Alle reali origini del massacro di Capo Matapan

La crittologia è la scienza e l'arte che si occupa delle scritture segrete. Ne fanno parte come sue branche la steganografia, la steganalisi, la crittografia e la crittanalisi. La steganografia si dedica allo studio degli artifizi che permettono di occultare un messaggio senza modificarne il contenuto. Se il messaggio viene individuato dal nemico questi lo può leggere subito senza compiere nessuna altra azione sul testo. La steganalisi, al contrario, si occupa di individuare i messaggi nascosti dalla steganografia, ad esempio in un'immagine digitale. La crittografia, mediante la cifratura, converte un messaggio chiaro in un messaggio solo apparentemente incomprensibile: il cifrato e mediante la decifrazione lo riconverte nel messaggio chiaro di partenza. La crittanalisi converte il cifrato della crittografia in un messaggio chiaro ricorrendo ad ogni espediente od arte o scienza, finanche alla tortura ed è operata dal nemico che in genere possiede ben poche informazioni sul sistema cifrante e soprattutto non ne conosce la chiave. Eppure la crittanalisi di un messaggio o di un sistema cifrante molto spesso ha successo! Trascuro in questa sede i codici segreti cioè quel tipo di messaggio segreto dove un'intera parola o un'intera frase è rappresentata da un numero come in un vocabolario bilingue: da parola in chiaro si passa al codice numerico corrispondente e viceversa per la sezione decodificante.

Ora facciamo un passo indietro ed analizziamo lo stato della crittologia militare europea alla fine del primo conflitto mondiale. L'ammiragliato inglese fece conoscere al mondo le prodezze dei suoi crittanalisti della Room 40 ai danni dell'impero tedesco: la decodificazione del telegramma Zimmermann, con la conseguente entrata in guerra degli Stati Uniti a fianco della Gran Bretagna, la cattura del codice SKM in seguito all'affondamento dell'incrociatore leggero tedesco Magdeburg, la cattura dei codici HVB e VB tedeschi. Questo ed altro bastò alle autorità militari e politiche del Terzo Reich per metterle alla ricerca di una crittografia più sicura e la loro attenzione si fissò sulla macchina cifrante elettromeccanica Enigma, inventata dall'ingegnere berlinese Arthur Scherbius. Questa macchina venne adeguata all'uso militare mediante numerose modifiche ed accorgimenti così che ogni forza armata nazista o loro alleata ne possedeva un suo tipo. Vi era l'Enigma dell'Abwehr [il servizio segreto], quella della Wehrmacht [l'Esercito], quella della Luftwaffe [l'Aeronautica], quella della Kriegsmarine [la Marina Militare], quella degli U-boot [i sommergibili], la versione Tirpitz [una Enigma commerciale K modificata ed usata nelle comunicazioni coi giapponesi], la versione delle Ferrovie e dei vari fronti armati dell'Esercito e così via. Enigma non era una macchina singola, ma una famiglia di macchine correlate!

Occorre sottolineare che i messaggi di un tipo di Enigma non potevano essere decifrati normalmente da una macchina Enigma di altro tipo, vi erano quindi distinti network radio di tali macchine. Incidentalmente vanno annoverate nel sistema delle comunicazioni segrete tedesche anche altre macchine come la Lorenz [utilizzata da Hitler e dagli alti comandi] o SZ 40-42 o Schlüsselzusatz 40/42 e la telescrivente cifrante Siemens e Halske T-52 [Schlüsselfernschreibmaschine].

Ebbene tutte queste macchine furono crittanalizzate ripetutamente dai nemici delle potenze dell'Asse. I primi a far breccia nel sistema Enigma furono i polacchi che ricorsero all'ingegno di tre loro matematici: Marian Rejewski, Henryk Zygalski e Jerzy Rozycki. Gli occidentali, invece, avevano gettato la spugna considerando Enigma inespugnabile. Come conseguenza, per tutti gli anni 30, i polacchi furono in grado di capire molti messaggi tedeschi cifrati con la macchina Enigma, mentre i francesi e gli inglesi nessuno. Poi l'invasione della Polonia ed il conseguente scoppio della Seconda Guerra Mondiale spostarono in Inghilterra la lotta ad Enigma. È da rimarcare che poco prima di essere invasi, i polacchi avevano donato agli inglesi ed ai francesi tutte le loro competenze crittanalitiche teoriche [il catalogo di Rejewski] e pratiche, che comprendevano anche apparecchiature come il ciclometro e la bomba di Rejewski [antesignana sia della bomba di Turing che della U.S. Navy Bombe dell'americano Joseph Desh], i fogli perforati di Zygalski e il metodo dell'orologio di Rozycki [antesignano del Banburismus di Alan Turing] e due repliche di Enigma.

La Lorenz (e non Enigma, come comunemente viene detto!) fu crittanalizzata mediante il Colossus, il primo computer elettronico della storia, costruito a Dollis Hill da Tommy Flowers. Invece la T-52,

nei suoi primi modelli, fu risolta dal grande matematico e crittologo svedese Arne Beurling, in una settimana e solo con carta e penna. I modelli successivi non sono stati crittanalizzati.
Eppure, le comunicazioni segrete italiane si basarono quasi esclusivamente sulla crittologia tedesca e neppure su quella di livello più sofisticato!
Gli inglesi avevano organizzato il loro centro codici a Bletchley Park [conosciuto anche come BP, Stazione X o Progetto Ultra]. Qui, in alcuni prefabbricati [HUT], arrivarono a lavorare 10.000 persone, uomini e donne, di fine intelligenza ed è qui che si ebbero le prime mosse della carneficina di Matapan. A Bletcley Park, la ragazza ventenne Mavis Batey in Lever decifrò il messaggio che Supermarina aveva inviato alla squadra navale dell'Ammiraglio Angelo Iachino, in mare con la missione di tagliare i rifornimenti marittimi del nemico partenti da Suez e diretti in Grecia. Il messaggio diceva testualmente: «Oggi è il giorno X-3». La crittanalisi britannica di tale messaggio consentì al nostro nemico, l'Ammiraglio Andrew Cunningham, capo della Mediterranean Fleet con sede ad Alessandria d'Egitto, di conoscere la data in cui la nostra flotta era nelle vicinanze della Grecia e di pianificare un attacco micidiale, unendo la flottiglia del Pireo con stanza in Grecia alla flotta di stanza ad Alessandria.
Per nascondere agli italiani le capacità e l'esistenza di Ultra, Cunningham ricorse, come altri comandanti inglesi in analoghe circostanze, all'espediente di inviare un aereo da ricognizione nei cieli sovrastanti la nostra squadra navale per far credere ai suoi comandanti che questi avesse proceduto all'avvistamento. E per rendere più credibile la faccenda, il ricognitore inviò astutamente alla sua base un messaggio radio, cifrato con un sistema già crittanalizzato dagli italiani, recante le coordinate della flotta. Come abbiamo visto sin qui, la posizione era ben nota a Cunningham grazie al progetto Ultra. È da sottolineare che senza la crittanalisi inglese del messaggio di Supermarina diretto all'Ammiraglio Iachino non si sarebbe potuta verificare la battaglia navale di Capo Matapan. Il resto è storia ben accertata, fummo inevitabilmente e duramente sconfitti in mare, in battaglia, date le altre e ben note deficienze della nostra Regia Marina, ma la guerra segreta dei codici l'avevamo già persa da tempo, anzi non l'avevamo neppure cominciata!

Silvio Coccaro
medico – chirurgo
ex allievo 1972-1973

Bibliografia di riferimento:

Massimo Zamorani: L'agguato di Matapan. 28-29 Marzo 1941. Mursia – 2006.

Mavis Batey - Dilly: The man who broke Enigmas. Edizione Kindle di Amazon.

Wladyslaw Kozaczuk, Jerzy Straszak - Enigma: How the Poles Broke the Nazi Code - Hippocrene Books.

Simon Singh: Codici & segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet. [Disponibile in inglese col titolo: The Codebook]. È un fisico inglese di origine pakistana, autore di libri di alta divulgazione scientifica e di programmi scientifici televisivi per la BBC.

David Kahn - The Codebreakers: The Story of Secret Writing, Scribner Ed.
È il testo più prestigioso e completo del più acclamato scrittore di storia della crittologia.

Cryptologia di Taylor & Francis [rivista online e cartacea, in lingua inglese, disponibile per abbonamento o l'acquisto anche di singoli articoli]. È una miniera inesauribile di argomenti crittologici di levatura mondiale, liberi e non soggetti a segreto militare. L'abbonamento alla rivista elettronica consente la consultazione ed il download di tutti gli articoli dal 1977 ad oggi.