nota agli studenti (particolarmente a quelli italiani). I crib erano, in altri termini, locuzioni standard (*Wetter* o "tempo atmosferico", *Keine besondere Ereignisse* o "niente da riferire", ecc.) che ci si aspettava figurassero in posizione fissa nel messaggio in chiaro perché utilizzati sistematicamente e meticolosamente, in accordo con l'ordinata mente teutonica. Un altro elemento indicatore era la frequenza del numero *Eins*,

[9] *Per completezza, occorre dire che vi furono altri due elementi importanti: i* depth *e i* pinch *(cfr., per esempio, [23] e [27]. I primi consistevano nell'ingenua ripetizione di messaggi molto simili con lo stesso settaggio della macchina Enigma da parte dell'operatore tedesco; i secondi denotavano le azioni degli Alleati per la cattura di Enigma e della documentazione pertinente.*

o "uno", scritto in lettere. Una quantità sufficiente di crib rivelati poteva essere molto utile nella ricostruzione delle chiavi giornaliere.

Gli importanti lavori di Miller e Ratcliff [29]-[31] riportano il numero di tutte le possibili impostazioni di Enigma e il numero complessivo delle sue chiavi. Il calcolo rappresenta il trionfo dell'analisi combinatoria – basata su fattoriali, coefficienti binomiali, ecc. – in cui compaiono numeri enormi a esponente com'è tipico delle permutazioni e delle combinazioni. Per esempio, la sicurezza teorica (o matematica) risultava in un astronomico 3×10^{114}, comprensivo di tutte le possibili combinazioni della versione-base di Enigma a tre rotori. Ricorrendo a un paragone suggerito in [29] per sottolineare quanto grande sia questo numero, si potrebbe ricordare che il numero di atomi dell'intero universo osservabile è stimato in 10^{80}. Nessuna meraviglia che l'intelligence tedesca confidasse così tanto nell'inviolabilità assoluta della sua macchina.

Tuttavia la sicurezza informatica non è soltanto puro calcolo matematico, ma significa anche tenere conto di ciò che è noto all'avversario, delle procedure seguite, di come gli operatori abbiano usato le macchine e quali differenti tipi di macchine siano state impiegate. Quindi, a causa di restrizione tecniche e operazionali, il numero effettivo delle possibili configurazioni decresceva drasticamente. Miller [29] ha calcolato questo numero nel già visto $1{,}07 \times 10^{23}$, un valore pur sempre impressionante perché paragonabile a una chiave lunga circa 77 bit. Anche se oggi per applicazioni commerciali si reputano necessari sistemi di cifratura con chiavi di 128 bit o anche 256 ([9], [11]), il far breccia in Enigma costituiva una sfida formidabile per la tecnologia elettromeccanica di allora.

Oltre a Turing, un altro grande artefice del sistema Bombe per infrangere la sicurezza di Enigma fu il matematico Gordon Welchman (la Bombe da molti studiosi è attribuita tanto a Turing quanto a Welchman), che, lavorando sul cablaggio di Enigma, ne individuò un punto particolarmente debole [32]. Poiché i collegamenti usavano un cavo per connettere una lettera all'altra, la seconda lettera era riportata automaticamente alla prima: se la "A" era inserita nella "E", la "E", simmetricamente, era connessa alla "A". Sfruttando ciò, Welchman propose a Turing di aggiungere a Bombe una tavola che collegava ogni lettera con tutte le altre seguendo uno schema regolare. Combinato con le tre tecniche di Turing sopra indicate, questo espediente ridusse drasticamente il numero delle impostazioni dei rotori facilitando enormemente il compito degli analisti. Dall'agosto 1940 le realizzazioni di Bombe inclusero anche l'artificio di Welchman, noto come "pannello o piastra diagonale" (*diagonal board*).

In definitiva, come già sottolineato al punto 3.1, esiste una differenza cruciale fra sicurezza teorica e sicurezza pratica. La sicurezza teorica può essere data con numeri certi, chiari, trasparenti. I numeri della sicurezza pratica dipendono, invece, da come il sistema di cifratura sia impiegato dal crittografo e dall'abilità del crittanalista. I tedeschi, abbagliati dai puri numeri teorici, non si resero conto di questa distinzione fondamentale. In [30] in forma sintetica e in [31] in forma più particolareggiata, si spiega chiaramente perché i tedeschi abbiano perso non solo la guerra dei codici cifrati ma l'intera guerra: i loro servizi segreti non

seppero mai che gli Alleati ne intercettavano e decrittavano il traffico di messaggi segreti in chiave strategica con regolarità assoluta.

Di fatto, come sempre avviene in crittanalisi, il successo si basò su una serie di piccoli errori commessi dagli operatori. Piccoli, ma imperdonabili – fra i quali l'uso ripetuto di locuzioni stereotipate – e dipendenti, in larga misura, dalla pigrizia e mancanza di fantasia degli addetti alla macchina, se non da incompetenza o frustrazione. Solo in rari casi, i risultati scaturirono da effettive attività di spionaggio.

Proprio nelle piccole debolezze tecniche e umane si insinua la bravura dell'analista crittografo. La lezione è che ogni schema di cifratura, per quanto studiato ed elaborato presenta sempre minute pecche, crepe, fessure in cui incuneare un grimaldello in modo da allargarle e forzare il sistema apparentemente inviolabile. Come accade con le serrature più sofisticate.

4.3 Probabilità e statistica nel Banburismo

Il cuore del metodo inventato da Turing per ridurre il numero dei test che una macchina Bombe doveva effettuare era una statistica intrinsecamente bayesiana [28], [33], soprannominata appunto Banburismo[10]. Il nome era derivato dalla città di Banbury, una cinquantina di chilometri da Bletchley Park, dove venivano prodotte le schede perforate necessarie al processo. Il metodo si basava su un'inferenza logico-statistica per ridurre il numero delle sequenze che Bombe doveva analizzare nella decrittazione finale. Turing, indipendentemente da Shannon, definì anche un'unità di misura dell'informazione su base logaritmica: il "ban" (oppure il suo decimo "deciban" o centesimo "centiban"), termine ancora derivato da Banbury. Poiché i logaritmi erano calcolati su base 10, non è difficile riconoscere che oggi il ban è chiamato "hartley" (per le relazioni di conversione tra le unità di misura dell'informazione, si veda il riquadro 3). Ovviamente un numero di ban per essere espresso in deciban deve essere moltiplicato per 10, o per 100 nel caso dei centiban.

Nel 1940, il termine statistica bayesiana non era ancora stato coniato e, quasi certamente, non sarebbe stato impiegato; la regola (o teorema) di Bayes non godeva, infatti, di buona reputazione tra gli statistici del tempo [28]. Paradossalmente, il fruttuoso ricorso ai metodi bayesiani sarebbe stata assai meno probabile da parte di chi avesse avuto un'educazione standard nei metodi statistici più ortodossi e in uso a quei tempi. Infatti, da decenni l'approccio bayesiano, che Turing avrebbe reso strumento perfetto per attaccare i sistemi di cifratura nemici, era sottoposto ad aspre critiche da parte dei professionisti della statistica.

Ma che si trattasse della regola di Bayes e che Turing ne fosse pienamente consapevole è testimoniato dalla domanda che il suo assistente Jack Good gli fece una volta: "Non stai utilizzando in fondo la regola di Bayes?" "Penso di sì",

[10] Si rinvia ai lavori [28], [34], [35] per approfondimenti sul teorema di Bayes e la relativa inferenza logico-statistica. In particolare, l'articolo [35] contiene in appendice il riquadro "Una cassetta degli attrezzi di probabilità", che riporta i principali strumenti di base utili per entrare in argomento.

fu la risposta di Turing [28], [33] (Turing, ovviamente, ne era pienamente consapevole come si evince anche dal lavoro [36] – cfr. dopo e il riquadro 3).

Probabilmente, pochi all'epoca compresero che il Banburismo era bayesianesimo camuffato dietro l'uso del termine "peso dell'evidenza" misurato secondo l'unita del ban e suoi derivati. In estrema sintesi, il metodo consisteva nel sovrapporre due porzioni del testo per individuarne le corrispondenze. Così si riducevano enormemente le possibili configurazioni di Enigma che una macchina Bombe doveva esaminare in un tempo limitato. Si avvaleva inoltre della statistica bayesiana per calcolare le configurazioni iniziali più probabili, ricorrendo alla frequenza di digrammi (coppie di lettere) o trigrammi tipici della lingua tedesca.

Nell'aprile 2012 (l'anno del centenario della nascita dello scienziato), il GCHQ ha autorizzato il rilascio di due preziosi documenti di Turing, non datati, ma risalenti probabilmente alla seconda metà del 1941, come ben argomentato da Sandy Zabell [36]. Il primo di questi, "The applications of probability to cryptography", discute l'uso generale delle probabilità in crittanalisi, ricorrendo a una versione del teorema di Bayes, che Turing chiama *factor principle*. Il secondo "Paper on statistics of repetitions" è una breve nota sulla classica tecnica di crittanalisi, suggerita, per esempio, dal già citato Sacco [3] e da William Friedman[11], per stimare l'indice di coincidenza nella ricerca di sequenze ripetute (da cui il successivo test di Good-Turing per la stima statistica dell'evenienza di digrammi, trigrammi ecc. nel linguaggio naturale). In [33], Good menziona il manuale di Sacco nella traduzione francese (1951), sia pure storpiando il cognome in "Saccho".

A chiunque possieda competenze statistiche di base sarebbe possibile, seppure alquanto laborioso, estrarre dai due documenti la sostanza del lavoro di Turing. Tuttavia il saggio di Zabell [36] è davvero prezioso poiché commenta estesamente e con chiarezza l'approccio adottato. Il fatto che i due studi siano stati diffusi soltanto nel 2012 dimostra l'enorme importanza loro attribuita dall'intelligence britannica, non solo nel periodo bellico[12].

Già prima della laurea Turing aveva svolto ricerche originali in teoria delle probabilità, dimostrando una forma generale del teorema del limite centrale per variabili aleatorie indipendenti, non necessariamente identicamente distribuite. Il saggio fu presentato come titolo a supporto della sua candidatura a *fellow* (membro del corpo docente) del King's College a Cambridge nel 1935 [23].

---

[11] Il colonnello William Friedman, che dominò la scena crittologica USA tra le due Guerre, è l'autore della pionieristica monografia The Index of Coincidence and its Applications to Cryptography *(1920). Il saggio rappresenta il primo importante passo in avanti verso l'analisi quantitativa in crittanalisi [4], proponendo un metodo che abbina le distribuzioni delle frequenze per ricostruire il testo in chiaro.*

[12] La versione LaTeX dei due manoscritti di Turing, opportunamente ripuliti e risistemati da Ian Taylor (Università di Oxford) sono anche disponibili, dal maggio 2015, su arXiv, rispettivamente ai link http://arxiv.org/abs/1505.04714 e http://arxiv.org/abs/1505.04715.

4.4 Non solo Enigma

Durante il resto della guerra, il traffico di messaggi cifrati, da entrambi i fronti belligeranti, e i tentativi di decrittazione reciproca furono davvero imponente. Per le successive vicende del Regno Unito che hanno contribuito alla nascita dei primi moderni computer – in parte ispirati direttamente o indirettamente da Turing – si rinvia agli ottimi testi [27] e [37].

Il prodotto tecnico-scientifico più importante di questa azione, che oggi definiremmo di *big science*, fu certamente la realizzazione della serie di dieci (proto)computer Colossus costruiti nel periodo dicembre 1943-giugno 1945 da ingegneri e tecnici britannici. Essi rappresentarono i primi elaboratori elettronici (ovviamente a tubi) programmabili di grosse dimensioni ma, per la solita ossessione alla segretezza dei britannici, furono smantellati a guerra conclusa. Almeno così si riteneva fino a poco tempo fa: lo studioso di Turing Jack Copeland argomenta in [27] che almeno due esemplari di Colossus furono impiegati nel dopoguerra per scopi ancora oggi non rivelati.

4.5 Fine dei segreti di guerra?

Dopo il 1940, il seme bayesiano, piantato da Turing, si sviluppò alquanto rigoglioso presso la comunità dei crittanalisti. Jack Good, che sarebbe diventato uno degli apostoli di questo credo, continuò a lavorare al GHCQ dal 1948 al 1959. Dopo la guerra, Good si prodigò per diffondere i capisaldi statistici del Banburismo [33] con determinazione, ancorché con estrema discrezione perché la maggior parte del lavoro crittanalitico bellico continuava ad essere segretato.

Le autorità britanniche permisero che questo velo di segretezza fosse parzialmente sollevato solo nel 1974, l'anno in cui uno dei partecipanti al progetto Ultra, Frederick W. Winterbotham, pubblicò *The Ultra Secret*. Esistono parecchie versioni sul perché Ultra sia stato mantenuto classificato così a lungo. La più accreditata, propugnata da Kahn [4], è che, dopo la guerra, i britannici abbiano raccolto il maggior numero possibile di macchine Enigma per rivenderle a Paesi del Terzo Mondo, fiduciosi di poterne leggerne i messaggi. Solo all'inizio degli Anni 1970 i vecchi apparati furono sostituiti da nuovi crittosistemi. Di sfuggita, si può menzionare che la recensione di Kahn, ripubblicata in [4], ha contribuito a far diventare *Ultra Secret* un bestseller mondiale.

Negli stessi anni cominciò anche a incrinarsi il silenzio sulle vere funzioni svolte da Bletchley Park e il pieno riconoscimento della sua importanza strategica. Sorprendentemente, in *The Ultra Secret*, il nome di Turing non appare. Compare invece, e frequentemente, in un altro libro – alle volte eccessivamente fantasioso – uscito nello stesso 1974: *Bodyguard of Lies* di Anthony Cave Brown, nel quale, Turing è spesso associato a termini quali *machine* e *Bombe*.

Dopo *Ultra Secret* e *Bodyguard*, fu pubblicata la prima edizione della monumentale e tuttora insuperata biografia su Turing di Hodges [23], cui si aggiunsero con ritmo accelerato resoconti, memoriali, reminescenze, ricordi dei membri originali del gruppo di crittanalisti, costretti per decenni a un sofferto quanto dignitoso silenzio. Kahn in [6] acutamente osserva che, se il primo più grande segreto della Seconda guerra mondiale fu la bomba atomica, il secondo fu che gli Alleati erano stati in grado di leggere i messaggi cifrati dei tedeschi a loro insaputa.

Negli ultimi decenni Turing è diventato un'icona mediatica su cui si è scatenata la fantasia di scrittori a registi, dal romanzo cult *Cryptonomicon* di Neal Stephenson[13] al film *The Imitation Game*, che ha dato ulteriore impulso al mito di Turing anche tra chi non lo conosceva affatto.

5. Conclusioni

Quanto detto in precedenza non ha solo un interesse storico, documentario, o aneddotico. Infatti, oggi le violazioni della sicurezza e gli attacchi di pirateria informatica costituiscono un problema diffuso e pervasivo [38] da diversi punti di vista: economico, politico, sociale, etico. Dal momento che i cyberattacchi, in ultima istanza, risultano da intendimenti dolosi condotti sulle configurazioni dei dati disponibili in una rete o in un elaboratore, non si può consentire che sistemi complessi (frutto dei nuovi paradigmi ICT[14] in forte sviluppo quali cloud computing, IoT/IoE, big data, software defined network/radio) siano vulnerabili ai prevedibili attacchi futuri. Il gioco di creare sistemi cifrati e quello di forzarli è sempre più vivo. E trova terreno alquanto fertile nel Web.

La crittografia è certamente uno strumento di sicurezza indispensabile per assicurare che il messaggio non sia letto da nessun altro se non dal destinatario autorizzato. Nel mondo economico – sia privato sia degli affari – i sistemi crittografici sono usualmente impiegati per proteggere i dati trasportati su reti pubbliche di telecomunicazioni e usano algoritmi matematici molto evoluti per "rimescolare" i messaggi (e i testi allegati).

Peraltro, online nulla è protetto, nessuna crittografia, benché strumento di protezione basilare, resiste per sempre, come osserva Cory Doctorow in *Information Doesn't Want to Be Free: Laws for the Internet Age*. Alla lunga gli invasori, ladri, pirati, militari – sempre più scaltri (*smart*) – trovano il Cavallo di Troia o la breccia per entrare nel sistema che si vorrebbe protetto. Identità personali, segreti economici, di stato o impresa, sono a rischio cyberguerra (cfr. Gianni Riotta, *La Stampa*, 21 dicembre 2014). Già Edgar Allan Poe ammoniva saggiamente: "Si può tranquillamente affermare che l'ingegnosità umana non può elaborare un cifrario che la stessa ingegnosità umana non riesca a risolvere". Così insegnano la violazione ripetuta di Enigma, la previsione eccessivamente ottimistica di Martin Gardner sulla robustezza dei sistemi a chiave pubblica [39], la quotidianità della pirateria informatica.

Peter Drucker, il grande guru del management nel secolo scorso, scrisse "Siamo viepiù consapevoli che la questione principale concernente la tecnologia non è tecnica ma umana". Parafrasandolo, potremmo quindi dire che stiamo ritornando consapevoli che la questione principale concernente la "sicurezza" non è tecnica ma umana: per una rassegna delle linee-guida di possibili soluzioni a criticità legate al fattore umano si veda il recentissimo [40].

---

[13] Una curiosità: il romanzo riporta una conversazione (ovviamente immaginaria) tra Turing e un personaggio fittizio, Lawrence Waterhouse, a riguardo del primo vocoder SIGSALY per comunicazioni vocali segrete (v. il riquadro 2).

[14] Information and Communications Technology.

Uno degli esiti principali di questo processo lungo più di settant'anni e del quale Shannon e Turing sono stati protagonisti assoluti è la "matematizzazione" della crittologia (crittografia + crittanalisi) nelle varie branche componenti: logica simbolica e algebra booleana, teoria della complessità, computabilità, probabilità e statistica, ecc. I loro studi hanno permesso di distinguere nettamente quanto in crittologia sia scienza da quanto sia arte (o soluzione ad hoc). Naturalmente, ed è stato prima ricordato, a questo sviluppo hanno cooperato molti altri fra cui il nostro Luigi Sacco e lo statunitense William Friedman. Viene in mente il celeberrimo aforisma di Bernardo di Chartres: "Siamo nani sulle spalle di giganti", ripreso secoli dopo da Isaac Newton, che con sottile perfidia scriveva al nano Robert Hooke: "Se ho visto più lontano è perché stavo sulle spalle di giganti".

Proprio come l'interesse primario di Turing non era nel *code-breaking* ma nella computabilità, così l'interesse precipuo di Shannon non era nell'occultare l'informazione ma nel trasmetterla e nel riceverla nel modo più accurato possibile, cioè (quasi) senza errori. Tuttavia la storia scientifica dei due studiosi dimostra che i loro interessi principali e secondari, strettamente interconnessi, si arricchirono a vicenda.

Tra di loro ci furono però differenze significative. Shannon stabilì i principi fondamentali dei sistemi segreti, cioè della crittografia. Da solo. Non si occupò direttamente delle implicazioni pratiche [41], a parte il contributo allo sviluppo del digital scrambler di SIGSALY. Le imprese di Turing furono piuttosto opera di un *primus inter pares*; tant'è che poté lasciare Bletchley Park per la collaborazione in America (nell'inverno 1942-43). In ruoli allo stesso tempo diversi e complementari, furono due giganti del pensiero, precursori della grande e migliore scienza (big science) in questo XXI secolo. Il lavoro a Bletchley Park è anche un esempio del paradigma universalmente noto come big data, un'etichetta oggi forse già un po' troppo alla moda, quasi un tic culturale.

Né Shannon né, tantomeno, Turing hanno contribuito direttamente agli sviluppi più importanti della disciplina emersi a partire dagli Anni Settanta del Novecento, per esempio, ai sistemi a chiave pubblica, nei quali una chiave segreta condivisa tra le parti comunicanti non è necessaria per garantire la segretezza. Tuttavia, questi e altri contributi – anche quelli più recenti – sono concettualmente debitori agli studi di entrambi.

Così mi pare di poter sintetizzare, al termine della lettura di svariati studi crittologici, in un articolo che più che inseguire un'ambizione di completezza ha cercato di restituire modalità di lavoro e di approccio ai problemi da parte di Shannon e Turing. Il vastissimo materiale sugli argomenti qui sommariamente trattati appare di mole ulteriormente crescente negli ultimi decenni dopo che il velo di segretezza riguardante i documenti dei servizi segreti in vari Paesi è stato parzialmente sollevato. Solo una parte di questi lavori è stata qui utilizzata benché in forma estremamente sintetica e panoramica. Una trattazione sufficientemente dettagliata di tutti gli argomenti, accompagnata da un commento adeguato, riempirebbe un volume di centinaia di pagine. Pertanto, nella rassegna si è accennato solo per sommi capi agli eventi e ai risultati principali, privilegiando l'aspetto tecnico-scientifico pur con qualche

divagazione storica e narrativa. Si rimandano al futuro eventuali approfondimenti su aspetti particolari o più circoscritti.

In conclusione, non sembra inutile sottolineare un'ultima lezione di carattere metodologico nel lascito di Shannon e Turing. Per imparare a gestire scelte sempre più complesse, occorre investire sulla propria intelligenza, sul pensiero logico e critico utilizzando due saperi di base: la teoria della probabilità e la psicologia del rischio. I risvolti pratici di queste competenze – delle quali molti, troppi, sono del tutto digiuni tanto nella mentalità quanto negli strumenti [34], [35] – sono oggetto di ricerche avanzate ben rappresentate da studiosi quali Daniel Kahneman [42] e Gerd Gigerenzer [43]. Beninteso, la razionalità pura deve essere integrata da un'ulteriore competenza basata sull'intuizione che porta all'euristica [43], ossia alla "regola del pollice", e che solo l'esperienza può insegnare.

In Italia, purtroppo, il vezzo di esibire la propria ignoranza in fatto di tecnoscienza era e resta uno degli esercizi preferiti di certa intellighenzia. Di tale ignoranza continua, infatti, a vigere la legittimazione sancita, ormai più di un secolo fa, dal "crocianesimo", l'idealismo crociano in tutte le sue declinazioni, e ribadita, in anni più recenti, dagli epigoni del pensiero debole e di Heidegger. Quest'ultimo con la sentenza lapidaria "la scienza non pensa" ha autorizzato generazioni di giovani a non impegnarsi nello studio di competenze cruciali per lo sviluppo di un Paese. Gli zelanti campioni nostrani delle cosiddette scienze umane (tutte le altre sono forse "inumane"? [44]) si compiacciono di svilire *in toto* i saperi afferenti alle discipline STEM – acronimo che denota l'insieme di scienza, tecnologia, ingegneria (*engineering*) e matematica [45] – anziché considerarne l'espansione una priorità nazionale, come tradizionalmente avviene negli USA e, in generale, nelle nazioni all'avanguardia culturale, civile, sociale, economica.

Ringraziamenti

Sono sinceramente grato a quanti mi hanno amichevolmente aiutato a reperire l'ampia documentazione di riferimento, rispondendo positivamente alle mie pressanti richieste: Alfredo Biocca, Marina Dambrosio, Letterio Gatto, Pietro Laface, Steven J. Miller, Maurizio Molinaro, Andrea Nicolotti, Giancarlo Pirani, Klaus Pommerening, Laura Porello, Rebecca A. Ratcliff, Dirk Rijmenants, Viola Schiaffonati, Fabrizio Trisoglio, Sandy Zabell. Spero che l'elenco non contenga dimenticanze imperdonabili.

Ringrazio, inoltre, un anonimo revisore le cui acute e pertinenti osservazioni mi hanno permesso di focalizzare i contenuti dell'articolo e di precisare i punti non sufficientemente chiari nella stesura iniziale.

Infine, mi sembra opportuno ricordare i molti strumenti tecnologici e culturali disponibili sul Web, soprattutto Google e Wikipedia, che liberano di continuo risorse altrimenti introvabili con i mezzi tradizionali. E, contrariamente alla vulgata corrente, queste fonti di documentazione – non solo di origine accademica – si sono mostrate, il più delle volte, affidabili e autorevoli.

Riquadro 1 – "1941: l'MI5 cerca la talpa di Agatha Christie"* e altri aneddoti

Nel 1941 la vita dell'ignara Agatha Christie divenne per qualche mese un racconto di Borges, fatto di specchi e allusioni inquietanti, mentre la trama del suo ultimo giallo si rovesciava, ben più temibile, nell'esperienza quotidiana.

I servizi segreti britannici erano infatti convinti che nel suo *N or M*, pubblicato nel novembre 1941, ma tradotto in Italia solo nel 1961 con il titolo *La quinta colonna*, ci fosse un riferimento alle attività del segretissimo centro di decifrazione [decrittazione] di Bletchley Park che era riuscito a trascrivere il codice cifrato tedesco Enigma, con enorme vantaggio per gli inglesi.

Il giallo racconta le avventure di una coppia di detective, Tommy and Tuppence, che danno la caccia a due agenti nazisti, infiltrati in Inghilterra per preparare un'invasione, noti appunto col nome in codice *N* e *M*. L'MI5, il controspionaggio britannico, rabbrividì quando lesse il nome di un personaggio secondario, il maggiore Bletchley, guarda caso, un "noioso ufficiale" che aveva servito in India e si vantava di conoscere molti segreti della guerra in corso.

I primo sospetti caddero su Dilly Knox uno dei più dotati decifratori [decrittatori] a Bletchley Park, che era amico della Christie. Fu subito scagionato ed escluse che la scrittrice potesse sapere qualcosa del centro segreto ma accettò di sentirla. Davanti a un vassoio di tè e pasticcini, nella sua casa nel Buckinghamshire le chiese perché avesse proprio scelto quel nome. "Bletchley? – rispose la scrittrice – Mio caro, ero proprio lì, bloccata in treno sulla linea Oxford-Londra, allora mi sono vendicata chiamando così uno dei miei personaggi meno gradevoli."

È già stato sottolineato che le vicende di Bletchley Park non hanno rappresentato un *one-man show* (cioè Alan Turing da solo), come si potrebbe invece supporre seguendo resoconti mediatici troppo superficiali e mistificanti. In realtà, i ragguardevoli personaggi che si sono occupati di crittanalisi durante la Seconda guerra mondiale sono stati in generale spiriti bizzarri e ameni, spesso dotati di grande creatività.

Assistente di Turing a Bletchley Park fu Jack Good che successivamente, dal 1967 al 1994, insegnò in USA al Virginia Polytechnic Institute and State University. Una sua arguta osservazione fu: "Sono arrivato a Blacksburg alla settima ora del settimo giorno del settimo anno nel settimo decennio, e fui alloggiato nell'Appartamento 7 dell'edificio 7… e tutto per caso"**. Quando si parla di coincidenze fortuite! (Su questo argomento non abbiamo certo nascosto il nostro scetticismo nell'articolo [35]). Good, che fu consulente di Stanley Kubrick per l'intelligente supercomputer HAL 9000 nel film *2001: Odissea nello spazio*, è anche noto per l'ironica

affermazione di avere contato "almeno 46.656 interpretazioni differenti" di teorie bayesiane [28], un numero ben superiore a quello degli statistici professionisti.

Uno dei più giovani colleghi di Turing a Bletchley Park fu Peter Hilton*** il quale, per puro *divertissement*, costruì in una notte insonne il palindromo di 51 lettere: DOC NOTE, I DISSENT. A FAST NEVER PREVENTS A FATNESS. I DIET ON COD, tuttora il più lungo della lingua inglese. Hilton ha ricordato nelle sue reminescenze di crittanalista [46] l'osservazione invero *tranchant* ma pertinente di Good: "Fortunatamente, le autorità di Bletchley Park non avevano la minima idea che Turing fosse omosessuale; altrimenti, avremmo perduto la guerra".

Un'altra figura da menzionare è Ian Fleming – il futuro creatore del mitico James Bond – che operò come ufficiale di collegamento tra Bletchley Park e la Naval Intelligence per tutto il periodo bellico. Fleming morì nel 1964, dieci anni prima che il velo di segretezza su Bletchley Park fosse sollevato. Perciò non poté mai svelare il suo coinvolgimento nelle faccende segrete di Enigma e Ultra, nonché i contatti con Turing per l'Operazione *Ruthless* [28], sebbene il suo avvincente lavoro in tempo di guerra abbia ispirato le imprese dell'Agente 007. Anche l'attore Christopher Lee, memorabile nelle sue interpretazioni del conte Dracula e cugino acquisito di Fleming, operò nei servizi segreti britannici durante la guerra.

** È il titolo dell'articolo di Giorgio Gallo (*La Stampa*, 5 febbraio 2013) dal quale sono ripresi (con adattamenti editoriali) i primi quattro capoversi del riquadro. Il curioso aneddoto sulla Christie è stato svelato dall'esperto di SIGINT Michael Smith [24].*

*** Cfr. http://en.wikipedia.org/wiki/I._J._Good.*

**** Hilton figura anche nel film* The Imitation Game.

Riquadro 2 – Turing incontra Shannon ai BTL: il sistema X (o SIGSALY)

Alla fine del 1941, con l'entrata degli USA in guerra, i BTL portavano avanti diversi progetti sui sistemi segreti, specialmente sullo *speech scrambling* (mescolamento vocale) per proteggere le comunicazioni da orecchie indiscrete. Uno di questi – denominato Sistema X o SIGSALY* [47] – era probabilmente il più segreto di tutti poiché riguardava lo sviluppo di un sistema radiotelefonico per connettere Churchill a Roosevelt. (Anche SIGSALY sarebbe rimasto fino al 1975 "un sistema del quale non si poteva parlare" [23]).

Shannon lavorò sul progetto benché, per ragioni di segretezza, non avesse accesso a tutti i particolari e fosse vincolato a non interagire con altri sull'argomento. Resta il fatto che si occupava del cuore del sistema, ossia proprio dello schema di cifratura, il blocco monouso di Vernam citato al punto 2.2. Il compito di Shannon era di verificare che nessun dettaglio fosse trascurato e che il metodo fosse veramente imbattibile.

Nel gennaio 1943, Turing andò New York per fornire consulenza su molti aspetti dello speech scrambling e, restando in USA per due mesi, ebbe saltuarie conversazioni con Shannon nella mensa aziendale dei BTL, durante le pause pranzo o del pomeriggio. Fatto abbastanza curioso è che essi non poterono discutere i rispettivi lavori sottoposti al vincolo del segreto militare. Parlarono invece di argomenti di interesse reciproco, allora ritenuti non confidenziali, come la nuova scienza dei computer e l'evenienza di macchine in grado di simulare il cervello umano.

La partecipazione di Turing e Shannon in questo progetto è descritta con abbondanza di particolari aneddotici da Hodges [23], per la verità con un linguaggio che nelle parti tecniche suona un po' datato a chi si occupa oggi di telecomunicazioni nell'ICT.

Lavorando per decrittare i messaggi di Enigma, Turing sviluppò un tipo di misura dell'informazione molto simile a quella pubblicata da Shannon solo nel 1948 [18]. L'unità di informazione di Shannon era il "bit", di Turing il "ban". Non sembra, tuttavia, che lo scienziato britannico abbia contribuito alle intuizioni fondamentali della teoria dell'informazione, infatti, Shannon su queste idee ricevette da Turing "… un bel po' di riscontri negativi" [41].

Volendo sottolineare una differenza tra Shannon e Turing, si può indicare il minor interesse pratico del primo per le applicazioni rispetto ai problemi: "Sembra che [Shannon] abbia preferito lavorare sui problemi allo scopo di comprendere e trovare soluzioni, senza preoccuparsi di applicazioni militari o essere distolto dal suo obiettivo puntando troppo su applicazioni di ogni tipo" [41]. Non è però del tutto vero: cfr. [17] per una descrizione dell'interesse molto pratico e remunerativo, benché non prioritario, di Shannon per l'azzardo e la finanza.

I due scienziati si incontrarono ancora in Inghilterra nel settembre 1950 in occasione di un simposio sulla teoria dell'informazione, nel quale Shannon era l'ospite d'onore. Si confrontarono su una strategia minimax proposta da Shannon per il gioco degli scacchi e sui calcoli di Turing sulla funzione zeta.

In definitiva, anche se le relazioni dirette tra Shannon e Turing furono scarse, peraltro la comunanza di interessi fu straordinaria come dimostra il complesso dei loro lavori, disponibili nei rispettivi *Collected Works* – un unico volume dell'IEEE Press per Shannon, e quattro (costosissimi) tomi della Norh Holland per Turing.

Tornando al sistema SIGSALY, un cospicuo gruppo di progettisti dei BTL, sotto la direzione di A. B. Clark (che successivamente avrebbe guidato le attività di ricerca e sviluppo della NSA nel biennio 1954-55), sviluppò il

codificatore vocale (vocoder) con particolare attenzione alla qualità della voce. L'articolo di rassegna storica [48] attribuisce al sistema varie priorità di tecnica delle comunicazioni, fra cui:

- la realizzazione della telefonia cifrata
- la quantizzazione del segnale vocale
- la trasmissione della voce in PCM (Pulse Code Modulation)
- l'impiego della modulazione numerica multilivello FSK (Frequency Shift Keying)
- la realizzazione della compressione di banda del segnale vocale
- l'impiego della tecnologia ad "allargamento dello spettro" (Spread Spectrum)

Per le sue peculiarità innovative SIGSALY potrebbe essere considerato addirittura come il primo passo verso la rivoluzione digitale. Le tecniche di spread spectrum avrebbero poi avuto un grande impatto sullo sviluppo delle attuali comunicazioni mobili cellulari (cfr. i contributi di Andrew Viterbi, studioso italiano di famiglia e di nascita).

Kahn in [47] ricorda che Shannon e Turing – insieme con un nutrito gruppo di esperti dei BTL, fra cui Harry Nyquist** – contribuirono alla concezione e allo sviluppo di SIGSALY sia per la parte di comunicazione sia per gli aspetti di sicurezza e riservatezza. Kahn cita anche il curioso episodio di Hedy Lamarr, celebre attrice della prima metà del Novecento, che ottenne nel 1942 il rilascio di un brevetto basato sul *frequency hopping*, un particolare schema di spread spectrum, con applicazione al controllo radio di siluri navali.

Di ritorno dall'America, Turing diede un altro grande esempio delle sue capacità di visione e progettualità creando per il Radio Security Service britannico a Hanslope Park lo scrambler *Delilah*, il primo esempio di sistema portatile e digitale per comunicazioni vocali sicure – realizzato purtroppo troppo tardi per poter diventare operativo.

** Il nome SIGSALY non significava alcunché, era solo un criptonimo somigliante a un acronimo.*

*** Il suo teorema del campionamento (1928) avrebbe contribuito ad aprire la strada alle comunicazioni numeriche e, subito dopo, all'era dell'informazione digitale.*

Riquadro 3 – Teoria dell'informazione e probabilità: terminologia e metriche

In un sistema di trasmissione dell'informazione (trasmettitore + canale + ricevitore), a mano a mano che si riceve l'informazione sul messaggio trasmesso, diminuisce l'incertezza nel ricevitore. Un semplice esempio consente di illustrare questo concetto apparentemente ovvio ma fondamentale. Si supponga di considerare: 1) un canale ideale che non introduce né rumore né distorsione, 2) che i messaggi possibili siano otto, tutti codificati in binario, e 3) che fra questi venga trasmesso il secondo, codificato nella successione 001. La ricezione del primo simbolo 0 elimina una parte dell'incertezza relativa al messaggio trasmesso: infatti, l'informazione rappresentata dallo zero restringe il campo dei messaggi trasmessi a solo quattro. Analogamente la ricezione del secondo 0 restringe il campo di possibili messaggi solo a 000 e 001, finché la ricezione dell'1 elimina ogni dubbio. La probabilità dei singoli messaggi dopo la ricezione di ciascun simbolo si può calcolare applicando la definizione di probabilità condizionata e, quindi, utilizzando la regola di Bayes [28], [34], [35] (non è necessario ipotizzare che la distribuzione di probabilità degli otto messaggi sia uniforme).

L'esempio della logica seguita (un'inferenza bayesiana a tre passi) fornisce il punto di partenza del ragionamento di Shannon, che è anche quello di Turing nel Banburismo, sia pure con una terminologia diversa: fattore bayesiano e peso dell'evidenza. Il fattore di Bayes è definito come la probabilità del dato osservato in una certa ipotesi, divisa per la probabilità in un'altra ipotesi – oggi detto "rapporto di verosimiglianza" (*likelihood ratio*). Il peso, o misura, dell'evidenza – il contenuto informativo secondo Shannon – ne è il suo logaritmo. Su una scala logaritmica, un fattore di soglia decisionale di 50 a 1 (*odds*) è rappresentato da un punteggio di 1,7 ban (oggi Hart), o 17 deciban, infatti, il logaritmo in base 10 di 50 è 1,7. Il peso dell'evidenza è sostanzialmente equivalente alla misura logaritmica dell'informazione, che Turing formulò e usò indipendentemente da Shannon.

Il peso dell'evidenza fu anche usato nel metodo – interamente manuale con carta, matita e gomma – noto come *Turingery* (1942), concepito sempre da Turing per dedurre l'impostazione delle ruote della macchina cifrante soprannominata "Tunny" a Bletchley Park (Tunny era una Lorenz della serie di telescriventi SZ sviluppate dopo Enigma: al volume collettaneo [27] si rinvia per una trattazione aggiornata ed esauriente). Come ricordato in 4.3, il Banburismo consentì a Turing di evitare il metodo computazionale della cosiddetta forza bruta (il tener conto di "tutti i casi possibili") nella ricerca del messaggio in chiaro. Questo sarebbe stato, infatti, un approccio destinato al fallimento con i mezzi di calcolo allora disponibili. Sostanziale fu la riuscita del processo di meccanizzazione del giudizio attraverso la quantificazione del peso dell'evidenza,

un'anticipazione dei sofisticati programmi inferenziali bayesiani oggi usati nelle applicazioni di intelligenza artificiale. Infine, gli stessi principi del Banburismo – fattori di Bayes e loro logaritmi, in una logica sequenziale, per discriminare tra due ipotesi – sono stati i fondamenti generali della ricerca operativa, a partire dal controllo di qualità.

Nella metrica dell'informazione, la base dei logaritmi determina l'unità impiegata secondo lo standard ISO/IEC [49]:

- shannon (simbolo: Sh) per i logaritmi di base 2
- unità naturale (simbolo: nat) per i logaritmi di base *e*
- hartley (simbolo Hart) per i logaritmi di base 10

Ne risulta la tabella di conversione:

- 1 Sh = 0,693 nat = 0,301 Hart
- 1 nat = 1,433 Sh = 0,434 Hart
- 1 Hart = 3,322 Sh = 2,303 nat

Benché il "bit" in pratica sia più comune dello "shannon", anche come misura dell'informazione binaria, diversamente però vorrebbe lo standard [49]: il bit, a stretto rigore, è un termine d'uso generico.

Probabilità e odds. Com'è caratteristico del mondo delle scommesse in Paesi di cultura anglosassone, Turing e i suoi collaboratori a Bletchey Park lavoravano con le *odds* (quote, posta, pronostico) a favore di un evento anziché con la probabilità dello stesso evento*. Odds e probabilità costituiscono due rappresentazioni, o forme, diverse per valutare la possibilità che un determinato evento accada. Si consideri, per esempio, il caso di due assi estratti da un mazzo di 52 carte. La probabilità di questo evento congiunto è $P = 4/52 \times 3/51 = 1/221$: statisticamente, una volta su 221 capita la coppia d'assi. Spesso, soprattutto nell'ambiente delle scommesse, si preferisce indicare che le possibilità contrarie rispetto a quelle favorevoli sono di 221 meno 1, cioè di 220 a 1, o anche che le quote a sfavore sono di 220 : 1. Statisticamente, per ogni 220 casi sfavorevoli ce ne sarà uno favorevole. Le quote a favore sono ovviamente il reciproco, cioè 1 : 200.

In generale, la probabilità $P(A)$ di un evento A è il rapporto tra il numero di casi favorevoli e il numero totale di casi; le quote (odds) a favore $OF(A)$ sono il rapporto tra il numero di casi favorevoli e il numero di casi sfavorevoli. Le relazioni tra probabilità $P(A)$ e odds a favore $OF(A)$ sono: $OF(A) = P(A)/[1 - P(A)]$ e $P(A) = OF(A)/[1+OF(A)]$. Si noti che $OF(A)$, funzione monotona crescente di $P(A)$, tende asintoticamente all'infinito quando $P(A) = 1$. Se $OF(A)$ è esprimibile con il rapporto m/n, la corrispondente probabilità diventa $m/(m + n)$; per esempio, $OF(A) = 1/3$ e $P(A) = 1/4$. Per un evento con probabilità di 2/3, le quote sono di 2 a 1 (o di 2 : 1), mentre, per un evento di probabilità 3/10, le quote sono 3 : 7. Una

remunerazione di *r* a 1 significa che il banco (o l'allibratore) onora la vincita del giocatore con *r* + 1 euro per ogni euro scommesso, altrimenti incamera la posta giocata.

In definitiva, i due termini probabilità e odds, pur esprimendo lo stesso concetto matematico, assumono valori numerici diversi, ancorché legati da semplici relazioni matematiche.

** Già secoli fa, il concetto di odds era stato efficacemente introdotto, con il termine latino di* proportio*, da Girolamo Cardano nel* Liber de ludo aleae*, opera pubblicata postuma nel 1663. Per un'eccellente ed esauriente trattazione di odds (definizioni, relazioni matematiche, esempi applicativi nei diversi contesti, riferimenti bibliografici), il lettore interessato può ricorrere, in prima istanza, alla voce omonima di Wikipedia (https://en.wikipedia.org/wiki/Odds).*

Bibliografia

[1] Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communications from Ancient Times to the Internet* (Nuova edizione), Scribner. Prima edizione (1967). Macmillan. Tr. it. parziale della prima edizione (1969). *La guerra dei codici. La storia dei codici segreti*, Mondadori.

[2] Kahn, D. (2004). *The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking*, Yale University Press.

[3] Sacco, L. (2014). *Manuale di crittografia* (Quarta edizione ampliata a cura di Bonavoglia, P.), Apogeo.

[4] Kahn, D. (1983). *Kahn on Codes: Secrets of the New Cryptology*, Macmillan.

[5] Kahn, D. (2012). *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943* (Edizione rivista), Frontline Books.

[6] Kahn, D. (2014). *How I Discovered World War II's Greatest Spy and Other Stories of Intelligence and Code*, CRC Press.

[7] Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Doubleday Books. Tr. it. (1999). *Codici & segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet*, Rizzoli.

[8] Bauer, C.P. (2013). *Secret History: The Story of Cryptology,* CRC Press.

[9] Simmons, G.J. (Contributore principale) (2012). "Cryptology", *Encyclopedia Britannica Online*, http://www.britannica.com/EBchecked/topic/145058/cryptology (ultimo accesso maggio 2015).

[10] Simmons, G.J. (a cura di) (1992). *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press-Wiley.

[11] Paar C., Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioner,* Springer.

[12] Martin, K.M. (2012). *Everyday Cryptography: Fundamental Principles and Applications*, Oxford University Press.

[13] Fabris, F. (2001). *Teoria dell'informazione, codici, cifrari*, Bollati Boringhieri, 2001.

[14] Kerckoffs, A. (1883). "La cryptographie militaire", *Journal des sciences militaires*, vol IX, n.1, 5-38 e n. 2, 161-191.

[15] Vernam, G.S. (1926). "Cipher printing telegraph systems for secret wire and radio telegraph communications", *Journal of the American Institute of Elecrical Engineers*, vol. 55, n. 2, 109-115.

[16] Bellovin, S.M. (2011). "Frank Miller: Inventor of the one-time pad", *Cryptologia*, vol. 35, n. 3, 203-222.

[17] Luvison, A. (2012). "Teoria dell'informazione, scommesse, giochi d'azzardo", *Mondo Digitale – Rassegna critica del settore ICT*, anno XI, n. 42, 1-16, http://mondodigitale.aicanet.net/2012-2/articoli/05_luvison.pdf (ultimo accesso maggio 2015). Id. (2012). "Quando la teoria dell'informazione gioca d'azzardo", *AEIT*, vol. 99, n. 10, 56-65. (Le due versioni dell'articolo differiscono marginalmente in pochi passaggi). Per un aggiornamento sintetico, cfr. Id. (2015). "L'azzardo di Shannon", *MIT Technology Review* (Edizione italiana), anno XXVII, n. 1, 52-53.

[18] Sloane, N.J.A., Wyner, A.D. (a cura di) (1993). *Claude Elwood Shannon: Collected Papers*, IEEE Press.

[19] Shannon, C.E. (1949). "Communications theory of secrecy systems", *Bell System Technical Journal*, vol. 48, n. 4, 656-715, ristampato in [18], 84-143.

[20] Massey, J.L. (1992). "Contemporary cryptology: An introduction", in [10], 1-39.

[21] Hinsley, F.H., Stripp, A. (a cura di) (1993, ristampa 2001). *Codebreakers: The Inside Story of Bletchley Park*, New York: Oxford University Press.

[22] Copeland, B.J. (a cura di) (2004). *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life; Plus the Secrets of Enigma*, Oxford University Press.

[23] Hodges, A. (1991). *Storia di un enigma. Vita di Alan Turing (1912-1954)*. Nuova edizione (2014). *Alan Turing. Storia di un enigma*, Bollati Boringhieri.

[24] Smith, M. (2013). *Bletchley Park: The Code-breakers of Station X*, Shire Publications.

[25] Rejewski, M. (1981). "How Polish mathematicians deciphered the Enigma", *IEEE Annals of the History of Computing*, vol. 23, n. 3, 213-234. (L'articolo contiene due commenti finali – il primo di Cipher Deavorus, esperto crittanalista, il secondo di Jack Good, collaboratore di Turing a Bletchley Park).

[26] Alexander, C.H.O'D. (circa 1945). *Cryptographic History of Work on the German Naval Enigma*, The National Archives – Government Communications Headquarters GCHQ, Reference HW 25/1, http://www.ellsbury.com/gne/gne-000.htm (ultimo accesso maggio 2015).

[27] Copeland, B.J. *et al.* (2010). *Colossus: The Secrets of Bletchley Park's Codebreaking Computers*, Oxford University Press.

[28] McGrayne, S.B. (2012). *The Theory That Would Not Die: How Bayes' Rule Cracked the Enigma Code, Hunted Down Russian Submarine, & Emerged Triumphant from Two Centuries of Controversy*, Yale University Press.

[29] Miller, A.R. (1995). "The cryptographic mathematics of Enigma", *Cryptologia*, vol. 19, n. 1, 65-80.

[30] Ratcliff, R.A. (2003). "How statistics led the Germans to believe Enigma secure and why they were wrong: Neglecting the practical mathematics of cipher machines", *Cryptologia*, vol. 27, n. 2, 119-131.

[31] Ratcliff, R.A. (2006). *Delusions of Intelligence. Enigma, Ultra, and the End of Secure Cyphers*, Cambridge University Press.

[32] Welchman, G. (1997). *The Hut Six Story: Breaking the Enigma Codes* (Seconda edizione rivista), Classic Crypto Books.

[33] Good, I.J. (1979). "Studies in the history of probability and statistics: XXXVII A. M. Turing's statistical work in World War II", *Biometrika*, vol. 66, n.2, 393–396. Ristampato, con un ampio commento di Good, in Britton, J.L. (a cura di) (1992). *Collected Works of A.M. Turing: Pure Mathematics*, North Holland, 207-223.

[34] Luvison, A. (2013). "Apologia della ragione scientifica", *Mondo Digitale – Rassegna critica del settore ICT*, anno XII, n. 45, 1-28, http://mondodigitale.aicanet.net/2013-1/articoli/05_LUVISON.pdf (ultimo accesso maggio 2015).

[35] Luvison, A. (2014). "Apologia della ragione scientifica – II: strumenti per decidere", *Mondo Digitale – Rassegna critica del settore ICT*, anno XIII, n. 55, 1-32, http://mondodigitale.aicanet.net/2014-7/articoli/03_Apologia_della_ragione_scientifica_II.pdf (ultimo accesso maggio 2015).

[36] Zabell, S. (2012). "Commentary on Alan M. Turing: The applications of probability to cryptography", *Cryptologia*, vol. 36, n. 3, 191-214.

[37] Hénin, S. (2014). *Come le violette a primavera. Storia dei molti personaggi e delle molte idee che contribuirono alla nascita dell'innovazione più incisiva del XX secolo: il computer,* AICA.

[38] Mezzalama, M., Lioy, A., Metwalley, H. (2013). "Anatomia del malware", *Mondo Digitale – Rassegna critica del settore ICT*, vol. XII, n. 47, pp. 1-20, http://mondodigitale.aicanet.net/2013-3/articoli/02_Anatomiadelmalware.pdf (ultimo accesso maggio 2015).

[39] Gardner, M. (1977). "Mathematical games: A new kind of cipher that would take millions of years to break", *Scientific American*, vol. 237, n. 2, 120-124.

[40] Winnefeld, J.A., Jr., Kirchoff, C., Upton, D.M. (2015). "Cybersecurity's human factors: Lessons from the Pentagon", *Harvard Business Review*, vol. 93, n. 9, 86-95.

[41] Price, R. (1984). "A conversation with Claude Shannon: One's man approach to problem solving", *IEEE Communications Magazine*, vol. 22, n. 5, 123-126. Estratto da "Oral history: Claude E. Shannnon", Interview # 423 conducted by Robert Price for the IEEE History Center, 28 July 1982, http://www.ieeeghn.org/wiki/index.php/Oral-History:Claude_E._Shannon (ultimo accesso maggio 2015).

[42] Kahneman, D. (2012). *Pensieri lenti e veloci*, Mondadori.

[43] Gigerenzer, G. (2015). I*mparare a rischiare. Come prendere decisioni giuste*, Cortina.

[44] De Mauro, T. (2011). "Scienze *inumane* e scienze *inesatte*?" in Lingiardi, V., Vassallo, N. (a cura di), *Terza cultura. Idee per un futuro sostenibile*, il Saggiatore, 102-108.

[45] Temes, G., Solymar, L. (2015). "In defense of engineering education", *Proceedings of the IEEE*, vol. 103, n. 8, 1243-1246.

[46] Hilton, P. (2000). "Reminescences and reflections of a codebreaker" in Joyner, D. (a cura di), *Coding Theory and Cryptography: From Enigma and Geheimschreiber to Quantum Theory*, Springer, 1-8.

[47] Kahn, D. (1984). "Cryptology and the origins of spread spectrum", *IEEE Spectrum*, vol. 21, n. 9, 70-80. Ristampato in [6], 135-163.

[48] Bennett, W.R. (1983). "Secret telephony as a historical example of spread-spectrum communications", *IEEE Transactions on Communications*, vol. COM-31, n. 1, 98-104.

[49] ISO/IEC 2382 – 16 (1996). *Information Technology – Vocabulary – Part 16: Information Theory*.

Biografia

Angelo Luvison è ingegnere elettronico dal 1969 (Politecnico di Torino) con successivi perfezionamenti in teoria statistica delle comunicazioni al MIT e management aziendale all'INSEAD-CEDEP di Fontainebleau. Per oltre trent'anni in CSELT, ha svolto e coordinato ricerche in teoria delle comunicazioni, reti di fibre ottiche ad alta velocità, società dell'informazione. È stato professore di *Teoria dell'informazione e della trasmissione* all'Università di Torino. Ha ricoperto la posizione di segretario generale dell'AEIT. È stato consulente per la formazione permanente dei dirigenti industriali. Detiene sette brevetti ed è autore, o coautore, di quasi 200 articoli, uno dei quali è stato ripubblicato (2007) nel volume celebrativo *The Best of the Best* della IEEE Communications Society. È *Life Member* dell'IEEE. Si occupa tuttora di temi di innovazione e formazione per l'ICT.

Email: angelo.luvison@alice.it