La crittografia
Da raffinata arte rinascimentale a moderna scienza

Marco Baldi – Michele Elia

Cultura e tecnologia hanno subìto una significativa evoluzione nei secoli dopo il Rinascimento. Nuove forme di pensiero scientifico e discipline originali si sono sviluppate: in un simile crogiolo, la crittografia ha registrato un progresso forse ancor più marcato, segnando il passaggio da ricercata arte utile a diplomazie ed eserciti a disciplina scientifica, utile a tutta la società e alla vita quotidiana. Si vedrà come dopo lenti passaggi, sul finire del XIX secolo furono introdotte macchine per cifrare necessarie all'impiego strategico e massivo della crittografia nei grandi eserciti e come le sfide lanciate prima e durante la Seconda guerra mondiale – al fine di proteggere o carpire informazioni tattiche o strategiche – abbiano determinato una prima convergenza di tale materia con le moderne teorie dell'informazione e del calcolo automatico.

«Si vedrà che la crittografia è più di un soggetto che permette una formulazione matematica, perché non sarebbe esagerazione affermare che la crittografia astratta coincide con la matematica astratta».

Adrian Albert (1939)

Con il Rinascimento la crittografia ha raggiunto una caratterizzazione compiuta per l'ambiente culturale dell'epoca. A tale periodo risalgono i primi sviluppi della scienza e della tecnologia che cambieranno in maniera sostanziale la società, e la matematica inizia un'evoluzione che la perfezione della geometria di Euclide (367-283 a.C.) non lasciava intravvedere. E durante quest'affascinante cammino, non ancora ultimato, sono stati forgiati i metodi di tipo algebrico fatti propri dalla crittografia moderna.
Dagli inizi del 1600 fino alla prima metà del 1800 si sono registrati piccoli ma efficaci cambiamenti nei sistemi crittografici, costituiti da varianti della cifratura polialfabetica e da più incisivi tentativi, seppur sporadici, di crittoanalisi della cifratura di Vigenère. Essendo quest'ultima ritenuta inattaccabile, non vi era ragione o stimolo per cercare

nuovi algoritmi di cifratura. Tuttavia, verso la fine del XVIII secolo cominciarono a sorgere dubbi sull'affidabilità dello schema di Vigenère finché, nel 1863, nel lavoro *Die Geheimschriften und die Dechiffrir-Kunst*, Friedrich W. Kasiski descrive come rompere con la crittoanalisi quella cifratura polialfabetica.

Nei successivi decenni, fino agli albori del ventesimo secolo, i passaggi più rilevanti furono costituiti dallo sviluppo delle macchine cifranti sull'esempio del disco di Alberti. Tali macchine permisero un più efficace uso della crittografia in diplomazia e un vastissimo impiego in ambito militare, consentendo a eserciti sempre più grandi, che si spostavano sempre più rapidamente su teatri operativi sempre più ampi, di effettuare scambi sicuri di grandi quantità di dati.

La necessità di molti operatori di cifrare i messaggi impose l'uso di macchine cifranti. Un sistema meccanico di cifratura basato su più rotori del tipo di Alberti fu introdotto da Thomas Jefferson (presidente degli Stati Uniti dal 1801 al 1809) nel 1790, quando ricopriva l'incarico di Segretario di Stato di George Washington. Il cilindro di Jefferson consisteva in 26 piccole ruote cilindriche di legno inserite su un asse metallico e rotanti in modo indipendente. Sull'esterno di ciascuna di esse erano riportate, equispaziate, le ventisei lettere dell'alfabeto in ordine casuale, diverso per ciascuna ruota. Le ruote erano numerate e la loro disposizione costituiva la chiave segreta di cifratura. Per cifrare si facevano girare le ruote in modo da comporre su una riga il messaggio e, come cifrato, si poteva scegliere una qualsiasi delle altre righe. Per decifrare si utilizzava lo stesso sistema: le ruote nello stesso ordine erano fatte girare fino a formare su una riga il messaggio cifrato, quindi si otteneva il testo in chiaro cercando la riga con senso. Perché le macchine cifranti divenissero strumenti pratici, veloci e affidabili fu però necessario attendere i grandi progressi della meccanica e delle tecnologie elettriche, manifesti sul finire del 1800.

Nel 1891, il francese Étienne Bazeries inventò una cifrante basata sullo stesso principio introdotto da Jefferson. Essa rimase in uso nell'esercito francese almeno fino alla Seconda guerra mondiale, e fu creduta inattaccabile anche nell'ipotesi che i dischi fossero noti, ma non il loro ordine, e solo il cifrato fosse sconosciuto. Tuttavia, nel 1893 il sistema fu decrittato dallo scienziato de Viaris, nome francese del marchese Gaetano Enrico Leone Viarizio di Lesegno.

Dopo la Prima guerra mondiale apparvero molte cifranti elettromeccaniche, tra cui la Hagelin ed Enigma. La prima, progettata dallo svedese Boris Hagelin intorno al 1920, ebbe notevole successo e fu anche adottata dall'esercito statunitense. La seconda fu inventata dall'ingegnere tedesco Arthur Scherbius e brevettata nell'aprile del 1918. Enigma ha una storia molto complessa e, per certi aspetti, ancora oscura ma, in ogni caso, essa giocò un ruolo fondamentale nel corso della Seconda guerra mondiale.

Inizialmente fu usata dalle poste tedesche per la cifratura dei telegrammi; dopo sostanziali miglioramenti fu adottata dalla Marina militare, nel 1926. Ulteriormente rafforzata con l'aggiunta di un nuovo rotore, al fine di conseguire un rassicurante grado di resistenza contro massicci attacchi crittoanalitici, Enigma fu infine adottata anche dall'esercito. Parallelamente ai progressi delle macchine cifranti, si ebbe una maggiore comprensione dei princìpi, dei metodi e delle tecniche per mascherare l'informazione. In due articoli, dal titolo La *Cryptographie militaire*, pubblicati sul «Journal des Sciences Militaires» (1883), l'olandese Auguste Kerckhoffs formulò sei criteri, teorici e pratici, che dovevano essere seguiti nel progetto e nella realizzazione delle cifranti per uso militare: queste norme hanno ancora validità quali princìpi base della crittografia. Nel 1917, l'americano Gilbert S. Vernam, lavorando per AT&T, ideò una cifrante per telescrivente, basata sulla cifratura polialfabetica, che fu adottata dallo U.S. Army Signal Corps. Nel suo progetto, Vernam introdusse due innovazioni di assoluto rilievo.

Con la prima, propose di ottenere il testo cifrato come combinazione bit a bit di due sequenze binarie, una costituita dal testo codificato in una sequenza di '0' e '1', l'altra, ugualmente binaria, detta sequenza di chiave (o verme). Questo semplice schema è divenuto il modello di molte attuali tecniche di cifratura, incluso il sistema di protezione della voce usato nei telefoni cellulari. Con la seconda, prospettò di usare un verme costituito da una sequenza della stessa lunghezza del testo da cifrare, composta di simboli binari casuali e da utilizzare una sola volta. Quest'ultima idea, sebbene non pratica, risultò di grande importanza teorica. Apparvero, inoltre, molti lavori di carattere generale, come il *Traité de cryptographie* di André Lange e Arthur Sourdat, pubblicato nel 1925, lo stesso anno dell'importante *Cours de cryptographie* del generale francese Marcel Givièrge. In Italia fu pubblicato nel 1936 il *Manuale di crittografia* del generale Luigi Sacco, divenuto uno dei più noti e apprezzati trattati sulla materia della prima metà del XX secolo. Il vero balzo verso una rigorosa teoria della crittografia di carattere matematico, tuttavia, avvenne nel corso della Seconda guerra mondiale e fu propiziato dai progressi forzati dagli eventi bellici. In quel periodo, infatti, il massiccio uso delle comunicazioni radio-telegrafiche e la necessità di proteggerle da ogni sorta d'intercettazione divennero evidenti a tutti i contendenti. Sono anni in cui le storie della crittografia e delle telecomunicazioni s'intrecciano e quasi si confondono in un proficuo interscambio di nozioni e concetti.

Negli anni Trenta, i vertici degli Stati Uniti e del Regno Unito comunicavano attraverso collegamenti radio transatlantici ad alta frequenza, mediante un sistema analogico cifrato denominato 'A-3'. Esso si basava su una tecnica di scrambling che proteggeva da intercettazioni improvvisate ma era vulnerabile agli attacchi profes-

sionali. Benché gli Uffici responsabili della sicurezza ne fossero consapevoli, il sistema A-3 continuò a essere usato anche dopo l'inizio della guerra, finché si scoprì che una stazione tedesca in Olanda decrittava in tempo reale tutte le radio-comunicazioni foniche. Ma nel 1940 né gli Stati Uniti né il Regno Unito disponevano di una soluzione alternativa, anche se già si conosceva una nuova tecnologia di trasmissione della voce, denominata 'vocoder' e sviluppata nei Bell Labs americani sin dal 1936, che meglio si prestava a più robusti sistemi di cifratura. Essa si basava sulla trasformazione del segnale vocale in dati numerici, mediante un campionamento a intervalli regolari e una quantizzazione a sei livelli. I dati numerici potevano poi essere trasmessi via radio e riconvertiti in segnali vocali intellegibili. Una dimostrazione pubblica del 'vocoder' fu fatta a New York durante l'Esposizione universale del 1939. Esso fu scelto come piattaforma per lo sviluppo di un nuovo metodo di trasmissione cifrata della voce, denominato 'the Green Hornet', ma solo nel 1942 l'esercito statunitense sottoscrisse un contratto per la fornitura dei primi due esemplari, che furono denominati 'Sigsaly'. Essi entrarono in funzione il 15 luglio del 1943 – in un collegamento tra il Pentagono e Londra – e furono impiegati per le comunicazioni telefoniche via radio tra il Presidente Roosevelt e il Primo Ministro Churchill. In totale furono posti in opera dodici terminali 'Sigsaly', istallati a Washington, Londra, Parigi, Algeri, Guam, Manila, alle Hawaii e in Australia e, dopo la guerra, anche a Berlino, Francoforte e Tokyo.

Per quanto concerne la cifratura in 'Sigsaly', un problema di notevole rilevanza era costituito dalla generazione delle sequenze di verme da usare una sola volta per cifrare il segnale numerico, secondo i princìpi stabiliti dal suo inventore. Alcuni dettagli possono chiarire la complessità della procedura. Le sequenze casuali di verme erano derivate dall'uscita di una valvola raddrizzatrice al mercurio che produceva rumore termico a banda larga. Questo rumore era trattato come la voce dal 'vocoder', ossia campionato e quantizzato. L'informazione sui livelli generati era usata per produrre un segnale audio che poteva essere registrato sui supporti in vinile dei fonografi dell'epoca. Di ciascuna registrazione erano prodotte tre copie: due erano fisicamente recapitate, tramite corrieri sicuri, alle due stazioni trasmittenti e riceventi, mentre la terza serviva come copia di sicurezza. L'introduzione del sistema 'Sigsaly' indusse, principalmente per merito dei ricercatori dei Bell Labs, la formulazione dei princìpi basilari delle trasmissioni vocali digitalizzate e codificate che costituiscono la tecnologia portante dei moderni sistemi di comunicazione. Tra coloro che lavorarono al sistema 'Sigsaly' si ricorda il matematico Claude Elwood Shannon (1916-2001), il quale fornì contributi teorici fondamentali, tanto alla crittografia quanto a una teoria matematica della comunicazione che, in seguito, prese il nome di 'teoria dell'informazione'.

Shannon si era laureato nel 1937 in ingegneria con la tesi A *Symbolic Analysis of Relay and Switching Circuits* in cui mostrava che la logica simbolica di George Boole (1815-1864) rivestiva grande importanza nello studio dei sistemi di commutazione, ad esempio, delle centrali telefoniche. Negli anni seguenti lavorò per la tesi di dottorato al Massachusetts Institute of Technology sotto la supervisione di Vannevar Bush, e in una lettera, scritta nel 1939 al suo tutore, descriveva i principali elementi della sua teoria dell'informazione, allora chiamata 'intelligence' in senso statistico. L'attività di Shannon, legata ai progetti di crittografia bellica e alla crittoanalisi dei cifrari tedeschi e giapponesi, contribuì alla maturazione del concetto matematico d'informazione che, pur mostrando una netta influenza proveniente dalla crittografia, non ne costituisce una diretta conseguenza. Tra il 1940 e il 1945, mentre lavorava ai Bell Labs, Shannon introdusse, in termini rigorosi, il concetto di segretezza perfetta che definì come la condizione in cui gli sforzi di un eventuale attaccante non sono minimamente agevolati dalle osservazioni del messaggio cifrato e dimostrò che tale condizione è soddisfatta dalla cifratura di Vernam, diventata nota come one-time-tape. Tale risultato riveste un'importanza notevole, benché la necessità di stringhe di chiave molto lunghe e monouso renda questi sistemi applicabili solo in casi limitati, come dimostrarono le complesse operazioni di generazione e distribuzione delle chiavi segrete nel sistema 'Sigsaly'. Il lavoro pluriennale di Shannon è testimoniato da molteplici memorandum classificati dei Bell Labs; in uno di questi, A *Mathematical Theory of Cryptography*, apparve per la prima volta, nel settembre 1945, la teoria dell'informazione di Shannon. Il memorandum fu poi avventurosamente declassificato e pubblicato nel 1949 in una versione revisionata, con il titolo *Communication Theory of Secrecy Systems*. Tuttavia, la teoria dell'informazione era divenuta pubblica con l'articolo A *Mathematical Theory of Communication*, apparso sul «Bell System Technical Journal» già nell'ottobre del 1948.

Le esigenze belliche non solo richiedevano comunicazioni protette, ma anche la capacità di attaccare i sistemi di comunicazione nemici. Esse, pertanto, accelerarono lo sviluppo della crittoanalisi e fecero sì che i sentieri della crittografia, delle telecomunicazioni e dei calcolatori elettronici s'incontrassero e le tre discipline s'influenzassero vicendevolmente.

L'attività dei Bell Labs su 'Sigsaly' contemplava una collaborazione con la Government Code and Cipher School, ubicata a Bletchley Park, a nord di Londra, centro nel quale era stato concentrato lo sforzo degli alleati per intercettare e decrittare le radiocomunicazioni dei tedeschi. Al gruppo dei crittoanalisti apparteneva, come coordinatore, il matematico Alan Mathison Turing (1912-1954), reclutato all'Università di Cambridge. Turing, nel 1936, aveva pubblicato *On Computable Numbers, with an Application to the Entscheidungsproblem*, un articolo in cui, risolvendo un problema posto da Hilbert, formulava la teoria matematica della computabilità, definendo per primo – in modo assiomatico – il concetto di algoritmo, e introducendo la nozione di calcolatore ideale, poi noto come la macchina di Turing. Le idee del matematico guidarono la costruzione dei primi calcolatori elettronici inglesi denominati 'Colossus', che a Bletchley Park furono impiegati per decrittare i messaggi cifrati con la macchina Lorenz, un miglioramento di Enigma, usata dagli alti comandi tedeschi. All'inizio del 1943, Turing compì una visita segreta alla sede centrale dei Bell Labs a New York, durante la quale s'incontrava con Shannon. Fu così che i due massimi teorici, rispettivamente, della scienza dei calcolatori e della teoria dell'informazione, ebbero modo di condividere idee e prospettive.

Il massimo sforzo a Bletchley Park era volto alla decrittazione dei messaggi cifrati con Enigma, soprattutto per contrastare la guerra sottomarina degli U-boat diretta contro i convogli che rifornivano le armate alleate in Europa. Enigma rappresentava l'apice dell'evoluzione dei sistemi cifranti elettromeccanici basati su rotori. La macchina era composta di una tastiera, come quella di una macchina per scrivere, di un pannello di lettere retroilluminate, di un insieme di 4 o 5 rotori e di un pannello per connessioni mobili. Per una fissata configurazione della macchina, premendo il tasto corrispondente a una lettera del testo in chiaro, sul pannello s'illuminava la lettera in cui era cifrata. Rilasciando il tasto, i rotori compivano delle rotazioni e si predisponevano per la successiva cifratura. L'operazione di decifratura era analoga: si premeva il tasto della lettera del cifrato e si riotteneva sul pannello illuminato la lettera del testo in chiaro.

Le posizioni iniziali dei rotori e le connessioni variabili della macchina erano modificate quotidianamente e costituivano le chiavi segrete trasmesse tramite dispacci. Il meccanismo di cifratura faceva sì che nel testo cifrato si perdessero le caratteristiche di correlazione tipiche della lingua (come le frequenze di apparizione di ciascuna lettera o combinazione di lettere) che erano state sfruttate fino ad allora dalla crittoanalisi. Inoltre, l'elevatissimo numero (3.10^{114}) di lettere che dovevano essere cifrate, prima che il ciclo ricominciasse, indusse i crittografi tedeschi all'errata convinzione che la macchina fosse inattaccabile. I primi non tedeschi a occuparsi della crittoanalisi di Enigma furono i polacchi, che vedevano con timore la crescente potenza germanica. Già nel 1928, essi riconobbero che i tedeschi avevano messo in campo nuove cifranti e ne acquisirono una versione commerciale a 4 rotori, ancorché diversa dalla macchina in uso alle Forze armate.

Ne iniziarono quindi la crittoanalisi e, con un'intuizione che ha della preveggenza, nel 1929 l'Ufficio cifra polacco (Biuro Szyfrów) organizzò un corso segreto di crittografia, basato sul testo di Givièrge – per selezionati studenti universitari talentuosi – a cui attesero Marian Rejewski, Jerzy Rozycki e Henryk Zygalski. Nello stesso anno Rejewski (1905-1980) si laureò, quindi si iscrisse a un master di statistica attuariale a Gottingen, che non completò poiché nel 1930 fu assunto come assistente di matematica all'università di Poznan. Iniziò, quindi, a lavorare part-time per l'Ufficio cifra e, nel 1932, fu arruolato nei Servizi di sicurezza militari assieme a Rozycki e Zygalski. Ai tre fu assegnata la crittoanalisi di Enigma, attività in cui fino ad allora non erano stati fatti progressi. In pochi mesi il loro contributo fu decisivo. In particolare Rejewski, combinando informazioni d'intelligence con uno sforzo di crittoanalisi sul cifrato, fu in grado di descrivere in termini matematici le connessioni caratterizzanti i rotori della macchina Enigma usata dai militari. Tale descrizione riduceva l'attacco alla cifrante alla risoluzione di equazioni algebriche; purtroppo la soluzione delle proposte di Rejewski richiedeva uno sforzo tuttora inarrivabile. Nel suo lavoro di sintesi, egli dimostrò un nuovo teorema sulla proprietà delle trasformazioni di Enigma, che riduceva in maniera eccezionale il numero di lettere da cifrare prima di ricominciare il ciclo: la complessità di attacco a Enigma era di molto inferiore a quella stimata dai crittografi tedeschi, pur restando tale da escludere qualunque attacco manuale.

Lo stesso Rejewski, in collaborazione con Rozycki e Zygalski, delineò un procedimento automatizzato di attacco basato su sistemi elettromeccanici, che chiamarono 'bombe' e che furono realizzati dall'AVA Radio Manufacturing Company.

Sfortunatamente, con l'aumentare del numero di messaggi, le 'bombe' elettromeccaniche non erano sufficienti alla decrittazione in tempi utili dei cifrati. Nel frattempo la situazione politica in Europa si aggravò, cosicché i vertici polacchi accettarono di trasferire tutta la loro documentazione sulla decrittazione di Enigma ai Servizi inglesi e francesi. Nel luglio del 1939, poco prima che nazisti occupassero la Polonia (1 settembre), il gruppo di Rejewski, in un incontro a Varsavia, passò dunque ai colleghi gli straordinari risultati cui erano pervenuti, con l'impegno che sarebbero stati informati dei successivi sviluppi, promessa non mantenuta fors'anche a causa dei drammatici eventi successivi. Peraltro, i geniali sistemi proposti non sarebbero stati sufficienti per condurre con successo attacchi sistematici a migliaia di radiomessaggi dell'esercito tedesco, ottenuti quotidianamente dalle stazioni d'intercettazione. Fu in tale fase che Turing ebbe un ruolo decisivo a Bletchley

Park per gestire i miglioramenti tecnologici delle 'bombe' da lui stesso suggeriti. Pur conservando il nome, le 'bombe' divennero macchine poderose, ciascuna del peso di circa una tonnellata e il cui funzionamento richiedeva numerosi addetti continuamente all'opera. Si stima che ne furono realizzate più di 200 dalla British Tabulating Machines (Btm) e che a Bletchley Park arrivarono a lavorare, contemporaneamente, diverse migliaia di operatori nelle fasi culmine del conflitto. Il centro fu attivo, con alterne fortune, per l'intera durata della guerra, ma una chiara descrizione della sua operatività non è mai stata fornita. È opinione sempre più accreditata, tuttavia, che i successi colà ottenuti nella decrittazione dei radio-messaggi tedeschi, forse non cambiarono il corso della guerra ma contribuirono ad abbreviarne la durata.

Anche in Italia nacque una variante di Enigma. Essa fu sviluppata dalla Ottico Meccanica Italiana (Omi), azienda di Roma fondata nel 1924 da Umberto Nistri (uno dei precursori della cartografia realizzata mediante prospezioni aeree), e specializzata nella produzione di apparecchi fotografici per l'Aeronautica militare, utilizzati nella ricognizione aerea. La macchina derivata da Enigma, e prodotta in pochi esemplari, vi aggiungeva la funzionalità di un rullo per la scrittura automatica del testo cifrato o decifrato. Essa fu usata dall'Esercito, dall'Aeronautica e dalla Marina durante la Seconda guerra mondiale.

Negli stessi anni, il Giappone continuò a usare dei codici manuali, anche se avrebbe potuto disporre di Enigma. I due più famosi furono il codice Purple (dal colore rosso della copertina del libretto che lo descriveva), in uso alla Diplomazia, e il codice JN-25 (Japanese Navy 25, numero della versione di codice) usato dalla Marina imperiale all'inizio degli anni Quaranta. Il codice JN-25 comprendeva una sovra-cifratura, ossia una trasformazione del messaggio prima di essere cifrato manualmente per essere poi trasmesso, usualmente in alfabeto Morse. La crittoanalisi, seppur parziale, di questo codice, da parte del gruppo del Comandante Joseph John Rochefort (1900-1976), permise alla flotta americana dell'ammiraglio Nimitz di sconfiggere la flotta giapponese nella battaglia di Midway (4-7 giugno 1942), ponendo fine al dominio del Giappone sul Pacifico per il resto della guerra.

Negli anni che seguirono si assistette allo sviluppo dei calcolatori elettronici e all'introduzione nel sistema civile di telecomunicazione della tecnologia 'vocoder'. Grazie allo straordinario progresso scientifico, raggiunto con la teoria della computabilità di Turing e dell'informazione di Shannon, le basi per l'affermazione del carattere digitale dell'informazione erano ormai solidamente fissate. Trasmissione, memorizzazione ed elaborazione sono, infatti, tre aspetti di un'unica tecnologia dell'informazione