~~TOP SECRET~~

CSDIC(MAIN)/

DISTRIBUTION

	Copy Nos
AC of S, G-2, AFHQ..........	1
G-2 (Sigs "I"), AFHQ........	2 - 4
G-2 (PW) AFHQ..............	5
GSI (s), AAI................	6
GSI 8, MEF.................	7
MI 8, UK....................	8 - 10
File........................	11 - 15

Of interest to Rumanian dipl + M. A. people.

NY-4

~~TOP SECRET~~

CSDIC(Main)/ 12.

N1
N14

FIRST DETAILED INTERROGATION OF VASSALLO TODARO, Giuseppe

Rank :	Lt. Col
Unit & Function:	SIM Cryptographic Section: Head of Rumanian Group in Diplomatic Sub-Section (till Armistice)
Interrogated :	CSDIC, CMF, 29 Oct 44

Subject of Report: Rumanian Diplomatic Codes and Ciphers

1. PREAMBLE.

Source is a 49 year old Sicilian, a regular artillery officer, who joined SIM Cryptographic Section in 1934. He speaks Rumanian, and was responsible for all work done by the Diplomatic Sub-Sec on Rumanian diplomatic codes and ciphers. When the Armistice was declared he went into hiding to avoid being forced into the SID

Reliability: Fairly good

2. RUMANIAN DIPLOMATIC CODES AND CIPHERS (till Armistice)

(a) Traffic passed

Source stated that Rumanian diplomats always had the habit of "talking a lot". Traffic was especially heavy when TITULESCU was Foreign Minister, and particularly when he was head of the League of Nations Assembly.

Military Attache traffic was more restricted in volume before the war, but during the war mil attaches also sent a large number of telegrams. During the war also LISBON traffic provided a good deal of useful info (SIM Crypto Sec being able to read it), as the Rumanian Minister there used to rely to all his conversations with foreign diplomats.

(b) General methods of handling codes and ciphers

Although the systems employed and the frequent changes in systems provided for fairly good security, cipher clerks were poor, the pre-war PARIS Legation clerks being the worst. Often BUCHAREST would ask for a telegram to be repeated as it could not be read.

Encoding and enciphering of texts in Rumanian was done without regard to the phonetic rules peculiar to the language, except in the case of "T" cedilla, which was spelt "TZ". The sound "SH", represented by "S" cedilla, and the vowels derived from "A" i.e., the "A" circumflex and the "A" with short vowel sign, were encoded or enciphered as "S" and "A" respectively.

(c) Diplomatic Codes.

Source confirmed BIGI's statement in CSDIC/CMF/Y 4, para.3.D.I.c, that SIM succeeded in reading all codes in use up to the time of the Armistice, photostat copies of each code being available. Codes were of the five-figure type, and several would be used at one and the same time, the most recent ones being employed for traffic of greater security value.

Recipher was used except where messages were not considered important. All Embassies and Legations used the same codes, only there were some, such as the HELSINKI Legation, not an important one, which had fewer books in use. The same applied to the diplomatic agencies in LONDON, WASHINGTON and MADRID during the war (1939-1941), when traffic was on a more reduced scale.

The recipher tables were built up on the principle of single substitution of digits ("inversione di numeri"). Each recipher table was allotted a number, which was given in the key group at the beginning of the massenigram.

Example: With recipher table:

CODE DIGITS	1	2	3	4	5	6	7	8	9	0
RECIPHER	2	4	6	7	3	0	8	9	1	5

recipher code groups:
10960 26700 56091 etc.

Encodigram text reads:
29105 40855 30512 etc.

Subtraction or addition recipher tables were NOT used. If telegrams were long, the clear text would be encoded in several codes and reciphered by means of several tables. Marconigram would still contain one key group, the use of a different code and recipher being notified in the text.

(d) Military Attaches' Codes and Ciphers.

Traffic between Mil Attaches and General Staff at BUCHAREST was in transposition cipher and five-figure code - of a more elaborate construction than the Diplomatic codes - with recipher tables.

(i) The "Memory Cipher" ("Cifrul de Memorie")

This was a transposition cipher system with 6 boxes of 6 x 5 small squares of which the clear text was written in after a certain pattern. If a message was, for example, 180 letters long, or more, the first 60 letters were written in the squards as shown by arrows 1-24 in App "A". The remainder of the letters was written in the other 120 free spaces from top to bottom, column by column (NB, or possibly also from bottom to top). The enciphered text was read off in groups of five from left to right line after line. If the text was shorter than 180 letters - which rarely happened - the first 60 letters were placed in position as above, and the remainder filled it, then read off line after line.

This cipher was used by the Rumanian Military Mission in ITALY, which had its main offices at MILAN, and one or two officers in ROME.

(ii) A Cipher on the lines of the"RASTERSCHLUESSEL".

An underlay was used for six months. It consisted of a large rectangle of 14 spaces across and 20 spaces down, subdivided into four equal rectangles of 7 spaces across and 10 spaces down. Some spaces were cancelled, on the pattern of cross-word puzzles. The clear text was written in, along a certain pattern, as may be seen from the suggested example at App. "B". The pattern varied from message to message and was indicated to the addressee by means of a key group.

Source could not remember if the lines were numbered; he thought that only the columns were numbered, consecutively from 1 - 14, and that the key group gave the column from which enciphering started, along a pattern drawn on the trace used in conjunction with the underlay.

(iii) Five-figure Code

This code was used by Mil Attaches and possibly by the Rumanian Mil Mission as well, in 1942-43. Various systems of recipher were used, two of which were remembered by Source in some detail. Source considered both the code and the recipher harder to break than the Diplomatic codes.

The five-figure code consisted of a book (size not given) in which each page was numbered by means of one of the four three-figure groups printed at the top. The page was divided into two parts, each part containing 5 blocks of 10 groups each. There were alternative groups for the same clear letter or word (words more commonly used). Inside each block of ten, the clear text was arranged in a quasialphabetic order and each group was indicated by means of a block-digit (common to all ten groups in the block), and a second digit which identified the group itself within the block. See APP. "C".

The earlier system of reciphering this code was known as "fise" (pronounced "FISHE"), whereby small cards or tables of conversion of figures were placed alongside the code-group columns (in App "C" columns 1 & 2 and 4 & 5) to enable the encoding or decoding clerk to read off the equivalents of the block and code-group digits.

This was replaced later by the following system:

The encoded version of any telegram was written on a form containing a number of rectangles, as illustrated in App "D". Each rectangle had 10 spaces across and 5 down. Five-figure groups would be written out in columns, from bottom to top according to a certain key, which changed every six months. The reciphered version of the telegram would then be copied out in groups of five, line after line. No key group was contained in the marconigram.

A.G.B.

F.G. ADAMS, CAPT.

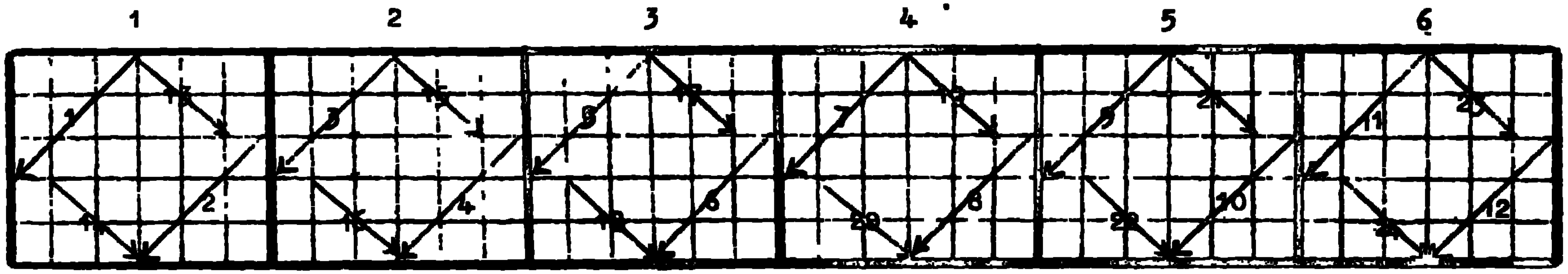
for (R.P.F. EDWARDS)
Lt. Col.
Comdt.CSDIC(MAIN)
CMF.

C.S.D.I.C.,(Main)
C.M.F.,
9 Nov. 44.

APPENDIX "A"

RUMANIAN MILITARY ATTACHES' CIPHER ("MEMORY CIPHER - "CIFRUL DE MEMORIE") TOP SECRET
(See para 2.d.i. of att report)

CSDIC/Main)/X 12.



ENCIPHER: FOR GENERAL GHEORGHE SECOND SECTION I HAVE THE HONOUR TO INFORM YOU THAT THE LARGE SCALE MAPS YOU DESPATCHED LAST WEEK HAVE NOT ARRIVED YET STOP MAPS ARE URGENTLY REQUIRED STOP GERMAN STAFF REFUSE TO LEND ME MAPS X POPA

[illegible]	A	F	T	M		T	H	E	O	[illegible]	L	V	T	E	R	E	T	A	I	S	N	Y	[illegible]	F	[illegible]	S	N	T	F	U	L	N	T	I	P
[illegible]	O	[illegible]	I	H	[illegible]	E	R	H	L	N	K	[illegible]	O	R	E	T		I	E	R	N	F	U	I	E	E	H	Y	R	S	I	N	E	H	O
R	[illegible]		I	R	G	A	T	L	P	[illegible]	L	R	A	I	U	T	G	C	E	[illegible]	T	R	O	C	I	S	N	R	T	H	L	U	M	[illegible]	R
	E	[illegible]	I	E	[illegible]	[illegible]	O	D		G	H	N	O	Y	Y	H	T	[illegible]	O	F	[illegible]	N	T	[illegible]	O	M	[illegible]	I	E	E	A	N	A	V	F
I	[illegible]	H	N	[illegible]	[illegible]	[illegible]		U	H	[illegible]	[illegible]	[illegible]	R	I	E	S	N	A	[illegible]	R	D	[illegible]	R	T	G	U	O	F	F	[illegible]	E	T	E	A	H

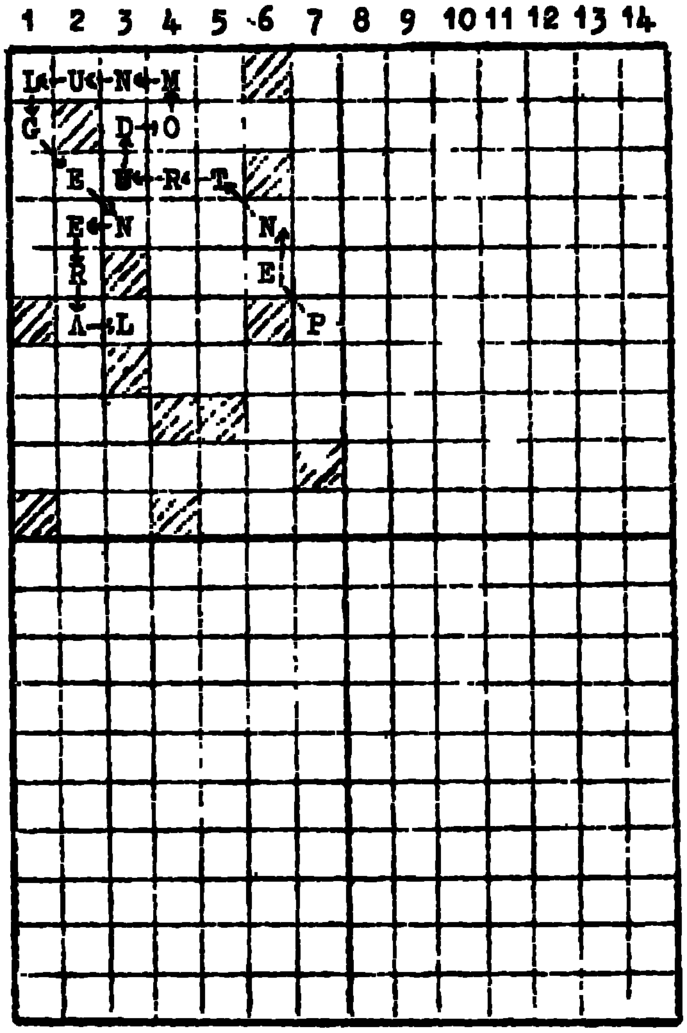
MARCONIGRAM READS: TAFTM SDAEO TEVTE RETAR SNYQE OSMTF UONTP PHOEA HYERH LNKEO RETOP ERNFU DEEAY RSINE HORRS LAGAT EAWLR AIDTG CEGTR OCPRN ATHLD MSAEE CEEOS ODSGH NOVYH PSOEL NISOM SIEEA MAVPL GHMPU POUHE AORIE. SMAUR DERTG UOFFT ETEXA

APPENDIX "B"

~~TOP SECRET~~

CSDIC(Main)/Y 12.

RUMANIAN MILITARY ATTACHES' CIPHER
(cf para 2.d.ii. of att report)



CLEAR TEXT:

PENTRU DOMNUL
GENERAL

ENCIPHERED:

LUM[illegible]/...../.etc.

1. The underlay was changed every six months.

2. Each telegram was enciphered on a different pattern, indicated by a key-group

~~TOP SECRET~~

CSDIC(Main)/Y 12.

APPENDIX "C"

RUMANIAN MILITARY ATTACHES' FIVE-FIGURE CODE PAGE
(cf para 2.d.iii. of att report)

989 '- 456 - 325 - 049

8	9	A			
	8	a			
	7	a			
	6	ANASTASIU			
	5	AM			
	1	.			
	3	.			
	2	.			
	4	.			
	0	.			
6	7				
	6				
	3				
	2				
	0				
	8				
	5				
	9				
	1				
	4				

```
      88         88         88         88
A = 98989  or  45689  or  32589  or  04989
      87         87         87         87
```

TOP SECRET

CSDIC(Main)/Y 12.

APPENDIX "D"

MILITARY ATTACHES' RECIPHER TABLE, CHANGED EVERY SIX MONTHS

EXAMPLE:

RECIPHER: 34750 04357 87549 67835 86003 73521 33269 43584 98989 04962

9	0	1	2	3	8	5	6	4	7	RECIPHER KEY
1	2	3	4	5	6	7	8	9	0	
9	5	3	9	9	4	2	1	0	7	
4	3	0	8	6	8	6	2	5	5	
5	8	0	9	2	5	9	5	7	3	
7	7	6	8	3	3	4	3	4	4	
8	6	8	9	3	4	0	7	3	0	

MARCONIGRAM READS: 95399 42107 43086 86255 58092 59573 77683 34344 86893 40730

Marconigram did NOT contain key-group.