

**FIRST DETAILED INTERROGATION OF
BIGI, Augusto**

Name: BIGI, Augusto
Rank: Capt (Italian Army)
Unit: Cryptographic Sec of SIM (later of SID)
Interrogated: OSDIC, CMF, 8 Sep 44

1. PREAMBLE

Source is 36 yrs old. He was formerly employed as an engineer by the Italian Ministry of Communications in ROME. He did mil service in the Artillery from 1930-31 and from 1935-36. During the war he was employed by the Cryptographic Sec of SIM (SERVIZIO INFORMAZIONI MILITARI) and after the Armistice (8 Sep 43) worked for the same sec of SID (SERVIZIO INFORMAZIONI DIFESA). He supplied info voluntarily.

Function: Cryptographer Reliability: Good

2. HISTORY AND MOVEMENTS

1 Nov 39 Sent to Cryptography Course at War Ministry.
10 May 40 Joined Cryptographic Sec of SIM at 48, Via POLE, ROME.
1 Jul 41 Promoted Capt.
21 Jan 42 Sent to BERLIN with Col COSMACINI (see App "A") to study orgn of German CHI ABTEILUNG and the use of HOLLERITH machines.
22 Feb 42 Returned to ROME.
23 Dec 42 Sent to BERLIN again to find out more about German methods and to negotiate for the purchase of HOLLERITH machines.
end Dec 42 Ordered back to ROME by the Germans.
10 Sep 43 SIM disbanded. Source returned to Ministry of Communications in ROME.
7 Oct 43 Ordered to report back to SIM. Reported to Dr FOSCHINI, who had taken over the Cryptographic Sec. Sent to SIM HQ at PADUA.
28 Oct 43 SIM renamed SID.
2 Nov 43 Sent with all other SID offrs to NOGARA (Province of VERONA).
beg Dec 43 Joined Cryptographic Sec of SID at CASTIGLIONE DELLE STIVIERE (F 2650 - ITALY 1:250,000 Northern ITALY Zone) where it had its offices in the LYCEO GIMNASIO and the SCUOLE AVVENIMENTO PROFESSIONALE.
25 Feb 44 Section ordered by Germans to stop all activities.
5 Apr 44 Asked to joined Republican Army. Refused.
15 Apr 44 Dismissed from SID and told to report to Regional Command at PADUA.
2 May 44 Visited CASTIGLIONE DELLE STIVIERE to collect his luggage. SID Cryptographic Section still there, but not working. Source returned to ROME and remained there until the arrival of the Allies.

AVVIAMENTO

3. SIM CRYPTOGRAPHIC SECTION (SEZIONE CRITTOGRAFICA SIM) (beg 40-8 Sep 43)

(1) Organisation, Strength and Role

Source states that, in spite of the wide nature of its duties, which overlapped into fields other than the purely military, the SIM Cryptographic Sec came directly under the orders of the Army Branch of SIM.

For purposes of working the Sec was divided into the following three sub-sections:-

1) Diplomatic Sub-sec

Responsible for the decoding and deciphering of all diplomatic intercepts. Subdivided into groups dealing with diplomatic sigs traffic of various states or groups of states.

ii) Military and Research Sub-sec

Normally dealt with only high-grade traffic. Results obtained would be handed over to the various cryptographic secs working in the fd, or in Italian overseas possessions (e.g. RHODES). To the research alt would be handed over work which was considered too difficult to be handled either by the other sub-secs or by the cryptographic secs in the fd. The Sub-sec was further subdivided into gps dealing with the mil sigs traffic or various states or gps of states in approximately the same manner as for the Diplomatic Sub-sec.

iii) Commercial Sub-sec

Dealt only with Italian Commercial codes. Its duties seem to have been mainly the censoring of commercial traffic and the detection of any attempts by Italian firms to insert "codes within codes".

Exclusive of guards and orderlies, personnel employed by the Cryptographic Sec numbered approx 45. Of these, 16-20 were cryptographers, and ranked as offrs. The remainder were NCO translators and clerks, the majority being drawn from the CC RR, the remainder from the Army. All personnel, incl guards, normally wore civilian clothes. Allotment of personnel between the three sub-secs varied in proportion to the volume of traffic and the priority of tasks at any given moment. Translators and typists seem to have been pooled between the sub-secs; Source gives the following as a typical allotment of cryptographers at any one time:-

Diplomatic Sub-sec

FRANCE and Colonies	2
TURKEY	2
BELGIUM (French)	1
SWITZERLAND (French and German)	1
RUMANIA	1-2
SPAIN	}
PORTUGAL	
LATIN AMERICA (incl MEXICO)	
Slav States	1 (later average higher : 3-4)
GREAT BRITAIN	}
DOMINIONS	
USA	
also SWEDEN	}
VATICAN	
	1
	<hr/> 12-16

Military Sub-sec (incl Research) 3-5

Commercial Sub-sec 1

Grand Total

16-22

(B) Sources of Traffic

The traffic given to the Cryptographic Sec for deciphering was normally derived from the following five main sources:-

- i) ITALORADIO
- ii) ITALCABLE
- iii) TELEGRAPH OFFICES
- iv) STATIC INTERCEPT Stns at ROME (FORTE BRASCHI)
ALBENGA/SAVONA
MONCALIERI/TURIN
VENICE

- v) MOBILE INTERCEPT Stns, incl those in LIBYA (1940-42)
 RHODES (after 1940)
 ENNA (Sicily) (until 1943)
 LECCE/BRINDISI (until 1943)
 FIUME area (after 1941)
 RUSSIA (with ARMR)

(C) Location

Work was carried out at 43, Via POLI, ROME. Reconstructed codes, photostat copies and cryptographic reports were kept in three safes in this bldg.

(D) Traffic Handled 1940 - 8 Sep 43

Source had knowledge of the following work as having been successfully carried out by SIM Cryptographic Sec during the period under review:-

I) Diplomatic Sub-sec

(a) FRANCE

In 1940 two diplomatic codes were under reconstruction (no further details known).

(b) TURKEY

Source states that SIM met with considerable success in its work on Turkish traffic, as the latter was found comparatively easy to read. Work was carried out on several Turkish codes:-

- 1) A four-figure diplomatic code (two books, one encipher and one decipher) used with two recipher tables. The code-group of four digits changed after reciphering, by process of substitutions of the first three digits; thus 1234 became 6894. SIM was in possession of photostat copies of this code, but NOT of the recipher tables. (Source states that the recipher table used for the ANKARA-BERLIN traffic was referred to as the "ZAFER", and the recipher table used for the ANKARA-MOSCOW traffic was referred to as the "SAKARIA").
- ii) A four-figure diplomatic code ("Codice paginato", i.e. one book) with a 40-figure recipher key, which changed daily. This code was broken by SIM Cryptographic Sec on 19 Jul 43.
- iii) A four-figure diplomatic code, used by the Turkish Embassy in ROME, with a 40-figure recipher key. This code was referred to as "ROMA".
- iv) A consular code - one book - with recipher. The clear of this code was reported to be in the Turkish language written in Arabic characters.
- v) A four-figure diplomatic code called the "Çankaya". This code was broken some time before 8 Sep 43. (See para 4.D.a.ii. below for details see App "F").
- vi) A five-figure Mil Attaché code, one book, which was in use until 1942. This code was broken by SIM. It was replaced by the code described in para 4.D.a.i. below and in App "E".

(c) BELGIUM

In 1940 SIM were reading traffic in an old diplomatic code of which they had photostat copies. Source did not remember any details; he believed that it was a four-figure code, the first two digits indicating the page in the book, and the latter two the code group.

(d) SWITZERLAND

Until 1941 a diplomatic code (in French) was being read. After this date the Swiss introduced cipher machines, and as a result no more decoding work was attempted.

(e) ROMANIA

All codes were read, as SIM had succeeded in obtaining photostat copies of all codes in use right up to the period of the Italian Armistice. Source states that during the period 1939-43 the Rumanians changed their codes frequently, but all the code-books were of approximately the same pattern, and SIM never encountered any serious difficulties. (For further details see para 4.2, a.iii, and 4.v. below).

(f) PORTUGAL

One diplomatic code was read; Source believes that it was of the five-figure type, with recipher table. SIM were in possession of photostat copies of the code itself. Each legation used different recipher tables, but SIM had succeeded in breaking and reconstructing some of these.

(g) URUGUAY

One diplomatic code was read, SIM being in possession of photostat copies. Source believes that this code was of the five-figure or four-figure type. Only traffic MONTevideo-ROMe was read.

(h) CHILE

One diplomatic code was read, SIM being in possession of photostat copies. This was a five-figure code, divided (for convenience) into three consecutive books, each with an enciphering and deciphering sec.

(i) MEXICO

SIM were working on three separate codes.

Of these, the first two were of the five-letter type ("Codese paginato" -- one book); both contained about 20,000 pronounceable gps, and were used in conjunction with a daily recipher table worked on the sliding scale principle (thus e.g. "DABAD" would become "DABAC"). The text of messages was interspersed with clear. These codes were both read and reconstructed by SIM.

The third code was of the polyalphabetic type, with 20 alphabets. There were a number of tables. About twenty different tables were read and reconstructed by SIM.

(j) SPAIN

Prior to 1939 SIM had succeeded in breaking and reconstructing several diplomatic codes which had been used in the late Republican and early FRANCO period. Source states, however, that these codes were all out of use by 1939, and so far as he is aware no other Spanish codes were read or reconstructed by SIM.

(k) YUGOSLAVIA

Source states that SIM had succeeded in breaking and reconstructing the following codes:-

Before April 41

- i) A diplomatic code (in figures) with recipher. Photostat copies were available.

After April 41

- ii) An USTACHA code (CROAT State). This was a fd code, of German origin, adapted to the CROAT language, and used in the CROAT Army. It was of the bigram type, derived from the DOPPELKASTENCHLUESSEL (two squares each of 25 letters, where the clear bigram was enciphered by taking as the cipher bigram the diagonal opposites, one from each square). In use from Jun 41 until Jan or Mar 43. Was first read at ROME, and handed over to the (?) Eighth Italian Army HQ at FIUME.
- iii) A second USTACHA cipher. This was a transposition system with incomplete rectangle.

- iv) A code used by Marshal TITO's forces. Source believed that this was a mil code. It was a F4 Code with substitution with bigrams. (For details see "D").

(1) GREAT BRITAIN

Source states that a diplomatic code (number of letters unspecified) was in process of reconstruction, and was being partially read. (Source could supply no further details).

(n) USA

SIM succeeded in reading the following codes:-

- i) The "BROWN" diplomatic code. This is stated to have been of the five-letter type. Photostat copies of this code were available to SIM.
- ii) The "SECRET" Military Attache' code. This is stated to have been a five-letter code with recipher tables. Photostat copies of the code were available to SIM, and the Research Sub-sec had succeeded in reconstructing a number of recipher tables.
- iii) The "CONFIDENTIAL" Military Attache' code. This is ^{also} stated to have been a five-letter code, with recipher tables. Photostat copies of the code were available to SIM, and the Research Sub-sec had succeeded in reconstructing a number of recipher tables.

Source believed that one of the photostat copies mentioned above was obtained by SIM from the Germans.

(n) SWEDEN

One Swedish diplomatic code was being read by SIM. (Source could supply no further details).

(n) VATICAN

Source states that the work on VATICAN sigs traffic was carried out by Gen GAMBA, head of the SIM Cryptographic Sec, in person. He stated that he carried out this work solely "for his own satisfaction". After Gen GAMBA retired (see para 5.I, below) the work was carried on by Capt BENNETT.

Traffic read consisted of two diplomatic codes; both were in use at the same period of time, and were still current on 8 Sep 43. Source states that these were both of the book type ("codice paginato" - one book) with trigrams. The book had 24 pages, each page having 24 blocks, and each block 24 lines. In each trigram, the first letter indicated the page, the second letter indicated the block, the third letter indicated the line. Thus, XYZ meant: "Page X, block Y, line Z", the latter giving the clear. In addition, "dud" letters ("NULLE") were sometimes added. These might be placed anywhere in the message, but never within the trigram. Their exact posn in the message varied in accordance with the particular Nuncio's Residence participating in the traffic. Source states that such duds were not to be found in every Marconigram gp of five letters.

(N.B. Source had no knowledge of work having been attempted on the cipher traffic of CHINA or JAPAN. He had personally never met any member of SIM Cryptographic Sec with any knowledge of either Japanese or Chinese).

II) Army and Research Sub-sec

(a) Army

1) Fighting French Army in the Middle East (1942-43)

A trigram code was successfully read by SIM during this period. Source believes that this code was in the first instance broken by the Germans. It was handed over by SIM to the Cryptographic Sec on RHODES, and the latter was responsible for the deciphering of subsequent messages. (For details of this code, see App "D").

ii) Turkish Army

A polyalphabetic code of five or more alphabets was read by the Cryptographic Sec at RHODES. (Source could supply no further details).

iii) Russian Army

Source knew of a Fd Code which had been broken by SIM.

This is described as a two-figure code with a key changing daily. A square of 10 x 10 small squares contained 100 groups incl the alphabet, figures, punctuation marks and a few words.

iv) British Army

Source has knowledge of four codes which had been read with complete or partial success by SIM Cryptographic Sec, viz the "SYKO", "ANNA", "CIPHER" and "WAR OFFICE" Codes.

Source describes the "SYKO" as a polyalphabetic code with 32 alphabets. Messages started with a Key Group of five letters, which indicated the order in which the enciphering had been carried out. For example, BOOCK might stand for 13795. The first digit of this key indicated from which of the first nine alphabets the enciphering had been carried out. Taking the above example as being used in the enciphering of a long message,

<u>With Key</u>	<u>Letters in clear text</u>	<u>LETTERS - CIPHER found in Alphabet No</u>
1	1st	1
3	33rd	3
7	63rd	7
9	89th	9
5	113th	5

and then the 141st letter of message from Alphabet No 1, and so on.

Source states that the "SYKO" code was broken in ROME and was handed over to the Italian Cryptographic Sec working with the intercept units in AFRICA.

The "ANNA" code is described by Source as being on the same principle as the "SYKO", and its system was known to SIM. The latter did not concern themselves with it to any great extent since, according to Source, it was discovered that the "ANNA" code was only used in the course of mil exercises in the UK itself.

The "CIPHER" was a code which, according to Source, was used down to a comparatively low level in the British Army. It was used in the UK, and at least two of its tables were known to the Italians as having been used in LIBYA and in the Middle East. The code was originally broken by the Germans, who communicated their results to the Italians in Jan 42. The "CIPHER" code is described by Source as involving the use of a square sub-divided into 26 x 26 smaller squares, with letters for each column and line. The 676 squares contained words, figures, punctuation marks and syllables. Key is believed to have changed daily.

The "WAR OFFICE" code is described by Source as a figure code, in two books (encipher and decipher), reciphered with a "continuous" key (out of a book). A copy of the code itself was captured in LIBYA early in 1942, and the Germans enjoyed a measure of success in breaking it. The Italians obtained it from the Germans but could not read it on account of the lack of HOLLERITH machines.

(b) Research

As stated above (sub-para A.ii.) this sec concerned itself chiefly with work which was considered beyond the immediate capabilities of the other subssecs or the various cryptographic parties. In general, work seems to have been on a small scale; it was not until May 43 that the project of obtaining WATSON-HOLLERITH machines was realised, and problems began to be tackled the solution of which had until then only been attempted by the Germans. Work carried out with the machines seems to have been of a general nature. Source has knowledge of the following as among the tasks undertaken:

- i) Statistics of language characteristics, such as the ascertaining of the relative frequencies of letters and combinations of letters.
- ii) Detection of repeats.
- iii) Statistics of sequences, e.g. TH in English
QU in French
CC in Italian.

- iv) In connection with the attempt to break the "WAR OFFICE" Code (see sub-para a.iv. above) work known as "differencing" was done with the aid of the tabulating machine. This was an attempt to break the subtractor key. The tabulating machine worked out the differences of frequent gps of code (in book form), and the differences of gps in text. Work in this connection had been carried out by the Germans, but Source could not specify the degree of success obtained.

III) Commercial Sub-sec

Source had little knowledge of the work done by this Sub-sec. He only knew that it worked as a censorship office on the various Italian Commercial Codes and other Commercial Codes used in ITALY.

(E) Publication of results obtained

Bulletins containing messages read by the Cryptographic Sec of SIM were issued daily. These bulletins were typewritten, with ten to fourteen copies. Distribution varied, normally incl:-

The King
Head of the Government
Director of SIM
Other Depts of SIM
Chief of Staff
Ministry of Popular Culture.

(F) Security

All working papers were burnt after perusal.

4. SID CRYPTOGRAPHIC SECTION (Oct 43-Apr 44)

(A) History

Formed as a part of SID at the time of the latter's reconstitution under Dr FOSCHINI in Sep/Oct 43, the nucleus to form the new Sec being drawn from personnel who had previously served in the Cryptographic Sec of SIM. It was intended that the Cryptographic Sec of the new SID should fulfil a similar function in working for the Republican Fascist Forces to that of the old Cryptographic Sec of SIM in working for the Italian Armed Forces up to the time of the Italian Armistice, but the new Sec was given the additional task of devising code and cipher systems for the use of the Republican Fascist Army (see sub-para D.b. below).

Formation took place in ROME in Sep/Oct 43, and in Oct/Nov 43 the Sec moved to CASTIGLIONE DELLE STIVIERE (F 2650 - ITALY 1:250,000 - Northern ITALY Zone) taking with them at least some of the codes which had previously been in possession of SIM (see sub-para D.a. below). Source explains that at the time of the Italian Armistice Gen FANTONI, the then Director of the Army Branch of SIM, ordered the destruction of all cryptographic documents. The codes taken with them by SID Cryptographic Sec were, Source believes, the only ones which were not in fact so destroyed.

Source states that during the entire period up to Apr 44 no work on current traffic was carried out by the Sec, since the Republican Fascist Forces had, so far as Source is aware, no intercept stns of their own, and all attempts to set up such stns were frustrated by the Germans. Source has no knowledge of the activities or movements of the Sec after 2 May 44. He believed that it was still located at CASTIGLIONE DELLE STIVIERE, but one rumour said that it was to be disbanded and that all cryptographic and intercept personnel of SID were to be attached to various German intercept units.

(B) Organisation and Strength

The orgn and functions of the various sub-secs of the SID Cryptographic Sec was in most respects identical with that of the old SIM Cryptographic Sec (see para 3.A. above) but Source states that up to Apr 44 the former was designed on a somewhat smaller scale. The actual cryptographic personnel were divided into specialist gps, and it was intended that men from the various gps should be sub-allotted to the DIPLOMATIC, MILITARY & RESEARCH or COMMERCIAL Sub-Seos as required.

/In Apr 44

In Apr 44 the constitution of these gps was as follows (figures indicate strength in offrs).

OC	1
English-speaking Nations	1
Turkish	}
Arabic	
Amharic	
Greek	1
Slav Languages	2
General Cryptographic work	4
Construction of new codes	2
VATICAN	1
Intercept	3
	<hr/>
Total	16
	<hr/>

(C) Location

On 2 May 44 the Sec was at CASTIGLIONE DELLE STIVIERE (F 2650 - ITALY 1:250,000 - Northern ITALY Zone) where it had its offices in the LYCEO.GIMNASIO and the SCUOLE AVIAMENTO PROFESSIONALE. Source has no knowledge of any subsequent change of location.

AVVIAMENTO
(D) Work of Section (Oct 43-Apr 44)

(a) Reading of Foreign Codes (Diplomatic and Mil Attachés)

As stated above (sub-para 4.A.) no work on current traffic was carried out during the period under review. The various codes and ciphers specified below are those which were broken and read and either partly or wholly reconstructed by SIM before the Italian Armistice, and which the Cryptographic Sec of SID took with them in their move to CASTIGLIONE DELLE STIVIERE. They are mentioned under this heading because they were thus always available for reading current material and may in fact be used for this purpose by either Italian or German cryptographers at the present time.

i) Turkish Military Attaché's Code
(c.f. para 3.D.I.b.vi. above. For details see App "E")

Photostat copies of this code were available.

Source states that this code is used by all Turkish Mil Attachés. It is described as a five-figure code with one book ("codice paginato").

This code was broken before 8 Sep 43 in its entirety. Up to that date about one message per day was intercepted. In Apr 44 the code was in the offices of SID Cryptographic Sec at CASTIGLIONE DELLE STIVIERE.

ii) Turkish Diplomatic Code
(c.f. para 3.D.I.b.v. above. For details see App "F")

Source describes this as the code used by the Turkish Embassies in BERLIN and (?)VICHY. It is stated to have been of the two-book (encipher and decipher) four-figure type.

SIM referred to this code as the "Çankaya" and had broken and reconstructed it to their own satisfaction by 8 Sep 43. Traffic was intercepted at the rate of about one message per day; the majority of these concerned chrome negotiations.

In Apr 44 the results obtained by SIM in reconstructing this code were in the offices of the SID Cryptographic Sec at CASTIGLIONE DELLE STIVIERE.

iii) Rumanian Diplomatic Code
(c.f. para 3.D.I.e. above)

This code was in use in Sep 43. SIM had succeeded in reading it. Photostat copies were available.

Source could supply no further details.

As far as Source knew, this code was still in the offices of the SID Cryptographic Sec at CASTIGLIONE DELLE STIVIERE in Apr 44.

iv) Rumanian Military Attaché Cipher
(c.f. para 3.D.I.e. above. For details see App "C")

This is described as a transposition cipher with squares each of 36 letters. It had been broken by SIM prior to 8 Sep 43, at which period it was still in use.

Results of SIM's work in breaking this cipher were also at the offices of SID Cryptographic Sec at CASTIGLIONE DELLE STIVIERE in Apr 44.

v) Spanish (?) Diplomatic Code

This had been reconstructed by SIM prior to 1940, at which period it was no longer in use.

Source states that SID Cryptographic Sec brought copies of this code with them when they moved to CASTIGLIONE DELLE STIVIERE, but could not explain their reasons for doing so, since the code had been obsolete for approx four years.

(b) Production of Codes and Ciphers for Fascist Republican Forces

Source knew only of a Naval Code used by the Army. This was an old four-figure code, with gps from 0000-9999, used in conjunction with a new recipher table ("sopracrittura a chiave continua"). The recipher table changed daily, (the tables for each day being drawn up by hand).

5. PERSONALITIES

(A) SIM Cryptographic Section (1940-43)

The following constitutes a list of Italian offrers or WOs whom Source remembers as having worked at one time or another in, or in liaison with, SIM Cryptographic Sec. Source stresses that offrers frequently changed appointments or were sent to the various cryptographic parties working abroad or in the fd, although the actual OCs of the depts changed less frequently. Offrs marked \$ in this list were working for SID Cryptographic Sec at CASTIGLIONE DELLE STIVIERE in Apr 44 (see sub-para B. below).

Function or
Nationality

Rank and Name

Personal Details

Permanently employed by
SID Cryptographic Sec,
of which he was Director
until Spring 43, when he
was placed in retirement.

Gen GAMBA

Aged 70. Considered eccentric,
but unquestionably the best
cryptographer in ITALY. Reads
French, English, German, Greek,
Rumanian and Turkish. Believed
at present in ROME area.

Present Director of SID
Cryptographic Sec. Was
2 i/o of SIM Cryptographic
Sec until Gen GAMBA's re-
tirement, when he took
over the post of Director.

\$ Col COSMACINI

Regular offr and cryptographer.
At one time trained recruits
for Sec. Believed at present
in Northern ITALY.

FRANCE

Lt-Col VALLETTA

Speaks French. Believed at
present in Northern ITALY.

"

Capt BONVINO

Engineer. Speaks French.
Thought possibly at present in
ROME area.

"

2/Lt AGOSTI

Speaks French. Milanese, may
be at present in MILAN.

"

Sjt-Maj M'INA

Worked in 1940 with the party
engaged on the reconstruction of
French codes. Present where-
abouts unknown.

~~TOP SECRET~~CSDIC/CMP/Y 4:

TURKEY	\$ Lt-Col CARUSI, Raoul	Inf offr. Speaks Amharic and Arabic. Believed at present in Northern ITALY.
"	Capt NORDIO, Ernani	Inf offr. Speaks French. Believed now living in retirement in Northern ITALY.
"	Capt MURATTI	Comes from TRIESTE. Speaks French. Believed at present in Northern ITALY.
"	Capt GRAMOLA, (?)Giovanni	Inf offr. Served in RHODES in 42. Speaks Turkish. Present whereabouts unknown.
"	Capt BATTISTICH, (?)Roberto	Nav offr. Lived previously in TURKEY and speaks Turkish. Present whereabouts unknown.
"	2/Lt RUSSO	Inf offr. Speaks Turkish. Present whereabouts unknown.
SWITZERLAND	Major GILOFARO, (?)Giuseppe	Cryptographer. At one time ran "Secretariate" of SIM Cryptographic Sec. Of Sicilian origin. Speaks English and French. Believed at present in ROME area.
RUMANIA	Lt-Col VASSALLO	(?) Arty offr. Speaks Rumanian. Believed at present in ROME area.
LATIN AMERICA incl MEXICO) SPAIN PORTUGAL	Capt LUCREZIO	(?) Inf offr. Speaks Spanish and Portuguese. Believed at present in ROME area.
SLAV STATES	\$ Lt-Col SERRAGLI, Luigi	Aged 60. Previous War Office employee; cryptographer. Was recently brought into Army with rank of Lt-Col. Comes from DUBROVNIK. Speaks Serbian and Croatian. At present in Northern ITALY.
"	2/Lt SMOLCICH	Inf offr. Comes from SPLIT. Speaks Serbo-Croat. On 8 Sep 43 was in DALMATIA. Believed at present in German Concentration Camp.
"	2/Lt CARELLI	Inf offr. Speaks Russian. Believed at present in ROME.
"	Capt ONESTI, Bruno	Arty offr. Comes from GENOA. Present whereabouts unknown.
"	Sjt-Maj NITLI	CCRR. "Taken away" by the Germans.
"	\$ Capt DE BEDEN, Giovanni	Comes from DALMATIA. Speaks Slovene. Believed at present in Northern ITALY.
ENGLISH SPEAKING STATES	\$ Col CROCI, Arturo	Aged 55-60. Civilian granted "honorary" rank. Was previously Italian Consul in SWEDEN. Wounded in last war, has a wooden leg. Speaks English and Swedish. Believed at present in Northern ITALY.

ENGLISH SPEAKING STATES	Capt	PIRLO-RULINO	Speaks English. Present whereabouts unknown.
"	Capt	LITTA	Speaks English. Stated to be anti-German. Present whereabouts unknown.
"	Capt	PERONI	Speaks English. At present in Northern ITALY.
GREECE	Major	GALIFI	(No details known).
VATICAN	Capt	BENNA	Took over this duty on retirement of Gen GAMBA (see above). No other details known.
Research	Lt-Col	SCUDERI, Francesco	Aged 40-45. Regular army offr. In Cryptographic Sec since 1939. Speaks French and a little English. Believed at present in ROME area.
Commercial Sub-sec	Lt	COLBI	(No details known).
Intercept	Col	PETRELLA	Was OC Static Intercept Stns in ITALY from May 40 onwards.
"	§ Lt-Col	GIOVANUZZI, Santo	Was OC FORTE BRASCHI (ROME) Intercept Stn in May 40. Believed at present in Northern ITALY.
"SERVIZIO "I" DEL ARMIR" (Intelligence Branch of Italian Army in RUSSIA)	Lt-Col	EMER	Stated to have been OC Cryptographic Party with Intercept Units on Russian front. Seen in ROME in Jul 44.

(B) SID Cryptographic Section

Source states that in Apr 44 this Sec employed the following offr, all of whom were at that date in C. STIGLIONE DELLE STIVIERE.

<u>Function or National Co</u>	<u>Rank and Name</u>	<u>Personal Details</u>
OC	Col COSMACINI	(See sub-para A above).
ENGLISH SPEAKING STATES	Col CROCI, Arturo	(See sub-para A above).
TURKEY (also Arabic and Amharic)	Lt-Col C. RUSI	(See sub-para A above).
SLAV STATES	Lt-Col SERRAGLI	(See sub-para A above).
"	Capt DE BIDENT	(See sub-para A above).
GREECE (also TURKEY)	2/Lt F. PERIO BELLA, Rodolfo	Brother of Marcello below. (No details given).
General Cryptography	Major de' ITT	(No details given).
"	Capt CHITTONI, Rafaelo	(No details given).
"	Lt UCELNGHI	(No details given).
"	Lt F. PERIO BELLA, Marcello	Brother of Rodolfo above. (No other details given).

~~TOP SECRET~~CSDIC/OMF/X 4.

Construction of new (?) typographic codes	Lt	AMATI, Carlo	Brother of Alberto below. (No other details given).
"	2/Lt	AMATI, Alberto	Brother of Carlo above. (No other details given).
Intercept	2/Lt	CARLINI	(No exact details given).
"	2/Lt	MERLO	(No exact details given).

(C) Italian Liaison Officers with German Cryptographic Section

Maj DEMARI	In BERLIN in Jan 42.
Maj LA TORRE (?DELLA TORRE)	Replaced the above in BERLIN in Dec 42.

(D) Personalities in SID (Reconstituted SIM)

Dr FOSCHINI	Source states that this man supervised the reconstitution of SIM (renamed SID) after the Italian Armistice, and occupied the post of Director.
Lt-Col de LEO	Replaced Dr FOSCHINI (after the dismissal of the latter in Feb 44) as Director? of SID.
Lt-Col DAL NEGRO	Occupied an unspecified post in SID in Northern ITALY in Oct 43. Recalled to ROME in Nov 43.
Lt-Col PAOLILLO	Succeeded the above in Northern ITALY in Nov 43.

(E) German Personnel liaising with SIM and SID

Col KEMP : KEMPF (OWW/CHI)	Believed by Source to be Director of the CHIASTEILUNG in GERMANY.
Col PFENNER	Actual title "MINISTERIALRAT" stated to be in charge of Diplomatic Branch of German Cryptographic Section.
Maj MANG	Stated to be in charge of Military Branch of German Cryptographic Section.

(F) Italian Naval and Air Force Cryptographers(Naval Ranks)

Capt DE MONTE	OC Naval Cryptographic Section at CASTIGLIONE DELLE STIVIERE.
---------------	---

Omdr DONINI (BONINI))	} At CASTIGLIONE DELLE STIVIERE in Apr 44. (Previously at VOLTA MANTOVANA (F 3842) ITALY; 1:250,000 - Northern ITALY).
Lt TRAMMAROLLO	
Lt GAETANO	
Mdsman BARBAGALLO	
Mdsman BENINI	

(Air Force Rank)

Wing-Omdr SALIRIS (Lt-Col)	OC Air Force Cryptographic Section at CASTIGLIONE DELLE STIVIERE in Apr 44.
-------------------------------	---

6. MISCELLANEOUS(A) Notes on Italian Ciphers

Source was not well acquainted with Italian ciphers. He supplied the following info spontaneously, and NOT in answer to detailed questioning.
/Before Sep 43

Before Sep 43 the Germans supplied the Italians with a number of ENIGMA Cipher Machines. Italians were instructed in the method of operation. ARMOR (the Italian Army on the Russian Front) used this type of machine for comm with ROME. Source states that these machines were also used by the Italian Forces in LIBYA. Source believes that one machine of this type is at present located at VOLTA MANTOVANA, and that another is at CASTIGLIONE DELLE STIVIERE.

(B) Training of Italian Cryptographic Personnel

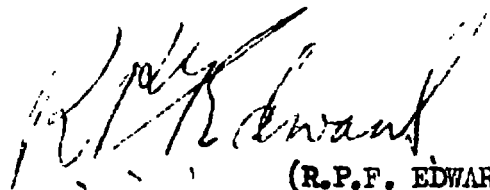
The course Source attended, in Nov 39, was the seventh or eighth of its kind. The first is believed to have been held shortly after the war in SPAIN. When the course assembled there were about 40-45 students, all ofrs (regtl, staff and sigs). The course lasted from 1 Nov 39 to 1 Mar 40. At the end of the course, 10-15 students were retained for a further Advanced Course which lasted from 1 Mar 40 to 1 May 40. The other students went as crypto specialists with Intercept units or as cipher ofrs with sigs units.

The course was directed by Col COSMACINI, Giuseppe, and was held in a bldg adjoining the Italian Ministry of War. It included lectures on the theoretical side of cryptography and practical exercises. For the latter, students worked in gps of two or three. Reports were made on the work of the students by the Directing Staff.

Tng included single and double transposition, playfair - incl re-ciphered playfair (by means of "systems" called BIPIDI and TRIFIDI) - polyalphabetic ciphers and grid ciphers. Students on the Advanced Course were trained in book-breaking (single book and encipher and decipher books "CODICI INTERVERTITI").

A.G.B.

C.S.D.I.C.,
C.M.F.,
20 Sep 44.



(R.P.F. EDWARDS)
Lt-Col.
Comdt, CSDIC, CMF.

SOURCE'S VISITS TO BERLIN (As mentioned in para 2 of attached report)(a) Object of First Visit

In Jan 42, Source was sent to BERLIN together with the 2 i/c SIM Cryptographic Sec, Col COSMACINI. Col COSMACINI was charged with the mission of obtaining info on the general orgn of the German Cryptographic Service, on its working and on specific problems connected with cryptographic work. Info was also to be acquired on the use of perforated card machines (patent WATSON-HOLLERITH). Source did not accompany the Col on all his visits but was able to gain a general idea how the German Service worked.

(b) German Cryptographic Service (CHI ABTEILUNG)1) Organisation

The Sec was divided into two distinct sub-secs or branches, viz Diplomatic and Mil. The Diplomatic Branch was directed by Ministerialrat (= Col) PFENNER and the Mil Branch by Maj MANG. The whole Sec was commanded by Col KEMPF.

Material was sent to the Sec from the Intercept Stns (? "H" Stellen) scattered all over GERMANY and the occupied countries. At the time of Source's visit there were two stns on the Russian front, two in FRANCE, one in GREECE and one in LIBYA.

All the work on the diplomatic side was done in BERLIN while the work on the mil side was done almost wholly outside BERLIN. The offices in BERLIN were grouped mainly in the TIERGARTEN district (MATTEIKIRCHE PLATZ, VIKTORIA STRASSE, STANDARTEN STRASSE and GRAF SPEE UFER).

ii) Methods and Success achieved

As far as Source could judge the Germans were achieving success on the mil side, except for the "grid" ("griglic") and "Type X" ("Typo X"). He did not have a chance to study their methods in detail but believed that they were normal - interrogation of PW, captured docs and straight cryptographic work.

At BERLIN work on the mil side was concerned with problems of a general nature and the treatment of systems which could not be broken either at the front or by detached secs in GERMANY.

iii) Museum and Laboratory

In BERLIN Source paid a visit to a small laboratory-museum where machines were kept which carried out quick substitutions of letters and numbers, graphs, statistics of letters, bigrams and trigrams. Any available type of captured machine was also held there - Source saw the French HAGELIN C 36, "Type X" without rollers (drums) and a Russian machine. He could give no details on the working of the machines as he only saw them once. They were all built with telephone eqpt, tables (with commutators) and jacks, selectors and relays.

iv) Group dealing with perforated card machines

The gp dealing with perforated card machines was large and employed about thirty persons not incl those working on perforators and verifiers (checkers).

Source states that work was being done on machines which had been requisitioned in PARIS. These machines were:-

- a) perforators, hand and motor driven, for figures and letters, with or without check ("controllo scriventi").
- b) verifiers
- c) duplicators
- d) selectors
- e) tabulators, alphabetical and numerical.

All the machines ran on 110 (120?) Volt DC.

The work carried out was of a statistical nature on at least 10,000 letters derived from original texts for the various languages on which they worked. The following were calculated:-

- a) frequencies of bigrams and trigrams for these languages.

- b) probability of combinations of letters.
- c) frequencies of polygrams in various texts and "statistica a catena", i.e. the number of times letters combine and their repeats.
- d) statistics on traffic of the various transmitting stns.
- e) substitution of numbers (figures) and letters for reciphered texts.
- f) making of "differences" and books of "differences" from the higher frequency code-words employed with recipher keys. This type of work was carried out in particular in the case of material derived from the "WAR OFFICE" Code.

In order to eliminate the effect of reciphering a tabulating machine was automatically doing the work of differencing between a certain gp of one text and so many other gps of other text placed in such a manner as to be capable of being reciphered by means of the same gp of the "continuous" key.

(c) Results of visit

On his return to ROME Source made a report to the head of SIM on what he had seen. As a result it was decided to undertake experiments in ITALY on a small scale with perforated card machines, with a view to expansion should they prove of use.

Plans were made to hire machines from S.A. WATSON in MILAN. Things went very slowly and before the hire contract was signed Source was sent to BERLIN again, because in ITALY there were no tabulators which without modifications would have been capable of working out the differences.

(d) Second visit to BERLIN

In Dec 42 Source visited BERLIN again but achieved poor results. The Germans preferred to send one of their technicians (Herr SCHENCK) to ROME, rather than let him see their installations again. They assured him these were being moved to another locality, "in some woods". Zrca.

The technician got in touch with the firm WATSON and proposed the exchange of some Italian machines for a tabulating machine of the type D-11 (German). This exchange was effected. The subsequent hire contract stipulated the hire to the Italian Cryptographic Sec of 12 machines, perforating, selecting, duplicating and tabulating machines.

(e) Work carried out by the Italians with the machines

About ten "lots" of work were carried out by the Italians. They included: Statistics for 10,000 letters for English, French and Spanish; a "chain-statistics" (statistica a catena) for a French system; a frequency count on an American code in process of reconstruction and a small volume of "differences" for a Turkish code.

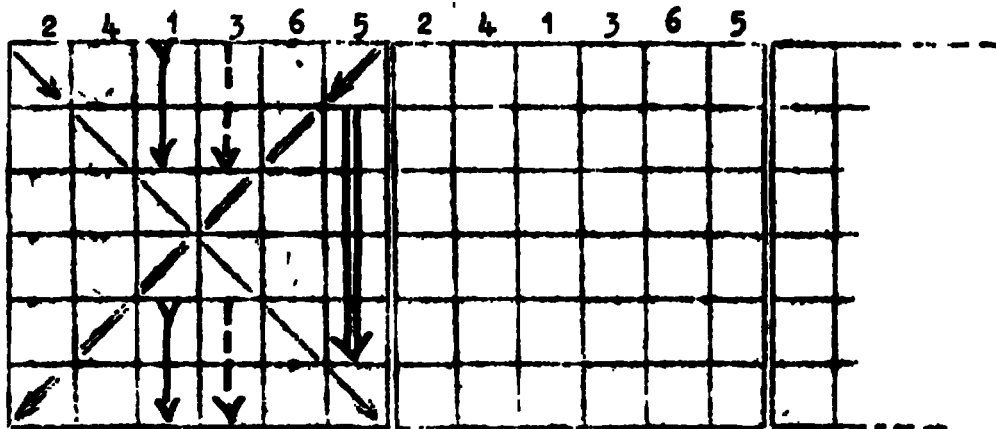
X

Code, stated by Source to have been used by TITO's Forces in YUGOSLAVIA (see para 3.D.K.k.iv. of report).

TABLE with 676 Squares (26 x 26)

	A	B	C	D	E
A					
B	1				
C	2				
D	3				
E	4				

1. The 676 squares contained figures, words, punctuation marks, names, etc.,
2. The alphabets (letters outside the squares) were moved about, text in the squares was not changed, (Alphabet moved "en bloc").
3. The KEY in which message was enciphered was given at the beginning of the message. It took the form of a trigram: Indicating the posn of the first letter of the alphabet or giving letters showing the posn of a certain square which contained a word or a figure.

ROMANIAN MILITARY ATTACHE CIPHER
(o.f. para 4.D.a.iv. in report)36 Letter SquareEXAMPLESTEXT:

OL

2 7 4 17 2 27 3 36
LA BOCCA SOLLEVO DAL FIERO PASTO QUEL PECU/5, OR FORBENDOLA...

KEY:

ENC

2	4	1	3	6	5
L	S	V	R	E	A
L	A	O	O	S	U
F	T	B	O	C	E
I	O	L	O	A	L
E	L	D	P	C	P
E	Q	A	A	T	C

Encipher on Key 241365

Start from the top left hand corner diagonally to bottom right hand corner, continue from top right hand corner diagonally to bottom left hand corner and then according to key fill in each line successively, from top to bottom.

TEXT FROM MARCONIGRAM (IN CIPHER)

OI.

.....
LSVREA LAOSU PTEOCE IOLOAL ELDECP EQAATO in group of five

DEC.

	2	4	1	3	6	5
	L	S	V	R	E	A
	L	A	O	O	S	U
	F	T	B	O	C	E
	I	O	L	O	A	L
	E	L	D	P	C	F
	E	Q	A	A	T	C

Decipher on key 241365

Maroonigram text is filled in the 36 squares (6 x 6) in the normal manner. The 12 letters on the diagonals are taken out and written down (and cancelled in the square). Then proceed as for enciphering, as per key.

- a) LA|BOCCA|SOLLE.
 b) VO|DA.L|FIE. RO|PA.STO|Q.VL|P.ECAT

ENCIPHER:

GENERAL STAFF FOR POPESCU STOP FUEHRER WAN/TS TO SEE CONDUCATOR
 STOP PLEASE INSTRUCT

2	4	1	3	6	5	2	4	1	3	6	5
G	O	F	C	R	L	T	A	C	P	U	E
O	E	O	U	S	I	R	S	A	C	P	N
P	P	N	T	W	H	S	S	T	O	C	S
E	F	A	E	A	R	E	E	N	O	T	T
S	F	R	S	R	E	O	D	T	L	S	R
F	V	P	T	N	A	V	I	O	E	X	E

The text on the Maroonigram read:

- i) either GOFOR LOEOU SEPPN etc.,
 ii) OR, if the text occupied more than one 36 letter square, it was copied in a straight line;

GOFOR LTACIP UEOEO USERS etc.,

CODE USED BY FIGHTING FRENCH ARMY IN MIDDLE EAST (1942-43)

O.f. para 3.D,II,a.1. of report.

As stated in the above para, this code is believed first to have been broken by the Germans. It was later broken by SIM, who handed it over for use to the RHODES Cryptographic Party.

Source describes it as a trigram code laid out like a book, the words in the clear part being laid out in alphabetical order, in blocks of 10-12, thus forming a column. There were 40-50 blocks or columns.

40-50

[illegible]

Thus "abandonné" or "abandonner" was encoded DAZ, "absolut" - JAZ, etc.,
The first letter in the trigram was the key to the line in the block
and the second and third indicated the block itself. The keys were changed every
month.

TURKISH MILITARY ATTACHE'S CODE

C.f. paras 3.D.I.b.vi. and 4.D.a.i. in attached report.

As stated in above para, this code was broken by SIM before 8 Sep 43. In Apr 44 the results obtained by SIM were in the offices of SID Cryptographic Section at CASTIGLIONE DELLE STIVIERE. Photostat copies were available.

Code is described as ~~cs~~ the one book five-figure type, with the following characteristics:

-00-	
bir (one)	020
"	"
"	"
"	"
"	"
"	"
"	"
"	"
a	"
b	"
c	"
ç	"
-99-	

Each page contained a number of three-figure gps (Gps from 000-999). The Pages are numbered both at the top and at the bottom, say page one: 00 at the top, 99 at the bottom. The number (word standing for figure) one (bir) is encoded on alternate months 00020 and 99020.

Page 1 of the book contains:

Numbers (one gp only for each)

The alphabet (two gps for each letter: One for the unaltered LATIN letters, and one for Latin letters adapted to the Turkish language, say 001 for C and 002 for Ç (tch).

Pages 2-3 of the book contain: punctuation marks, etc.,

End pages of the book contain: geographical names.

Very often the encoded version of the message is deciphered by means of a five-figure addition key ("chiave addittiva"), say 00020

24152

24172 (Non carrying addition).

Messages had the address in clear worded:

TURKCE MILITARE ATTACHE

BERLIN, LONDON, Etc., and started with a five-figure gp.

TRUTH DIPLOMATIC CODE ("qankeya")

C.f. paras 3.D.I.b.v. and 4.D.a.ii. in attached report.

As stated in the above para, this code was broken by SIM before 8 Sep 43. In Apr 44 the results obtained by SIM were in the offices of SID Cryptographic Section at CASTIGLIONE DELLE STIVIERE.

Code is described as being of the two-book (encipher and decipher), four-figure type. Pages contained gps for words, syllables, letters of alphabet and figures, and punctuation marks.

The gp for a letter of the alphabet would be used for a figure as well. There are several code-gps for the same figures, letters of the alphabet, punctuation marks and particles such as -DA, -DE, -DET used to indicate the cases in the declensions of Turkish nouns, etc.,

Words in clear on the pages of the book or books were NOT in alphabetical order, nor were they in blocks beginning with the same letter, e.g.

BERLIN	0001
TAKE	0002
Q	0003
ONE	0004
A	0005, etc.,

The encoded text was deciphered by means of a 40-figure key, which changed every seven-ten days. (One length of key deciphered ten code gps or eight Marconigram gps).

NO check gps were used with this code.

Address and signature of message were in clear. Message did NOT contain any "key gp" ("gruppo di riconoscimento").

DISTRIBUTION

A.C. of S, G-2, AFHQ.....	1
G-2 (Sigs "I") AFHQ.....	3
G-2 (CSDIC) AFHQ.....	1
GSI (s) AAI.....	1
MI 8, MEF.....	1
MI 8, UK.....	1
File.....	3
<u>Now SCU</u>	1