NUOVA ANTOLOGIA MILITARE
RIVISTA INTERDISCIPLINARE DELLA SOCIETÀ ITALIANA DI STORIA MILITARE

Fascicolo Speciale 2021

Intelligence militare, guerra clandestina e Operazioni Speciali

a cura di
GÉRALD ARBOIT

Società Italiana di Storia Militare

Nuova Antologia Militare
Rivista interdisciplinare della Società Italiana di Storia Militare
Periodico telematico open-access annuale (www.nam-sism.org)
Registrazione del Tribunale Ordinario di Roma n. 06 del 30 Gennaio 2020

Direzione, Via Bosco degli Arvali 24, 00148 Roma
Contatti: direzione@nam-sigm.org ; virgilio.ilari@gmail.com

Grafica: Nadir Media Srl - Via Giuseppe Veronese, 22 - 00146 Roma
info@nadirmedia.it

Gruppo Editoriale Tab Srl -Viale Manzoni 24/c - 00185 Roma
www.tabedizioni.it

ISSN: 2704-9795

ISBN Fascicolo Speciale 2021: ISBN: 978-88-9295-270-6

Violatori di cifrari

I crittografi del Regio Esercito (1915-1943)

di Cosmo Colavito

Abstract. The codebreaking and the interpretation of coded enemy dispatches have assumed increasing importance for the Intelligence Services of the warring Countries from the WWI to the WW II. Italian scholars, authors of many books on the Royal army Intelligence Services during the two World Wars have, up to now, dealt with this topic only *en passant,* leaving room for biased and often poorly documented interpretations. A book reviewed in this issue of the magazine Antologia Militare made up to the abovementioned shortcoming for the WWI,[1] while this article intends to provide a contribution to clarify the role and importance of the Italian army cryptographic offensive activity during the WWII. Continuities and distinctions with respect to the previous war are also highlighted.

Keywords: Intelligence Services, Italian Army, Diplomacy, Comint, Cryptology, Codes Breaking, Tabulating Machines

1. Introduzione

Il primo e il secondo conflitto mondiale differirono, come è noto, per le modalità operative e per la tipologia delle forze in campo, poiché nella gran parte della prima 1ª GM i combattimenti si svolsero tra opposte trincee in una guerra di posizione, mentre nella 2ª GM assunse un ruolo prevalente il movimento di grandi unità motorizzate e corazzate appoggiate da interventi massicci dell'aviazione. Di conseguenza, mentre nella Grande Guerra le comunicazioni poterono utilizzare frequentemente portanti fisici come cavi e linee aeree, nel secondo conflitto, l'impiego del mezzo radio divenne indispensabile, a livello sia strategico che tattico. Contestualmente, nel periodo tra le due guerre, la diffusio-

1 Cosmo COLAVITO, Filippo CAPPELLANO *La Grande Guerra Segreta sul Fronte Italiano (1915-1918) - La Communication Intelligence per il Servizio Informazioni*, Stato Maggiore della Difesa, Roma, 2018

ne delle Onde Corte aveva reso disponibili bande di frequenza molto più ampie rispetto a quelle usate nella 1ª GM, consentendo di incrementare considerevolmente il numero di canali telegrafici e telefonici utilizzabili per comunicazioni militari e civili. Inoltre, durante il secondo conflitto, le innovazioni introdotte da alcuni Paesi belligeranti condussero all'impiego di frequenze più elevate caratterizzate da capacità ancora maggiori.[2]

La crescente quantità di radiogrammi cifrati che venivano trasmessi determinò l'ulteriore sviluppo della Communication Intelligence (COMINT),[3] comprendente l'intercettazione, l'analisi del traffico e l'interpretazione dei dispacci avversari, posta in atto da tutte le Forze belligeranti. Le risorse umane e tecnologiche impegnate in questo importante lavoro di Intelligence divennero, nella Seconda Guerra Mondiale, quantitativamente più ingenti e meglio attrezzate per cercare di superare le sfide poste dalle tecniche sempre più efficaci della Communication Security (COMSEC) e segnatamente dall'impiego di varie tipologie di macchine cifranti-decifranti iniziato ancor prima del conflitto. Tuttavia, il segreto di una parte rilevante delle comunicazioni, non soltanto campali, restò ancora affidato a cifrari basati sull'impiego di carta e penna e su metodi non molto diversi da quelli utilizzati più di vent'anni prima.

Tra gli strumenti tecnologici che supportarono il lavoro di schiere sempre più numerose di crittoanalisti sono da menzionare sia le macchine di calcolo di impiego generale applicate alla crittologia, denominate generalmente tabulatori, sia macchine *ad hoc* che crebbero in complessità per esempio con il passaggio, nella fucina dei decrittatori britannici in Bletchley Park, dalla 'bomba' elettromeccanica di Alan Turing realizzata per forzare l'ENIGMA I a uno dei primi calcolatori

2 Divenne abbastanza frequente l'impiego delle Onde cortissime (VHF o Very High Frequencies) e si iniziarono ad utilizzare le *microonde,* soprattutto per i Radar. I progressi realizzati in questo settore negli USA, Regno Unito e Canada furono resi noti nell'immediato dopoguerra mediante i 28 volumi della Radiation Laboratory Series dell'MIT (Massachusetts Institute of Technology), contenenti «a great body of information and new techniques in electronics and high-frequency field» (Lee Alvin DU BRIDGE, President of MIT, *Foreword to all the volumes*). Per le grandi innovazioni tecniche conseguite, la collana destò enorme sorpresa nel mondo degli specialisti italiani e degli altri Paesi dell'ex Asse.

3 Nella 2ª GM si sviluppò la ELINT (Electronic Intelligence) basata sull'intercettazione e lo sfruttamento a fini informativi di segnali diversi da quelli di comunicazione, segnatamente dei segnali Radar. La SIGINT (Signal Intelligence) comprende sial la COMINT che la ELINT. Oggetto del presente articolo è solo la COMINT.

elettronici: il COLOSSUS, specializzato nel decrittare dispacci generati da macchine cifranti del tipo telescrivente come la tedesca 'Lorenz SZ-42' usata per le comunicazioni strategiche tra gli alti comandi fino a livelli di Armata. L'impiego di strumenti ausiliari specifici non fu prerogativa soltanto dei Britannici, ma anche di altri belligeranti, specie di Americani e Tedeschi.

In questo scenario generale, le capacità crittografiche dell'Esercito italiano, pur progredite dal 1918 al 1940, non consentirono di progettare macchine *ad hoc* come quelle poc'anzi citate per la forzatura dei cifrari nemici e l'impiego di tabulatori divenne possibile solo pochi mesi prima dell'Armistizio dell'11 settembre 1943. Ciò nonostante, come si vedrà nel seguito di questo articolo, i risultati ottenuti furono globalmente degni di nota anche se ottenuti ancora con l'ausilio di carta e matita, sul solco delle tradizioni della Grande Guerra.

Né mutarono rispetto al conflitto precedente alcune impostazioni organizzative e funzionali, come l'affidamento all'Esercito, piuttosto che al Ministero degli Affari Esteri, della soluzione dei codici diplomatici e la netta separazione, nelle strutture centrali così come nelle grandi unità mobilitate, delle attività di analisi crittografica rispetto alle altre funzioni di COMINT sopracitate. Si ritiene però che il lascito fondamentale della 1ª GM fu il libro *Nozioni di crittografia* di Luigi Sacco,[4] capo del Reparto crittografico, pubblicato, a scopo interno dallo Stato Maggiore dell'Esercito nel 1925 e posto in libero commercio cinque anni dopo. Vittorio Gamba, successore di Sacco dal primo dopoguerra fino alla Seconda Guerra Mondiale, e gli altri violatori di cifrari italiani si giovarono certamente degli insegnamenti contenuti in quel volume.[5]

Nel presente articolo, pur senza voler ricostruire per intero la storia della crittologia militare e diplomatica italiana nelle due Guerre Mondiali, si cercherà di evidenziare non soltanto le analogie, ma anche le profonde differenze tra i protagonisti e le metodologie adottate negli organismi dell'Esercito italiano incaricati di svolgere le attività crittologiche offensive nei due conflitti. Si confronteranno

4 Nel seguito di questo articolo si fa riferimento a Luigi SACCO *Manuale di Crittografia*, 3ª Edizione aggiornata e aumentata, Roma, 1947.

5 David Kahn, 27 anni dopo l'edizione del libro di Sacco del 1947, lo considerava ancora come «il miglior lavoro in unico volume sugli aspetti tecnici della crittologia» e aggiungeva «Sacco è stato perciò una delle più grandi figure del panteon della crittologia» (David KAHN «Interview with Cryptologists», in Cipher DEAVOURS et *alii Cryptology. Machines, history & methods,* Arthec House, Norwood, 1989, pp. 36-41).

poi i risultati ottenuti, rilevando i meriti ma anche le manchevolezze rilevate soprattutto nella 2ª GM.

Tra le fonti per la storia della crittografia nel secondo conflitto, sono stati largamente utilizzati i verbali degli interrogatori dei criptologi militari italiani condotti nel 1944 dal War Office inglese, coadiuvato dalle Agenzie di Intelligence britanniche MI5 e MI9, mediante una struttura creata a questo scopo e denominata 'Combined Services Detailed Interrogation Centre' (CSDIC).[6] Gli organi di Intelligence americani costituirono, a loro volta, il TICOM (Target Intelligence Committee) che dal 1944 iniziò a investigare al fine di «conoscere con certezza la misura in cui le comunicazioni americane fossero sicure o insicure» poiché non erano note «le reali dimensioni della capacità, della forza e del materiale crittologico del nemico». Il TICOM pubblicò, in nove volumi, i risultati ottenuti anche dal CSDIC, una parte dei quali riguarda i cifrari violati dagli Italiani.[7] Nel seguito si è cercato, ove possibile, di verificare le notizie così ricavate tenendo presente, tra l'altro, che le deposizioni di alcuni Ufficiali Italiani, e in particolare quella del Generale Gamba, furono riduttive e parziali, omettendo per esempio la forzatura di alcuni codici importanti.

---

6 Il CSDIC operò in diverse parti del mondo dal 1942 al 1947, interrogando agenti dell'Intelligence dei Paesi nemici, soprattutto nazisti e giapponesi e poi anche persone sospettate di lavorare per i Servizi sovietici.

L'autore del presente articolo ha conosciuto personalmente alcuni degli Ufficiali italiani interrogati e in particolare l'Ingegnere Augusto Bigi, divenuto Ispettore Generale del Ministero PT, Segretario e poi membro del Consiglio Superiore Tecnico delle Telecomunicazioni e il Dottor Ernani Nordio, Direttore Generale della Società telefonica TELVE e poi della Seconda Zona della SIP.

7 ARMY SECURITY AGENCY *European Axis signal intelligence in WAR II as revealed by TICOM investigations and by other prisoner of war interrogations and captured material, principally German,* in nine volumes, Washington D.C., 1 May 1946. Il virgolettato riportato nel testo è tratto dal 1° volume dal titolo *Synopsis*, p. 3. Particolarmente interessante nel 1° volume è la chart 2 dal titolo *Results of European Axis cryptanalysis as learned from TICOM sources,* in cui sono esposti, in forma tabellare, i risultati, suddivisi per Paese belligerante, ottenuti dall'elaborazione degli interrogatori di prigionieri italiani e tedeschi, relativi a ciascun cifrario da questi conosciuto. A tali tabelle si fa riferimento nel seguito con la semplice indicazione ASA, Vol. 1 seguita dalla indicazione del cifrario con il Paese di appartenenza e il numero d'ordine.

2. I PROTAGONISTI

Vite convergenti di due Generali

Luigi Sacco e Vittorio Gamba nacquero rispettivamente ad Alba (CN) e a Vercelli, a circa 75 chilometri di distanza, il primo nel 1883 e il secondo nel 1880. Sacco entrò in Accademia all'età di 18 anni e si dimostrò particolarmente versato nelle discipline scientifiche tanto da confermarsi 'capoclasse' del suo corso per tre anni consecutivi, ottenendo per questo una medaglia dal Ministero della Guerra. Nominato Sottotenente del Genio nel 1904, venne invitato, dopo tre anni, dall'allora Maggiore Morris a presentare domanda per passare nei Radiotelegrafisti, specialità in cui operò lungo l'intero arco della sua carriera militare.[8]

Gamba entrò invece in Accademia all'età di 22 anni, avendo trascorso all'estero, dopo le scuole superiori, un periodo dedicato a perfezionarsi nelle lingue, con una passione che continuò a coltivare per tutta la vita, fino a conoscerne - si dice - almeno 25, più i relativi dialetti. Dopo l'Accademia, divenne Ufficiale degli Alpini e tale rimase per tutta la durata del suo servizio nell'Esercito.

La Guerra di Libia vide impegnati ambedue i Tenenti in zona di guerra, Sacco come realizzatore e gestore della rete radiotelegrafica della Tripolitania e Gamba come traduttore e interprete da e nella lingua araba.

Durante la Prima Guerra Mondiale l'allora Capitano Luigi Sacco costruì dal nulla, con un immane sforzo personale iniziato negli ultimi mesi del 1915, il primo Reparto crittografico dell'Esercito che, inserito l'anno successivo nell'ambito del Servizio Informazioni, raggiunse quasi miracolosamente livelli qualitativi comparabili a quelli degli analoghi servizi nemici e alleati entrati in guerra con migliore preparazione e più ampie risorse. Oltre a numerosi elogi e riconoscimenti, a Sacco fu conferita la nomina a Tenete Colonnello per meriti speciali.[9]

---

8 Molte notizie sulla vita di Vittorio Gamba qui riportate sono tratte dal Comunicato ANSA *Morto asso del Controspionaggio italiano*, 23 gennaio 1965, mentre per Luigi Sacco si sono usate le fonti riportate in COLAVITO, CAPPELLANO e nell'archivio custodito dal nipote del Generale, Prof. Paolo Bonavoglia che si ringrazia per la cortese disponibilità.

9 Dallo Stato di servizio risulta che Sacco venne elogiato nel luglio del 1916 dal Capo della Missione Militare francese in Italia e poi dal Generale Porro, Sottocapo di Stato Maggiore, «per l'opera assidua intelligente e geniale e per i risultati ottenuti nella ricerca di cifrari radiotelegrafici nemici della Marina e dell'Esercito nonché delle chiavi variabili adoperate nell'impiego di tali cifrari». Ciò dimostra ancora una volta che le decrittazioni delle comu-

Dopo la fine della Guerra, il Reparto crittografico subì, come molti altri organismi dell'Esercito, un radicale ridimensionamento. Pochi giorni dopo l'armistizio, lo stesso Sacco, stressato per l'immane lavoro svolto, preferì abbandonare la crittologia operativa, pur continuando a insegnare questa materia nei Corsi per Ufficiali Informatori e curando la redazione delle successive edizioni del suo Manuale.

Subito dopo, il Reparto cominciò a svuotarsi dei più abili criptologi poiché questi non erano, per la maggior parte, Ufficiali di carriera e tornarono perciò gradualmente alla vita civile. Il Servizio Informazioni tentò ripetutamente di reperire nuovi elementi validi soprattutto per interpretare i dispacci diplomatici e cercò di trattenere in servizio coloro che venivano trasferiti ad altri incarichi, ma inesorabilmente le capacità crittografiche dell'Esercito si andarono attenuando.[10] In queste circostanze giunse al Reparto crittografico Vittorio Gamba uscito dal conflitto con il grado di Capitano.

Nei Diari della Sezione R del Servizio Informazioni italiano, il nome di Vittorio Gamba non risulta compreso tra quelli degli Ufficiali entrati a far parte del Reparto Crittografico nel corso della Grande Guerra, ma non si può escludere che egli abbia prestato saltuariamente la propria opera di traduttore da lingue quali il turco e il russo. È noto invece come le sue indubbie capacità di poliglotta siano state utilizzate e apprezzate dagli alti Comandi Italiani e sembra anche dai Generali Diaz e Badoglio.

Negli anni seguenti, Gamba operò con continuità come Capo del Reparto Crittografico, inserito nel SIM all'atto della costituzione del Servizio nel 1925. La sua competenza crittologica andò affinandosi nel tempo tanto da venir prescelto nel 1931 come redattore delle voci "Cifrari" e "Crittografia" della Enciclopedia Italiana, segno evidente che all'epoca le conoscenze dell'Esercito in questa disciplina erano considerate ancora tra le più avanzate esistenti nel nostro Paese.[11]

Il SIM, specie nell'era Roatta (1934-39), conferì crescente importanza alla

---

nicazioni nemiche erano iniziate al più tardi nella primavera di quell'anno.

10 Il Capo del Servizio Informazioni Odoardo Marchetti lanciò un allarme, con una lettera inviata allo Stato Maggiore del Ministero della Guerra nel marzo del 1919 in cui ammoniva di evitare la smobilitazione del Reparto crittografico.

11 La voce 'Cifrario' comparve nel Volume 10 e quella 'Crittografia' nel Volume 11, ambedue pubblicate nel 1931. L'Enciclopedia venne gradualmente pubblicata dal 1929 al 1937.

crittologia, anche per i risultati positivi ottenuti nelle guerre di Abissinia e di Spagna, così che il Reparto divenne la quinta delle cinque e poi sette Sezioni del Servizio Informazioni Militari. Vittorio Gamba poté quindi vedere riconosciuti i propri meriti con avanzamenti di carriera fino al grado di Generale di Brigata.[12]

Fig. 1 Il Generale di Brigata Vittorio Gamba (Archivio fotografico ISCAG)

Fino all'8 settembre del 1943, la Sezione crittografica mantenne una fisonomia unitaria, per la maggior parte del tempo sotto il suo comando, nonostante le riforme del Servizio Informazioni dell'Esercito.[13]

Intanto Luigi Sacco, nominato nel 1919 Direttore dell'Officina Militare di Radiotelegrafia ed Elettrotecnica - dal 1927 Officina Militare delle Trasmissioni (O.M.T.) - fornì contributi fondamentali per la realizzazione di gran parte degli apparati radio progettati e costruiti per l'Esercito, tra cui i ricevitori l'RI-1 e l'RI-2 impiegati per l'intercettazione delle comunicazioni radiotelegrafiche e i radiogoniometri a cominciare dall'RGP entrato in servizio nel 1933.[14] Promosso Generale nel 1935, continuò a coordinare le attività dell'O.M.T. e dell'Istituto Militare Superiore delle Trasmissioni. Durante la Seconda Guerra Mondiale non prese parte direttamente alle attività di decrittazione,[15] ma pro-

12 Ambrogio VIVIANI, *Servizi Segreti Italiani, 1815-1985*, adnkronos, Roma, 1985, Vol. II, p. 192.

13 La Sezione crittografica passò al SIE (Servizio Informazioni Esercito) a seguito della riforma del 1° novembre 1941 e poi nuovamente nel SIM dal 1° giugno 1943.

14 Questo radiogoniometro forniva una precisione maggiore di quelli prodotti in Germania e Francia nella gamma delle Onde corte (Carmine PICONE, Carlo MICHELETTA, «Il Tenete Generale Luigi Sacco», Bollettino ISCAG, N° 4, 1970, p. 441.

15 Nell'edizione del libro del 1947 si trovano alcuni riferimenti a cifrari nemici usati durante il conflitto recentemente concluso. Nel 1939 Sacco era stato promosso Tenente Generale, il massimo grado consentito agli Ufficiali del Genio e disaccato presso il CNR per studi di

Fig. 2 Il Tenente Generale del Genio Luigi Sacco. (Archivio fotografico Luigi Sacco a cura di Paolo Bonavoglia)

gettò una macchina cifrante "a catena" costruita presso gli stabilimenti OMI-Nistri di cui purtroppo si è persa ogni traccia, probabilmente perché andata distrutta.[16]

Una notizia singolare: l'avversario di Sacco durante la Grande Guerra, il capo del potente ufficio crittografico austriaco, Andreas Figl, fu invece cooptato nella R.S.H.A. (Direzione Centrale per la Sicurezza del Reich), uno sei dipartimenti delle SS, ove operò nell'ambito dell'AMT V IF (Ufficio V, Servizio Informazioni sull'Estero), contribuendo a risolvere alcuni cifrari nemici.[17]

Il Generale di Brigata Gamba e il Tenente Generale Sacco furono posti entrambi in congedo, per raggiunti limiti di età, il primo in aprile e il secondo nell'agosto del 1943.[18]

Gli altri analisti dell'Esercito italiano

Tra gli appartenenti al Reparto crittografico durante la 1ª GM, Sacco cita nel suo libro solo «due ottimi irredenti, gli Ingegneri e Tenenti di complemento Tullio Cristofolini da Trento e Mario Franzotti (italianizzato da Franzot NdA) da Gorizia, nonché un valentissimo poliglotta il Prof. Remo Fedi», ma accenna anche

radio propagazione.

16 Questa vicenda è testimoniata dal nipote del Generale Sacco, Prof. Paolo Bonavoglia. La macchina è descritta in: SACCO, p. 80-84. La OMI Nistri produsse durante la II GM, anche se in un limitato numero di esemplari, la macchina cifrante decifrante denominata "Cryptograph Alfa", simile alla Enigma, con 5 rotori.

17 Wilhelm HOTTL *Hitler Paper Weapons*, Rupert Hart-Davis, London, 1955, p. 132.

18 In realtà Sacco compiva sessanta anni il primo agosto del 1943, mentre Gamba li aveva compiuti allo scoppio della guerra. La data del congedo di Gamba risulta da: CSDIC, CMF/Y4 *First detailed Interrogation of Capt. Bigi, Augusto*, 8 Sept. 1944, p. 10.

ad «altri bravi traduttori e interpreti» aggregati successivamente».[19] Dall'esame del taccuino di Sacco del 1916 risulta che soltanto il Fedi era compreso, insieme ad altri sette addetti, nello staff iniziale del Reparto durante il periodo in cui operava ancora a Codroipo, mentre Cristofolini e Franzot si aggiunsero dopo il novembre del 1916, cioè dopo il trasferimento a Roma di Sacco insieme ad alcuni dei più validi elementi del gruppo.

Dai Diari della Sezione R del Servizio Informazioni si deduce che, dal 1916 al 1918, entrarono a far parte del Reparto i Tenenti, Bresciani, Modica, Giorgio Levi della Vida, il Sottotenente Savino Lalloni e l'Aspirante Petrelli. L'organico non superò complessivamente una ventina di addetti, tra cui solo alcuni, forse proprio quelli citati da Sacco, possedevano il così detto 'bernoccolo crittografico'.

All'inizio della 2ª GM gli ufficiali analisti della Sezione crittografica erano divenuti esattamente 22, affiancati da 14 sottufficiali e da un solo impiegato civile.[20] Questo numero non aumentò sensibilmente durante il conflitto: il Generale Cesare Amè, capo del SIM, afferma che nel 1943 gli Ufficiali destinati alla Sezione erano 35, 14 dei quali però in corso di trasferimento ad altri reparti. Si stima quindi che l'organico non possa aver superato di molto cinquanta addetti.[21]

Le risorse suddette furono suddivise, in modo flessibile, in tre sottosezioni dedicate rispettivamente ai cifrari diplomatici, militari e commerciali. Dalle informazioni fornite al CSDIC, si deduce che, nelle diverse fasi del conflitto, circa il 70% degli analisti era destinato alla violazione dei codici diplomatici, il 25% a quella dei codici e cifrari militari, mentre la parte restante si occupava di dispacci commerciali in codice, verificando in particolare che non contenessero informazioni di carattere riservato.[22]

Il vice Comandante della Sezione era il Colonnello Cosmacini che sostituì

19 SACCO, p. 308. I primi collaboratori furono oltre a Remo Fedi, Massara, Ospici, Biancolini, Giovannuzzi, Franceschini, Peretti e Rebec, per la maggior parte appartenenti al Reparto RT e impiegati per svolgere compiti ausiliari come statistiche, traduzioni, ecc. (COLAVITO, CAPPELLANO, cit., p. 250).

20 AUSSME, Diario Storico del SIM, 23 maggio 1941, Allegato n°1 *Relazione sull'attività svolta dalla Sezione crittografica dal 10 giugno 1940 al 10 maggio 1941*. Prima dell'entrata in guerra dell'Italia, gli Ufficiali erano 10, i sottufficiali 14 a cui si aggiungeva un impiegato civile.

21 Cesare AMÉ *Guerra segreta in Italia 1940 - 1943*, a cura di Carlo De Risio, Bietti, Milano, 2011, p. 212.

22 Tali percentuali si deducono da CSDIC, CMF/Y4, Bigi, p. 2 e da altre deposizioni.

Gamba all'atto del congedo di quest'ultimo. Nella sottosezione diplomatica, i gruppi linguistici con più addetti erano di norma comandati da un Tenente colonnello: Luigi Serragli[23] per le lingue slave, Raul Carusi per il turco, Valletta per il francese e Giuseppe Vassallo Todaro per il rumeno. Il gruppo di lingua inglese era comandato da Arturo Croci, che aveva ricevuto il grado onorario di Colonnello.[24] Ai cifrari del Vaticano si dedicava personalmente Vittorio Gamba; dopo il suo congedo, tale compito passò al Capitano Benna. Il Tenente colonnello Francesco Scuderi guidava il gruppo incaricato della ricerca, cioè di ricostruire i cifrari militari le cui difficoltà superavano la capacità analitica dei reparti crittografici delle Armate. Contavano un solo addetto: il gruppo svizzero (francese e tedesco) presidiato dal Maggiore Garofaro, lo spagnolo-portoghese affidato al Capitano Lucrezio e il greco del Maggiore Galifi.[25]

Nella lista dei nominativi citati dal Capitano Bigi, colpisce che questi attribuisca la qualifica di crittografo soltanto a quattro personaggi cioè al Comandante della Sezione, al suo Vice, al T. Colonnello Serragli e al Maggiore Giuseppe Garofalo. Un numero certo esiguo anche se sembra evidente che altri addetti, come ad esempio il già citato T. Colonnello Scuderi, possedevano buone capacità di analisti.

Dopo l'8 settembre 1943 alcuni tra i componenti della Sezione crittografica, al comando del Colonnello Cosmacini, dettero vita a un'analoga sezione nel SID (Servizio Informazione Difesa) della Repubblica Sociale, dislocata prima a Roma e poi a Castiglione delle Stiviere (Mantova). Secondo alcune deposizioni, questa branca del SID cessò l'attività di analisi crittologica per ordine del Comando

23 Il Serragli, con il grado di Sottotenente della Regia Marina, militava nel Reparto crittografico sin dl 1919. Egli, nato a Dubrovnik, esperto di lingue slave era allora considerato particolarmente utile per la minaccia rappresentata dal nuovo Regno dei Serbi, Croati e Sloveni (AUSSME, *Diari della Sezione R, 1° agosto 1919*, Fondo B1, 101S, 341d, Vol. 95). Successivamente era passato nell'Esercito.

24 Arturo Croci aveva perso una gamba nella Grande Guerra, lasciando quindi l'Esercito per divenire Console in Svezia,

25 CSDIC, CMF/Y4, Bigi, p. 9-12. Gli altri Ufficiali citati da Bigi sono: per la lingua francese il Capitano Ingegner Bonvino e il Tenente Agosti: per il Turco i Capitani Nordio, Muratti, Gramola. Battistych e il Tenente Russo; per le lingue slave i Capitani Oneste e De Beden e i Tenenti Smolcich e Carelli; per l'Inglese i Capitani Pitta, Rullino e Peroni. Della Sottosezione commerciale si occupava il Sottotenente Colbi. Non è noto se i 29 componenti della Sezione dei quali Bigi ricordava i nomi, fossero contemporaneamente presenti nella sede della Sezione.

tedesco, nel febbraio del 1944, mentre altre testimonianze portano a ritenerne possibile la prosecuzione fino al 1945. Alla Sezione fu affidata anche la redazione di cifrari e codici impiegati dall'Esercito, com'era avvenuto durante la 1ª G M. Prima dell'Armistizio questo compito era conferito a una organizzazione distinta comandata dal Colonnello Picinocchi.

La sede della Sezione era in un palazzo di via Poli 48, a Roma. Durante la 1ª GM il Reparto aveva operato nell'edificio non molto distante di via Nazionale 74.

A conclusione di questo breve excursus sui componenti del Reparto/Sezione crittografica dell'Esercito italiano, si rileva come, sia nel primo come nel secondo conflitto mondiale, il numero degli addetti destinati a questo servizio sia rimasto notevolmente inferiore a quello impiegato in analoghi comparti dai più importanti avversari e alleati.[26] Il cronico sottodimensionamento italiano, su cui si ritornerà nel seguito, può venir ascritto a numerosi fattori. Almeno per la 2ª GM si ritiene di poster escludere motivi connessi con ristrettezze finanziarie, dati i larghi mezzi di cui il SIM era dotato, mentre mancò senza dubbio la disponibilità di risorse umane adeguate, in quantità e qualità, alla difficile sfida affrontata. Su tale carenza si ritiene abbiano influito sia la persistente limitata diffusione nel Paese di una cultura crittologica di carattere scientifico, sia la ristretta cerchia in cui venivano reclutati i criptologi, costituita da Ufficiali o al più Sottoufficiali in servizio, evitando il coinvolgimento di personale civile - soprattutto matematici, statistici, linguisti e ingegneri, - attuato invece in larga misura da Inglesi, Americani e persino dai Tedeschi.[27]

26 Durante la 1ª GM, il solo ufficio centrale crittografico dell'Esercito austriaco a Vienna contava su non meno di 26 crittoanalisti a cui si aggiungevano quelli decentrati negli almeno 5 o 6 Penkala al fronte italiano. Le notevoli disparità tra il numero di componenti della Sezione crittografica italiana e dell'analoga Sezione dell'OKW/chi (Servizio Informazioni del Comando Supremo delle Forze Armate germaniche), durante la 2ª GM, sono esposte più dettagliatamente nel seguito.

27 Lo stesso Gamba durante il suo interrogatorio attribuì alla mancanza di personale sufficientemente esperto, le performance da lui ritenute insoddisfacenti della Sezione crittografica durante il conflitto (CSDIC/CMF/Y 7 *First detailed Interrogation of Vittorio Gamba, director of SIM Cryptographic Section until Armistice*, 16 Oct. 1944, p. 1).

3. Continuità organizzative e funzionali

I Cifrari diplomatici e il ruolo della HUMINT

Come si è accennato, una delle principali eredità tramandate dal Reparto crittografico alla omonima Sezione dell'Esercito italiano è ravvisabile nel compito di condurre l'analisi crittologica anche della corrispondenza diplomatica, iniziata allora dallo stesso Capitano Sacco. Il trasferimento del Reparto crittografico a Roma, nell'ottobre del 1916, perseguiva anche lo scopo di porre le capacità di Sacco al servizio del Ministero degli Affari Esteri e di altre Istituzioni dello Stato prive di competenze in materia. Si istaurò così una collaborazione che condusse a forzare i codici diplomatici dei Paesi nemici, dei principali Paesi neutrali, della Russia bolscevica e persino degli Stati Uniti d'America, oltre a quelli del Vaticano.[28]

L'origine di questi successi sembra possa ascriversi, almeno in parte, a operazioni di HUMINT.[29] In realtà, prima della Grande Guerra né l'Ufficio Informazioni dell'Esercito, né altri organismi di Intelligence italiani avevano provveduto a procurarsi i cifrari diplomatici o militari, specie Austro-Ungarici. Vi sono però concreti indizi per ritenere che il Servizio Informazioni dell'Esercito italiano abbia acquisito, durante il conflitto, alcuni codici. In particolare, la decrittazione integrale di tutti i gruppi cifranti dei dispacci vaticani, trasmessi da Sacco al Ministero degli Esteri sin dagli ultimi mesi del 1916, dimostrerebbe la disponibilità degli interi cifrari giunti in qualche modo nella disponibilità del Reparto crittografico.[30]

---

28 Tra i cifrari diplomatici forzati erano compresi, oltre a quelli citati nel testo, l'austriaco, il tedesco, lo svizzero, lo spagnolo, il bulgaro e il greco. Più di 3.500 dispacci cifrati con questi codici, tradotti in chiaro, furono trasmessi al Ministero degli Esteri, alla Presidenza del Consiglio, ad altri Ministeri e alle Missioni Militari Alleate in Italia

29 David ALVAREZ «Faded Lustre: Vatican Cryptography», 1815 - 1920*, Cryptologia*, Vol. XX, n°2, April 1996, pp. 97-131; David ALVAREZ, «Left in the dust: Italian Signal Intelligence, 1915 - 1943»*, National Journal of Intelligence and Counter intelligence*, Vol. 14, n°3, 2001, p. 404, note 8; Cosmo COLAVITO, «I Cifrari Diplomatici e Il Reparto Crittografico dell'esercito Italiano durante La Grande Guerra»*, GNOSIS, Rivista italiana di Intelligence*, n°1, 2019, pp. 106-117.

30 D. ALVAREZ, «Faded Lustre», p. 120-121. Nel corso del conflitto non mancarono inoltre occasioni in cui gli Italiani vennero in possesso di cifrari nemici catturati nel corso di combattimenti o recuperati nei relitti di navi nemiche affondate (COLAVITO, CAPPEL-

La propensione a utilizzare, sin dalla Grande Guerra, la HUMINT a supporto dell'attività di decrittazione è dimostrata dal famoso "colpo di Zurigo" condotto dal Servizio Informazioni della Regia Marina con il supporto di quello dell'Esercito. A questo proposito, il Generale austriaco Maximilian Ronge dichiarò che il maggior danno subito in quella occasione dai Servizi d'Informazione austriaci fu proprio la sottrazione del cifrario.[31]

Dopo la fine della guerra, gli analisti dell'Esercito continuarono a occuparsi di codici diplomatici fino a tutta la Seconda Guerra Mondiale, anche se in alcune circostanze, intorno al 1922, la decrittazione di dispacci inglesi e francesi sembra fosse affidata, secondo quanto sostenuto da Enrico Cernuschi, a due promettenti giovani Ufficiali della Regia Marina, Giorgio Verità Poeta e Luigi Donini, che usufruirono dei codici prelevati nelle rispettive Ambasciate da un gruppo di Carabinieri, operativo a tale scopo dal 1919 e forse da tempi anteriori. [32]

Il gruppo, poi denominato "P" (Prelevamento), portò a termine negli anni seguenti numerosi 'colpi' tra cui, nel 1934, la riproduzione dei codici inglesi sottratti temporaneamente dai fratelli Francesco e Secondo Costantini dalla cassaforte dell'Ambasciata inglese in Roma, ove essi lavoravano come impiegati. L'impresa richiese molti mesi di accurata preparazione e venne replicata più volte nella stessa Ambasciata, per esempio con la sottrazione del Rapporto Maffey, ove si dimostrava che, contrariamente alle tesi propagandistiche sostenute pubblicamente dal Governo inglese, gli interessi britannici non erano stati affatto danneggiati dalla conquista italiana dell'Etiopia.[33]

L'attività di prelevamento divenne ancora più intensa nella seconda metà degli anni Trenta con il trasferimento al SIM del Maggiore dei Carabinieri Manfredi Talamo chiamato a comandare il Centro di controspionaggio di Roma, e raggiunse il massimo vigore nel periodo immediatamente precedente l'entrata dell'Italia

LANO, pp. 204- 206).

31 Maximilian RONGE *Spionaggio*, Editrice Tirrenica, Napoli, 1939, p. 293.

32 Per i due Ufficiali di Marina, si trattò quindi di risolvere le sopra cifrature adottate nei dispacci. Enrico CERNUSCHI, «Il Comandante Giorgio verità Poeta, la crittografia e il suo contributo personale al giorno d'oggi», in. *Il Comandante Giorgio Verità Poeta*, Atti del Convegno 18 ottobre 2014, in edibus, Milano, 2016, pp. 138-176.

33 The West Australian «The Maffey Report. Leakage a Mystery. Effect of Disclosure. Britain's Strong Position», February 22, 1936. La disponibilità in mano italiana di questo rapporto riservatissimo venne resa nota dal Giornale d'Italia a cui era stato probabilmente inviato dallo stesso Mussolini.

nella 2ª GM, quando un'operazione programmata da tempo consentì, in soli quattro giorni tra il 31 maggio e il 3 giugno 1940, di sottrarre centinaia di documenti, tra cui un elevato numero di cifrari, nelle sedi di Ambasciate e Legazioni presso lo Stato italiano e la Santa Sede.[34]

Simili imprese ebbero luogo anche nei successivi anni del conflitto, per esempio a danno dell'Ambasciata americana ove, prima della dichiarazione di guerra dell'Italia contro gli Stati Uniti, il gruppo P sottrasse alcuni importanti cifrari con l'aiuto di un certo Loris Gherardi, un semplice fattorino che riscuoteva la fiducia dell'Ambasciatore. Nel corso del 1941«i documenti segreti venuti in possesso del Servizio Informazioni dell'Esercito furono circa tremila: i materiali crittografici una cinquantina».[35]

Nel corso del conflitto, le attenzioni del gruppo P furono rivolte anche agli Ambasciatori di Paesi nemici presso la Santa Sede che si erano rifugiati in Vaticano e comunicavano con i propri governi mediante la valigia diplomatica del Vaticano o talvolta anche attraverso la stazione radio pontificia. Angelo Greffi, uno dei Marescialli dei Carabinieri che operò dopo il 1940 agli ordini di Talamo, testimoniò di almeno sette azioni da lui condotte ai danni delle Ambasciate belga e inglese. David Alvarez narra, tra l'altro, la rocambolesca operazione condotta per sottrarre il codice diplomatico inglese all'Ambasciatore D'Arcy Osborne dalla sua residenza nel Convento di Santa Marta ove si era trasferito dopo la dichiarazione di guerra dell'Italia all'Inghilterra[36].

Vedremo poi come tutto questo materiale sia stato utilizzato dalla Sezione crittografica che, tra l'altro, sembra fosse ignara della sua provenienza. La disponibilità di grandi quantità di codici diplomatici fornì senza dubbio a quest'ultima un notevole vantaggio competitivo, ma l'impiego di tabelle frequentemente variabili che servivano per operare una seconda cifratura sui gruppi di cifre ottenuti dai libri dei codici, costituì una sfida che, come vedremo, non poté esser vinta dalla

34 A tale scopo si utilizzò, com'era avvenuto in precedenza, il personale italiano impiegato con diverse funzioni nelle sedi diplomatiche. I documenti sottratti venivano consegnati agli agenti che, dopo averli rapidamente fotografati, li restituivano per rimetterli al proprio posto. La storia di alcune tra queste imprese è raccontata da Giorgio. PILLON: *Spie per l'Italia. Come fecero la guerra gli 007 dei nostri servizi segreti*, prefazione del Generale Cesare Amè, I libri del NO, Roma, 1968, pp. 11-14.

35 AMÉ, p. 63.

36 David ALVAREZ *I servizi segreti del Vaticano. Spionaggio. Complotti, intrighi da Napoleone ai giorni nostri*», Newton Compton, Roma, 2009, pp. 248-251.

Sezione solo nei casi più difficili dal punto di vista crittologico.

Contrariamente a quanto avvenuto per i dispacci diplomatici, lo studio dei cifrari navali e la decrittazione dei relativi dispacci non rientrò tra i compiti dalla Sezione crittografica dell'Esercito nella 2ª GM. Sacco aveva iniziato a decrittare i dispacci della Marina Austro Ungarica sin dagli ultimi mesi del 1916, ma verso la fine del conflitto,[37] la Regia Marina con l'aito di valenti criptologi francesi e inglesi, iniziò a rendersi indipendente. Nel dopoguerra. dopo varie fasi di collaborazione, anche con l'invio di alcuni Ufficiali a far esperienza nel Reparto crittografico,[38] nel 1934 la Marina italiana, creò su basi stabili, un proprio servizio inserito nel SIS (Servizio Informazioni Segrete), come 5ª Sezione.

La scarsa integrazione tra le funzioni della COMINT

Tra le innovazioni più rilevanti introdotte durante la Grande Guerra e applicate fino alla Seconda Guerra Mondiale vanno annoverate la netta separazione delle attività di radio intercettazione e localizzazione da quelle crittografiche a livello centrale, come anche la costituzione nelle Armate mobilitate di reparti distinti per queste due funzioni.

Ancor prima del trasferimento a Roma, l'Ufficio RT di Codroipo diretto da Sacco effettuò sia le intercettazioni e le localizzazioni delle radio comunicazioni nemiche, sia le prime decrittazioni dei dispacci militari austriaci e tedeschi. Dopo quella data, le due attività vennero scisse perché Sacco, con pochi collaboratori, si occupò prevalentemente di crittografia, mentre le intercettazioni e l'analisi del traffico radio rimasero affidate alla Prima Sezione Radiogoniometrica nella zona di guerra.[39] Nonostante questa suddivisione, il legame tra i servizi di intercettazione e decrittazione fu strettissimo durante tutto il conflitto.

Queste componenti della radio Intelligence rimasero, a livello centrale, netta-

37 Sacco risolse, tra l'altro, le sopra cifrature del codice navale austriaco denominato KOD che era stato catturato in un sommergibile posamine tedesco battente bandiera austriaca, affondatosi per un incidente nel golfo di Taranto. Verso la fine del conflitto gli addetti alla crittografia della Regia Marina ottennero anche il supporto di esperti francesi e britannici.

38 Ufficio del Capo di SM della Regia Marina, *Promemoria n° 751 sul Servizio crittografico presso il Ministero della Guerra*, Roma, 18 settembre 1934.

39 La Sezione era comandata da Franco Magni con sede a Codroipo e dopo Caporetto, nei pressi di Padova.

mente distinte fino alla fine della Seconda Guerra Mondiale, pur non mancando, specie negli ultimi anni, numerose critiche che evidenziavano i vantaggi ottenibili mediante una più stretta collaborazione tra i diversi comparti della COMINT, dimostrati tra l'altro dal modello integrato adottato dagli alleati tedeschi.[40]

Durante il secondo conflitto, la gran parte delle operazioni di intercettazione venne effettuata da Forte Braschi in Roma a cui si aggiunsero altri centri in numero crescente nel tempo.[41] I radiogrammi in codice intercettati provenienti anche da altre fonti, come i Centri del SIM all'estero, e dai Servizi I delle Unità operanti nei vari settori, si trasmettevano via filo con telescriventi, alla sede della Sezione in via Poli 48. Le trasmissioni radio verso i centri del Servizio Informazioni[42] e le Unità dell'Esercito partivano invece da forte Boccea, dovendo le ricezioni a onde corte avvenire in sedi opportunamente distanziate dalle trasmissioni.

Il tema del decentramento crittologico venne affrontato durante la Grande Guerra, subito dopo la disfatta di Caporetto, quando il traffico radio soprattutto di origine tedesca si intensificò sul fronte del Grappa-Piave. Nell'aprile dell'anno successivo, con la ripresa delle radiocomunicazioni Austro-Ungariche fino ad allora rimaste quasi sempre silenti, fu istituito presso ciascun Comando d'Armata sia un gruppo per l'intercettazione e la localizzazione delle comunicazioni nemiche sia un servizio crittografico comprendente almeno un Ufficiale.[43]

Dopo la fine del conflitto, il decentramento crittografico andò estinguendosi per mancanza di risorse umane adeguatamente preparate, essendo quelle dispo-

40 Questa critica traspare dalla deposizione di Vittorio Gamba (CSDIC/CMF/Y7, Gamba, p. 1 e da quelle di altri Ufficiali italiani.

41 Le stazioni di intercettazioni erano suddivise secondo il tipo di corrispondenza in diplomatiche, militari e in una terza categoria che provvedeva all'ascolto delle radiodiffusioni, alle intercettazioni delle radio clandestine e al controllo delle nostre stesse trasmissioni. Mentre le corrispondenze diplomatiche erano curate da 26 postazioni dislocate tra Forte Braschi e Venezia, del settore militare si occupava un numero elevato di stazioni distribuite nei diversi teatri di combattimento, oltre a quelle di Forte Braschi, Torino ed Albenga (AUSSME, *Diario Storico del SIM, 23 maggio 1941*, Allegato n° 1, cit.).

42 I centri SIM all'Estero stabilmente collegati via radio con Roma erano almeno 23 (Carlo DE RISIO «Tutti gli Uomini del SIM», Storia Illustrata, n°271, giugno 1970, p. 30).

43 Negli ultimi mesi di guerra, queste unità sgravarono il Reparto crittografico centrale di una parte del lavoro di routine e riuscirono per esempio a ottenere informazioni di prima mano sulla preparazione e sullo stato d'animo delle truppe nemiche che attendevano ansiosamente il decisivo attacco italiano sferrato il 24 ottobre del 1918 (COLAVITO, CAPPELLANO, pp. 384 - 386).

nibili appena sufficienti a presidiare il Reparto centrale. Restarono invece attivi, specie nei corpi di spedizione operanti all'estero, le intercettazioni e i rilevamenti radiogoniometrici affidati a gruppi speciali di radiotelegrafisti, operanti sulla base di «programmi compilati dall'Ufficio Informazioni del Comando Supremo, d'accordo con il direttore superiore dei collegamenti».[44]

Durante le Guerre di Abissinia e di Spagna, nelle grandi unità combattenti furono costituiti organismi di analisi crittografica, accanto a quelli di intercettazione e controllo del traffico nemico. Nel primo dei due conflitti, dopo l'impiego di ricevitori più evoluti rispetto a quelli inizialmente in dotazione,[45] un piccolo gruppo di analisti forzò i cifrari nemici, complicati principalmente a causa dell'impiego della lingua aramaica.[46] Il Viviani poté così affermare che «l'Ufficio informazioni del SIM in Africa Orientale» agì «a favore delle truppe operanti specie con un efficiente servizio di intercettazione e di decrittazione».[47]

Durante la guerra di Spagna, il SIS della Regia Marina si distinse nelle attività di intercettazione e decrittazione di indole non soltanto navale, condotte dalla base stabilita nel 1937 a Palma de Majorca.[48] Tuttavia, anche il Corpo Truppe Volontarie (C.T.V.) disponeva di un Ufficio I comprendente quattro sezioni, tra cui una dedicata alla decrittazione (sezione D) presidiata da pochi elementi che

---

44 Stato Maggiore dell'Esercito, Ufficio Informazioni *Istruzione sul Servizio Informazioni presso le truppe* (Filippo CAPPELLANO, «Il Servizio intercettazioni e radiogoniometrico del Regio Esercito 1915-1945», *Radiofronte 1835-1945*, Museo Storico Italiano della Guerra, Rovereto, 2003, p. 18). In questo saggio sono illustrati gli sviluppi delle comunicazioni radio e della radiogoniometria nell'Esercito italiano per tutto il periodo indicato nel titolo.

45 I primi ricevitori non funzionavano nella gamma delle onde corte usata dagli Abissini. Furono allora inviati urgentemente dall'Italia ricevitori "OC7" dell'Allocchio e Bacchini e alcuni Telefunken (CAPPELLANO, p. 32).

46 Maria Gabriella PASQUALINI *Breve storia dell'organizzazione dei Servizi d'Informazione della R. Marina e R. Aeronautica, 1919-1945,* Commissione Italiana Storia Militare, Roma, 2013, p. 231. La difficoltà della lingua fu superata aggregando un traduttore locale al nucleo di tre analisti italiani. Il cifrario militare in aramaico conteneva soltanto, secondo la Prof. Pasqualini, cento gruppi cifranti sillabici corrispondenti ad altrettanti termini in chiaro

47 VIVIANI, Vol.1, p. 205.

48 Secondo le informazioni raccolte dal TICOM, il SIS violò nel 1938 almeno un cifrario navale e otto cifrari dell'Esercito repubblicano spagnolo utilizzanti vari metodi di sostituzione polialfabetica, effettuati di solito mediante listelli di carta scorrevoli (ASA, Spain, 73 – 80 e nel seguito per le codifiche con sostituzione polialfabetica).

dettero però buona prova delle proprie capacità nel forzare alcuni cifrari delle truppe repubblicane.

Un'assegnazione sistematica ai Comandi d'Armata di analisti, scelti in base alle conoscenze linguistiche, poté iniziare nel 1938 dopo la fine dei primi corsi di specializzazione organizzati dalla Sezione crittografica e diretti dal Colonnello Cosmacini. Alla fine dei quattro mesi di durata di ciascun corso, tra i 40-45 partecipanti venivano selezionati i 10-15 migliori allievi che seguivano, per due mesi, un ulteriore periodo di formazione. Questi ultimi raggiungevano la Sezione crittografica centrale a Roma o alcuni importanti centri di Intelligence all'estero, mentre i rimanenti erano destinati ai Comandi delle Armate per svolgervi servizi di decrittazione, soprattutto dei dispacci cifrati mediante sistemi già forzati a livello centrale.[49]

I gruppi crittografici costituiti presso i Comandi d'Armata, e anche a livello inferiore, restarono per la maggior parte del conflitto, scissi rispetto alle compagnie di radiotelegrafisti impegnate nella intercettazione e localizzazione delle radio comunicazioni nemiche, senza conseguire i vantaggi di una più stretta collaborazione tra gli operatori dei due settori.[50] Solo nell'estate del 1943, sulla scorta della positiva esperienza maturata, in questo comparto, dall'Armata Italiana in Russia e ispirandosi al modello tedesco, si costituì una Sezione IRID (Intercettazione, Radiolocalizzazione, Interpretazione, Decrittazione) con l'incarico di facilitare, presso tutte le Armate l'integrazione tra le diverse componenti della COMINT. Questa riforma poté però attuarsi solo in modo parziale nel breve tempo disponibile prima dell'8 settembre 1943.[51]

---

49 Analoghi corsi furono tenuti durante il conflitto nel tentativo di incrementare con elementi validi le scarse risorse umane disponibili nel settore crittologico, ricercandoli sempre rigorosamente nell'ambito di ufficiali dell'Esercito. Vedasi per esempio AUSSME, Diario Storico SIE, 13 novembre 1941, Allegato 2 *Corso di abilitazione di ufficiali di complemento al servizio crittografico.*

50 Nonostante l'esperienza dei conflitti precedenti, fu necessario sostituire gran parte degli apparati di intercettazione e radiogoniometria con cui l'Italia era entrata in guerra poiché, per esempio, la localizzazione dei trasmettitori ad onde corte, oltre le brevi distanze, era falsata per effetto della così detta onda di cielo. Si impose perciò l'impiego dei radiogoniometri Adcock di cui erano già largamente provviste le truppe tedesche e quelle nemiche.

51 CSDIC/CMF/Y10 *First detailed interrogation of Guido Emer*. Il Colonnello Emer aveva realizzato nell'8ª Armata combattente in Russia la fusione tra il servizio di intercettazione e quello crittografico. Egli fu quindi incaricato di organizzare un'analoga struttura nelle altre Armate.

4. GLI ANALISTI ITALIANI AL LAVORO

I limiti al miglioramento

La quantità dei dispacci intercettati e decrittati crebbe nel corso della 1ª GM con un massimo negli ultimi dodici mesi, quando la somma di telegrammi e radiogrammi, interpretati e inseriti nei bollettini, cioè diffusi all'esterno del Reparto crittografico in quanto ritenuti di interesse per il Comando Supremo, il Ministero Affari Esteri, ecc., raggiunse circa 3.200 unità.[52] Nel primo anno della 2ª GM, si disponeva giornalmente di più di quattrocento radiogrammi intercettati, alcuni dei quali spesso originati dalle stesse fonti e cifrati con lo stesso codice. Di questi circa il 20%, dopo la decrittazione, era inserito nei bollettini, in quantità circa 10 volte maggiore rispetto alla fine del conflitto precedente.[53]

Come già accennato, nella 2ª GM la maggior parte dei dispacci decrittati dagli analisti dell'Esercito italiano erano cifrati con metodi analoghi a quelli impiegati durante il conflitto precedente, cioè con procedure di sostituzione o di trasposizione, ovvero mediante codici quasi sempre sopra cifrati, alcuni dei quali impiegavano però metodologie più sofisticate di quelle utilizzate in passato.[54]

In particolare, i metodi di sostituzione polialfabetica largamente applicati nella Grande Guerra anche dall'Esercito Austro-Ungarico e risolti dal Reparto crittografico (figura 3) trovarono, durante il primo dopoguerra, applicazione nelle macchine cifranti-decifranti elettromeccaniche a rotori del tipo Enigma o Hagelin. Questi dispositivi sostituivano, in un primo rotore, ciascuna lettera dei

52 AUSSME, *Diari del Reparto R del Servizio Informazioni, 110 S, 307d-327d*. In ambedue le guerre, venivano inseriti nei Bollettini solo i crittogrammi decrittati ritenuti degni di interesse. Nella 2ª GM i bollettini giornalieri venivano inviati al Capo del Governo che li trasmetteva ai Ministri di volta in volta interessati, all'Aiutante di campo del Re, al capo del SIM e, a volte, ad altri Enti.

53 Il numero di dispacci intercettati ammontò in media a circa 13.000 al mese dei quali circa 90 al giorno inclusi nei bollettini. Circa il 57% di questi ultimi era di carattere diplomatico, il 13% militare e la parte rimanente commerciale (AUSSME *Diario Storico del SIM, 23 maggio 1941*, Allegato n°1).

Numeri diversi, ma riconducibili ai precedenti, soro riportati dal Generale Amé con riferimento all'intera durata del conflitto: 8.000 crittogrammi intercettati in un mese, escludendo probabilmente quelli commerciali; circa il 45% posti in chiaro e in qualche modo utilizzati, ma non necessariamente inseriti nei bollettini (AMÉ, p. 67).

54 Maggiori dettagli su questi metodi sono contenuti negli Annessi del presente articolo.

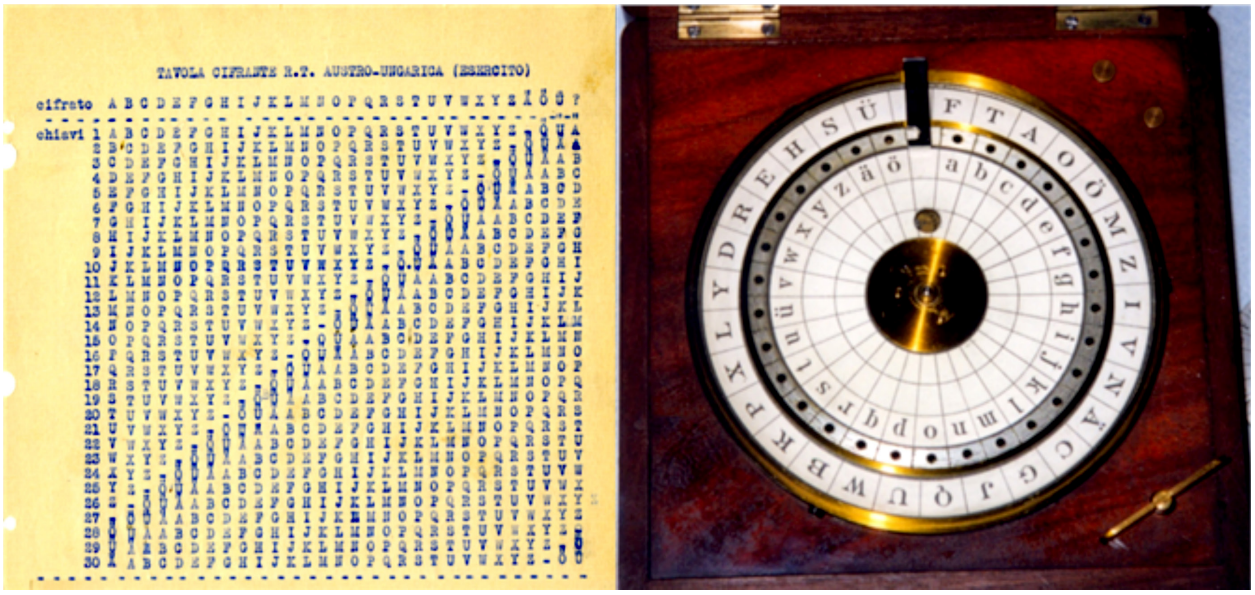

Fig. 3 1ª GM, tavola cifrante-decifrante (Flavia Reed Owen Collection & Archives, McGraw Page library, Randolph-Macon College, Ashland, Virginia) e a destra disco rotante (Colavito, Cappellano, p. 273), ambedue usate dagli Austro Ungarici e forzati dagli Italiani

dispacci in chiaro con una lettera di un alfabeto disordinato e ripetevano più volte la procedura con alfabeti diversi nei rotori successivi, in modo da ridurre la probabilità di soluzione dei crittogrammi mediante "forza bruta". I tentativi condotti dalla Sezione crittografica per decrittare le comunicazioni cifrate con tali macchine impiegate da numerosi eserciti, tra cui quelli inglese e americano, non risulta abbiano condotto a risultati positivi.[55]

Cifrari campali

Gli analisti della Sezione crittografica riuscirono invece a forzare numerosi cifrari a sostituzione polialfabetica, realizzati non solo mediante carta e penna, ma anche con piccoli dispositivi meccanici come dischi rotanti, regoli cifranti, tamburi o strisce scorrevoli, usati prevalentemente per comunicazioni di carattere tattico.

55 La macchina cifrante-decifrante inglese, denominata TYPEX, derivava dall'Enigma tedesca e funzionava con 5 rotori. La M-209 dell'Esercito americano era una versione portatile e migliorata della Hagelin C-36 impiegata anche dalla Marina italiana. La SIGABA statunitense detta anche Converter M-134 funzionava con ben 15 rotori.

Tra questi dispositivi rientra la seconda versione del SYKO, brevettata in Inghilterra dal suo ideatore Morgan O'Brien nel 1939 e usata dalla RAF nella 2ª GM soprattutto per le comunicazioni aereo-terra. Oltre alla prima versione quella successiva, meccanizzata mediante un piccolo telaio (figura 4), furono forzate dagli Italiani, come descritte nell'Annesso 1.[56] La tempestiva interpretazione, sin dai primi mesi di guerra, delle comunicazioni cifrate con il SYKO o con la versione della Marina britannica denominata MYKO, anch'essa forzata dal SIS, si rivelò decisiva nella guerra dei convogli per il rifornimento delle truppe combattenti in Libia.[57] Infatti, gli analisti italiani riuscivano a ricostruire, in tempi brevissimi, l'ordine degli alfabeti disordinati variabile giornalmente, così che i crittogrammi per il resto della giornata venivano letti agevolmente.

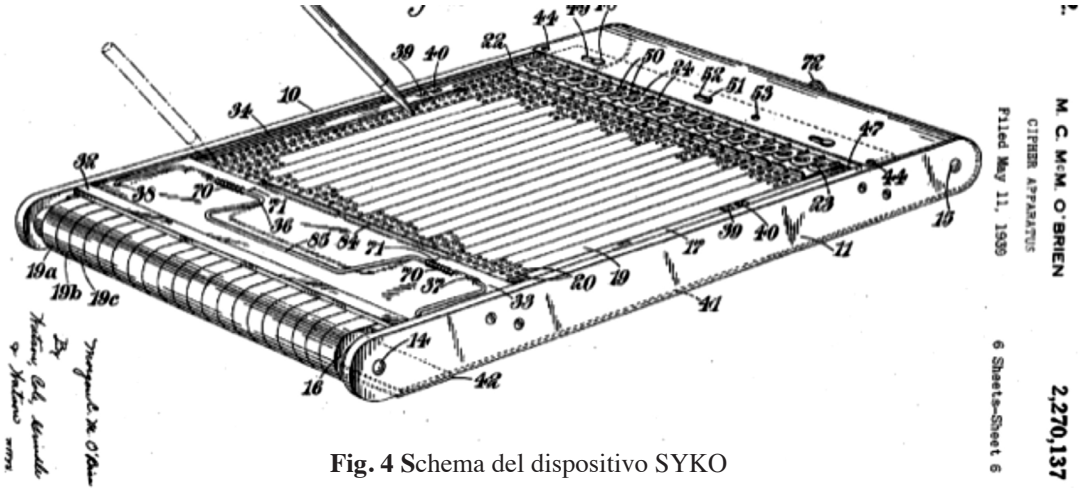

Fig. 4 Schema del dispositivo SYKO
(US Patent Office N° 2,270,137, Jan. 13, 1942)

Nell'Esercito americano fu largamente impiegato per circa 20 anni, dal 1922 fino a oltre il 1942, un cilindro del tipo Jefferson-Bazeries, perfezionato dal Colonnello Joseph O. Mauborgue e denominato M-94. Il dispositivo, anch'esso a

56 ASA, Vol. 1, United Kingdom 30. Bigi cita anche la versione del SYKO denominata ANNA che sembra sia stata impiegata solo per esercitazioni nel Regno Unito (CSDIC/CMF/Y4, Bigi, p. 6.)

57 Vincent O'HARA and Enrico CERNUSCHI «Signal Intelligence and the battle of supply Rommel attack toward Suez», Naval War College Review, Summer 2013, Vol. 68, 3, pp. 117-138.

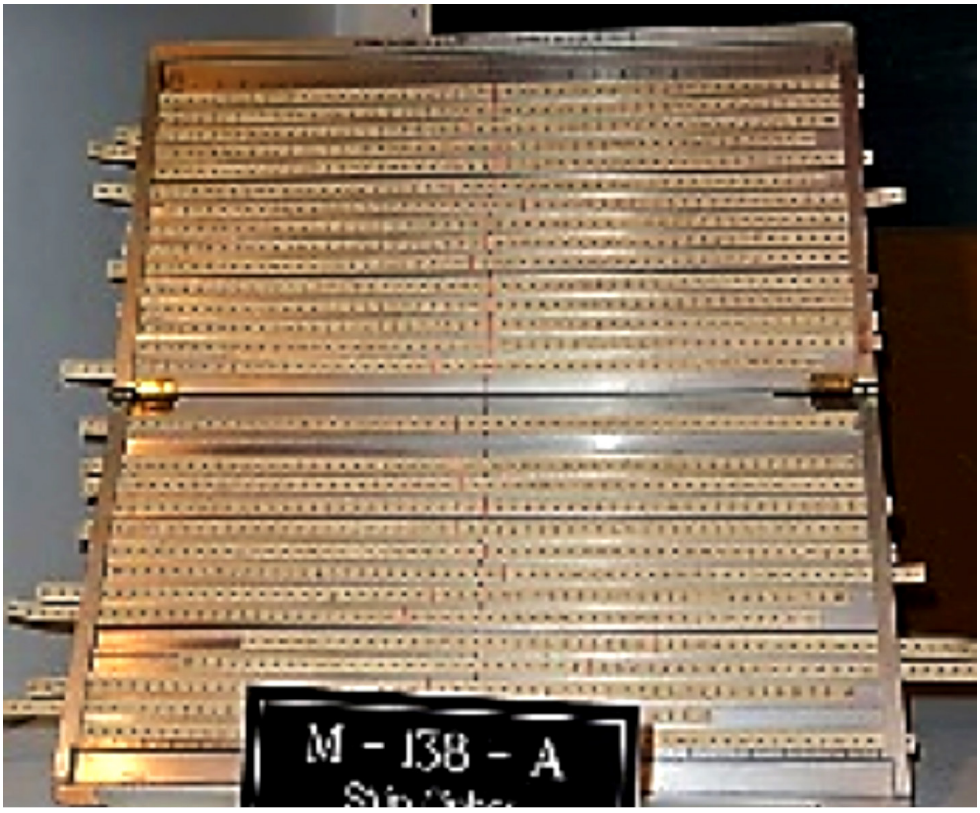

Fig. 5 Dispositivo M138-A, (National Cryptologic Museum, Fort Meade, Maryland, USA (Creative Commons CCO 1.0)

sostituzione polialfabetica, era composto da dischetti metallici con un foro al centro per il loro montaggio su un asse, come descritto nell'Annesso 1, ove si illustra anche lo 'Strip Cipher Device' M-138 che sostituì in gran parte l'M-94 a partire dal 1943. Non risulta che gli Italiani abbiano risolto questo tipo di cifrario, la forzatura della versione M-138-A fu portata a termine dal criptologo tedesco Hans Rohrbach nel 1944.[58]

Tra i numerosi cifrari a sostituzione polialfabetica risolti invece dalla Sezione crittografica italiana si citano quello dall'Aeronautica turca con 5-13 alfabeti,

58 Friedrich L. BAUER *Decrypted Secrets, methods and maxims of cryptology,* Springer-Verlang, Berlin, 1997, p, 123.

e variazione mensile della chiave costituita da nomi geografici,[59] e quelli, più semplici, impiegati per esempio dalla Polizia turca e dall'Esercito Jugoslavo.[60]

La Sezione crittografica, in continuità con quanto avvenuto nella 1ª GM, forzò anche numerosi cifrari che applicavano il metodo a trasposizione, semplice o doppia. Sistemi, non molto più complessi rispetto ai campali germanici della Grande Guerra, furono adottati per esempio dall'Esercito jugoslavo, degli Attaché militari romeni (figura 6) e, per emergenza, anche degli Attaché militari degli Stati Uniti.

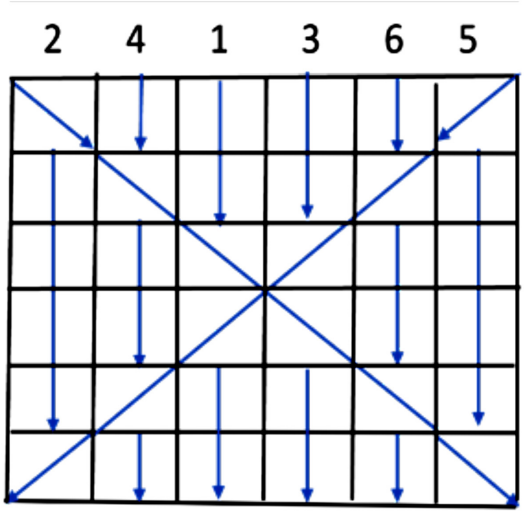

Fig. 6 Metodo a trasposizione utilizzato dagli Attaché militari romeni secondo le regole illustrate nell'Annesso 2 (CSDIC/CMF/Y4, Bigi, Appendix C)

Gli Eserciti belligeranti, per redigere i cifrari campali, ricorsero in ambedue i conflitti anche a tabelle delle più svariate forme in cui erano inseriti lettere, numeri e frasi con gruppi cifranti che si leggevano nella prima riga e nella prima colonna a sinistra della tabella. Questi sistemi resistevano alla forzatura in ragione del disordine dei termini inseriti nelle diverse posizioni, delle dimensioni e della frequenza di sostituzione delle chiavi. Va ricordato che i cifrari tabellari equivalgono a codici di piccole dimensioni rispetto ai quali presentano il vantaggio di un più facile impiego.[61]

59 ASA, Vol. 1, Turkey, 13.

60 In un cifrario della polizia turca le lettere del dispaccio in chiaro erano sostituite con due o tre cifre variabili mensilmente e raggruppate nei crittogrammi in gruppi da 4 a 6 cifre (ASA, Vol. 1, Turkey, 26, Policy). Un altro cifrario impiegava una sostituzione monoalfabetica variabile giornalmente (Turkey, 27). Nel caso della Jugoslavia, il SIM risolse tutti i numerosi sistemi utilizzati: dalla semplice inversione del testo chiaro (Yugoslavia, 22, Air) alla sostituzione polialfabetica con 5 alfabeti (Yugoslavia Michailovitch, 28, Military), a un doppio Playfair, non è noto di quale tipologia (Yugoslavia, 21, Army).

61 Durante la 1ª GM, gli Austro - Ungarici utilizzarono tabelle di cifratura meno frequentemente degli Italiani i quali, per i propri cifrari di servizio, adottarono spesso la forma tabellare, prima ordinata e poi sempre più disordinata.

	AZ	IV	OL	
M	A			
D	abandonner			
C	aborder			
J	absolut			
Z				

Fig. 7 Cifrario di un'Armata francese ricostruito dalla Sezione Crittografica (CSDI/CMF/Y4, Bigi, Appendix D)

Tra i numerosi cifrari di questo tipo, risolti dagli analisti italiani nella 2ª GM, si ricordano sia quello utilizzato dall'Armata francese combattente in Medio Oriente negli anni 1942-43 schematizzato nella figura 7 e descritto nell'Annesso 3, sia un cifrario dell'Armata Rossa, con gruppi di tre cifre una delle quali identificava dieci colonne e le altre cento righe, forzato dagli Italiani anche perché i Russi preferivano cifrare lettera per lettera invece di usare le parole intere contenute in diverse posizioni della tabella.[62]

Il codice campale, in forma tabellare, impiegato dall'Esercito inglese in Libia e nel Medio Oriente, conteneva 676 (26x26) posizioni con lettere, parole e numeri convertiti in gruppi cifranti di due lettere, e chiave variabile con cadenza giornaliera. Nella deposizione di Augusto Bigi, la tabella anzidetta ricostruita dagli analisti italiani è indicata con il nome CYPHER.[63]

62 CSDIC/CMF/Y *First detailed Interrogation of Carrelli, Adriane*, p. 1. Questo Tenente nato a Leningrado nel 1908 da famiglia italiana faceva parte del gruppo slavo che decrittava il traffico russo, croato, bulgaro e cetnico, di natura diplomatica e militare, al comando del T. Colonnello Serragli. Egli descrive anche un'altra tabella dell'Esercito russo con 10x10 posizioni e gruppi cifranti costituiti da due numeri. Il cambio giornaliero della posizione di questi 10 numeri secondo chiavi prestabilite procurò, secondo Carrelli, difficoltà di decrittazione per la Sezione crittografica.

63 CSDI/CMF/Y4, Bigi, p. 6; ASA, Vol. 1, United Kingdom, 62, Military. Questo cifrario somigliava a un altro impiegato nelle operazioni combinate dei bombardieri della RAF e della Air Force americana.

La beffa di Scutari

Nell'Annesso 3 si descrivono anche alcuni cifrari tabellari dell'Esercito jugoslavo completamente ricostruiti dalla Sezione crittografica che aveva acquisito, ancor prima dell'inizio della guerra, una profonda conoscenza di tutti i cifrari campali jugoslavi, come si deduce dalle frequenti citazioni dei sistemi adottati da quell'Esercito contenute nel precedente paragrafo e dalla sintesi operata dal TICOM, ove la forzatura della maggior parte dei cifrari jugoslavi non è attribuita ai Tedeschi, ma agli Italiani. Questi ultimi avevano penetrato profondamente anche le metodologie crittografiche e le consuetudini procedurali, oltre all'organizzazione gerarchica dell'Esercito jugoslavo, nonostante quel Paese fosse considerato, fino al colpo di stato del 1941, un fedele alleato dell'Italia e della Germania.

Tali conoscenze consentirono al SIM di effettuare la magistrale e famosa operazione di *deception* posta in atto allo scoppio delle ostilità tra Italia e Jugoslavia. In quelle circostanze, le Forze armate italiane che, a seguito del conflitto in corso contro la Grecia, erano concentrate nel sud dell'Albania, mostravano, per dirla con David Kahn e parafrasando Wiston Churchill, il proprio *naked rear* all'Esercito jugoslavo.[64] Infatti, il 13 aprile del 1941 si erano intensificati gli attacchi di due Divisioni nemiche contro le poche unità italiane poste a difesa del confine settentrionale dell'Albania, e in particolare delle città di Scutari e Kukes.

Il SIM inviò allora ai Comandi delle suddette Divisioni, due marconigrammi a firma del Generale Dusan Simovic,[65] redatti esattamente secondo le usuali procedure dell'Esercito jugoslavo, con l'ordine di sospendere l'offensiva e ritirarsi sulle precedenti posizioni. L'inganno funzionò alla perfezione poiché alla richiesta di conferma dell'ordine non giunse alcuna immediata risposta e soltanto dopo 48 ore, cioè il giorno 15, il Comando d'Armata di Sarajevo comunicò di non aver mai emesso alcun ordine di ritirata. Era ormai troppo tardi perché gli Italiani si erano ormai sganciati, attestandosi su posizioni meglio difendibili.[66]

Il Generale Amé evidenzia le conseguenze di carattere generale di questa operazione sul successivo svolgimento della campagna contro la Jugoslavia,

64 David KAHN *The Codebreakers. The story of Secrete Writing» Scribner*, New York, 1996, pp. 469-471.

65 Il Generale Simovic era il protagonista del colpo di stato che aveva spostato la posizione della Jugoslavia da favorevole a contraria all'Asse Berlino-Roma. Egli, oltre a comandare le Forze Armate, si era proclamato Presidente del Paese.

66 AMÉ, cit., pp. 86-90.

perché i Comandi di quell'Esercito ormai consapevoli della compromissione dei propri cifrari, non potendoli cambiare rapidamente, furono costretti a richiedere controlli accurati per verificare l'autenticità di ogni marconigramma, con «effetti ritardatori nel funzionamento dei Comandi proprio nel momento in cui il precipitare degli eventi richiedeva rapidità di decisione e di azione».[67]

Crittografia e Poesia

Non sono note ai più le circostanze che portarono all'impiego di un cifrario a trasposizione, più adatto ad applicazioni campali, per le comunicazioni tra gli Alti Comandi italiani in una fase molto critica della 2ª GM, in relazione alle trattative per l'Armistizio.

Un sistema di tal fatta era correntemente adottato dal SOE (Special Operations Executive), la struttura di Intelligence voluta nel 1940 da Winston Churchill al fine di proteggere i collegamenti con gli agenti inviati nei paesi occupati dai Nazisti, per effettuare azioni di sabotaggio e collaborare con le forze di resistenza clandestine. Questi agenti, dotati di stazioni radio portatili, usavano come chiave del cifrario alcune parole tratte da un poema conosciuto a memoria e indicate all'inizio del crittogramma mediante cinque lettere. Si evitava così di conservare scritti, difficilmente cancellabili in caso di cattura, ma che d'altra parte avrebbero consentito un più frequente cambio delle chiavi.[68]

Le modalità di impiego di questo cifrario sono confermate da uno studio approfondito su una serie di crittogrammi trasmessi a Londra, durante gli ultimi anni di guerra, dall'agente del SOE Antonio Marzi che operava nell'Italia occupata dai Tedeschi. Il poema usato dal Marzi era il 'Corradino di Svezia' di Aleardo Aleardi.[69]

---

67 Ibidem, p. 90.

68 I brani erano tratti da autori noti come Shakespeare, Keats, Molière, Poe o dalla Bibbia. Le parole del poema erano ordinate secondo le lettere dell'alfabeto e scelte in base alle lettere contenute nell'indicatore. Ciascuna lettera delle parole prescelte del poema veniva poi convertita in numero. La sequenza così ottenuta serviva per identificare l'ordine di lettura delle colonne nella tabella rettangolare in cui il messaggio in chiaro era stato scritto riga per riga. Le due trasposizioni erano effettuate con la stessa chiave (Leo MARKS *Between Silk and Cyanide. A Codemakers War*, 1941-1945, Simon & Shouster, New York, 1998, pp. 11, 31-33).

69 Paolo BONAVOGLIA *La crittografia da Atbash a RSA. I crittogrammi di Antoni Marzi,* http://www.crittologia.eu/storia/critMarzi.html. In questo caso solo due o tre lettere della

Poiché i poemi prescelti erano spesso conosciuti anche da alcuni raffinati analisti tedeschi, questo metodo venne modificato coniando apposite filastrocche nelle diverse lingue, inventate da apposite 'ragazze' del SOE e a volte dagli stessi agenti.[70] Alla debolezza crittografica del sistema, quando non supportato da un frequente e sicuro cambio delle chiavi, sembra sia da ascriversi la causa dei numerosi insuccessi e delle catture di massa subite soprattutto dalla resistenza francese.

Il SOE riteneva tuttavia che questo metodo garantisse una accettabile grado di sicurezza, quando le chiavi potevano cambiarsi frequentemente e gli agenti operare in tranquillità, senza commettere gli errori che spesso rendevano indecifrabili i crittogrammi e/o facilitavano la loro decrittazione. Furono considerazioni di questo tipo che indussero i Servizi britannici a utilizzare il metodo sopra sommariamente descritto anche per le comunicazioni italiane nelle trattative che portarono, il 3 settembre del 1943, alla firma dell''Armistizio corto' tra l'Italia e gli Alleati anglo-americani.[71]

Il Servizio britannico fornì infatti il mezzo radio di contatto tra i Generali Pietro Badoglio e Giuseppe Castellano quando quest'ultimo si recò a Lisbona allo scopo di condurre le negoziazioni con gli Angli-Americani. Per costituire il terminale radio in Italia si utilizzarono i servizi di crittografo e radiotelegrafista dell'agente inglese Dick Mallaby, liberato dal carcere di Verona ove era stato rinchiuso dopo la cattura avvenuta, unitamente al suo equipaggiamento radio, nei pressi del Lago di Como. La nuova chiave fu inventata per l'occasione, fornendo al Mallaby, mediante un dispaccio trasmesso con il vecchio codice mnemonico in suo possesso, le istruzioni per confezionarla inserendovi nomi di persone e di luoghi note soltanto a lui e naturalmente al SOE.

Il Generale Amé rimase all'oscuro sull'esistenza del canale inglese e per questo si domandò il motivo dell'assenza di ogni comunicazione da parte del Generale Castellano durante la sua missione.[72]

---

chiave venivano utilizzate per identificare altrettante parole del poema mentre le rimanenti costituivano un riempitivo. La chiave diversamente sopra cifrata non si inseriva all'inizio ma in quarta posizione e alla fine del crittogramma.

70 MARKS, p. 38.

71 Questo canale di comunicazione fu scelto nel tentativo di aumentare la riservatezza, escludendo il collegamento radio tra Roma e Lisbona predisposto dal SIM insieme «a un ermetico cifrario destinati a entrare in funzione in caso di estrema emergenza» (AMÉ, p. 286).

72 Ibidem.

Anche alcune successive comunicazioni dirette tra i Generali Badoglio ed Eisenhower utilizzarono il servizio di Mallaby,[73] ma lo stesso Leo Marks - autore del libro da cui sono tratte le notizie precedenti - ipotizza che la conoscenza acquisita dai Tedeschi sulle trattative armistiziali potrebbe esser stata ottenuta mediante la decrittazione dei radiogrammi del SOE, favorita dal non previsto intenso impiego della stessa chiave, errore questo che gli Inglesi identificavano con il termine *depht*.[74]

5. Una molteplicità di codici

Successi e difficoltà degli analisti italiani

I sistemi di cifratura sopra enumerati, per la maggior parte di tipo campale, rispondevano generalmente a limitate esigenze di segretezza, in quanto avevano la funzione di resistere alla decrittazione solo il tempo necessario per svolgere l'azione a cui il crittogramma faceva riferimento. Tuttavia, per decrittare tempestivamente i messaggi, non bastava conoscere la struttura del cifrario, come le tabelle o gli alfabeti nelle sostituzioni polialfabetiche, ma occorreva anche ricostruire celermente le chiavi, dopo i cambiamenti operati dagli avversari. In molti casi la Sezione crittografica riuscì a soddisfare ambedue queste condizioni, nonostante non disponesse fino a pochi mesi prima dell'8 settembre 1943, delle macchine di calcolo, utilissime anche a questo scopo.

Per i dispacci di carattere militare o diplomatico di maggiore segretezza, destinati a rimanere segreti per tempi più lunghi, si utilizzarono, in ambedue i conflitti, codici costituiti da un solo libro cifrante e decifrante per i codici 'ordinati' oppure, per quelli 'disordinati' da due libri (o due parti di un libro), uno cifrante e l'altro decifrante.[75] La tipologia e le dimensioni dei codici variavano a secon-

73 L'agente Dick Mallaby divenne poi famoso non solo per aver accompagnato il Re e Badoglio fino a Brindisi, a bordo della Corvetta Baionetta, proprio per garantire le comunicazioni con i vertici militari Anglo-Americani, ma anche per aver convinto, in occasione di una sua seconda cattura nell'Italia occupata dai Tedeschi, il Generale delle SS Karl Wolff a intraprendere le trattative che portarono alla resa delle truppe tedesche in Italia.

74 MARKS, pp. 358-362; 379; 383-384. Evidentemente, non era stato possibile far pervenire al Mallaby una nuova chiave dopo la costruzione della prima.

75 Nel caso di codici disordinati o 'intervertiti' i gruppi di codice corrispondenti a ogni termine in chiaro non seguono un ordine numerico o alfabetico quindi per decifrare occorre un secondo libro in cui questi gruppi sono riportati in modo ordinato.

da del tipo di applicazione: dai grandi volumi contenenti di solito più di 10.000 termini usati dalle Ambasciate e dagli alti Comandi a quelli di livello inferiore, per esempio divisionali, con un numero di termini generalmente minore di un migliaio. Per mantenere la segretezza dei dispacci, anche nel caso di cattura dei codici o di loro 'compromissioni', veniva spesso applicata una seconda cifratura mediante uno dei metodi di sostituzione o di trasposizione sopra illustrati ovvero, nel caso di codici numerici, sommando o sottraendo cifre predefinite, inizialmente costanti e successivamente realizzate mediate serie casuali di numeri variabili da un messaggio all'altro.

Nell'ultimo anno della 1ª GM, l'Esercito austriaco impiegò, come gli altri belligeranti, codici campali di medie dimensioni, con circa mille termini, applicando la sopra-cifratura a quelli ordinati ma evitandola di norma nei codici disordinati, anche se talvolta per questi ultimi erano disponibili tabelle di sopra-cifratura preparate da esperti crittografi. Ambedue queste tipologie di cifrari vennero forzate da Sacco e dai suoi collaboratori durante la Battaglia del Solstizio e prima dell'offensiva finale che portò alla Battaglia di Vittorio Veneto.[76] Inoltre, come precedentemente accennato, il reparto crittografico si era impegnato anche nella decrittazione di dispacci diplomatici, sin dalla fine del 1916 e disponeva, alla fine del conflitto, di più di una decina di codici regolari o irregolari, ricostruiti o in qualche modo conosciuti.[77]

Durante il secondo conflitto mondale, specie in diplomazia, vennero generalmente privilegiati codici disordinati e sopra-cifrati mediante metodi sempre più complessi, con chiavi cambiate molto frequentemente, anche se si verificarono numerose eccezioni. Quindi, nonostante la disponibilità di interi cifrari ottenuta talvolta mediante azioni di HUMINT, restavano comunque da risolvere le tabelle

76 COLAVITO, CAPPELLANO, pp. 361-369; 384-387.

77 I cifrari diplomatici noti al Reparto crittografico nella 1ª GM erano: l'austriaco, il tedesco, lo svizzero, lo spagnolo, il bulgaro e il greco, quello della Russia bolscevica e persino degli Stati Uniti d'America Più di 3.500 dispacci cifrati con questi codici, tradotti in chiaro, vennero inviati, in appositi Bollettini, al Ministero degli Esteri, alla Presidenza del Consiglio, ad altri Ministeri e alle Missioni Militari Alleate in Italia. I telegrammi diplomatici trasmessi o ricevuti dalle Ambasciate dei Paesi neutrali presenti in Italia o scambiati tra il Vaticano e i Nunzi Apostolici, specie se residenti nei Paesi nemici fornirono preziose informazioni all'Intelligence italiana. La maggior parte di questi messaggi non era intercettata via radio come nella 2ª GM, ma prelevata in copia dall'Ufficio telegrafico centrale di Piazza San Silvestro a Roma.

di seconda cifratura. Gamba e i suoi collaboratori, oltre alla ricostruzione di alcuni codici, forzarono un elevato numero di tali tabelle che, nei primi tredici mesi della 2ª GM, ammontava complessivamente a ben 223, mentre altre 225 restavano allo studio. Inoltre, nello stesso periodo risultavano ricostruiti o allo studio 35 cifrari.[78]

Dalle deposizioni degli analisti italiani si deduce che nel 1944 essi conservavano il ricordo di almeno ottanta codici diplomatici o militari, del periodo bellico o immediatamente anteriore per i quali, anche nel caso di sopra cifratura, era stata possibile una buona interpretazione dei crittogrammi intercettati. Questi codici, in parte ricostruiti dalla Sezione e in parte disponibili in copia fotostatica, appartenevano agli Stati Uniti, all'Inghilterra, alla Francia e sue colonie, al Vaticano, oltre che a Brasile, Cile, Egitto, Equador, Grecia, Jugoslavia, Messico, Portogallo, Romania, Svezia, Svizzera, Turchia e Uruguay. Particolarmente numerosi erano i codici delle diplomazie romena,[79] greca e jugoslava,[80] ma il primato quantitativo spettava a quelli delle Ambasciate e degli Attaché militari turchi dei quali ben 11 venivano letti regolarmente.[81]

I metodi di seconda cifratura basati su trasposizione o sostituzione dei gruppi cifranti vennero in genere risolti dalla Sezione crittografica, mentre i tentativi della Sezione per penetrare sistemi di sopra cifratura basati sulla sottrazione di serie disordinata di numeri, adottati soprattutto gli Inglesi, non condussero a risultati positivi. Una situazione analoga si verificò per le seconde cifrature russe che prediligevano la tecnica OTP.[82] Gli Americani, per comunicazioni diplomatiche

78 AUSSME *Diario Storico del SIM*, *23 maggio 1941*, Allegato n°1.

79 CSDIC/CMF/Y 12, *First detailed Interrogation of Vassallo Todaro, Giuseppe*, 29 Oct.1944, pp.1-2. I numerosi codici impiegati dalla diplomazia romena furono letti dalla Sezione crittografica anche se sopra cifrati con semplici inversioni dei gruppi cifranti ovvero con sostituzioni fisse di ciascuna cifra.

80 ASA, Vol. 1. Almeno 4 codici diplomatici greci erano letti dagli Italiani, tra i quali uno in due parti e sopra cifrato in uso dal 1942 (Greece 7, Diplomatic). Gli altri erano stati utilizzati in tempi precedenti (Greece 1, 8, Diplomatic), o in un periodo non noto, ma sembrano più semplici del primo. Ben sei erano i codici diplomatici jugoslavi, croati, serbi o degli Attaché militari jugoslavi (Yugoslavia, 1, 3, 4, 5, 12, 13, 14, Diplomatic or Miltary attaché).

81 ASA, Vol. 1, Turkey 1-11, Diplomatic or Miltary attaché.

82 Le serie di numeri casuali da addizionare o sottrarre erano spesso numerose, in modo che ciascuna potesse venir impiegata raramente, oppure contenute in appositi blocchetti con pagine 'usa e getta' (OTP = one time pad). Quest'ultima tecnica, usata per la seconda cifratura dei codici diplomatici russi, impiegava quindi una serie di nume-

a elevata segretezza, utilizzavano di solito macchine cifranti-decifranti, anche queste precluse a ogni tentativo di soluzione della Sezione crittografica.

L'offensiva contro i cifrari inglesi nella 2ª GM

Secondo la sintesi operata da TICOM, i successi conseguiti dagli Italiani nei confronti dei cifrari inglesi di ogni tipo costituivano circa il 39% - ripartiti tra SIM (16%) e SIS (23%) - dei circa 70 cifrari britannici penetrati interamente o parzialmente dagli analisti dell'Asse. Si trattava in gran parte di cifrari militari, impiegati da esercito, marina e aeronautica, e in qualche caso di codici diplomatici.[83]

Nelle tabelle della TICOM sono contenuti tre codici appartenenti a quest'ultima tipologia, letti o ricostruiti dai Servizi italiani, sui quali non vengono fornite ulteriori informazioni riguardanti, per esempio, la loro struttura.[84] Inoltre, un codice regolare a 5 cifre simile al Gray americano, di cui si dirà tra breve, e un altro a 4 lettere e due parti, letti dalla Sezione crittografica e inclusi nella lista senza alcuna attribuzione del loro impiego specifico, facevano anch'essi parte con ogni probabilità di quelli usati dalla diplomazia britannica.[85] Si trattava comunque di cifrari generalmente non utilizzati per comunicazioni di massima segretezza.

Grazie alla soluzione di questi codici con relative sopra cifrature e alla interpretazione di dispacci di maggiore segretezza, per periodi limitati di tempo, la Sezione crittografica, poté vantare alcuni successi, già da diversianni prima dell'inizio della 2ª GM, come emerge da alcuni passi dei Diari di Galeazzo Ciano. L'affare riguardante il Ministro degli Estri austriaco Guido Schmidt, nel novembre del 1937, traeva infatti origine da dispacci radio inglesi intercettati e interpretati dal SIM: si trattava di due documenti segreti britannici, consegnati al Cancelliere austriaco Kurt Alois von Schuschnigg, che svelavano contatti tra il Ministro austriaco e il Foreign Office.[86]

---

ri diversa in ogni dispaccio, posseduta da entrambi i corrispondenti opportunamente sincronizzati.

83 ASA, Vol. 1, United Kingdom.

84 ASA, Vol. 1, UK 57, 58, 59, Diplomatic.

85 Ibidem, UK 76, 77, unknown.

86 Galeazzo CIANO *Diario 1937-1943*, a cura di Renzo De Felice, Rizzoli, Milano, 1980, p. 56, 69, 73.

Le rivelazioni di Ciano in questa, come in altre circostanze, ci permettono di confermare la 'lettura' da parte della Sezione crittografica non solo di numerosi dispacci diplomatici inglesi, ma anche di quelli turchi, belgi e rumeni, per la gran parte della sua permanenza a capo del Ministero degli Esteri. Tuttavia, non scusano l'imprudenza crittografica da lui manifestata in numerose occasioni.[87]

Nei Diari di Ciano, i riferimenti alla decrittazione di dispacci inglesi si fermano nei primi mesi del 1940, presumibilmente in coincidenza con l'adozione di metodi di sopra cifratura più complessi che in precedenza, per riprendere alla fine del 1942. I radiogrammi inglesi decrittati nel dicembre del 1942 riguardano il progettato bombardamento di Roma da parte degli Alleati. Più precisamente, il 24 del mese, una comunicazione del Ministro degli Affari Esteri Antony Eden agli Alleati americani svelava che, per evitare il bombardamento, gli Inglesi pretendevano l'allontanamento da Roma di Mussolini, del Governo, dei Comandi militari e persino del Re, il tutto sotto il controllo di funzionari svizzeri. Gli Americani risposero però che non intendevano «procedere a un'azione di forza contro la città di Pietro poiché ne risulterebbe per gli alleati più danno che vantaggi». [88]

Un altro radiogramma intercettato e decrittato nel gennaio successivo conteneva la sintesi del colloquio tra il generale tedesco Wilhelm von Thoma catturato in Africa e il generale inglese Bernard L. Montgomery. Con riferimento alle dichiarazioni del Generale tedesco, Ciano confessa: «Se sono vere, sono preoccupanti. Von Thoma ha detto che i Tedeschi sono convinti di aver perso la guerra e che l'Esercito è antinazista perché attribuisce a Hitler tutte le responsabilità».[89]

La ripresa delle intercettazioni e decrittazioni alla fine del 1942 potrebbe spiegarsi con la citata riproduzione del codice diplomatico e delle relative tabelle di sopra-cifratura condotta dal gruppo P ai danni dell'Ambasciatore britannico presso la Santa Sede D'Arcy Osborne. Questa ipotesi naturalmente è tutta da verificare.

87 I Diari di Ciano includono la 'confessione' di molte incaute indiscrezioni che avrebbero potuto compromettere il lavoro dei criptologi italiani. Tra le altre, si ricordano quella compiuta nei confronti dell'Ambasciatore belga al quale Ciano fece capire di aver letto la sua corrispondenza in cui si affermava che gli Italiani non amavano la guerra (CIANO, p. 211, 12 novembre 1938). A un'analoga imprudenza Ciano si lasciò andare con l'Ambasciatore turco (CIANO, p. 245, 31 gennaio 1939).

88 CIANO, pp. 678-681, 689. L'inizio dei bombardamenti su Roma, per il momento scongiurato, fu rinviato, come è noto, al 19 luglio dell'anno successivo.

89 CIANO, p. 689.

D'altra parte, risulta che gli Italiani non vennero a capo delle tabelle di seconda cifratura applicate all' ID (Interdepartmental Cipher), il più comunemente utilizzato dal Foreign Office, dagli Uffici consolari, dagli Attaché militari, ecc., rimasto invariato dall'inizio del conflitto fino al giugno del 1943, offrendo numerose opportunità di cattura agli agenti dell'Asse.[90] La sicurezza dei dispacci cifrati con l'ID poteva però, come si è detto, contare sulla seconda cifratura effettuata mediante tabelle molto vaste, contenenti numeri casuali da sottrarre ai gruppi di prima cifratura. Per penetrare questa tipo di tabelle era stato individuato il 'metodo delle differenze' descritto nell'Annesso 4 che richiedeva però lunghe e complesse operazioni implementabili con la necessaria rapidità mediante particolari 'macchine tabulatrici' ottenute dalla Sezione crittografica soltanto all'inizio dell'estate del 1943.

Al contrario, grazie appunto alla disponibilità di queste macchine riprodotte in notevoli quantità sul modello di quelle catturate in Francia, i Tedeschi, riuscirono a forzare le tabelle del codice ID almeno fino al 1943. La circostanza che però colpisce maggiormente è la penetrazione da parte del SIS della Regia Marina di analoghe sopra cifrature applicate al NAVAL CYPHER britannico. Questo successo può essere attribuito sia alla precoce disponibilità di idonee macchine di calcolo, sia al merito di criptologi di alto livello come il già citato Ammiraglio Donini, sia infine ai così detti *depth* attribuibili in particolare all'uso prolungato da parte britannica delle stesse tabelle e dello stesso ordine di utilizzo di numeri casuali.[91]

Analoghe difficoltà la Sezione crittografica incontrò per penetrare le tabelle di seconda cifratura del WOC (War Office Cypher), il principale codice impiegato dall'Esercito britannico, dagli alti comandi fino a livello divisionale, nonostante possedesse il relativo codice dal 1942.[92]

---

90 ASA, Vol.1, UK, 10, Diplomatic. I Tedeschi avevano catturato il cifrario nel 1940 o nel 1941. Il codice era disordinato con gruppi cifranti di 4 cifre e sopra cifrato sottraendo gruppi casuali di 5 cifre.

91 Luigi DONINI *I Servizi crittografici delle Marine Britannica e Italiana. Una analisi comparativa delle loro attività nel secondo conflitto mondiale,* Rivista Marittima, gennaio 1983, pp. 69-94. I tabulatori sembra fossero a disposizione della Regia Marina almeno dal gennaio del 1942.

92 ASA, Vol. 1, United Kingdom, 15; CSDIC/CMF/Y4*,* Bigi, p. 6.

Le carenze dei codici del Dipartimento di Stato americano

I tre livelli di segretezza di questi codici erano identificati, in ordine crescente, con i termini 'riservato', 'confidenziale' e 'segreto'. Alla prima categoria appartenevano il 'Gray' e il 'Brown' ambedue con gruppi cifranti di cinque lettere, contenenti un numero molto elevato di termini. Il Brown, con più di 150.000 termini era composto da tre volumi che servivano ciascuno per cifrare una parte di ogni messaggio. Il Gray, detto anche B3, includeva circa 59.000 termini. I due codici, ambedue ordinati e non sopra cifrati, non avevano segreti per gli analisti del SIM e per quelli tedeschi.[93]

Dei cifrari del Dipartimento di Stato catturati dal Gruppo P nell'Ambasciata di Roma, prima dell'entrata in guerra dell'Italia contro gli Stati Uniti, faceva parte il codice diplomatico A1 considerato dagli Americani di media segretezza, cioè 'confidenziale'. Vittorio Gamba, con una lettera del 3 ottobre 1941 inviò al suo corrispondente tedesco Colonnello Kempf della OKW/chi (Servizio Informazioni del Comando Supremo delle Forze Armate germaniche), il codice suddetto unitamente alla tabella di sopra-cifratura già scaduta e annunciò di avere allo studio la nuova tabella.[94] A questo cifrario fa probabilmente riferimento Ciano nel suo Diario del 30 settembre, quando dichiara che tutti i dispacci dell'Ambasciatore statunitense a Roma William Phillips venivano letti dal SIM. Evidentemente a quella data le tabelle di sopra-cifratura non erano ancora state cambiate![95]

I codici del Dipartimento di Stato di bassa e media segretezza furono violati da Italiani e Tedeschi, a causa sia della loro vetustà - si pensi che il B3 era stato introdotto nel 1918 e rimase in vigore fino al 1943, mentre l'A1 durò dal 1920 al

93 ASA, Vol.1, United States, 3, 9, Diplomatic.

94 La corrispondenza reperita dagli Alleati negli archivi del OKW contiene quattro lettere del 1940-41 tra Gamba e Kempf con scambi di informazioni su cifrari di varia origine (TICOM/D-71 *German and Italian Correspondence on Miscellaneous cipher,* 6th March 1946). In una di tali lettere Gamba, oltre ad annunciare l'invio dell'A1, chiede al corrispondente tedesco di inviargli i cifrari americani dello stesso gruppo (disordinati e sopra-cifrati) C1 e D1 che probabilmente sapeva in suo possesso. Non si conosce la riposta a questa richiesta. Fino alla metà del 1942, le tabelle di sopra cifratura dei codici confidenziali del Dipartimento di Stato si basavano su sostituzioni bi-letterali, mentre dopo quella data gli Americani passarono a tabelle mono-letterali. Si noti che la conoscenza da parte del SIM dell'A1 - in due libri, gruppi di 5 lettere, sopra-cifrato - non è riportata nella sintesi di TICOM che l'attribuisce solo ai Tedeschi.

95 CIANO, 30 settembre 1941, p. 540.

1944 - sia perché le tabelle di cifratura restavano in vigore per diversi mesi, anche durante il conflitto. Inoltre, la quasi totalità dei codici usava, come gruppi cifranti, insiemi di lettere e non di numeri, rendendo più complessa l'applicazione di seconde cifrature efficaci basate sull'addizione o la sottrazione di gruppi casuali di cifre.

Solo per le comunicazioni con elevato grado di segretezza, escluse quelle degli Attaché militari, il Dipartimento americano impiegò macchine cifranti fornite dalla Forze armate e, come riserva in caso di malfunzionamento delle macchine, il già citato sistema M-138 facente parte dei sistemi denominati "strip ciphers" (cifrari a listelli o a strisce) descritti nell'Annesso 2. I cifrari a listelli, secondo le notizie raccolte da TICOM, furono letti dai Tedeschi, ma non dagli Italiani.[96]

Chi era la 'Volpe'?

La cattura da parte del gruppo P dei due codici degli Attaché diplomatici americani - il Military Intelligence Code, detto anche 'Black Code', e il War Department Confidential Code, con relative tabelle di sopra cifratura - risale alla stessa occasione ovvero a un'impresa successiva al trafugamento dell'A1, ma comunque a una data anteriore all'11 dicembre 1941, data di dichiarazione di guerra dell'Italia agli Stati Uniti. Augusto Bigi, nella sua deposizione, dichiarò che la Sezione crittografica disponeva delle copie dei due cifrari degli Attaché, uno 'segreto' e uno 'confidenziale', ambedue con gruppi cifranti di 5 lettere e sopra-cifrati. Quello confidenziale protetto probabilmente, con una seconda cifratura più semplice rispetto al primo. Per quest'ultimo si utilizzavano 10 tabelle mono-letterali ciascuna con 20 alfabeti casuali che servivano, a scelta del cifrista, per ogni 4 gruppi cifranti ottenuti dalla prima cifratura. La Sezione crittografica ricostruì numerose tabelle di ambedue questi codici[97] e anche i Tedeschi sarebbero riusciti a forzare il cifrario, utilizzando le intercettazioni dei dispacci in codice e le corrispondenti versioni in chiaro fornite dagli Italiani.[98]

---

96 ASA, Vol.1, United States, 14, Diplomatic.

97 CSDIC/CMF/Y4, Bigi, p. 5. Al contrario nella sintesi di TICOM si attribuisce a SIM la 'conoscenza' del Black Code segreto e di quello di emergenza degli Attaché militare costituito, come già illustrato da un cifrario a doppia trasposizione, ma non del codice confidenziale (ASA, Vol.1, United States, 16, 19, Military Attaché). La notizia relativa alla conoscenza di quest'ultimo da parte della Sezione crittografica era dedotta da CSDIC/CMF/Y7, Gamba.

98 Secondo altre fonti, il SIM avrebbe trasmesso ai Tedeschi il codice e le prime tabelle di ci-

Dopo l'inizio delle ostilità con l'Italia, gli USA non cambiarono il Black Code e nemmeno, immediatamente, le tabelle di seconda cifratura. Mediante la ricostruzione di quelle successive, la Sezione crittografica fu in grado di leggere la corrispondenza tra gli Addetti militari presso numerose Ambasciate e il Dipartimento di Washington. In particolare, è nota la disavventura occorsa all'addetto militare al Cairo Bonner Frank Fellers che trasmise a Washington, mediante il Black Code e con continuità per circa sei mesi, dall'inizio di gennaio 1942 fino agli ultimi giorni di giugno, importanti informazioni sui piani dell'8ª Armata britannica attinenti alle operazioni in Libia, a lui comunicati dai Comandi inglesi.[99]

I dispacci di Feller fornirono al Generale Rommel, ben noto come la 'Volpe del deserto' notevoli vantaggi strategici e tattici, in particolare durante la seconda controffensiva italo-tedesca (gennaio-febbraio 1942) e l'offensiva culminata con l'avanzata fino a El Alamein (maggio-giugno 1942). Tra la notevole quantità di informazioni così raccolte, si ricordano quelle utilizzate per sventare l'attacco agli aeroporti dell'Asse dislocati non solo in Africa settentrionale, mediante il lancio di truppe paracadutate britanniche che fallì miseramente.[100]

Anche se il rovesciamento delle sorti nella Campagna di Libia avvenne con la battaglia di El Alamein per motivi connessi con il cambiamento del rapporto di forze tra gli opposti schieramenti, appare singolare che l'inizio delle sconfitte subite dalle forze dell'Asse abbia coinciso con la fine delle informazioni ottenute dalle comunicazioni dell'Addetto statunitense. L'esaurimento delle informazioni fornite da Feller sarebbe avvenuto, secondo una fonte tedesca considerata affidabile dai Servizi americani, in un modo che può definirsi incedibile e al contempo tragicomico. Il 27 giugno del 1942 una stazione di radiodiffusione germanica avrebbe trasmesso una commedia in cui un attore che ricopriva la parte dell'Attaché militare americano al Cairo parlava apertamente dell'invio di informazioni riservate a Washington.[101] In realtà, a partire dal 25 giugno «i marconigrammi

fratura ed essi avrebbero ricostruito le successive.

99 La storia dei dispacci Feller è stata ricostruita da numerosi storici. Prima tra tutti si ricorda la testimonianza del Generale Amé che, sin dalla prima edizione del suo libro del 1954, fornì informazioni dettagliate su tutta la vicenda (AMÉ, pp. 105-116, pp. 253-259), riprese da David Kahn (KAHN, pp. 472-477).

100 AMÉ, pp. 113-115.

101 Wilhelm F. FLICKE, *War Secrets in the Ether*, translated by Ray W. Pettengill, National Security Agency, Washington D. C., 1953, pp. 162-163,

intercettati, pur contenendo notevoli apprezzamenti ed osservazioni, non davano più la visione estesa della situazione avversaria, limitando il loro contenuto a particolari argomenti di carattere tattico o a notizie operative di interessa parziale».[102]

Evidentemente Feller era divenuto più prudente, o molto più probabilmente gli Inglesi, insospettiti da qualche intercettazione di crittogrammi tedeschi trasmessi con l'Enigma da Monte Cavo alla Libia, e/ovvero informati dalle interrogazioni di qualche prigioniero, avevano deciso di limitare le informazioni passate all'Addetto americano. La prova definitiva dei danni procurati dai dispacci Feller fu ottenuta dai Britannici il 10 luglio quando, durante la battaglia di El Alamein, gli Australiani catturarono la principale stazione intercettatrice del Deutsches Africa Korps.

6. La mancata automazione dei calcoli

Le macchine tabulatrici

Le macchine così denominate erano state inventate dall'americano Herman Hollerith e usate per la prima volta per il censimento effettuato negli Stati Uniti nel 1890. Esse leggevano schede perforate su cui venivano impresse, nei diversi campi, le informazioni, poi comparate o addizionate dalla macchina. Dopo i primi esemplari prodotti, i tabulatori si andarono perfezionando e consentirono sia di aumentare la velocità di lettura delle schede, sia di elaborare dati alfabetici oltre che numerici, sia di effettuare sottrazioni e via via operazioni più complesse come moltiplicazioni o divisioni. I risultati venivano stampati o presentati in forma numerica su appositi contatori.

Sin dagli ultimi anni dell'Ottocento, i tabulatori furono progressivamente utilizzati per numerose applicazioni: dalle assicurazioni alle ferrovie, dalla gestione aziendale alle Telecomunicazioni.

Nel 1911 Hollerith vendette la sua azienda - la Tabulating Machine Company - a Thomas J. Watson che apportò notevoli miglioramenti alle macchine. Successivamente, attraverso fusioni con altre Società del settore e vari cambi di denominazione, l'impresa assunse, nel 1924, la ragione sociale di International Business Machines Corporation, la ben nota IBM.

102 AMÉ, p.111.

Prima che il marchio IBM divenisse famoso, la rete di filiali creata da Watson-Hollerith continuò fino alla fine degli anni Quaranta del Novecento a mantenere la precedente denominazione, sviluppando, in Europa e in altre parti del mondo, il business basato sul leasing delle apparecchiature di calcolo. La Watson Italiana contava su una fabbrica a Milano e su un ufficio commerciale a Roma che fornivano tabulatori ad Aziende come le Ferrovie dello Stato, l'ITALCABLE e l'INA (Istituto Nazionale delle Assicurazioni).[103] Dalle vicende illustrate nel seguito si deduce però che le macchine prodotte o esistenti in Italia all'inizio della 2ª GM erano tabulatori Hollerith concepiti verso la fine degli anni Venti e non quelli IBM del decennio successivo, già definiti macchine calcolatrici.

Il primo approccio della Sezione crittografica

La Sezione crittografica dell'Esercito Italiano si rese conto solo a guerra inoltrata, forse grazie a informazioni provenienti dalla Regia Marina o dalla Germania, dell'importanza di utilizzare i tabulatori per accelerare molte funzioni di calcolo, comprese in particolare quelle necessarie per la forzatura di complesse tabelle di seconda cifratura.[104] Ciò è dimostrato dal fatto che la prima missione esplorativa in Germania, organizzata dalla Sezione per acquisire conoscenze riguardanti l'impiego di tali macchine, venne attuata nel 1942: dal 21 gennaio al 22 del mese successivo.

La missione, guidata dal Colonnello Comancini, presso il servizio crittografico dell'Esercito tedesco - l'OKW/chi di Berlino - perseguiva lo scopo generale di ottenere informazioni sull'organizzazione e sui metodi di lavoro adottati da quel Servizio, mentre il compito di prendere visione dei tabulatori e della loro utilizzazione era affidato principalmente al secondo componente del gruppo: l'Ingegnere Augusto Bigi.[105]

---

103 CSDIC/CMF/Y29 *First detailed Interrogation of Samuraghi, Giuseppe*, Appendix A. Giuseppe Samuraghi era stato il Responsabile della Watson Italiana.

104 I crittogrammi venivano riportati su schede predisposte con una lunga serie di alfabeti ciascuno su righe diverse. Si perforava quindi la prima lettera del crittogramma sulla prima riga, la seconda sulla seconda riga e così via. Sovrapponendo per esempio due o più schede così perforate, un lettore meccanico o ottico poteva identificare automaticamente l'esistenza e la posizione di caratteri coincidenti che venivano passati al tabulatore per i calcoli successivi.

105 La maggior parte delle notizie riportate in questo paragrafo sono tratte dalla citata deposizione di Augusto Bigi (CSDIC/CMF/Y4, Appendix A).

Quest'ultimo poté visionare sia il cuore del sistema di calcolo automatico costituito da macchine tabulatrici alfanumeriche che, secondo quanto dichiarato dagli analisti del OKW/chi, sarebbero state requisite in Francia, sia da vari dispositivi ausiliari, come perforatori di schede, selettori di schede, verificatori, ecc. Al funzionamento del sistema provvedevano circa trenta addetti, oltre a un'officina di riparazione usata anche per cambiare rapidamente le funzioni espletate dalle macchine tabulatrici, germe di ulteriori interessanti sviluppi. [106]

I tabulatori a disposizione dei Tedeschi eseguivano numerose importanti operazioni quali, per esempio, il calcolo delle frequenze di occorrenza di lettere, bigrammi, trigrammi o poligrammi, ovvero della probabilità di combinazioni di lettere, ed effettuavano 'statistiche a catena', facilitando le decrittazioni di dispacci protetti, per esempio, con cifrari a sostituzione polialfabetica con alfabeti disordinati. [107]

Inoltre, i tabulatori risultavano, come si è detto, preziosissimi per forzare le tabelle di sopra cifratura applicate a protezione di codici e costituite da serie disordinate di numeri sottratti senza riporto dai gruppi cifranti ricavati dai codici. Il primo passo per iniziare la penetrazione di queste tabelle era il calcolo delle differenze tra gruppi di codice più frequenti contenute in diversi dispacci, secondo la procedura delineata nell'Annesso 4.

Il lento recupero

Non è facile comprendere i motivi per cui, una volta preso atto dell'intensivo e utile impiego dei tabulatori da parte tedesca, i Responsabili della Sezione crittografica e del SIM non abbiano assunto i provvedimenti necessari per ottenere la rapida disponibilità di queste macchine e compiere tutti gli sforzi per il loro immediato utilizzo. Fu deciso invece di procedere con cautela, cercando di affittare uno dei tabulatori esistenti presso la fabbrica Watson - Hollerith di Milano, per condurre qualche esperimento in piccola scala finalizzato a prendere dimestichezza con il suo impiego.

---

106 Queste macchine comprendevano, oltre a tabulatori alfabetici e numerici, una serie di dispositivi ausiliari per la perforazione delle schede, la loro selezione, verifica, ecc.

107 I primi tabulatori alfanumerici furono prodotti nel 1933 con la sigla IBM 401 e poi l'anno successivo con la serie IBM 405. Prima della Seconda Guerra Mondiale non vennero costruite altre macchine di questo tipo (http://www.columbia.edu/cu/computing). Se ne deduce che quelle requisite dai Tedeschi in Francia erano tra le più moderne prodotte dalla Società.

Tuttavia, anche i tempi necessari per sottoscrivere un contratto con la Watson italiana si dilatarono notevolmente anche perché, nel frattempo, si appurò che i tabulatori disponibili in Italia non erano in grado di effettuare il calcolo delle differenze che, come accennato, risultava indispensabile per risolvere alcuni importanti sistemi di sopra cifratura. Poiché si riteneva di poter ottenere tale prestazione mediante alcune modifiche alle macchine esistenti in Italia, fu programmata una seconda missione in Germania del Capitano Bigi allo scopo di ottenere assistenza per porre in atto tale operazione o, in alternativa, per negoziare l'acquisizione di tabulatori tedeschi.

Nel frattempo, si provvedeva a convocare presso la Sezione crittografica l'Ufficiale di Artiglieria Giuseppe Samuraghi, già responsabile della ditta Watson Italiana, affidandogli l'incarico di preparare i locali dei suoi uffici dislocati a Roma al n° 1 di Via Veneto - tra l'altro, non molto distanti dalla sede di via Poli - per ospitarvi le macchine che sarebbero arrivate dalla fabbrica milanese e/o dalla Germania.[108]

La missione di Bigi in Germania durò questa volta pochissimo - dal 23 dicembre del 1942 alla fine di quel mese - e ottenne l'assicurazione che un tecnico tedesco, un certo Herr Schenke, sarebbe stato inviato in Italia per risolvere il problema della 'sottrazione'. Tuttavia, il vero motivo della breve durata del soggiorno di Bigi in Germania era dovuto alla riluttanza dei Tedeschi nel mostrare agli Alleati italiani l'impiego ormai molto diffuso e i progressi ottenuti nel funzionamento dei macchinari da loro riprodotti o creati *ad hoc*, con il pretesto che erano stati trasferiti in una località segreta. In questo modo, essi dimostrarono, ancora una volta, una scarsa fiducia nei confronti dell'Alleato italiano, comportandosi del resto come i Francesi che nel 1915 non avevano fornito al Capitano Sacco, in visita presso il loro Quartiere Generale, alcun aiuto per decrittare i dispacci nemici.

In realtà, sappiamo che, in particolare, la Sezione IVb dell'OKW/chi, negli 11 mesi trascorsi dalla prima missione italiana, non si era limitata alla riproduzione e al miglioramento dei tabulatori, ma aveva già realizzato alcuni dispositivi ausiliari di nuova concezione, come testimoniato da recenti studi in materia.[109]

---

108 La convocazione del Samuraghi era avvenuta tra il settembre e l'ottobre del 1942 (CSDIC/CMF/Y29, Samuraghi, p. 1).

109 Carola DAHLKE *The Auxiliary Devices of OKW/chi*, Proceedings of the 3rd International Conference on Historical Cryptology, HistoCrypt 2020, pp. 63 - 67.

Schenke, giunto a Roma, prese contatti con la Watson e decise di effettuare uno scambio tra apparati disponibili in Italia, non adatti ad effettuare le differenze, e una macchina tabulatrice D11 fornita dai Tedeschi, capace di condurre a termine tali operazioni. Su queste basi, poté concludersi il contratto di leasing tra la Watson e il SIM, riguardante 12 macchine tra cui una D11 e una coppia di riproduttori-perforatori costruiti in Germania. Comunque, soprattutto le macchine tedesche tardarono ad arrivare a Roma e di conseguenza la Sezione crittografica poté giovarsene solo per pochi mesi prima dell'Armistizio.[110]

Tenendo conto del tempo necessario per assemblare, far funzionare il sistema e dare inizio alle prime più semplici procedure, gli analisti italiani portarono a termine solo 'dieci lotti' di lavoro, comprendenti alcune statistiche di carattere generale sulle lingue inglese, francese e spagnola, conteggi di frequenze per la ricostruzione di un codice americano e un primo tentativo di applicazione del metodo delle differenze su un codice turco, non meglio specificati.

Alcuni tentativi di soluzione delle tabelle di seconda cifratura del già citato WOC (War Office Code) - il codice ad alta segretezza dell'Esercito britannico - furono condotti dalla sottosezione 'Ricerca' della Sezione crittografica mediante la macchina tabulatrice, senza successo nonostante gli Italiani possedessero, come si è detto, il codice fornito loro dai Tedeschi che lo avevano catturato in Libia.[111]

CONCLUSIONI

Durante la Grande Guerra, Luigi Sacco e il Reparto crittografico, da una situazione iniziale caratterizzata dall'assenza di ogni capacità crittologica, avevano raggiunto alla fine del conflitto un livello di competenza sufficiente a conseguire i successi 'offensivi' illustrati brevemente in quanto precede e la vittoria 'difensiva' finale ottenuta cambiando, nell'ultimo mese di guerra, i più importanti cifrari con

110 CSDIC/CMF/Y29, Samuraghi, p. 1. Le machine da Milano arrivarono nel febbraio del 1943 e quelle tedesche alcuni mesi più tardi.

111 Il WOC usava un codice disordinato a quattro cifre, quindi con al massimo 10.000 termini compresi numerosi omofoni e sopra-cifrato mediante il metodo delle sottrazioni, con tabelle diverse per ciascuna area geografica, cambiate ogni 2 settimane. Dal 1943 la sopracifratura fu effettuata con OTP (One Time Pad) cioè con chiave diversa per ogni crittogramma. I tedeschi avevano catturato questo codice sin dal 1940 in almeno due occasioni e, avevano forzato le tabelle in numerose circostanze, grazie al metodo descritto nell'Allegato 4 facilitato da numerosi *depth* commessi dai cifristi nemici (ASA, Vol.1, United Kingdom, 15, Army - Corps - Division).

sistemi così complessi da impedire al nemico ogni tentativo di 'aggressione', nel breve tempo disponibile prima della battaglia decisiva di Vittorio Veneto. La Prima Guerra Mondiale segnò la rinascita non solo dell'analisi crittologica militare italiana, ma della crittologia italiana *tout court*, per merito di Sacco e del suo Reparto.

Le capacità del Reparto/Sezione crittografica del SIM si svilupparono nell'intervallo tra le due guerre, supportate anche da una intensa attività di HUMINT che consentiva non soltanto di acquisire importanti codici e relative tabelle di sopra cifratura, ma anche di conoscere i metodi più avanzati messi a punto dai 'concorrenti' stranieri per proteggere le proprie comunicazioni. Nonostante gli strumenti utilizzati per sfidare i nuovi sistemi crittografici restassero, fino a pochi mesi prima dell'8 settembre 1943, quelli impiegati fin dalla Grande Guerra cioè le tradizionali 'carta e matita', il numero di cifrari forzati e le difficoltà superate dalla Sezione non possono non suscitare un'elevata considerazione, tenendo conto tra l'altro delle limitate risorse umane disponibili.

Come si è visto, i componenti della Sezione crittografica nella 2ª GM superavano appena la cinquantina, numero questo senza alcun dubbio esiguo rispetto alle centinaia di addetti presenti nell'analoga struttura germanica[112] e ancor più a fronte delle organizzazioni britannica e americana che contavano ciascuna diverse migliaia di risorse umane impiegate a vario titolo. Non si ritiene comunque che quest'ultima carenza sia stata l'unica causa di manchevolezze e ritardi accusati dalla Sezione Crittografica nell'attaccare i crittogrammi generati da macchine cifranti o mediante codici protetti con seconde cifrature complesse.

Non vi è dubbio che, oltre alle citate difficoltà incontrate per larga parte del conflitto nell'integrare le componenti della COMINT, la lentezza nell'ammodernare i mezzi ausiliari per l'analisi crittologica e segnatamente per adottare i così detti tabulatori, abbia giuocato un ruolo fondamentale nel ridurre il campo d'azione dei violatori di codici dell'Esercito italiano.

112 Nel 1941 durante una visita in Germania, gli Ufficiali italiani rilevarono che nell'OKW/chi lavoravano ben 150 esperti militari e civili (AUSSME, Diari storici SIM, 27 febbraio 1941, Alleg.1, *Collaborazione col servizio Germanico nel campo crittografico*). La decrittazione dei dispacci diplomatici era affidata anche alla Sezione 'Pers z' del Ministero Affari esteri germanico. Una fonte tedesca stima che l'OKW/chi comprendesse nel 1942 circa 250 addetti (DAHLKE, p. 61). L'intera sezione B nell'OKW/chi, addetta all'analisi contava, alla fine del conflitto, 500 addetti (ASA, Vol. 3, *The Signal Intelligence Agency of the Supreme Command, Armed Forces,* Chief, Army Security Agency, Washington D. C., 1 May 1946, chart 2, *Organization as of April 1945*).

Ci si può naturalmente chiedere quanto i motivi di tali ritardi siano ascrivibili alle gelosie tedesche, suscitate anche da alcuni successi conseguiti dagli Italiani nelle operazioni di COMINT o alla nota mancanza di fiducia dell'alleato germanico nei confronti dell'intero Regio Esercito, e quanto invece sia dipeso da fattori interni come la 'visione' dei Comandi del SIM e della stessa Sezione e dal tipo di risorse umane disponibili. A quest'ultimo proposito, sembra opportuno sviluppare qualche considerazione sulla composizione delle organizzazioni crittografiche operanti nella 2ª GM, soprattutto con riferimento alla suddivisione tra linguisti, matematici e ingegneri.

In linea generale, risulta molto difficile individuare la misura in cui le competenze nei due settori - matematico e linguistico - influirono nel forzare i cifrari più difficili durante il Secondo conflitto mondiale. Si può certo concordare con il Bauer sul fatto che l'analisi crittologica pura di natura soltanto matematica consente di affrontare e risolvere, a prescinde dalle conoscenze linguistiche, numerosi problemi crittologici come quelli creati dai già ricordati sistemi di sopra cifratura, mentre alcuni metodi di decrittazione come quelli basati sull'analisi delle frequenze, indispensabile per la soluzione di cifrari monoalfabetici, o sull'individuazione delle parole o delle frasi più probabili, richiedono la conoscenza non solo della lingua, ma talvolta anche della fraseologia e del modo di esprimersi usati dal nemico.[113]

Quindi, esperti in ambedue i settori furono necessari per porre in atto i vari metodi di decrittazione, ma sin dai primi anni Trenta divenne sempre più evidente la necessità di applicare strumenti puramente matematici. Infatti, nel 1932, un piccolo gruppo di matematici polacchi guidati da Miriam Rejewski, al fine di ricostruire i collegamenti interni di ciascun rotore della macchina Enigma, applicò con successo formule matematiche, con l'ausilio soltanto di carta e matita «da cui sgorgarono, quasi per magia, i numeri che fornivano le connessioni ricercate».[114]

113 BAUER, pp. 431-432. L'impiego di farsi di circostanza o ben note come 'Heil Hitler' oppure di chiavi come Patria, vittoria, ecc. può aiutare l'inizio di penetrazione di un cifrario, come avvenuto con le parole 'radio station' cifrate lettera per lettera dal telegrafista austriaco che aiutò Sacco a forzare il cifrario campale austriaco durante la Battaglia del Solstizio. Queste disattenzioni o manchevolezza erano indicate dagli Inglesi con la parola *cribs*. Si noti che Sacco non conosceva il Tedesco.

114 Hugh SEBAG-MONTEFIORE *ENIGMA The battle for the code,* Weidenfeld & Nicolson. London, 2017, pp. 41-42. Del Biuro Szyfrov di Varsavia facevano anche parte i matematici Herzyk Zygalsky e Jerzy Rozycky. Per risolvere il sistema di equazioni valido per l'Enig-

Questo successo consentì ai Polacchi di decrittare i dispacci cifrati con Enigma almeno fino al 1937.

D'altra parte, la mole di operazioni richieste per venire a capo di codifiche sempre più complesse richiedeva l'impiego di mezzi di calcolo automatico quali erano i così detti tabulatori, antesignani dei moderni computer, e/o di dispositivi *ad hoc,* progettati da ingegneri, come la macchina elettromeccanica polacca denominata 'bomba' impiegata nel 1938 per decrittare i dispacci cifrati con Enigma, dopo le complicazioni introdotte dai Tedeschi nelle procedure di codifica.[115]

Le nuove esigenze, ben note ai servizi crittografici delle maggiori potenze che si preparavano a entrare in guerra, imposero di reclutare i migliori matematici tratti specialmente dalle proprie Università, oltre a tecnici esperti in altri settori quali i sistemi automatici di commutazione telefonica. Ad esempio, nella GC&CS (Government Code & Cipher School) del Governo britannico, dislocata dal 1939 a Bletchley Park, confluirono professori provenienti da Oxford e da Cambridge, tra i quali Alan Turing, Max Newman e Gordon Welchman.[116]

I Tedeschi non furono da meno: il Professore Hans Rohrbach dell'Università tedesca di Praga operò nell'ufficio crittografico del Ministero degli Esteri: il Pers-z. Per quanto riguarda il WOK/chi, il Dottore Erich Hüttenhain entrato a farne parte nel 1937, vi trovò circa 40 analisti prevalentemente linguisti raggruppati nel Referat G, al comando di Wilhelm Fenner. Ma già all'inizio della guerra, nel 1939, in questa struttura era stato formato un gruppo di matematici separato rispetto a quello dei linguisti.[117] Hüttenhain divenne poi il capo del Gruppo IV incaricato della ricerca critto analitica che comprendeva un sottogruppo incaricato di forzare i sistemi più difficili e di sviluppare la teoria critto-analitica, sotto la guida del Professore Wolfang Franz, dispensato dalle lezioni nell'Università di Francoforte, e con l'impiego di 48 addetti tra cui alcuni matematici di chiara fama.[118] Anche i Servizi americani non tardarono a dotarsi di valenti matematici.

---

ma a tre rotori, furono necessarie anche le informazioni fornite dal traditore tedesco Hans Thilo Schmidt giunte ai Polacchi attraverso i Servizi di Informazioni francesi.

115 Ibidem, pp. 355-356. La complicazione era dovuta all'impiego di una posizione iniziale dei rotori non più comune a tutti gli operatori, ma diversa per ciascun messaggio. La bomba era costituita inizialmente da quattro macchine Enigma interconnesse. I matematici polacchi tentarono, contemporaneamente alla bomba, di impiegare tabulatori con schede perforate.

116 BAUER, p. 90.

117 ASA, Vol. 3, pp. 12-13.

118 Ibidem, chart 2*, Organization as of April 1945.*

Nello stesso Gruppo IV del WOK/chi era compreso un team di circa trenta tra Ingegneri e Tecnici incaricato dello sviluppo e della costruzione di macchine critto analitiche.[119]

Ogni commento riguardo alla disparità tra le elevate competenze matematiche dei principali Eserciti belligeranti e le risorse disponibili presso la Sezione crittografica dell'Esercito italiano sembra superfluo. Come ricordato in precedenza, il Generale Gamba apparteneva alla categoria di analisti esperti nel ramo linguistico. La gran parte dei suoi collaboratori veniva scelta sulla base della conoscenza di lingue straniere e indottrinata sui principi della crittologia mediante un corso della durata massima di sei mesi. Tra loro solo due Ingegneri e qualche Ufficiale di Artiglieria potevano vantare una formazione di base in matematica.

Se è vero che maggiori competenze nelle discipline scientifiche e d'ingegneria avrebbero aumentato considerevolmente le capacità offensive della Sezione e facilitato l'impiego dei tabulatori, si ritiene che una maggiore consapevolezza delle potenzialità delle macchine di calcolo, unita a un tempestivo dinamismo tendente a predisporne l'impiego, avrebbe, comunque, migliorato sia la quantità che la qualità dei risultati ottenuti. Non si può escludere che la formazione di base del responsabile e del personale della Sezione, possa aver contribuito, almeno inizialmente, a sottovalutare l'utilità di tali macchine.

In linea più generale, si può affermare che nella 2ª GM l'Italia, come la maggior parte dei Paesi belligeranti, rimase esclusa dall'inizio della prima 'rivoluzione digitale' manifestatasi durante il conflitto per rispondere alle esigenze dettate dalla guerra per la Communication Intelligence e che ha dato poi luogo, attraverso rivoluzioni successive, all'odierno mondo digitalizzato. Componente fondamentale di tale rivoluzione fu la concretizzazione del disegno di 'macchina universale', concepito teoricamente da Alan Turing nel 1936, nella realizzazione del computer multifunzionale COLOSSUS, interamente a valvole e, come già accennato, utilizzato nel 1944 a Bletchley Park per l'analisi crittologica delle più avanzate macchine di codifica tedesche.

Un'altra espressione significativa della prima trasformazione digitale fu il sistema SIGSALLY realizzato dai Laboratori Bell nel 1943 per aumentare la segretezza delle radiocomunicazioni telefoniche in onde corte e impiegato, tra l'altro, nei colloqui transoceanici tra Winston Churchill e Franklin D. Roosevelt,

119 Ibidem.

prima di allora comodamente intercettati e interpretati dai Tedeschi. Il dispositivo utilizzava il brevetto depositato cinque anni prima da Alec H. Reeves per la trasmissione digitale delle comunicazioni vocali ed era completamente a valvole, occupando però, con numerosi telai, un'intera grande sala.[120]

L'Italia, esclusa da questa fase iniziale, diverrà anch'essa protagonista della prima rivoluzione digitale a cominciare dal 1957, con la realizzazione dell'ELEA (Elaboratore Elettronico Aritmetico), il primo computer interamente allo stato solido a livello mondiale e, all'inizio degli anni Sessanta, con la precoce introduzione, rispetto agli altri Paesi europei, delle tecniche numeriche di trasmissione nella rete pubblica di Telecomunicazioni.

Post Scriptum

Dopo il congedo del 1943, Sacco continuò a prestare la propria opera per le Forze Armate come consulente dell'ISCAG (Istituto Superiore di Cultura dell'Arma del Genio) e per il Ministero PT, partecipando anche alle Assemblee plenarie degli Enti regolatori internazionali nel settore delle radiocomunicazioni, in rappresentanza dell'Italia. Gamba non smise di occuparsi di letterature straniere e soprattutto di greco antico, ma si dedicò anche allo studio di una macchina elettronica capace di trasformare il parlato in testo scritto.[121]

Nel secondo dopoguerra l'abilità di Gamba come criptologo venne esaltata da alcuni media italiani, ma la sua fama rimase limitata nell'ambito del nostro Paese. A proposito della notorietà internazionale di Gamba, si riportano alcune frasi estratte da una lettera di Sacco alla figlia Maria del 1° giugno 1962, a commento dell'intervista da lui concessa a David Kahn alcuni giorni prima: «È venuto qui a casa a farmi visita un giornalista americano (David Kahn) che sta scrivendo un libro di aneddoti crittografici sulle ultime guerre e, per documentarsi si è preso il gusto di intervistare tutti i crittologhi conosciuti in America e in Europa. […] Gli ho chiesto se avesse l'intenzione di intervistare anche il Generale Gamba: mi disse di non averlo mai sentito nominare!»[122] Kahn, subito dopo il colloquio con

120 Reeves aveva denominato il sistema PCM (Pulse Code Modulation).

121 Le notizie sulla vita di Gamba sono tratte in parte dal già citto Comunicato ANSA.

122 Luigi SACCO *Lettera manoscritta del 1° giugno 1962* (gentile concessione di Paolo Bonavoglia custode dell'Archivio Sacco). Il motivo della lettera furono alcuni commenti della figlia del Generale su una trasmissione TV in cui sembrava che si esaltasse la figura di

Sacco, incontrò infatti il Generale Amé e le notizie riportate nel suo libro sulla Sezione crittografica e su Gamba furono tratte da quest'ultima intervista e dal libro di Amé.[123]

Nella stessa lettera, Sacco pone però in risalto le conoscenze linguistiche di Gamba, affermando che egli «era ed è bravissimo nelle lingue occidentali e nel Russo (con relative derivazioni slave) ma specie nel greco antico (recita a memoria in greco antico tutta l'Iliade e l'Odissea)».[124]

Luigi Sacco e Vittorio Gamba, negli ulti anni della loro vita, vissero a Roma a non grande distanza, il primo a Lungotevere Flaminio e il secondo a Viale Glorioso in Trastevere. In quel periodo, ambedue i Generali si occuparono, come dilettanti, di Astronomia.[125] Il Generale Gamba si spense nel gennaio del 1965 a seguito di un incidente stradale provocato da un'auto che l'aveva investito, mentre Luigi Sacco morì nel dicembre del 1970.

ALLEGATO 1: Dispositivi a sostituzione polialfabetica

I metodi di sostituzione polialfabetica si basano sulla sostituzione di ogni lettera o cifra del dispaccio in chiaro con un elemento di un altro alfabeto scelto, mediante una chiave, tra un insieme di alfabeti disponibili. Il disco cifrante di Leon Battista Alberti è considerato il sistema più antico idoneo a realizzare una sostituzione polialfabetica, mentre quello più universalmente noto è la tabella di Vigenère. Ambedue questi sistemi furono largamente impiegati dall'Esercito austriaco durante la 1ª GM, come è dimostrato dal disco cifrante e dalla tabella riportati nella figura 3 del testo.

Un sistema a sostituzione polialfabetica forzato dagli Italiani nella 2ª GM è il SYKO di cui Augusto Bigi descrive, nella sua deposizione, la prima versione che utilizzava 32 alfabeti disordinati riportati su una *card*. Un indicatore all'inizio di

Gamba, ma che in realtà riguardava il citato libro del Generale Amé. La lettera contiene alcune altre informazioni interessanti come quelle riguardanti gli stretti legami tra Kahn e il Servizio cifra americano «con il quale ha collaborato nello studio dei cifrari delle spie russe».

123 KAHN, p. 1069, nota 469

124 SACCO, *Lettera manoscritta,* cit.

125 Numerose sono le pubblicazioni di Sacco, anche dopo il 1943, di cui l'ultima del 1962 è un piccolo manuale dal titolo *Caccia ai pianeti con un piccolo cannocchiale* (http://luigi.sacco.crittologia.eu/mappa.html).

ciascun messaggio conteneva cinque lettere da convertire in cifre, la prima delle quali individuava l'alfabeto da cui iniziare la cifratura fino alla 33ª lettera o numero del dispaccio in chiaro. La seconda cifra individuava l'alfabeto impiegato dalla 34ª fino alla 64ª e poi di seguito come riportato nella tabella seguente in cui la chiave numerica è 13795.[126]

Con chiave	Lettere del testo chiaro	Numero dell'alfabeto
1	1ª	1°
3	33ª	3°
7	63ª	7°
9	89ª	9°
5	113ª	5°

Successivamente, le operazioni di cifratura e decifratura furono rese più agevoli mediante un dispositivo meccanico riprodotto nella figura 4 del testo e contenente 32 alfabeti ordinati scritti su strisce di carta verticali che si facevano ruotare fino a comporre all'estremo basso del telaio le prime 32 lettere del messaggio in chiaro. Con questo movimento, le strisce lasciavano liberi e visibili altrettanti alfabeti disordinati scritti in una *card* sottostante variabile giornalmente su cui si leggeva il cifrato immediatamente sopra le A di ciascun alfabeto ordinato.[127]

Tra i sistemi di questa tipologia utilizzati nella 2ª GM sono ricordati nel testo quelli dell'Esercito americano identificati rispettivamente con la sigla M-94 (denominato CSP-488 quando impiegato dalla Marina degli Stati Uniti) e con la sigla M-138.

Il primo, derivato dal noto cilindro di Jefferson-Bazeries, era formato da 25 dischetti sui cui bordi erano incisi alfabeti disordinati di 26 lettere, tutti diversi tra loro. La sequenza di inserimento dei dischetti forati al centro lungo un asse costituiva la chiave da modificare il più spesso possibile. Per cifrare, le prime 25 lettere del messaggio in chiaro si componevano su una riga del tamburo facendo ruotare i dischetti, e si leggeva il cifrato su una delle altre righe precedentemente convenuta. Si procedeva poi analogamente per le lettere successive del messaggio in chiaro. Il decifratore doveva soltanto riscrivere il cifrato sul tamburo in suo possesso, uguale a quello usato in trasmissione, e ricercare tra le altre righe quella

126 L'alfabeto numero 5 veniva utilizzato fino alla 141ª lettera del messaggio in chiaro, dopo di che si tornava all'alfabeto iniziale numero 1.

127 SACCO, pp. 40-41.

contenete una sequenza con un senso compiuto.

Il dispositivo M-138-A (figura 5 del testo), si basava sullo stesso principio, sostituendo le rondelle con 30 strisce di carta contenenti alfabeti disordinati e scorrevoli orizzontalmente (la precedente versione M-138 ne conteneva 25). La posizione delle strisce nel contenitore in alluminio costituiva la chiave. In questo caso il messaggio in chiaro veniva composto in verticale facendo scorrere le strisce e quello cifrato si ricavava per esempio sulla posizione adiacente o distante di un numero prestabilito di passi.

In generale, i metodi di decrittazione dei dispacci cifrati con sostituzione polialfabetica, noti sin dalla fine dell'Ottocento, consistevano nel ridurre i crittogrammi ad insiemi di lettere cifrate con lo stesso alfabeto (sostituzione monoalfabetica), quindi risolubili mediante l'analisi delle frequenze. Il metodo basato sull'individuazione della lunghezza della chiave, dedotta dal rilievo delle distanze tra gruppi cifranti uguali, va sotto il nome di Babbage - Kasinski, mente quando si dispone di più crittogrammi cifrati con lo stesso cifrario e la stessa chiave si può applicare la procedura suggerita da Kerckhoffs.

Nella 2ª GM gli analisti degli Eserciti tedesco, inglese e americano utilizzarono per forzare sistemi polialfabetici metodi matematici più raffinati, come il 'K test' di Friedman che, oltre a determinate il numero di alfabeti usati in un testo crittato, consente di calcolare la lunghezza della chiave, ovvero il 'Phi test' di Kullback, valido anch'esso per stimare le periodicità di un crittogramma o di un insieme di crittogrammi.[128] Per effettuare in tempi ragionevoli tali operazioni, occorrevano però macchine di calcolo che dai primi tabulatori a schede si andarono evolvendo durante il conflitto verso veri e propri calcolatori elettronici.

Inoltre, per la soluzione dei sistemi 'a lucchetto' del tipo M-94 e M-138, era nota sin dai tempi precedenti alla 1ª GM la procedura suggerita da De Viaris applicabile, quando si posseggono i dispositivi, ma non sia nota la chiave cioè l'ordine in cui sono disposte le rondelle nei cilindri o le strisce nelle 'rastrelliere' nei dispositivi del tipo M-138.[129] Dagli interrogatori degli analisti dell'Asse emerge

128 BAUER, pp. 300 -340.

129 M. DE VIARIS *L'art de chiffrer et dechiffrer les dépèches secrètes*, Gauthier-Villars et Masson, Paris, 1893, p. 99. Si tratta di provare a penetrare il cifrario mediante una serie di parole considerate come 'probabili'. Per esempio, nel caso dell'M-94, ciascuna di queste parole viene inserita successivamente nelle diverse generatrici del lucchetto. Se la sequenza delle rondelle coincide con quella usata dal cifrista, il che equi-

chiaramente che i Tedeschi forzarono i cifrari a strisce, mentre gli Italiani non li citano affatto, anche perché questi ultimi, al contrario dei Tedeschi, non avevano avuto modo di catturare i suddetti dispositivi.[130]

Allegato 2: Anagrammi

Durante la Grande Guerra, il metodo di trasposizione colonnare fu largamente utilizzato da tutti gli Eserciti per la sua semplicità, perché bastava riportare il messaggio in chiaro su un rettangolo convenuto, riga per riga, e trascrivere il cifrato leggendo per colonne secondo un ordine definito da una chiave numerica, ovvero letterale trasformata in numerica. I dispacci tedeschi a singola o doppia trasposizione cioè con due trasposizioni successive, con rettangoli completi o incompleti, furono tra i primi decrittati da Luigi Sacco nella primavera - estate del 1916.[131]

Per tentare di sfuggire alle decrittazioni evitando la doppia trasposizione considerata troppo laboriosa non solo per l'impiego sui campi di battaglia,[132] durante la 2ª GM si adottarono diversi stratagemmi uno dei quali è rappresentato nella figura 6 del testo (cifrario degli Attaché militari romeni).[133] Le lettere del dispaccio in chiaro venivano allocate nella scacchiera partendo dalla diagonale da sinistra a destra, passando poi alla diagonale opposta e infine seguendo l'ordine della chiave costituita dalla sequenza dei numeri posti sulla tabella in alto, nel verso

vale a possedere anche la chiave, l'operazione diventa una semplice decifrazione. In caso contrario, si può applicare la procedura descritta da SACCO, p. 191-192.

130 ASA, Vol.1, United States 26, Army-Navy. Dopo il 1943, l'Esercito americano fece molto più frequentemente ricorso a machine cifranti, così che i dispacci furono decrittati dai Tedeschi in percentuali molto inferiori rispetto al passato.

131 Un sistema a trasposizione doppia denominato T1 fu introdotto dallo stesso Sacco nel settembre del 1918 per le comunicazioni di servizio delle piccole stazioni radio italiane. La sicurezza di questo sistema era incrementata mediante la variazione giornaliera delle chiavi e la disposizione del testo chiaro in rettangoli irregolari di nove colonne, tanto che il suo impiego continuò nel dopoguerra con la variante T2 (COLAVITO, CAPPELLANO, p. 373-375).

132 Tra gli eserciti che, nonostante le complicazioni sopra accennate, ricorsero, nella 2ª GM, a cifrari a trasposizione doppia, era compreso quello tedesco che li impiegò fino ad oltre il 1942, come cifrari di emergenza per le comunicazioni dai reggimenti alle unità di minor livello, con il rischio realmente concretizzatosi di venir decrittati dagli analisti Inglesi.

133 CSDIC/CMF/Y4, Bigi, Appendix C.

delle frecce. Il dispaccio cifrato si otteneva trascrivendo le lettere secondo una sequenza prestabilita, per esempio colonna per colonna da sinistra a destra della tabella. Gli Attaché militari romeni impiegarono anche altri metodi di trasposizione trascrivendo le parole in chiaro in una o più tabelle di diverse dimensioni, lungo "percorsi" predisposti, secondo quanto illustrato dal T. Colonnello Vassallo Todaro durante il suo interrogatorio.[134]

Come accennato nel testo, tra i cifrari da campo impiegati Esercito jugoslavo completamente noti agli analisti italiani, erano compresi sistemi a trasposizione semplice con chiavi numeriche di lunghezza variabile e rettangoli incompleti e quelli a doppia trasposizione con chiave unica e tabelle larghe 12-13 lettere.[135] Anche gli Attaché militari degli Stati Uniti erano dotati di un cifrario d'emergenza a doppia trasposizione e rettangoli incompleti risolto dal SIM nel 1942.[136]

La soluzione dei cifrari a doppia trasposizione non si presentava, di solito, facile e immediata. Per esempio, il metodo degli 'anagrammi multipli' ben noto dalla seconda metà dell'Ottocento per la soluzione generale dei sistemi a trasposizione, poteva applicarsi solo quando si disponeva di almeno due crittogrammi di uguale lunghezza cifrati con la stessa chiave, circostanza molto rara quando le chiavi venivano cambiate di frequente. I numerosi errori dei cifristi favorirono indubbiamente le forzature operate dalla Sezione crittografica, nonostante la mancanza di macchine a schede perforate denominate 'comparatori' e adottate a questo scopo da Tedeschi e Americani nella 2ª GM.[137]

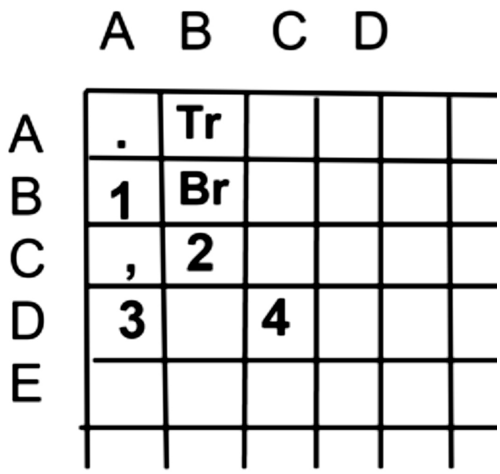

Fig. 8 Ricostruzione della parte iniziale della tabella con 676 posizioni dell'Esercito di Tito

134 CSDIC (main)/Y12 *First detailed Interrogation of Vassallo Todaro, Giuseppe*, 29 Oct.1944, p. 2; ASA, Romania, 21, 22, Military Attaché.

135 ASA, Vol.1, Yugoslavia Serbia, 56, Military, cifrario a trasposizione semplice e Yugoslavia Michailovič, 25, Military cifrario a doppia trasposizione.

136 ASA, Vol.1, United States, 19, Military Attaché.

137 SACCO, pp. 142-163; BAUER, pp. 418-423.

Allegato 3: Tabelle cifranti

La forma tabellare assunta sin dalla 1ª GM per i piccoli codici campali consentiva un facile e rapido impiego. Le tabelle contenevano lettere, numeri, sillabe o intere parole che si convertivano in gruppi cifranti letti in parte sulla prima riga e in parte sulla prima colonna. Nel testo è citato un codice campale in forma tabellare adottato da un'Armata francese combattente in Medio Oriente nel 1942-43 e ricostruita da Augusto Bigi (figura 7). I termini in chiaro erano riportati, in sequenze alfabeticamente ordinate, in 40/50 colonne di 10/12 righe ciascuna, tradotte in codice mediante trigrammi pronunciabili (absolut = JAZ). Il primo trigramma dei dispacci conteneva la chiave cioè le lettere iniziali delle righe e delle colonne. Poiché la chiave cambiava solo mensilmente, gli analisti italiani potevano accumulare materiale crittografico sufficiente a penetrare il cifrario.[138]

Alcune tabelle di questo tipo erano adottate dall'Esercito jugoslavo da tempi anteriori al 1941 e sin da allora forzate dalla Sezione crittografica. Un analogo sistema che comprendeva nella tabella anche intere parole fu risolto dagli Italiani nel giugno del 1943.[139]

Anche l'Esercito di Josip Broz Tito fece uso di questo tipo di cifrari sistematicamente risolti dalla Sezione crittografica, come la tabella quadrata di 676 (26x26) posizioni di cui si fa cenno nel testo e rappresenta nella figura 8. I termini in chiaro (numeri, segni di interpunzione, coppie di lettere, ma anche lettere singole, ecc.) contenuti in ciascuna posizione erano cifrati ciascuno con una coppia di lettere. La chiave consisteva di solito in una disposizione disordinata di queste lettere ottenuta mediante una frase o un verme costituito da una breve parola ripetuta, ambedue facilmente memorizzabili.[140]

La forzatura di questo tipo di cifrari veniva facilitata dalla necessità di rispettare una sequenza in qualche modo ordinata dei termini posti all'interno delle tabelle, in modo da consentire un'agevole decifratura. Le difficoltà per gli analisti derivavano quindi principalmente dal disordine e dalla lunghezza delle chiavi. Per ottenere una struttura del cifrario del tutto casuale occorreva adottare soluzioni diverse rappresentate, per esempio, da codici disordinati con due libri, uno per cifrare e l'altro per decifrare

138 ASA, Vol.1, France, 109, Army; CSDIC/CMF/Y4, Bigi, Appendix D.
139 ASA, Vol.1, Yugoslavia, 17, 18, Army; 23, Military.
140 CSDIC/CMF/Y4, Bigi, Appendix B.

ALLEGATO 4: Lo 'stripping' della seconda cifratura

Per la forzatura dei codici ordinati e non sopra-cifrati, una volta individuata la struttura e la corrispondenza tra un termine in chiaro e un gruppo cifrante, basta un semplice vocabolario per scoprire il significato dei gruppi vicini. La ricostruzione di un codice disordinato richiede un lavoro analitico più complesso che può richiedere molto tempo anche solo per l'individuazione di una percentuale di gruppi cifranti sufficiente a effettuare una corretta interpretazione dei crittogrammi. Il lavoro degli analisti si complica ulteriormente quando i gruppi risultanti dai libri di codice sono sopra cifrati. Mentre la ricostruzione di un codice richiede soprattutto competenze linguistiche, la soluzione delle tabelle di seconda cifratura si effettua di solito mediante calcoli matematici.

In molti casi, alcuni dei quali sono menzionati nel testo, i codici erano 'compromessi' cioè in possesso dei decrittatori in copie fotostatiche perché catturati in battaglia, negli scafi di navi affondate o acquisiti con diversi metodi come la sottrazione dalle casseforti delle Ambasciate. Ciò nonostante, si continuava spesso a impiegarli anche per le difficoltà di operare cambiamenti che coinvolgevano numerose sedi sparse in tutto il globo e si affidava la sicurezza delle comunicazioni solo alla seconda cifratura sulla cui soluzione si concentravano gli sforzi dei decrittatori. La soluzione della seconda cifratura attuata mediante metodi di sostituzione mono o polialfabetica oppure di trasposizione era stata conseguita da Sacco e dai suoi collaboratori sin dalla Prima Guerra Mondiale con i metodi esposti nel Manuale di Crittografia.

Anche nel secondo conflitto mondiale, numerose sopra cifrature di codici diplomatici e militari, per esempio di Jugoslavia, Turchia e Grecia, applicavano questi sistemi, talvolta rinforzati mediante ingegnose varianti. Invece l'Inghilterra, prima ancora dell'inizio della 2ª GM, applicò una seconda cifratura più complessa in particolare alle comunicazioni con segretezza elevata che impiegavano il codice diplomatico ID (Interdepartmental Cipher), quello militare WOC (War Office Cypher) e il NAVAL CYPHER. Come si è accennato, questa seconda cifratura era realizzata sottraendo dai gruppi di prima cifratura delle serie di numeri casuali variabili da un crittogramma a quelli successivi, con ripetizioni il più possibile distanti l'una dall'altra. Altri Paesi, tra cui l'Italia soprattutto per le comunicazioni navali e la Germania, seguirono l'esempio inglese.[141]

141 Luigi DONINI «Sistemi crittografici nella Regia Marina», *Rivista Marittima*, luglio 1994, p. 111-113.

In linea del tutto generale, il 'metodo delle differenze' adottato per risolvere questo tipo di seconda cifratura richiedeva *in primis* l'individuazione, sfruttando alcuni indizi, di quelle parti di un crittogramma, o più spesso di più crittogrammi, sopra cifrate con la stessa sequenza di numeri casuali.[142] Se si sottraggono tra loro due o più serie di gruppi cifranti con le suddette caratteristiche, si ottiene per ogni coppia sottratta un risultato uguale alla differenza tra i corrispondenti gruppi di prima cifratura. Perciò se si conosce, o si può ragionevolmente ipotizzare la corrispondenza con il testo chiaro di uno dei due gruppi, si ottiene immediatamente il significato reale o ipotetico dell'altro.

Per ricostruire le tabelle di sopra cifratura e, quando possibile il codice, è necessario ripetere questo tipo di operazione numerose volte, fino a raccogliere una quantità di materiale tale da consentire di attribuire con certezza ad alcuni gruppi di codice il loro reale significato. Questo processo molto più complesso di quanto appare dalla precedente sintesi intuitiva richiedeva una quantità notevole di calcoli e, per essere attuato celermente, imponeva l'impiego di macchine di calcolo che all'epoca erano costituite dai così detti tabulatori descritti brevemente nel testo.[143]

Bibliografia

Alvarez, David, *I servizi segreti del Vaticano. Spionaggio. Complotti, intrighi da Napoleone ai giorni nostri*», Newton Compton, Roma, 2009.

Amé, Cesare, *Guerra segreta in Italia 1940 - 1943*, a cura di Carlo De Risio, Bietti, Milano, 2011.

Army Security Agency, *European Axis signal intelligence in WAR II as revealed by TICOM investigations and by other prisoner of war interrogations and captured material, principally German,* in nine volumes, Washington D.C., 1 May 1946.

Cernuschi, Enrico, *«ULTRA» La fine di un mito. La guerra dei codici tra gli Inglesi e le Marine italiane, 1934-1943*, Mursia, Milano, 2014.

Bauer, Friedrich L., *Decrypted Secrets, methods and maxims of cryptology,* Spriner-Verlang, Berlin, 1997.

142 È chiaro che la possibilità di reperire brani di questo tipo dipendeva anche dai *depth,* cioè in definitiva dall'intensità dell'impiego di una tabella di seconda cifratura. Un modo per individuare brani cifrati con le stesse sequenze, si basava sul controllo degli 'indicatori' posti all'inizio di ciascun crittogramma che fornivano il primo gruppo della sequenza casuale di numeri da cui iniziava la seconda cifratura.

143 Kahn, pp. 440-444.

CIANO, Galeazzo, *Diario 1937-1943*, a cura di Renzo De Felice, Rizzoli, Milano, 1980.

COLAVITO, Cosmo e Filippo, CAPPELLANO, *La Grande Guerra Segreta sul Fronte Italiano (1915-1918) - La Communication Intelligence per il Servizio Informazioni*, Stato Maggiore della Difesa, Ufficio Storico, Roma, 2ª Ed., 2018.

CONTI, Giuseppe, *Una guerra segreta, il SIM nel secondo conflitto mondiale*, il Mulino, Bologna, 2009.

DAHKLE, Carola, *The Auxiliary Devices of OKW/chi*, Proceedings of the 3rd International Conference on Historical Cryptology, HistoCrypt 2020.

Cipher, DEAVOURS, David, KAHN et alii *Cryptology. Machines, history & methods,* Arthec House, Norwood, 1989.

DE VIARIS, M., *L'art de chiffrer et dechiffrer les dépèches secrètes*, Gauthier-Villars et Masson, Paris, 1893

FLICKE, Wilhelm F., *War Secrets in the Ether*, translated by Ray W. Pettengill, National Security Agency, Washington D. C., 1953.

HOTTL, Wilhelm. *Hitler Paper Weapons*, Rupert Hart-Davis, London, 1955.

Il Comandante Giorgio Verità Poeta, Atti del Convegno 18 ottobre 2014, in edibus, Milano, 2016.

KAHN, David, *The Codebreakers. The story of Secrete Writing*, Scribner, New York, 1996.

MARKS, Leo, *Between Silk and Cyanide. A Codemakers War*, 1941-1945, Simon & Shouster, New York, 1998

PASQUALINI, Maria Gabriella, *Breve storia dell'organizzazione dei Servizi d'Informazione della R. Marina e R. Aeronautica, 1919-1945,* Commissione Italiana Storia Militare, Roma, 2013.

SEBAG-MONTEFIORE, Hugh., *ENIGMA The battle for the code,* Weidenfeld & Nicolson. London, 2017.

PILLON, Giorgio, *Spie per l'Italia. Come fecero la guerra gli 007 dei nostri servizi segreti*, prefazione del Generale Cesare Amé, I libri del NO, Roma, 1968.

Radiofronte 1835-1945, Museo Storico Italiano della Guerra, Rovereto, 2003.

RONGE, Maximilian, *Spionaggio*, Editrice Tirrenica, Napoli, 1939

SACCO, Luigi, *Manuale di Crittografia*, 3ª Edizione aggiornata e aumentata, Roma, 1947.

VIVIANI, Ambrogio, *Servizi Segreti Italiani, 1815-1985*, Adnkronos, Roma, 1985, Vol. I e II.

MANUAL FOR THE SOLUTION OF MILITARY CIPHERS

BY

PARKER HITT
Captain of Infantry, United States Army

Introduction

THE history of war teems with occasions where the interception of dispatches and orders written in plain language has resulted in defeat and disaster for the force whose intentions thus became known at once to the enemy. For this reason, prudent generals have used cipher and code messages from time immemorial. The necessity for exact expression of ideas practically excludes the use of codes for military work although it is possible that a special tactical code might be useful for preparation of tactical orders.

It is necessary therefore to fall back on ciphers for general military work if secrecy of communication is to be fairly well assured. It may as well be stated here that no practicable military cipher is mathematically indecipherable if intercepted; the most that can be expected is to delay for a longer or shorter time the deciphering of the message by the interceptor.

The capture of messengers is no longer the only means available to the enemy for gaining information as to the plans of a commander. All radio messages sent out can be copied at hostile stations within radio range. If the enemy can get a fine wire within one hundred feet of a buzzer line or within thirty feet of a telegraph line, the message can be copied by induction. Messages passing over commercial telegraph lines, and even over military lines, can be copied by spies in the offices. On telegraph lines of a permanent nature it is possible to install high speed automatic sending and receiving machines and thus prevent surreptitious copying of messages, but nothing but a secure cipher will serve with other means of communication.

Parker Hitt, Captain of Infantry, U. S. A., *Manual for the Solution of Military Ciphers*, Press of the Arny Service Schools, Fort Leavenworth, Kansas, 1916. Digitalized by Microsoft Corporation From University of California Libraries. May be used for no-commercial purposes.

Lieutenant A. FROMENT

L'ESPIONNAGE Militaire

LES FONDS SECRETS DE LA GUERRE ET LE SERVICE DES RENSEIGNEMENTS EN FRANCE ET A L'ÉTRANGER

PARIS
F. JUVEN, ÉDITEUR
10, RUE SAINT-JOSEPH, 10

Intelligence militare, guerra clandestina e Operazioni Speciali

Articles

Reviews