IL CASO ENIGMA
LA STORIA 1

Massimiliano Sala – Michele Elia

La storia di Enigma, la macchina cifrante impiegata dalle armate dell'asse durante la Seconda guerra mondiale, è diventata paradigmatica dei miti e delle sfide intriganti che pervadono l'universo dei sistemi di sicurezza. Oggi la crittografia è un'arma indispensabile negli enormi conflitti d'interesse politici, finanziari, militari ed economici che stanno scuotendo gli equilibri planetari. Ormai Enigma è un oggetto lontano, tuttavia le narrazioni delle vicende che la coinvolsero sono avvolte dal pathos di avvincenti racconti romantici in cui la morte, le sconfitte e le vittorie si mescolano come in un feuilleton ottocentesco. In questa breve esposizione si cercherà di raccontare, ancora una volta, gli eventi salienti e di porre in risalto i ruoli dei personaggi principali, ma in una forma che si vorrebbe, insieme, appassionante e aderente alla realtà dei fatti.

Una buona decisione è basata sulla conoscenza
e non sui numeri.
Platone (428-348 a.C.)

La storia della crittografia è permeata d'intriganti episodi che colpiscono la fantasia collettiva, forse perché alla base del mistero vi era la sopravvivenza delle nazioni. Gli eventi motivo del suo fascino, veri o presunti, hanno portato la crittografia a dominare quella parte del mondo mediatico popolato di agenti segreti e d'investigatori geniali. Nei racconti fantastici confezionati per colpire l'immaginario popolare risulta molto difficile comprendere dove finisca il reale e cominci l'invenzione. Così, per decenni, le vicende di Enigma sono state narrate in pretenziosi racconti storici, talvolta contraddittori, ingenerando una confusione che ha fatto della macchina cifrante un mito. Tuttavia, dopo più di mezzo secolo, come da un torbido stagno, stanno emergendo brandelli di verità sia sugli impieghi della crittografia nella Seconda guerra mondiale sia sui fatti rimasti sconosciuti a tutti quelli che non li vissero in prima persona.

Sicuramente, la reale lotta dei servizi crittografici alleati contro i sistemi di cifratura tedeschi, aspra e incerta, appare più affascinante che nelle stesse invenzioni letterarie. Questo il dispiegamento delle forze in campo. La Wehrmacht era composta dalla Marina militare (Kriegsmarine), dall'Aeronautica militare (Luftwaffe) e dall'Esercito (Heer). Le varie Armi impiegarono diversi sistemi di cifratura; mentre la Kriegsmarine e la Heer utilizzavano quasi esclusivamente Enigma, in molteplici versioni di crescente sicurezza, la Luftwaffe usava la stessa cifrante principalmente nella realizzazione base. Infine, gli alti comandi della Wehrmacht si scambiavano i messaggi crittografati con la cifrante Lorenz. La crittoanalisi dei cifrati tedeschi, intercettati da un poderoso sistema di ascolto, fu gestita con un'organizzazione complessa data l'esigenza, in primis, di distinguere tra le diverse cifrature di differente difficoltà (crittoanalisi blackbox) e, secundum, di trattare e valorizzare le informazioni così acquisite. La crittoanalisi blackbox è tuttora molto ardua, essendo veramente laborioso riconoscere il sistema di cifratura dal solo cifrato. E ancora oggi molte di queste attività sottaciute sono probabilmente coperte dal segreto di stato, se mai una qualche documentazione sia sopravvissuta a vari mascheramenti e a distruzioni fortuite o deliberate.
Nella mitica letteratura dedicata ai Servizi segreti alleati, Bletchley Park, un paesino nella campagna a circa 75 chilometri a nord di Londra, è diventato un cult. È un fatto che in molteplici monografie, rapporti storici e racconti agiografici dedicati a quella località è sempre stato dato rilievo alla decrittazione dei messaggi della Kriegsmarine, cifrati con macchine Enigma identificate in quest'utilizzo col nome «Shark», sebbene questa versione fosse propriamente riservata agli U-Boot. Anche se il caso Enigma paia intenzionalmente enfatizzato, è incontrovertibile che la cifrante campeggi sullo sfondo dello scenario crittologico dell'ultima guerra. Era una macchina elettro meccanica, il cui principio di cifratura base consisteva di tre rotori in cascata, come tre cifrature successive fatte col disco di Alberti[1]. Inventata dall'ingegnere elettrotecnico tedesco Arthur Scherbius, fu brevettata nell'aprile del 1918 e adottata dalle Poste tedesche per la cifratura dei telegrammi. Nella sua struttura originaria non offriva una grande protezione e per questo fu giudicata non idonea per impieghi militari. Tuttavia, gli errori commessi nella cifratura dei messaggi nella Grande Guerra avevano insegnato ai Comandi tedeschi che era necessario tutelare adeguatamente le comunicazioni, garantendo nel contempo la protezione e la certezza della consegna del messaggio; con il vincolo aggiuntivo che questi obiettivi dovevano essere raggiunti impiegando operatori che non erano necessariamente esperti crittografi. Probabilmente fu la relativa semplicità d'uso di Enigma ad attrarre l'attenzione degli ambienti militari sicché, dopo sostanziali miglioramenti, nel 1926 fu adottata dalla Kriegsmarine.

1. «Gnosis» XXI (2015) 2, pp. 122-131.

Questa prima versione fu scelta anche dalla Luftwaffe. Ulteriormente rafforzata (con l'aggiunta di rotori e altri accorgimenti) al fine di avere un rassicurante grado di resistenza contro robusti attacchi crittoanalitici, a essa fece infine ricorso anche l'esercito. Va ricordato che anche in Italia nacque una variante di Enigma che – sviluppata dall'azienda romana[2] Ottico Meccanica Italiana (Omi) e prodotta in pochi esemplari con l'aggiunta di un rullo per la scrittura automatica del testo cifrato o decifrato – fu usata dall'Esercito, dall'Aeronautica e dalla Marina durante la Seconda guerra mondiale.
Enigma rappresentava l'apice dell'evoluzione dei sistemi cifranti elettromeccanici basati su rotori. La sua presunta robustezza contro attacchi determinati, condotti con ingenti risorse, ancorché plausibile per quanto concerneva l'algoritmo si rivelò troppo ottimistica. I tedeschi non avevano considerato che gli attacchi ai messaggi cifrati potessero sfruttare sia le debolezze dell'algoritmo, sia reconditi vizi del protocollo, oltre alla molteplicità dei messaggi cifrati anche con chiavi diverse.

TEATRO STORICO-POLITICO

Il riarmo della Germania preoccupò seriamente Varsavia, soprattutto per le rivendicazioni dei territori 'perduti' a est, assegnati alla Polonia dal trattato di pace di Versailles nel 1919. Inoltre, messaggi radio intercettati, sia della diplomazia sia dell'esercito, rivelarono che i tedeschi impiegavano un sistema di cifratura resistente a tutti gli attacchi di crittoanalisi, tradizionalmente manuali, condotti dai pochi addetti agli uffici cifra polacchi. E nella stessa situazione d'impasse languivano anche i Servizi di sicurezza inglesi e francesi. Per rimediare alla carenza di crittografi e per reclutare giovani talenti, nel 1929 il Governo polacco, attraverso l'intelligence, formulò un piano che coinvolse il professor Zdzisław Krygowski, Direttore del Dipartimento di matematica all'Università di Poznań.
Quel piano, ora, non solo appare lungimirante e geniale, ma è diventato un modello di riferimento per i sistemi di reclutamento di molteplici Servizi di sicurezza. Non dovrebbe sorprendere l'impiego di matematici talentuosi, poiché tra gli addetti ai lavori in tutto il mondo occidentale era ormai assodato che crittografia e matematica fossero strettamente connesse: si pensi al generale Luigi Sacco in Italia, a William Friedman negli Usa, al generale Marcel Givierge in Francia, per non dire dei crittografi che lavorarono su Enigma in Germania.

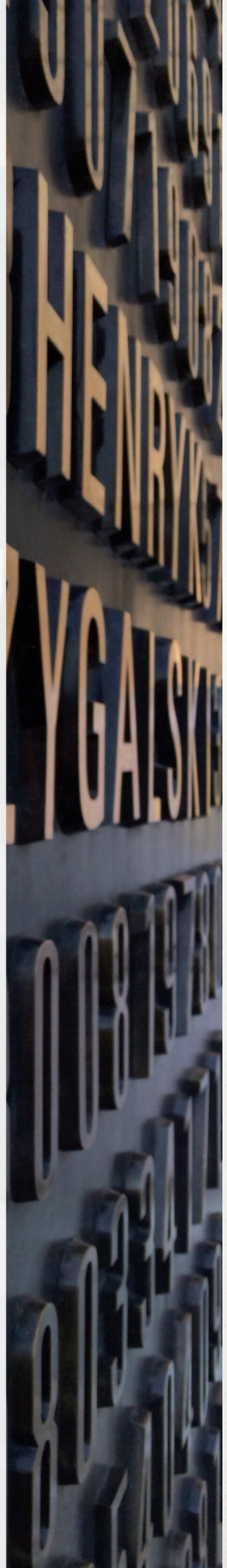
2. «Gnosis» XXI (2015) 3, pp. 134-143.

Furono scelti un centinaio di studenti, selezionati tra i più dotati in matematica di tutta l'università, ai quali fu impartito un addestramento basato sul *Course de cryptographie* (1925) del generale Marcel Givierge. Al termine del corso una decina dei migliori furono 'arruolati' (con i criteri in uso al Biuro Szyfrów, l'Ufficio Cifra polacco) come crittografi per la sede di Poznań: tra questi, Marian Rejewski, Jerzy Różycki e Henryk Zygalski, un terzetto che si rivelò straordinariamente efficace. Quando, nel 1932, l'Ufficio fu chiuso, essi furono assunti dal Biuro Szyfrów di Varsavia e, nello stesso anno, incaricati della crittoanalisi di Enigma, attività in cui fino ad allora non erano stati registrati utili progressi. Il loro contributo, in pochi mesi, si rivelò decisivo. In particolare, Rejewski, combinando informazioni d'intelligence ottenute forse dai francesi, con uno sforzo di crittoanalisi solo sul cifrato fu in grado di descrivere in termini matematici le caratteristiche dei rotori delle macchine Enigma usate dai militari e di decrittare alcuni messaggi. La notizia del successo raggiunse i Servizi di sicurezza francesi e inglesi, che iniziarono una forma di negoziazione per entrare in possesso delle scoperte conseguite. Dopo molte resistenze, quando la situazione politica in Europa si aggravò, i vertici polacchi accettarono di passare tutte le loro informazioni sulla decrittazione di Enigma agli alleati. Nel luglio del 1939 – il 1° settembre 1939 la Polonia fu occupata dalle truppe naziste – in un incontro a Varsavia il gruppo di Rejewski, Różycki e Zygalski comunicò a colleghi inglesi e francesi i risultati acquisiti ricevendone la promessa di essere tenuti informati dei successivi sviluppi, promessa non mantenuta fors'anche a causa dei tumultuosi e incalzanti sviluppi della guerra[3].

L'ATTACCO MATEMATICO

Nei suoi lavori Rejewski dimostrò alcuni nuovi teoremi di natura matematica che gli permisero di ridurre il numero di tentativi richiesti da attacchi esaustivi per trovare la chiave segreta dal cifrato Enigma. Riuscì inoltre a trarre vantaggio da una debolezza nel protocollo di utilizzo, anche se non è chiaro se fosse stata scoperta da una sua formidabile intuizione o grazie a un contributo dell'intelligence francese. Purtroppo, anche sfruttando al meglio i risultati di Rejewski, il numero di tentativi da compiere era ancora troppo elevato perché fossero possibili attacchi sistematici a una grande quantità di messaggi con metodi manuali.
Una descrizione di questi attacchi sarà riportata in un prossimo articolo, con dettagli che – pur senza far uso di raffinate nozioni matematiche – consentiranno di apprezzare l'elegante piano di Rejewski e dei suoi compagni. I polacchi subito riconobbero che per condurre attacchi su grande scala, tali da ottenere informazioni

3. D. Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes*, 1939-1943, Hougthon Mifflin, Boston 1991.



in tempi utili, era indispensabile eseguirli con l'ausilio di macchine. A tal fine furono inventate le *bombe* da Rejewski, il *ciclometro* da Różycki e i *fogli perforati* da Zygalski. Pur con i limiti di carattere tecnologico, ristretti alla parte automatizzata, i piani proposti possedevano in forma embrionale tutti i concetti, i metodi e gli accorgimenti indispensabili alla decrittazione del cifrato di Enigma. Le *bombe* – l'elemento più appariscente e costoso per consentire attacchi di crittoanalisi con buon successo – erano macchine elettromeccaniche realizzate dalla polacca Ava, Radio Manufacturing Company che, pur assicurando successi contro le versioni di Enigma nella loro struttura più semplice, si mostrarono insufficienti a decrittare velocemente gli ingenti volumi di messaggi radiointercettati e furono poi migliorate grandemente dagli inglesi e quindi dagli americani.

BLETCHLEY PARK

All'inizio degli anni Trenta il governo inglese installò o potenziò diversi centri, disseminati sul territorio inglese, insediandovi varie sezioni tecnico-operative dei Servizi segreti. Con lo spettro di una dura lotta alle porte, alla fine del decennio furono arruolati matematici di provata abilità per la crittoanalisi. Fin dall'inizio del conflitto, Bletchley Park[4] divenne la principale sede di crittoanalisi (nota anche come Stazione X) dedicata alla decrittazione di tutti i messaggi delle truppe dell'Asse radiointercettati. Ivi venne collocata la sede della Government Code and Cipher School (Gc&Cs).
A Bletchley Park, già prima della guerra, un gruppo di crittografi guidato da Dilly Knox aveva lavorato per attaccare i messaggi cifrati da Enigma. Seguendo un'idea originale dello stesso Knox, fu sviluppata una tecnica che si avvaleva di fogli perforati molto simili, peraltro, a quelli ideati da Zygalski. Inizialmente gli attacchi degli inglesi non ebbero successo, anche se consentirono di maturare una buona esperienza e conoscenze che solo dopo il luglio 1939 – quando furono disponibili le informazioni trasferite dai polacchi – permisero loro di decrittare rapidamente i messaggi cifrati da Enigma. Va rimarcato che il grande merito degli inglesi fu lo sviluppo di sistemi e di organizzazione di attacchi in grado di fornire informazioni, tratte dai messaggi cifrati e d'intelligence, in tempo utile per il loro impiego: questo piano operativo fu denominato *Ultra*. Il contributo angloamericano divenne decisivo quando, nel corso del conflitto, le macchine Enigma furono migliorate al punto che gli attacchi richiesero tecnologie elettroniche e dovizia di risorse che sarebbero state inarrivabili per i polacchi. A Bletchley Park operarono matematici e crittografi militari molto abili, coadiuvati da oltre 10.000 operatori ausiliari. La complessa struttura e i nomi di coloro che la diressero sono parzialmente noti. In un piccolo volume del 1974, un ufficiale superiore di collegamento, Frederick W. Winterbotham, rivelò il grande segreto del progetto *Ultra* dal punto di vista gestionale

4. «Gnosis» XXI (2015) 3, pp. 134-143.

delle informazioni rese disponibili dal gruppo della crittoanalisi. Una descrizione più tecnica dei successi crittografici di Bletchley Park è riportata nel libro *The Hut six*, in cui il matematico Gordon Welchman, tra i maggiori responsabili della crittoanalisi di Enigma, descrive le funzioni dei gruppi di lavoro che operarono nelle baracche (*hut*) 3, 6 e 11. Tuttavia, sull'intero lavoro di Bletchley Park campeggia la figura del matematico Alan Mathison Turing (1912-1954). Nel 1936 Turing era diventato inopinatamente famoso nel mondo scientifico dopo la pubblicazione di *On Computable Numbers, with an Application to the Entscheidungsproblem*, un articolo in cui, risolvendo un problema posto dal matematico David Hilbert nel 1928, aveva formulato una teoria astratta della computabilità (ossia una teoria che stabilisce cosa un qualsiasi calcolatore può e non può fare, prima che i calcolatori elettronici fossero inventati)[5]. Turing definì per primo, in modo assiomatico, il concetto di algoritmo introducendo la nozione di calcolatore ideale diventato noto come *macchina di Turing*. Reclutato per Bletchley Park dall'Università di Cambridge, fu aggregato ai gruppi che lavoravano alla crittoanalisi di Enigma e in seguito a quella dei cifrati Lorenz. Come responsabile della *Hut* 8, migliorò in maniera importante le *bombe* di Rejewski, rendendo la crittoanalisi di grossi volumi di cifrati Enigma eseguibile con successo in tempi utili per l'utilizzo delle informazioni ottenute. Con il contributo di Turing, pur conservandone il nome, le 'bombe' divennero – assieme a una rilevante parte elettronica – macchine poderose realizzate dalla British Tabulating Machines (Btm), ciascuna del peso di circa una tonnellata e per il cui funzionamento era necessaria la continua opera di numerosi addetti. Nell'inverno del 1941 Turing compì un viaggio negli Stati Uniti dove visitò i Laboratori Bell ed ebbe lunghi colloqui con Claude Elwood Shannon, padre della teoria dell'informazione. Al riguardo è dato sapere solo che si parlò di calcolatori per giocare a scacchi e di come riconoscere l'intelligenza umana. Tuttavia, lo scopo vero del viaggio e le questioni trattate non furono mai rivelati. È un fatto che dal 1942 gli americani costruirono 'bombe' per decrittare i messaggi di Enigma ancor più efficienti di quelle inglesi e di conseguenza, nella battaglia dell'Atlantico, le decrittazioni dei messaggi degli U-Boot cifrati con Enigma, anche nella sua forma più complessa, riscossero un accettabile successo. Seppur con alterna fortuna, per l'intera durata della guerra permisero di limitare le perdite causate dai sommergibili tedeschi ai convogli americani che trasportavano i rifornimenti indispensabili per le armate alleate in Europa.

5. Ivi.

IL PIÙ GRANDE SEGRETO: COLOSSUS

Conoscere il contenuto dei messaggi cifrati con Enigma si rivelò d'importanza tattica per la vitale battaglia dell'Atlantico, mentre i messaggi scambiati tra gli alti comandi della Wehrmacht, cifrati con la macchina Lorenz, rivestirono un elevato valore strategico per la condotta della guerra. La cifrante Lorenz era basata sul sistema di Vernam: ciascuna lettera era prima codificata in 'Baudot code', cui seguiva una cifratura bit a bit. In teoria, questo schema realizzava una cifratura perfetta, come dimostrò Claude Elwood Shannon proprio durante il periodo bellico[6], ma anche in questo caso il protocollo d'impiego era affetto da una debolezza che permise di attaccare con successo il cifrato. Va rimarcato che la protezione era comunque più robusta rispetto a Enigma e che la decrittazione dei messaggi richiedeva strumenti nettamente più raffinati, sia teorici che tecnologici. Fu sicuramente merito delle idee di Alan Turing la realizzazione, probabilmente anche sotto la sua guida, del primo calcolatore elettronico, denominato *Colossus* – indispensabile strumento per decrittare con successo i messaggi cifrati Lorenz – che rappresenta il più grande segreto di Bletchley Park. Un segreto a lungo custodito in maniera quasi maniacale, ancorché inutile, come ha dimostrato lo sviluppo dei calcolatori elettronici che ha portato agli attuali personal computer i quali, con una potenza di calcolo incomparabile con quella dei loro precursori, pervadono la nostra vita quotidiana.

CONCLUSIONI

Una fedele descrizione delle strutture operative di Bletchley Park non è mai stata resa pubblica, né forse lo sarà mai, anche se ora il sito è un museo aperto al pubblico. È opinione sempre più accreditata che i successi colà ottenuti nella decrittazione dei radiomessaggi cifrati con Enigma o con la macchina cifrante Lorenz furono decisivi nel cambiare il corso della guerra e sicuramente contribuirono ad abbreviarne la durata. Il mito che circonda Bletchley Park e gli avvenimenti che videro quel centro come palcoscenico centrale delle battaglie segrete di spie e controspie sono destinati a restare per sempre in ombra e a essere raccontati più su basi di fantasia che su documenti e informazioni riscontrabili. Resta l'indiscutibile realtà che in quel luogo si ebbe l'incontro di personaggi eccezionali, geniali matematici e strateghi lungimiranti, sorretti da volontà ferrea e da irriducibile determinazione. I meriti, pur difficili da riconoscere, di chi condusse una lotta apparentemente incruenta ma risolutiva per le sorti del conflitto, non vanno sottovalutati con la presunzione o la speranza che, «o fortuna imperatrix mundi», non abbia più a ripetersi una tale necessità. Dopo settant'anni di pace incerta e turbinosa, è certo che le vicende di Enigma sono assurte a modello di moltissime storie che catturano la fantasia umana con la bellezza e il mistero

6. Ivi.