I servizi crittografici delle Marine Britannica e Italiana.

L. Donini

Una analisi comparativa della loro attività nel secondo conflitto mondiale

Sebbene non ci siano elementi sufficienti per stendere un bilancio completo, ritengo possibile effettuare un'analisi comparativa delle attività dei due servizi crittografici indipendentemente dallo sfruttamento di esse attività fu o non fu fatto dai rispettivi Alti Comandi in campo strategico e tattico. Effettuare cioè un confronto esclusivamente tecnico sulla struttura e la qualità dei sistemi di cifratura, sui gradi di difficoltà dei relativi decrittografici, sulla incapacità dimostrata nel raggiungere successi o subire fallimenti.

Un'analisi del genere, che servirà anche a chiarire le cause del successo inglese nella penetrazione delle nostre cifrature meccaniche, deve prendere in considerazione sia la crittografia offensiva o decrittografia, cioè l'attacco alle radiocomunicazioni segrete nemiche, sia quella difensiva, cioè la tutela delle proprie cifrature.

Mi sembra giusto limitare l'analisi ai sistemi di uso pressoché generale per i radiomessaggi di alto grado di segretezza, cioè: i cifrari navali sopracifrati (inglesi e italiani) e le cifrature meccaniche (italiane). Per queste ultime ritengo di poter trascurare in questa sede la macchina ENIGMA impiegata dal SIS (Servizio Informazioni Segrete, della Marina), sia perché essa non fu di uso navale generale, avendola impiegata solo Supermarina in rare occasioni (L'opera ufficiale britannica "British Intelligence in the 2 W.W." - che d'ora in avanti citeremo con la sigla B.I. - a pag.210 del 1° Vol. dice: «solo uno o due messaggi al giorno») e solo nei primi 9 mesi di guerra, sia perché le sue vicende sono assorbite da quelle della ENIGMA delle FF.AA. tedesche, già penetrata dagli Inglesi nel 1940.

2. - I cifrari navali sopracitati

2.1. - Come è noto alla maggior parte dei lettori, tale cifratura è articolata su due operazioni successive. La prima consiste nel sostituire alle parole o frasi del «chiaro» gruppi letterali o numerici segreti (quadricifre, per entrambe le Marine in questione) reperiti nel cifrario o codice vero e proprio. Per esempio (parole e quadricifre sono di fantasia):

chiaro .... Hush most secret stop Cincmed from Adm.London stop ...

1ª Cifr. (C) 1782 8130 6615 8469 0983 3561 1565 8469

La seconda operazione, detta 2ª cifratura o sopracifratura, consiste nel sottrarre cifra, senza i rapporti cioè con modalità 10, i gruppi della 1ª cifratura dai gruppi del cosiddetto «verme di sopracifratura» prelevato da apposite tabelle. Per esempio:

Verme	**(V)**	**2916**	**3410**	**9226**	**0880**	**4534**	**8117**	**4036**	**1912** ..
-1ª cifr.	**(C)**	**-1782**	**8130**	**6615**	**8469**	**0983**	**3561**	**1565**	**8469** ..
Sopra-cifrato	**(S)**	**1234**	**5380**	**3611**	**2421**	**4651**	**5656**	**3571**	**3553**

Vale a dire: S = V - C, per sopracifrare e C = V - S, per eliminare la sopracifratura. E' ovvio che nessun crittografo, anche se in possesso del cifrario nemico, potrà mai decrittare un messaggio sopracifrato non verme casuale o, comunque, incoerente, a lui non noto e usato esclusivamente per quel messaggio. Ma, se nella massa del materiale sotto esame esistono coppie, o terne etc., di messaggi sopracifrati con lo stesso verme, si apre un piccolo spiraglio alla penetrazione, in base a una semplicissima considerazione algebrica. Infatti, la differenza fra due gruppi S_2 e S_1 in 2ª cifratura, sopracifrati con lo stesso gruppo V di Verme è uguale alla differenza fra i due gruppi del codice in 1ª cifratura (C_2 e C_1) che hanno generato i rispettivi gruppi sopracifrati:

$$\begin{array}{r} S_1 = V - C_1 \\ S_2 = V - C_2 \\ \hline S_1 - S_2 = C_2 - C_2 \end{array}$$

Ne consegue che solo le coppie, terne, etc. di messaggi cifrati con lo stesso cifrario e sopracifrati con lo stesso verme costituiscono le basi per avviare la penetrazione.

Per fare ciò il decrittatore deve:

- individuare, se ve ne sono, le coppie o terne, etc. di messaggi sopracifrati con lo stesso verme;

- effettuare, per ciascuna coppia individuata, le differenze fra gruppi omologhi, cioè gruppi che occupano nei due messaggi uguale posizione;

- registrare le differenze che si sono presentate con frequenza sensibilmente maggiore di quella prevedibile secondo le leggi di probabilità;

- per ogni differenza ($S_1 - S_2 = C_2 - C_1$) accettata come significativa assegnare valori numerici arbitrari (C_2 e C_1) ai gruppi di codice che l'hanno generata, cercando poi di collegare fra loro i valori arbitrari in modo da ridurli tutti a una stessa base relativa, tale cioè che detti gruppi «arbitrari» differiscano dai corrispondenti gruppi «reali» (non ancora noti) del codice per una «costante» comune, che col tempo si riuscirà forse a definire, sebbene ciò non sia indispensabile.

Il lavoro anzidetto proseguirà fino ad aver raccolto una quantità di materiale tale da poter attribuire ad alcuni dei gruppi arbitrari di codice il rispettivo significato per iniziare così e poi sviluppare la ricostruzione vera e propria del codice o cifrario in uso, assieme a quella delle relative tabelle di sopracifratura.

2.2. - Non occorre sprecare parole per illustrare quanto sia arduo e faticoso il lavoro che ho succintamente descritto e che il servizio crittografico della nostra Marina riuscì a portare a compimento per i vari cifrari o codici navali inglesi che si avvicendarono dal 1938 a tutto il 1942.

Gli analoghi tentativi inglesi contro i nostri cifrari navali del periodo bellico incontrarono invece completo fallimento, onestamente ammesso dai nostri avversari e più volte lamentato anche nei due volumi del B.I.. Per esempio, a pag.210 di B.I. vol.1° si legge: «I principali cifrari navali italiani, che erano i cifrari usati dalla loro flotta per la maggior parte delle sue comunicazioni importanti, non fu-

rono mai più letti dopo il luglio 1940, eccetto che per pochi brevi intervalli, come risultato di catture, dopo la metà del 1941». Di questo insuccesso non sappiamo quanto fu dovuto a loro minore capacità e impegno e a presumibile minore intensità del nostro traffico radio, e quanto a maggiore efficacia degli accorgimenti e delle contromisure che avevamo introdotto nel nostro complesso «cifrari/sopracifratura» entrato in vigore a metà luglio 1940, proprio perché avevamo potuto sfruttare la conoscenza delle debolezze riscontrate nell'analogo sistema inglese e gli appigli di cui a mano a mano avevamo imparato ad avvalerci per penetrarlo.

2.3. - Le debolezze del sistema inglese erano varie e di vario peso. Mi limito a citarne alcune:

- a) reimpieghi totali di verme, abbastanza frequenti e fino a tre/quattro volte per uno stesso verme; reimpieghi parziali frequentissimi;

- b) periodi di validità, anche se di pochi giorni, delle tabelle di sopracifratura mal commisurati alla intensità del traffico radio;

- c) imperfetto controllo della usura delle tabelle dei vermi. Quando veniva ordinata, con messaggio cifrato, la abrogazione di vermi troppo usati, quasi sempre il danno era già avvenuto;

- d) nelle tabelle che contenevano i vermi di sopracifratura esistevano qua e là (forse per esigenze di rapidità di compilazione) intere righe già esistenti in tabelle abrogate;

- e) i «gruppi indicatori» che, posti all'inizio dei messaggi in cifra, indicavano ai destinatari quale verme era stato usato, furono per molti anni impiegati senza «mascheratura», cioè non disguisati, sicché l'eventuale reimpiego di un verme era direttamente rivelato dall'uguaglianza dei gruppi indicatori;

- f) quando, nel dicembre '40 e fino a buona parte del 1941, gli Inglesi introdussero la «mascheratura» degli indicatori, essa fu piuttosto banale e per di più usata male dai cifratori, tanto da crearci solo due settimane di crisi;

- g) i cifrari non contenevano «omofoni», cioè non assegnavano due o più gruppi segreti diversi per cifrare una data parola di uso molto frequente. Per esempio «fullstop»

poteva essere cifrato in un solo modo (nei nostri cifrari: una ventina di modi diversi); analogamente per «from» etc.;

- h) le voci geografiche erano abbinate, come interpretazione alternativa, a voci di vocabolario iniziati con le stesse due o tre lettere. Così, solo a titolo esemplificativo: 7184 = Give/Gibraltar, 0921 = Last/La Spezia, 4650 = Make/Malta, 2935 = All Concerned/Alexandria, 7714 = Left/Leghorn. Ciò ci era di grande aiuto per identificare la voce geografica quando avevamo già identificato la voce di vocabolario ad essa abbinata, e viceversa;

- i) i messaggi iniziavano quasi sempre con l'indirizzo completo: (to) ..... from .....;

- j) i cifrari si componevano di due parti: la prima parte, che serviva soprattutto per cifrare gli indirizzi, conteneva i nomi dei Comandi, delle Autorità, delle Unità Navali e, inoltre, i numeri, le date, i gradi e i primi di latitudine e longitudine; la seconda era il vocabolario vero e proprio. In entrambe le parti i gruppi cifranti segreti (quadricifre) erano presi a caso dalla sue naturale da 0001 a 9999, sicché quasi tutte le quadricifre si trovavano sia nella prima che nella seconda parte.

Se l'indirizzo prendeva 1, 2, 3 ....., 9 gruppi, il primo gruppo del messaggio in prima cifratura era, rispettivamente, 1111, 2222, 3333, ..., 9999 per indicare al destinatario che per 1, 2, 3, ... 9 gruppi doveva usare la prima parte del cifrario. Se l'indirizzo prendeva più di 9 gruppi, il primo gruppo era 9900 e alla fine dell'indirizzo veniva posto il gruppo 0099 a indicare di passare ad usare la seconda parte. 0099 era anche posto come primo gruppo quando doveva usare subito la seconda parte anziché la prima. Questa particolarità, che ovviamente avevano scopo mnemonico e rimasero in uso per alcuni anni, facevano sì che le differenze relative al 1° gruppo di coppie di messaggi aventi uguale gruppo indicatore, cioè sopracifrati con lo stesso verme (1) avevano solo i seguenti valori 0000, 1111, 2222, ..., 9999, 1122, 2233, ..., 8899, 2211, 3322,

(1) Vds. parag.2.1. Si ricordi che la differenza fra due gruppi in 2ª cifratura, sopracifrati con lo stesso verme, è uguale alla differenza tra i due rispettivi gruppi in 1ª cifratura.

....., 9988, 1199, 9911. Dalla constatazione di questa singolarità al darne la logica spiegazione, per noi il passo fu breve e ci aprì il primo spiraglio per la penetrazione. Fra l'altro potevamo subito sapere quanti gruppi prendevano gli indirizzi, dove si trovava il gruppo segreto per «from» (che non aveva «omofoni», vedi comma g. e dove iniziava il testo vero e proprio con le sue spesso stereotipate frasi iniziali (riferimento ..., risposta ..., prosecuzione ... etc.).

Ma a mio parere, la più grave imprudenza o imprevidenza inglese fu l'aver mantenuto in uso, per tutto il primo anno di guerra con la Germania, lo stesso cifrario navale principale che era in vigore fin dall'epoca della guerra civile spagnola, penetrato da noi (e dai Tedeschi) fin dal 1938. Quando dovetti lasciare il comando di una unità subacquea per prendere nel SIS la direzione della sezione crittografica in cui avevo lavorato, con poche interruzioni, dal 1934, rimasi sorpreso - ma anche molto lieto - nel constatare che il principale bersaglio era ancora quello contro cui mi ero io stesso cimentato dal 1938 all'inizio del 1940.

Era stato questo il motivo che aveva consentito alla nostra sezione crittografica di decrittare, il 4 luglio 1940, l'ordine di operazioni del Comandante della Mediterranean Fleet, che portò al fatto d'armi di Punta Stilo il 9 dello stesso mese, prima occasione, nella storia, di incontro di guerra fra le due flotte, incontro peraltro rimasto inconcludente (2).

Purtroppo, solo due settimane dopo il mio ritorno al servizio crittografico, gli Inglesi abrogarono quel cifrario sostituendolo con due cifrari diversi e introdussero alcuni accorgimenti che però non ci impedirono di riprendere la padronanza della situazione, per entrambi i nuovi cifrari, dopo qualche mese.

---

(2) Pare che in quella occasione anche gli Inglesi avessero ottenuto informazioni, sebbene piuttosto incomplete, sulla intenzione della nostra flotta, da intercettazioni di nostri segnali in chiaro e anche attraverso decrittazione di radiomessaggi ancora cifrati col nostro cifrario prebellico, penetrato a suo tempo dagli Inglesi, che - forse per difficoltà logistiche - fu da noi sostituito solo a metà luglio 1940.

In definitiva, a conclusione della sommaria analisi tecnica svolta relativamente alla «guerra dei cifrari» ritengo di poter affermare che il servizio crittologico della nostra Marina sopravanzò di parecchie lunghezze l'analogo servizio britannico.

3. - La cifratura meccanica della Marina Italiana

Indicherò con la stessa sigla «C38m» usata dal B.I. la nostra macchina cifrante, che era una modifica - pressoché irrilevante dal punto di vista crittografico - di una macchina cifrante svedese disponibile in commercio.

3.1. - L'adozione della C38m - secondo i miei ricordi personali.

E' noto che una precedente versione di quella macchina, offerta alla nostra Marina dall'inventore e costruttore intorno al 1934-'35, era stata respinta dal SIS dopo un accurato esame condotto da una commissione di 4 crittografi, fra i quali il sottoscritto. Nel 1935 quella stessa macchina, evidentemente ritenuta valida dagli specialisti francesi, fu acquistata in massa per quelle FF.AA..

Qualche anno dopo, forse nel 1938, il costruttore svedese ne presentò al nostro Stato Maggiore un nuovo esemplare nel quale aveva introdotto qualche miglioramento, portando i rotori da 5 a 6; ma il principio originale del meccanismo cifrante era sempre quello del 1935. Non so se fu nuovamente consultato il SIS, dato che io ne ero assente perché imbarcato; fatto sta che più tardi, credo nel corso del 1940, quella macchina fu introdotta, ma solo per le comunicazioni segrete di pochi Alti Comandi, a terra e a bordo. Nel frattempo essa era stata acquistata anche dall'Esercito USA che la usò come sistema di medio livello dai Comandi di Divisione in giù fino ai Battaglioni.

Posso pensare che i miglioramenti apportati dal costruttore e la conoscenza degli acquisti fatti in gran quantità da Francia e USA abbiano indotto i nostri organi tecnico-amministrativi a trascurare il parere negativo espresso dal SIS alcuni anni prima.

Io ritengo che per l'epoca, cioè lo stadio in cui si trovava la crittologia, e per le circostanze che l'accompagnarono, essa trova più di una giustificazione. Altro di-

scorso andrà fatto, come vedremo, per il modo in cui la C38m finì per essere impiegata, specie nel periodo cruciale dei nostri trasporti per il Nord Africa.

3.2. - Funzionamento della C38m - Cifratura e decifrazione

3.2.1. - La C38m realizzava attraverso i suoi meccanismi una cifratura a sostituzione polialfabetica con l'impiego di 26 alfabeti segreti ordinati e rovesciati che si ottengono facendo slittare di un posto alla volta il normale alfabeto anglosassone rovesciato. Questi alfabeti sono riportati parzialmente nella Tavola 1, che può essere usata manualmente per questo tipo di cifratura polialfabetica: ogni lettera del testo chiaro viene sostituita con quella ad essa corrispondente nell'alfabeto segreto di volta in volta usando, secondo una successione che costituisce la «chiave» o «verme» di cifratura. Per esempio, utilizzando la Tavola 1:

verme (cioè n.ri degli alfabeti segreti usati)	**23**	**14**	**0**	**12**	**25**	**2**	**13**	**1**	**15**	**12**	**0**
testo chiaro:	**r**	**i**	**f**	**e**	**r**	**i**	**m**	**e**	**n**	**t**	**o**
testo segreto:	**G**	**G**	**V**	**I**	**I**	**U**	**B**	**X**	**C**	**T**	**M**

La stessa tavola può essere usata per decifrare:

verme:	**23**	**14**	**0**	**12**	**25**	**2**	**13**	**1**	**15**	**12**	**0**
testo segreto:	**G**	**G**	**V**	**I**	**I**	**U**	**B**	**X**	**C**	**T**	**M**
testo chiaro:	**r**	**i**	**f**	**e**	**r**	**i**	**m**	**e**	**n**	**t**	**o**

3.2.2. - Il meccanismo cifrante era costituito da:

- a) un certo numero di elementi metallici nelle parti rotanti e fisse all'interno della macchina; piolini, sbarrette, cursori, ciascuno dei quali poteva essere posto, dall'operatore, in posizione attiva o inattiva, venendo così a formare la cosiddetta «chiave interna», in realtà costituita da due componenti, chiamate W e X. Il numero delle chiavi interne diverse che l'operatore poteva impostare era astronomico, vicino ai ventilioni (un numero di 60 cifre), ma l'impostazione, assai laboriosa, richiedeva molta attenzione e molto tempo, sicché si finiva per dover mantenere in

uso una stessa chiave interna per un tempo non breve.

- b) 6 rotori di uguale diametro, affiancati, calettati su un asse orizzontale, ciascuno dei quali poteva essere fatto ruotare, anche manualmente a mezzo di ingranaggi che avevano diverso numero di denti per i diversi rotori, e precisamente 26, 25, 23, 21, 19, 17.

Tavola I

TAVOLA PER LA CIFRATURA MANUALE POLIALFABETICA
CON ALFABETI REGOLARI ROVESCIATI

(chiaro)		ALFABETI SEGRETI																									(chiaro)
n°		0	1	2	3	.	.	.	.	12	13	14	15	.	.	.	.	23	24	25							
0	a	A	B	C	D	.	.	.	.	M	N	O	P	.	.	.	.	X	Y	Z							a
1	b	Z	A	B	C					L	M	N	O					W	X	Y							b
2	c	Y	Z	A	B					K	L	M	N					V	W	X							c
3	d	X	Y	Z	A					J	K	L	M					U	V	W							d
4	e	W	X	Y	Z					I	J	K	L					J	U	V							e
5	f	V	W	X	Y					H	I	J	K					S	T	U							f
6	g	U	V	W	X					G	H	I	J					R	S	T							g
7	h	T	U	V	W					F	G	H	I					Q	R	S							h
8	i	S	T	U	V					E	F	G	H					P	Q	R							i
9	j	R	S	T	U					D	E	F	G					O	P	Q							j
0	k	Q	R	S	T					C	D	E	F					N	O	P							k
11	l	P	Q	R	S	.	.	.	.	B	C	D	E	.	.	.	.	M	N	O							l
12	m	O	P	Q	R					A	B	C	D					L	M	N							m
13	n	N	O	P	Q					Z	A	B	C					K	L	M							n
14	o	M	N	O	P					Y	Z	A	B					J	K	L							o
15	p	L	M	N	O					X	Y	Z	A					I	J	K							p
16	q	K	L	M	N					W	X	Y	Z					H	I	J							q
17	r	J	K	L	M					V	W	X	Y					G	H	I							r
18	s	I	J	K	L					U	V	W	X					F	G	H							s
19	t	H	I	J	K					T	U	V	W					E	F	G							t
20	u	G	H	I	J					S	T	U	V					D	E	F							u
21	v	F	G	H	I					R	S	T	U					C	D	E							v
22	w	E	F	G	H					Q	R	S	T					B	C	D							w
23	x	D	E	F	G					P	Q	R	S					A	B	C							x
24	y	C	D	E	F					O	P	Q	R					Z	A	B							y
25	z	B	C	D	E	.	.	.	.	N	O	P	Q	.	.	.	.	Y	Z	A							z
n°		0	1	2	3	.	.	.	.	12	13	14	15	.	.	.	.	23	24	25							
(chiaro)		ALFABETI SEGRETI																									(chiaro)

Sulla corona esterna di ciascun rotore erano incise, in ordine regolare, le lettere dell'alfabeto anglosassone, rispettivamente da A a Z, da A a Z con esclusione di W, da A a Z con esclusione di W, da A a U, da A a S, da A a Q. Lungo la periferia della faccia di destra di ogni rotore erano alloggiati rispettivamente 26, 25, 23, 21, 19, 17 piolini, in corrispondenza delle altrettante lettere incise sui bordi esterni. Come già accennato, ogni piolino poteva essere posto, dall'operatore, in posizione attiva o inattiva. Il numero e la disposizione dei piolini attivi costituiva la com-

ponente X della chiave interna, come detto poc'anzi. Il numero delle componenti X diverse che l'operatore poteva impostare era grandissimo, 2 elevato alla 131ª potenza (un numero di 40 cifre) anche se molte di esse erano sconsigliabili perché troppo semplici.

3.2.3 - Facendo ruotare a mano ciascuno dei 6 rotori, si potevano allineare le rispettive lettere rispetto a una linea di fede costituita da 6 finestrelle praticate nel coperchio della macchina. L'allineamento, così creato dall'operatore, costituiva la cosiddetta «chiave esterna» che l'operatore doveva impostare prima di iniziare la cifratura del messaggio. Nel corso dell'operazione di cifratura, lettera per lettera, ad ogni «battuta» i 6 rotari avanzavano simultaneamente di un passo (vedi Tavola 2) facendo così entrare in gioco, per cifrare la lettera battuta, uno dei 26 alfabeti segreti di sostituzione della già citata tavola 1, secondo una successione, detta «Verme», che era caotica solo apparentemente, poiché in realtà dipendeva dalla legge di formazione generata delle due componenti W e X della chiave interna predisposta dall'operatore.

Per spiegare l'effetto dell'azione combinata delle componenti W e X della chiave interna sarà meglio fare un esempio, anche se un po' «addomesticato» (vedi Tavola 3).

Abbiamo visto in che cosa consisteva la componente X: i 131 (cioè 26+25+23+21+19+17) piolini posti parte in posizione attiva e parte inattivi. La componente W (3) era in realtà costituita da 7 componenti, una per ogni rotore (W_1 W_2 W_3 W_4 W_5 W_6) e una (W_o) indipendente dai rotori. Quando l'operatore impostava la chiave interna poteva far assumere al W_o i valori 1 o 2 e a ciascuno dei restanti w valori da 1 a 9 (4) ma la somma dei sette W doveva dare sempre 27.

---

(3) Per brevità omettiamo di descrivere la struttura meccanica, piuttosto complessa, della componente W. Diciamo solo che si trattava di un cilindro con alcuni cursori, e di sbarrette che l'operatore poteva predisporre in posizione attiva o inattiva.

(4) Materialmente quelli che per semplicità abbiamo chiamato «valori 1 o 2 e valori da 1 a 9» erano il numero di sbarrette poste in posizione attiva dall'operatore (vedi nota precedente).

Consideriamo l'allineamento che nella Tavola 2 corrisponde alla posizione 30 000 000 nel verme generato dalla chiave interna impostata dall'operatore, di cui riportiamo qui di seguito la componente W (vedi Tavola 3):

rotori 1 2 3 4 5 6 0

componente W 5 + 1 +8 + 2 +6 + 3 +2 = 27

allineamento (chiave esterna) E A T J H P

Secondo la componente X della chiave interna predisposta, i 6 piolini alloggiati nei 6 rotori sotto le 6 lettere

Tavola 2

SCHEMA DELLA GENERAZIONE DI UN «VERME» COMPLETO RELATIVO A UNA DATA CHIAVE INTERNA E DELLA CIFRATURA DI UN MESSAGGIO CON CHIAVE ESTERNA DATA

	ROTORI								
	1 (26)	2 (25)	3 (23)	4 (21)	5 (19)	6 (17)	posizione nel verme	(verme) n° della allabeto segreto	
	A	A	A	A	A	A	0	8	
	B	B	B	B	B	B	1	11	
	C	C	C	C	C	C	2	13	
	D	D	D	D	D	D	3	11	
	.	.	.	.	.	.	.	.	
	Q	Q	Q	Q	Q	Q	16	17	
	R	R	R	R	R	A	17	2	
	S	S	S	S	S	B	18	11	
	T	T	T	T	A	C	19	12	
	U	U	U	U	B	D	20	1	
	V	V	V	A	C	E	21	18	
	W	X	X	B	D	F	22	2	
	X	Y	A	C	E	G	23	12	
	Y	Z	B	D	F	H	24	8	
	Z	A	C	E	G	I	25	13	
	A	B	D	F	H	J	26	5	
	.	.	.	.	.	.	.	.	
(.) chiave esterna	E	A	T	J	H	P	30 000 000	14	vedi Tavola 1: chiaro / segreto
	F	B	U	K	I	Q	30 000 001	23	r / G
	G	C	V	L	J	A	" 2	14	i / G
	H	D	X	M	K	B	" 3	0	l / V
	I	E	A	N	L	C	" 4	12	e / I
	J	F	B	O	M	D	" 5	25	r / I
	K	G	C	P	H	E	" 6	2	l / U
	L	H	D	Q	O	F	" 7	13	m / B
	M	I	E	R	P	G	" 8	1	e / X
	N	J	F	S	Q	H	" 9	15	n / C
	O	K	G	T	R	I	" 10	12	i / T
	P	L	H	U	S	J	" 11	0	a / M
	Q	M	I	A	A	K	" 12	3	v / I
	R	N	J	B	B	L	" 13	14	a / A
	S	O	K	C	C	M	" 14	24	s / G
	.	.	.	.	.	.	.	.	. / .
	Y	Y	V	T	R	P	101 405 848	13	. / .
	Z	Z	X	U	S	Q	101 405 849	15	. / .
	A	A	A	A	A	A	0	8	
	B	B	B	B	B	B	1	11	

dell'allineamento dato e in quelli successivi, nel corso della cifratura, potevano trovarsi in posizione attiva o inattiva. Quelli attivi rendevano attivo il rispettivo w mentre quelli inattivi lo lasciavano inattivo. Il W_0 indipendente dai rotori, era però sempre attivo. Ad ogni avanzamento simultaneo dei 6 rotori i meccanismi interni della macchina facevano entrare in gioco l'alfabeto segreto di sostituzione avente il numero d'ordine (vedi Tavola 1) uguale alla somma, con modalità 26, dei w attivi. L'alfabeto entrato in gioco cifrava la lettera che era stata battuta e che aveva provocato l'avanzamento dei rotori.

Tavola 3

GENERAZIONE DEL «VERME» DI CIFRATURA
PER IL MESSAGGIO DELLA TAVOLA 2

Componente W della chiave interna								verme n° dello alfabeto segreto
Rotori		(1)	(2)	(3)	(4)	(5)	(6)	(0)	
		w_1	w_2	w_3	w_4	w_5	w_6	w_0	
		5	1	8	2	6	3	2	
posiz.	30 000 000	E	A	T	J	H	P		
		+5		+8	+2	6		+2	= 23
"	30 000 001	F	B	U	K	I	Q		
		·	+1	·	+2	+6	+3	+2	= 14
"	" 2								
		+5	·	+8	+2	+6	+3	+2	= 26 = 0
"	" 3								
		·	·	+8	+2	·	·	+2	= 12
"	" 4								
		+5	+1	+8	·	+6	+3	+2	= 25
"	" 5								
		·	·	·	·	·	·	+2	= 2
"	" 6								
		+5	·	·	·	+6	·	+2	= 13
"	" 7								
		+5	+1	+8	+2	+6	+3	+2	= 27 = 1
"	" 8								
		+5	·	+8	·	·	·	+2	= 15
"	" 9								
		·	+1	·	·	+6	+3	+2	= 12
"	" 10								
		+5	·	+8	+2	+6	+3	+2	= 26 = 0
"	" 11								
		·	+1	·	·	·	·	+2	= 3
"	" 12								
		·	+1	+8	·	·	+3	+2	= 14
"	" 13	R	N	J	B	B	L		
		+5	+1	+8	+2	+6		+2	= 24
"	" 14								

verme (per gli alfabeti segreti di sostituzione vedi Tav. 1)

Componente X della chiave interna

+ piolino in posizione attiva
· " " " inattiva

Possiamo ora renderci conto, nella Tavola 3, di come è stata generata la porzione di verme che ha cifrato il testo riportato nella Tavola 2.

Per quanto riguarda la chiave esterna, abbiamo già visto che essa era costituita dall'allineamento impostato dall'operatore prima di iniziare la cifratura, nel corso della quale i 6 rotori avanzavano simultaneamente di un passo alla volta. Poiché un giro completo di ciascuno dei 6 rotari comportava un numero di passi diverso: 26, 25, 23, 21, 19, 17, un allineamento impostato all'inizio si ripresentava identico solo dopo 26 x 25 x 23 x 21 x 19 x 17 = 101 405 850 passi simultanei dei 6 rotori (vedi Tavola 2). Questa era dunque la «lunghezza» totale del verme generato dalla chiave interna. Ovviamente, ad ogni chiave interna possibile corrispondeva un verme totale, sempre di quella lunghezza, ma dis struttura (cioé: successione degli alfabeti segreti) sempre diversa.

3.3. - Decrittazione della C38m

3.3.1 - Riprendiamo in esame l'esempio di cifratura riportato nel punto 3.2.1 e nella Tavola 2:

Verme	**(V)**	**23**	**14**	**0**	**12**	**25**	**2**	**13**	**1**	**15**	**12**	**0**	**3**	**14**	**24**
Chiaro	**(C)**	**r**	**i**	**f**	**e**	**r**	**i**	**m**	**e**	**n**	**t**	**o**	**v**	**o**	**s**
SEGRETO	**(S)**	**G**	**G**	**V**	**I**	**I**	**U**	**B**	**X**	**C**	**T**	**M**	**I**	**A**	**G**

Sostituiamo ad ogni lettera il numero che indica la posizione da essa occupata nell'alfabeto ordinato (A = 0, Z = 25, vedi Tavola 1) e riscriviamo il tutto (vedi Tavola 4, sezione I). Constatiamo che ogni lettera segreta può essere ottenuta sottraendo algebricamente, con modalità 26, la lettera chiara dal rispettivo elemento del verme (V-C = S)

27 - 17 = 6, 14 - 8 = 6, 0 - 5 = -5 + 26 = 21,....

2 - 8 = -6 + 26 = 20, etc.

Dunque, l'operazione di cifratura è identica a quella della sopracifratura nel caso dei cifrari numerici descritta nel punto 2.1, con l'enorme vantaggio, per il decrittatore, che in questo caso non esiste codice segreto; anzi si potrebbe addirittura dire che il codice gli è talmente noto che lo conosce tutto a memoria (se è padrone della lingua).

3.3.2 - Stando così le cose, le decrittazioni di due messaggi cifrati con lo stesso verme non è più un problema serio. Infatti, se si può ipotizzare l'esistenza, in uno dei due testi, di parole o frasi «probabili» - come spesso accade specialmente per i tratti iniziale e finali dei messaggi - si può controllare direttamente sull'altro la validità della ipotesi perché (vedi Tavola 4, Sezione II) essendo, come già detto nel punto 2.1, $S_1-S_2 = C_2-C_1$ si ha $S_1-S_2+C_1 = C_1 = C_2$ e $S_2-S_1+C_2 = C_1$.

Di solito sono sufficienti pochi tentativi per avviare una decrittazione che poi può proseguire passo passo senza grandi difficoltà, fornendo contemporaneamente gli elementi della porzione del verme che ha cifrato i due messaggi:

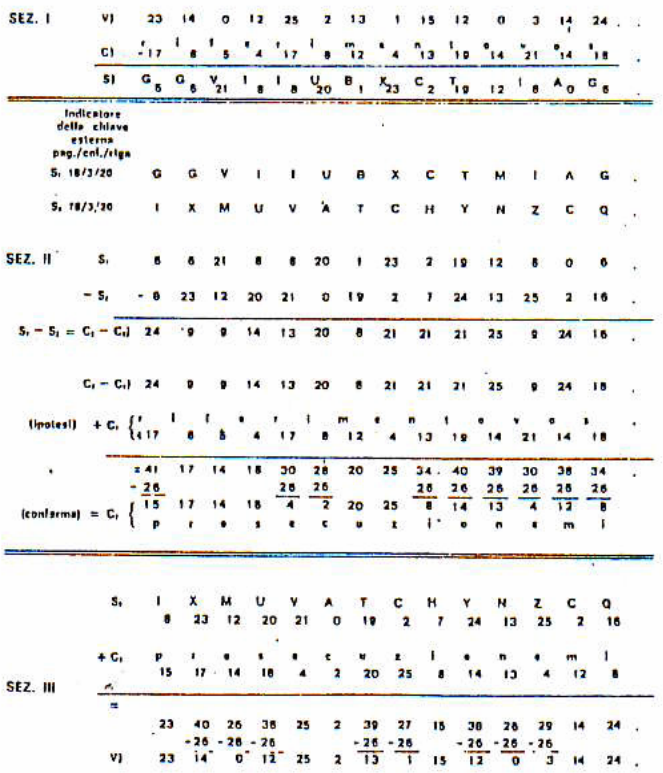
$V-S_2 = C_2$, quindi $S_2+C_2 = V$ (vedi Tavola 4, Sez.III).

3.3.3 - Ultimata la decrittazione (anche se incompleta) dei due messaggi, il decrittatore ha in mano un buon tratto del verme generato dalla chiave interna predisposta dal cifratore. A questo punto, mentre nessuna supposizione sulle rimanenti porzioni del verme sarebbe possibile, in situazione analoga, nel caso di cifrari numerici sopracifrati con vermi casuali o incoerenti (vedi para 2), nel caso della C38m un crittografo abile, se conosceva profondamente la macchina, era in grado di entrare in possesso di tutto il verme (101 405 850 elementi) attraverso la ricostruzione delle componenti W e X delle chiavi interne (vedi Tavola 3) impostando e risolvendo equazioni con un numero di incognite da 1 a 6, oppure empiricamente con reiterati tentativi. Di solito è sufficiente disporre di circa 100 elementi del verme per ricostruire la chiave interna; in casi fortunati possono bastare 40 elementi circa.

Va precisato che il verme così ottenuto dal decrittatore è uguale a quello generato dalla macchina del cifratore ma è «sfasato» rispetto ad esso, nel senso che l'elemento al quale il decrittatore assegna arbitrariamente la posizione 0 (chiave esterna AAAAAA) in realtà occupa nel verme originale una posizione sconosciuta, fra 0 e 101 405 849. Per chiavi interne diverse di sfasamenti saranno, in un primo tempo, diversi ma si riuscirà a mano a mano a ridurli a uno sfasamento arbitrario comune.

Tavola 4

ESEMPIO DI DECRITTAZIONE DI DUE MESSAGGI CIFRATI CON LO STESSO «VERME» E RICOSTRUZIONE DELLA RELATIVA PORZIONE DI «VERME» COL METODO DELLA «PAROLA PROBABILE»



3.3.4 - Una volta in possesso di una chiave interna e quindi di tutto un verme, i crittografi inglesi sarebbero stati in grado di decrittare tutti i messaggi cifrati con quella chiave interna e con qualsiasi chiave esterna senza essere minimamente disturbati dallo sfasamento accennato poco anzi. Ma, data la lunghezza del verme, il numero di prove da fare era così grande che non mi è possibile ora azzardare un giudizio su quale poteva essere il rendimento di tale lavoro, che dipendeva dalla quantità di personale impiegato e, soprattutto, dal sostanziale ausilio di speciali apparec-

chiature «ad hoc» che la tecnologia congiunta anglo-americana era in grado di produrre nel 1941 (5). Comunque, in generale, tali decrittazioni potevano risultare tempestive solo casualmente e certamente il lavoro più redditizio, come quantità e tempestività, era quello di «attaccare» direttamente ogni messaggio ipotizzando l'esistenza di parole o frasi probabili che, se azzeccate, fornivano una porzione di verme di cui non era difficile individuare la posizione occupata nel verme totale, individuare cioè la chiave esterna (fittizia, cioè arbitraria) impostata dal cifratore avversario e quindi decrittare tutto il messaggio.

Nella Tavola 5 è riportato un esempio di determinazione della chiave esterna di un messaggio (S), con chiave interna X e W già nota, partendo dal possesso di un porzione di verme (V) ottenuta ipotizzando il probabile inizio del testo in chiaro (C):

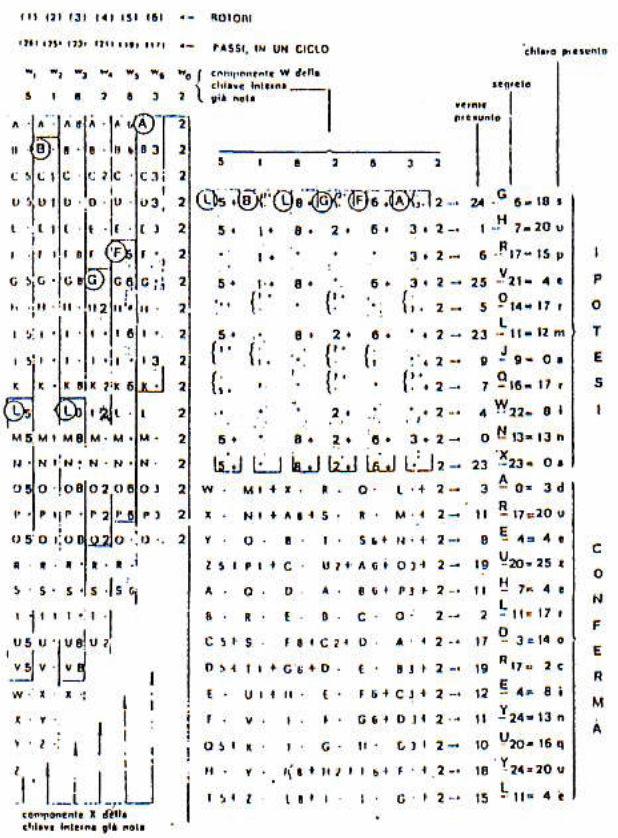
(S)	G 6	H 7	R 17	V 21	O 14	L 11	J 9	Q 16	W 22	N 13	X 23	A R E U H L D R E Y U Y	
+(C)	s 18	u 20	p 15	e 4	r 17	m 12	a 0	r 17	i 8	n 13	a 0		
	24	27	32	25	31	23	9	33	30	26	23		
		-26	-26		-26			-26	-26	-26			
=(V)	24	1	6	25	5	23	9	7	4	0	23		

Può sembrare che con tale metodo la decrittazione sia affidata soltanto al caso; ma se i decrittatori possiedono una profonda esperienza e conoscenza degli argomenti trattati nei messaggi, delle abitudini dei cifratori, del mondo con cui iniziano e terminano di solito i testi, del frasario usato, etc., il metodo anzidetto può divenire quello normale e sistematico e sovente può fruttare anche decrittazioni tempestive.

(5) Lo stesso B.I. accenna più volte all'uso di apparecchiature del genere (le «Bombes», elettromeccaniche; il «Colossus», elaboratore elettronico) nel lavoro di penetrazione del traffico radiocifrato ENIGMA. Del resto anche noi, per accelerare il lavoro contro i cifrari navali inglesi sopracifrati, avevamo realizzato, nel 1942, una modesta apparecchiatura che, utilizzando schede perforate, eseguiva le numerose prove necessarie per individuare quali porzioni di un lungo verme, già da noi ricostruito, avevano sopracifrato altri messaggi non ancora decrittati.

Tavola 5

ESEMPIO DI DETERMINAZIONE DELLA «CHIAVE ESTERNA» ("LBLGFA" POSIZ. 30 002 401) E CONSEGUENTE DECRITTAZIONE DI UN MESSAGGIO CON IL METODO DELLA «PAROLA PROBABILE»



3.3.5 - Il reperimento, nel traffico intercettato, di due o più messaggi cifrati con uguale verme è ovviamente immediato se i «gruppi indicatori» delle chiavi esterne usate non sono «mascherati», come nell'esempio della Tavola 4; altrimenti, ma con maggior lavoro e minor possibilità di successo, si devono ricercare porzioni di cifrato uguali in messaggi diversi, di solito all'inizio e alla fine del testo segreto.

3.3.6 - Se non esistono casi di «reimpiego» di verme, cosa possibile anzi probabile se l'avversario ha impartito oculate norme d'impiego della macchina, non rimane che «attaccare» i messaggi uno alla volta con il metodo delle «parole o frasi probabili» già menzionato, fino a disporre di

tratti di verme abbastanza sicuri e abbastanza lunghi da riuscire a ricostruire le chiavi interne e procedere poi come detto nei punti 3.3.3 e 3.3.4.

3.3.7 - Per concludere, da quanto finora esposto, si evince che la macchina cifrante C38m offriva possibilità di penetrazione incomparabilmente maggiori di quelle offerte dal sistema cifrari navali/sopracifratura descritto nel paragrafo 2.

3.4. - L'uso della C38m da parte della Marina italiana durante il conflitto

3.4.1 - Si tenga presente che, la scelta, la produzione, la regolamentazione la distribuzione dei sistemi di cifratura e il controllo sul loro impiego non erano compiti del SIS - Servizio crittografico, bensì del Reparto Telecomunicazioni (TLC). Il servizio crittografico forniva solo consulenze quando ne era richiesto ma, mentre so con certezza che ciò accade e fu determinante per la sicurezza del complesso «cifrari-sopracifratura» del periodo bellico, ignoro se e in quale misura ciò sia avvenuto per la C38m.

Tavola 6

QUANTITA' DI CHIAVI ESTERNE ASSEGNATE AI VARI COMANDI

2ª Edizione in vigore dal marzo 1942		R.P.	3ª Edizione (aprile 1942) in vigore dal maggio/giugno 1942	
Supermarina e M.M.	3 500	300	Supermarina	1 200
Reparto Comunicazioni		200	Reparto Comunicazioni	1 800
Com. FF.NN. e Com. 1ª Sq.	500	100	Com. FF.NN. e Com. 1ª Sq.	300
Com. 2ª Sq. e Com. 5ª Div.	300	100	Com. 2ª Sq. e Com. 5ª Div.	200
Com. 3ª Div.	200	100	Com. 3ª Div.	100
Com. 7ª Div.	200	100	Com. 7ª Div.	100
Com. 8ª Div.	200	100	Com. 8ª Div.	100
Com. 9ª Div.	200	100	Com. 9ª Div.	100
Marina Napoli	200	100	Marina Napoli	200
» Taranto	200	100	» Taranto	200
» Messina	200	100	» Messina	200
» Brindisi	200	100	» Brindisi	00
» Albania	500	100	» Albania	500
» Morea	1 500	100	» Morea	1 200
» Sud est	800	100	» Sud est	800
» Egeo	800	100	» Egeo	1 200
» Lero	300	100	» Lero	600
» Libia	2 000	100	» Libia	1 500
» Tripoli	1 000	100	» Tripoli	800
» Bengasi	500	100	» Bengasi	800
» Tobruk	—	100		
Riserva	1 700	600	Riserva	2 900
Totale	15 000	3 000	Totale	15 000

3.4.2 - Secondo gli elenchi di distribuzione contenuti nei documenti tuttora reperibili le autorità dotate della C38m erano pochissime (6): Solo Alti Comandi a terra e a bordo (vedi Tavola 6 e para 3.4.5), nessuna unità singola di superficie o subacquea.

3.4.3 - Il numero astronomico, intorno ai ventilioni, delle possibili chiavi interne diverse offriva, in teoria, ottime garanzie di sicurezza che però in pratica non potevano essere sfruttate appieno perché la impostazione delle chiavi interne era così delicata, laboriosa e lunga (si pensi che per la sola componente X si dovevano manipolare 131 piolini) che si dovette rinunciare a cambi frequenti come sarebbe stato desiderabile. Perciò all'inizio si stabilì di usare chiavi interne comuni a tutti gli utenti e di cambiarle ogni mese. Questa norma, in vigore almeno fino a tutto il 1942, ma probabilmente fino all'armistizio, era certamente accettabile nel primo periodo del conflitto, con traffico radio C38m non inteso (B.I. dice: nel mese di agosto 1941, 600 messaggi) (7), ma, a mio parere, fu imprudente mantenerla quando quel traffico stava acquistando intensità sempre crescente (B.I. dice: 4000 messaggi nel mese più denso, luglio 1942). In quella situazione fu preferito aumentare il numero delle chiavi esterne a disposizione, passando da 18 00 a circa 40 000.

3.4.4 - Era stato giustamente percepito che il pericolo maggiore stava nel «reimpiego» dei vermi, cioè due o più passaggi cifrati, nello stesso mese, con la stessa chiave esterna; perciò questo fu tassativamente proibito e a ciascuna delle autorità depositarie della C38m furono assegnate serie di chiavi non usabili dalle altre autorità.

Naturalmente non posso escludere che vi sia stata qualche trasgressione alle norme, ma deve essersi trattato di casi del tutto eccezionali, dato il numero delle chiavi esterne a disposizione. Nella Tavola 6 è riportato il prospetto numerico delle assegnazioni delle chiavi esterne nella 2ª e 3ª edizione delle cosiddette «Tabelle delle chiavi esterne per macchina cifrante». Della 1ª edizione non ho

---

(6) Pochissime, in confronto col numero di utenti del cifrario navale generale sopracifrato, che era assegnato anche a quasi tutte le unità navali e ai Comandi Marina minori.

(7) B.I., vol.2°, pag.283.

trovato traccia.

Questi quantitativi erano, a mio parere, oculatamente commisurati alla prevedibile intensità del traffico radio C38m di ogni mese, cioè nell'ambito di una data chiave interna.

3.4.5 - Fin qui, tutto bene; ma vediamo come erano state scelte le chiavi esterne e poi vedremo in che modo veniva indicata, in ogni messaggio, la chiave usata.

Come abbiamo visto nel paragrafo precedente, le chiavi esterne teoricamente possibili erano 101 405 850, ma ci si doveva giustamente preoccupare di evitare che la porzione iniziale di un messaggio potesse casualmente venire cifrata con il tratto di verme che aveva, o avrebbe poi, cifrato la «coda» di un altro messaggio, per non fornire all'avversario un reimpiego, sia pure parziale, di verme. A tal fine, poiché era prescritta per ogni messaggio una lunghezza massima di 500 lettere, si dovevano distanziare le chiavi esterne nel verme totale, generato dalla chiave interna, di un numero di elementi maggiore di 500. Per non ridurre troppo la quantità di chiavi disponibili sarebbe stato largamente sufficiente un distacco medio di circa 1 000 elementi, che avrebbero ridotto in maniera non preoccupante il numero delle chiavi esterne possibili, cioè circa 100.000 (101 405 850 : 1 000.

Fu invece scelto un distanziamento maggiore, che riduceva a circa 40 000 le chiavi esterne disponibili. Evidentemente si pensò, con qualche fondamento, che quel numero era più che sufficiente per coprire le esigenze di un mese. La riduzione predetta non avrebbe recato sensibile vantaggio ai crittografi inglesi perché, una volta ricostruita attraverso fortunate descrizioni la chiave interna del mese, per individuare la chiave esterna di ogni altro messaggio nello stesso mese, avrebbero ugualmente dovuto «provare» tutti i circa cento milioni di possibili chiavi esterne. Ho usato il condizionale perché, purtroppo, nella nostra pianificazione il distanziamento fra le chiavi fu stabilito in un numero fisso di elementi: 2497. Stando così le cose, l'avversario, dopo aver individuato, attraverso qualche decrittazione di messaggi intercettati in un certo mese, alcune chiavi esterne (arbitrarie), poteva constatare che esse erano tutte distanziate fra loro, nel verme totale, di un multiplo di 2497

(8) e a questo punto aveva la possibilità di individuare, con un semplice calcolo, tutte le 40 611 chiavi esterne (arbitrarie) previste nella nostra pianificazione, riducendo così di circa cento milioni a solo circa 40 000(nel caso peggiore) (9) le «prove» da fare per decrittare ogni altro messaggio del mese (10).

Non posso pensare che ai crittografi inglesi sia sfuggita questa imprudente particolarità della nostra pianificazione, devono essersene accorti abbastanza presto e ne hanno certo tratto gran vantaggio per decrittare quei messaggi, ritenuti importanti, che avevano resistito all'attacco diretto con il metodo delle parole o frasi probabili (vedi punto 3.3.5).

3.4.6. - E veniamo ai «gruppi indicatori», come primo e ultimo gruppo del messaggio segreto per indicare al destinatario quale chiave esterna aveva impostato nella macchina prima di iniziare la cifratura di quel messaggio.

I fascicoli che contenevano le «Tabelle delle chiavi esterne» avevano un certo numero di pagine, ripartite fra i vari utenti in base al quantitativo di chiavi a ciascuno assegnate (vedi Tavola 6). Ogni pagina conteneva, disposte su righe e colonne, un certo numero di chiavi prese a caso, senza mai ripeterle, fra le 40 611 della pianificazione. Il cifratore sceglieva ogni volta, in una delle pagine di sua

---

(8) Vedi Tavola 7, in cui sono riportate alcune «chiavi esterne» prese a caso dalle nostre Tabelle delle «chiavi esterne» in uso nel 1941/'42, con le rispettive posizioni nel verme totale, le distanze parziali e le rispettive scomposizioni in fattori primi.

(9) In realtà, poiché il decrittatore non conosceva la posizione, nel verme originale, a partire dalla quale essa stata sviluppata la nostra pianificazione delle 40 611 chiavi a passo 2 497, e poiché 101 405 850 non è multiplo di 2 497, le prove da fare, in un primo tempo, erano circa 80 000 nel caso peggiore, ma presto - a mano a mano che si allargava il campo delle chivi identificate - le prove diminuivano fino a ridursi, nel caso peggiore, a un massimo di circa 40 000.

(10 Qualcosa di simile accadde anche nel nostro lavoro contro i cifrari navali inglesi sopracitati: ci accorgemmo che i vermi prelevati da uno stesso blocco di tabelle di sopracifratura erano distanziati fra loro sempre di un multiplo di 20 elementi (5 quadricifre). Così potemmo ridurre dell'80% le prove da fare.

pertinenza, la chiave da usare e la «smarcava» a matita per evitarne un secondo impiego prima di aver smarcato tutte quelle a sua disposizione. Ultimata la cifratura del messaggio, poneva come 1° e ultimo gruppo del testo segreto un «gruppo indicatore» che, attraverso apposito indice (cioè non in modo esplicito come per semplicità abbiamo posto nell'esempio della Tavola 4, Sezione II), forniva al destinatario pagina, colonna e riga di appartenenza della chiave scelta.

Con tale procedimento è ovvio che solo chi possiede i predetti fascicoli segreti era in grado di interpretare i gruppi indicatori, conoscere cioè le chiavi esterne impiegate nei messaggi. Con una certa imprudenza, fino all'autunno 1942, i gruppi indicatori furono usati senza «mascheratura» di modo che, per l'avversario, gruppi indicatori uguali significavano chiavi esterne uguali. Questa imprudenza, analoga a quella, che si rilevò ben più pericolosa, commessa dagli Inglesi nella sopracifratura dei loro cifrati navali (vedi para 2.3, comma e.), fu probabilmente dovuta all'affidamento posto nella rigida ottemperanza delle norme che vietavano tassativamente il reimpiego delle chiavi. Comunque, vediamo quali potevano essere le conseguenze, a vantaggio dei crittografi inglesi, della «non mascheratura» dei gruppi indicatori. Distinguiamo vari casi:

- a) gruppi indicatori usati una sola volta. Nessuna utilità per i decrittatori;

- b) gruppi indicatori usati due volte in un dato periodo di validità della chiave interna (cioè nel mese). Era il classico caso di due messaggi cifrati con lo stesso verme: conseguenze gravissime (vedi punti da 3.3.2 a 3.3.5 e Tavola 4). Tuttavia, ripeto, un evento del genere non doveva verificarsi e, se eccezionalmente è accaduto, non giustifica, a mio parere, la penetrazione sistematica e tempestiva affermata da B.I.;

- c) gruppi indicatori usati due volte ma in mesi diversi, cioè con chiavi interne diverse e quindi non con lo stesso verme. Questo evento, anche esso vietato dalle norme, poteva eccezionalmente verificarsi a distanza di mesi per esaurimento delle chiavi assegnate ad un dato utente (ma erano previste chiavi di riserva, vedi Tavola 6). Poteva essere di qualsiasi utilità, se i due messaggi venivano decrittati, per fissare fra loro i vermi totali relativi alle

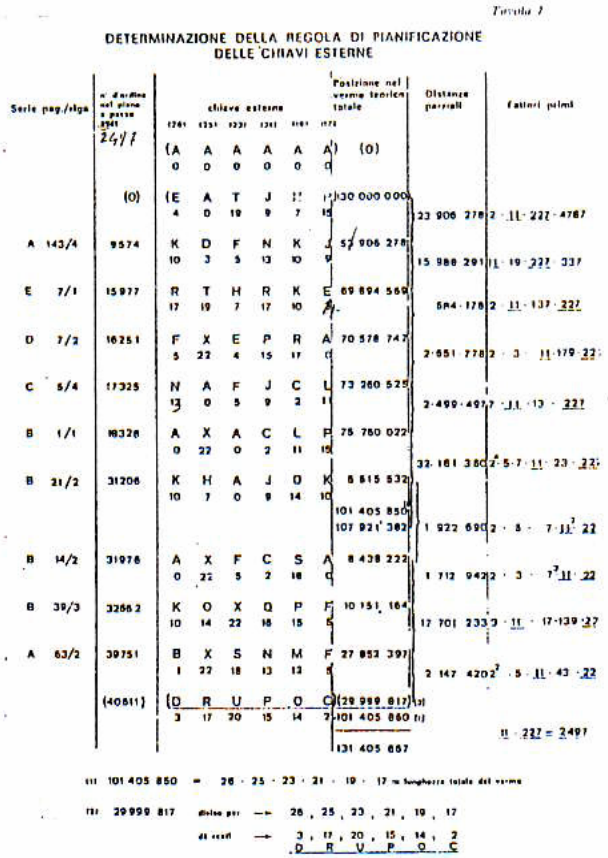


Tavola 3

DETERMINAZIONE DELLA REGOLA DI PIANIFICAZIONE DELLE CHIAVI ESTERNE

Serie pag./riga	n. d'ordine nel piano a passo 2441	chiave esterna (1261 1351 1221 1241 1161 1171)	Posizione nel vortice teorico totale	Distanze parziali	Fattori primi
	2411	(A A A A A A) (0)			
		0 0 0 0 0 0			
	(0)	(E A T J I I)	(30 000 000)		
		4 0 19 9 7 15		23 906 278	2 · 11 · 227 · 4787
A 143/4	9574	K D F N K J	53 906 278		
		10 3 5 13 10 9		15 988 291	11 · 19 · 227 · 337
E 7/1	15977	R T H R K E	69 894 569		
		17 19 7 17 10 5		584 178	2 · 11 · 137 · 227
D 7/2	16251	F X E P R A	70 578 747		
		5 22 4 15 17 0		2 651 778	2 · 3 · 11 · 179 · 22?
C 5/4	17325	N A F J C L	73 260 525		
		13 0 5 9 2 11		2 499 497 ?	11 · 13 · 227
B 1/1	18328	A X A C L P	75 760 022		
		0 22 0 2 11 15		32 161 380	2² · 5 · 7 · 11 · 23 · 227
B 21/2	31206	K H A J O K	8 815 532		
		10 7 0 9 14 10			
			101 405 850		
			107 921 382	1 922 690	2 · 5 · 7 · 11² · 22
B 14/2	31978	A X F C S A	8 438 222		
		0 22 5 2 18 0		1 712 942	2 · 3 · 7² 11 · 22
B 39/3	32862	K O X Q P F	10 151 164		
		10 14 22 16 15 5		17 701 233	3 · 11 · 17 · 139 · 227
A 63/2	39751	B X S N M F	27 852 397		
		1 22 18 13 12 5		2 147 420 ?	2² · 5 · 11 · 43 · 227
	(40811)	(D R U P O C)	(29 999 817) (3)		
		3 17 20 15 14 2	101 405 850 (1)		
			131 405 667		11 · 227 = 2497

(1) 101 405 850 = 26 · 25 · 23 · 21 · 19 · 17 = lunghezza totale del verme

(3) 29 999 817 divisa per → 26 , 25 , 23 , 21 , 19 , 17

di resti → 3 , 17 , 20 , 15 , 14 , 2
D R U P O C

due chiavi interne ricostruite (vedi punto 3.3.3) e poi sfruttare meglio altri eventuali reimpieghi di gruppi indicatori fra i due mesi interessati.

Con l'edizione delle «Tabelle delle chiavi esterne» entrata in vigore il 1° ottobre 1942 fu introdotta finalmente una buona procedura per mascherare i gruppi indicatori. Ciò fa pensare che nell'estate 1942, periodo di massima intensità del traffico radio C38m, qualche trasgressore alle norme sia realmente avvenuta e sia stata constatata dal servizio di controllo esercitato dal reparto Comunicazioni dello Stato Maggiore Marina. Si dovrebbe anche dedurre che trasgressori preoccupanti non ve ne siano state in precedenza, se con le edizioni entrate in vigore nel marzo e maggio/giugno 1942 fu mantenuta la «non mascheratura» dei

gruppi indicatori.

3.4.7. - I testi in chiaro dei messaggi segreti

Qui stava, a mio parere, un altro punto debole del nostro traffico radio C38m, forse quello che - dopo una laboriosa e fortunata penetrazione iniziale - ha progressivamente agevolato sempre più i decrittatori inglesi, a mano a mano che acquistavano esperienza e conoscenza degli argomenti e del modo in cui essi venivano trattati nei messaggi. Inizi e finali stereotipati, abitudini dei cifratori, ed altro, devono aver permesso ai decrittatori di azzardare, spesso con fondamento, parole e frasi probabili, come ho accennato nel punto 3.3.2, per «attaccare» messaggi singoli senza bisogno di attendere i reimpieghi di verme, forse veramente rarissimi. Nei periodi di massima intensità del traffico radio questo può essere stato il modo più generalizzato per penetrare largamente le nostre comunicazioni C38m.

3.5. - La penetrazione inglese nella C38m della Marina italiana

3.5.1. - La C38m, come le altre macchine HAGELIN che da due decenni l'avevano preceduta nel mercato non era sconosciuta per gli inglesi.

Quella ditta era svedese, con fabbrica a Stoccolma, e il suo titolare, uomo d'affari anch'esso svedese subito dopo l'occupazione nazista della Norvegia aveva raggiunto gli Stati Uniti d'America, piazzando subito una cinquantina di esemplari presso le FF.AA. americane. Già nel 1935, come detto nel parag.3.1., aveva largamente fornito le FF.AA. francesi. La macchina doveva dunque essere ben nota agli Inglesi che non avranno mancato di studiarla attentamente dal punto di vista della sicurezza crittografica.

C'è da supporre con fondamento che, data l'alleanza con la Francia e gli stretti legami con gli Americani, qualche esemplare molto simile alla C38m fosse già nello loro mani all'inizio del conflitto.

Nonostante questa situazione decisamente vantaggiosa gli Inglesi, dopo avere constatato l'uso della C38m nelle comunicazioni radio segrete della Marina italiana, per ben se mesi, dal dicembre '40 al giugno '41, non ottennero alcun risultato.

3.5.2. - Vediamo cosa dicono gli Inglesi. Nel 2° volume del B.I. a pag.22 si legge:

«La C38m italiana, intercettata per la prima colta nel dicembre 1940, fu penetrata a partire dall'estate 1941» e a pag.283-284:

«Per la fine di giugno 1941 furono ricostruite le chiavi interne della C38m per i mesi di maggio e giugno e furono letti un po' di messaggi attuali. La prima intelligence da quella fonte per il Medio Oriente fu inviata il 23 giugno 1941. (...omissis) Per il 10 luglio furono ricostruite le chiavi interne di luglio, dopodiché si andò avanti fino all'armistizio decrittando regolarmente (with routine) con poco o nessun ritardo e con interruzioni progressivamente sempre più brevi alla fine di ogni mese, quando gli Italiani introducevano nuove chiavi interne, ma con interruzioni più serie in una o due occasioni durante il 1942. Verso la fine del 1941 le interruzioni mensili furono ridotte a meno di tre giorni e verso la fine del 1942 a meno di 24 ore».

Dunque, fra dicembre '40 e giugno '41;
- a) non ci sono stati casi di reimpiego di vermi, cosa verisimile dato il tassativo divieto della nostra regolamentazione, specie in rapporto al non ancora intenso traffico C38m; oppure
- b) se c'è stato qualche reimpiego, gli Inglesi non hanno saputo sfruttarlo, cosa poco verosimile;
- c) non avendo decrittato messaggi, i crittografi inglesi non hanno ancora acquisito né l'esperienza tale da poter applicare con successo il metodo delle «parole e frasi probabili» (vedi punti 3.3.4 e 3.3.6) né la conoscenza del punto debole della nostra pianificazione delle chiavi esterne (vedi punto 3.4.3).

Nonostante tutto ciò, a fine giugno '41 gli Inglesi hanno «sfondato» la C38m in maniera tale da poter ricostruire anche le chiavi interne del mese precedente, ricostruite in 10 giorni le chiavi interne di luglio e da quel momento iniziare una decrittazione sistematica e tempestiva, addirittura «with routine», tanto da «dare dal luglio 1941 in poi notizie in anticipo di praticamente ogni convoglio o nave isolata che partivano con truppe e rifornimenti attraver-

so il Mediterraneo, identificando di solito le navi di scorta coinvolte» (11).

Quale improvvisa folgorazione ha illuminato le menti dei crittografi inglesi sul finire della primavera 1941? Francamente un così rapido e sostanziale salto di qualità e di quantità mi lascia perplesso.

Si deve pensare che nella primavera del 1941 sia accaduto qualcosa che ha aiutato in modo sostanziale gli inglesi a "sfondare" la nostra C38m. Soltanto il Naval Intelligence britannico potrebbe rivelare che cosa accadde.

4. CONCLUSIONE

Da quanto ho esposto si conferma, a mio parere, che nel 2° conflitto mondiale il servizio crittografico della Marina italiana - sotto l'aspetto strettamente tecnico e tenuto conto dei diversi gradi di difficoltà e di vulnerabilità dei sistemi contrapposti - non ha avuto nulla da invidiare a quello britannico. Tutt'altro.

Tengo però a precisare che la valutazione semplicistica sopra riportata non ha valore assoluto nei riguardi del confronto con i nostri avversari di allora, perché non dimentico la vasta ed efficiente penetrazione inglese nelle radiocomunicazioni cifrate con la ENIGMA tedesca, problema che presentava un grado di difficoltà ben più alto che non con la C38m. Mi mancano, per ora, elementi sufficienti per trattare criticamente quell'interessante argomento.

LUIGI DONINI

(11) B.I. vol. pag.284.2