

ACC

10000/120/1708

X/502/1

NOV 199

10000/120/1708

X/502/1 British + Italian Ciphers

NOV. 1943 - NOV. 1945

55

SECRET

SUBJECT : Italian Ciphers.

Land Forces Sub Commission A.O.
(M.M.I.A.)

S/7502/1

3 Nov 45

TO : Chief Signal Officer, GCHQ, GCHQ.Herewith copy of Italian Cipher which the Ministry
of War propose to use as W/T Group to their Territorial Fds.

Please acknowledge receipt on attached A.F.A.16.


 A.G. BELL, Major,
 S.O.R. Sign,
 M. M. I. A.
Enclosure: Copy No.191 of Publication No.S.E.1002 - Series No.1.
(Cipher "ALFA")In list of A.F.A.16TO : Land Forces Sub Commission A.O.
(M.M.I.A.) ROMEReceipt is acknowledged of S/7502/1 dated 3 Nov 45 and
enclosure as therein specified.

2818

Signature

Appointment

Unit

Date45

Subject:- O.P. Cipher

SECRET

Headquarters
15 Army Group (BR)

Tel: FILPOT 39

2788X 2

30 Jul 45

OC Signals MHLA

Copy to:- CSO (Cipher Security (Br)) AFHQ

1. On instructions of Cipher Security (Br) AFHQ, this HQ is forwarding to you all Italian O.P. cipher which is held at the close of 15 Army Group.
2. Please acknowledge receipt direct to Cipher Security (Br) AFHQ.

The above ciphers were
handed to Sgt Beran by
Capt Jackman who said
E/3A that it was not
necessary to send receipt
to AFHQ. d. 8/5

F.R. Jackman

F.R. JACKMAN,
Captain, R Signals.
CSO (Cipher)

2817

52
SECRETSUBJECT: Ciphers - Italian.Land Forces Sub Commission A.G.
(M.M.I.A.)
S/1502/1

30 July 45

TO : Chief Signal Officer, A.F.H.Q.

We have been informed by the Ministry of War that the existing ciphers used on the wireless network in Sicily will cease to operate as from 31 July.

With effect from 0001 hours 1 August new ciphers will come into operation for an indefinite period. Copies of such cipher tables, Nos. 21 and 22, are forwarded herewith for your information.

Please acknowledge receipt on attached A.F.A.16.

W. GARDNER
W. GARDNER, Major,
S.G.R. Sigs.
M. M. I. A.

Enclosures: Copies Nos. 21 & 22 of Publication No. 103 S.E.
(Vascicole di tabelle di chiavi per Cifratura e Sopracifratura)

TO : Land Forces Sub Commission A.G.
(M.M.I.A.) ROME

A.F.A.16.

2816

Receipt is acknowledged of S/1502/1 of 30 Jul 45 and enclosures as therein specified.

Signature

Appointment

Unit

Date45.

MA/laa

74

RACCOMANDA
A MANO

MINISTERO DELLA GUERRA
STATO MAGGIORE REGIO ESERCITO
Ufficio "I" - 4^a Sezione

N. 110966/4/Cif. di prot.P.M. 3800, li 15 luglio 1945

O G G E T T O : cifrario per esigenze di ordine pubblico - fascicoli
tabelle di cifratura e sopracifratura.

*ciphering deciphering*Allegati : 2

ALLA LAND FORCES SUB COMMISSION A.C. (M.M.I.A.)
(Maggiore Calveley)

R O M ASEGRETO

Al 31 luglio 1945 scade il blocco di tabelle in uso per la
cifratura e sopracifratura dei dispacci relativi alle esigenze d'or
dine pubblico per la Sicilia a mezzo del sistema descritto nel cifra
rio "TALAMO BIS" - pubblicazione n. 101 S.E.

A partire dalle ore zero del giorno 1° agosto 1945 entreranno
in vigore le nuove tabelle di cifratura e sopracifratura, di durata
indeterminata, riunite in fascicoli di cui s'inviano n. 2 copie, con
trassegnate dai nri 21 e 22.-

Si prega di voler restituire, firmata, l'acclusa ricevuta.-



IL CAPO SEZIONE
(Ten. Col. P. Ducrest)

que

TRANSMISSION	
IN	Time <u>11/45</u>
	Date <u>25/7</u>
OUT	Time <u>045</u>
	Date <u>26/7</u>

*Please translate
return to Sec 425
A. 25/76.*

WAR MINISTRY
MAIN ARMY STAFF
I.A.I. - 4th Section

N. 110768 / 4-Cif.di prot. P.M.3800, 11/18 giugno 1945

SUBJECT: radio communications in Sicily.

To: LA AND FORCES SU COMMISSION A.C. (M.M.I.A.)
(att.: Major Calveley)

R O M E

1. - In accordance with the concerted agreement, we communicate that the cipher "Talamo bis" for exigencies of public order in Sicily is come into force 1 June 1945. =

P. DUCROS Lt.Col.
Commanding Officer
4th Section

2844

RI/gr.

MINISTERO DELLA GUERRA
STATO MAGGIORE R. ESERCITO
Ufficio Informazioni

N. 110768/4-Cif. di prot. P.M. 3800, 11/3 giugno 1945

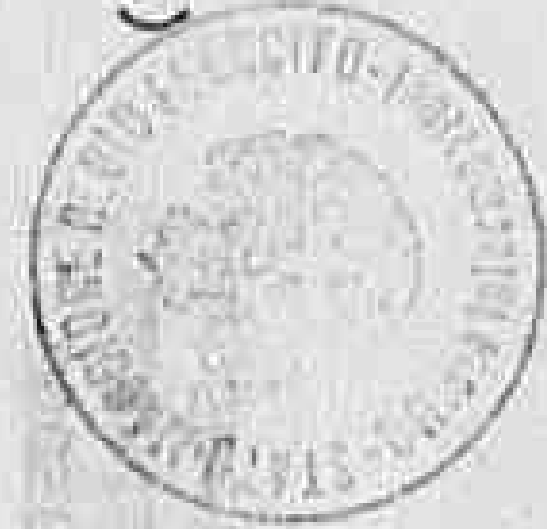
OGGETTO: radio comunicazioni in Sicilia. -

ALLA LAND FORCES SUB COMMISSION A.C. (M.M.I.A.)
(Maggiore Calveley)

R O M A

SECRET

In conformità degli accordi intercorsi, vi comuniciamo che
il cifrario "Talamo bis" per esigenze di ordine pubblico in Sicilia è
entrato in vigore il 1° giugno corrente. =



IL CAPO SEZIONE
(Ten.Col. P. Ducros)

translation on the back

COPIA

STATO MAGGIORE GENERALE

Ufficio Inform.mi

N. 110456/4^a Cif.di prot.

P.N.3800, 13 aprile 1945

ALLO STATO MAGGIORE REGIO ESERCITO

-Ufficio C.A.-

OGGETTO: Cifrario per addestramento -

a mano

Sig 1811

Riferimento foglio n.2914/C del 9 corrente.

Si informa che a mezzo del Capitano Cesare CRASSI -
aiuto maggiore del IV Gruppo del 155° Rgt.Art.- sono sta-
te inviate, in data 5 corrente, al Comando del Gruppo di Combat-
timento "Mantova" n. 10 copie del cifrario "O.P." per l'adde-
stramento del personale dipendente.

d'ordine

IL TEN.COL.VICE CAPO UFFICIO

F/to Renato De Francesco

STATO MAGGIORE R.ESERCITO = UFF.C.A. =

N. 305082/C.A.

Roma, 13^a aprile 1945 *2843*

ALLA LAND FORCES SUB COMMISSION A.C. (M.M.I.A.)

R O M A

-Ufficio C.A.-

a manoOGGETTO: Cifrario per addestramento -

Riferimento foglio n. 2914/C del 9 corrente.

Si informa che a mezzo del Capitano Cesare CRASSI -
 aiutante maggiore del IV Gruppo del 155° Rgt. Art. - sono sta-
 te inviate, in data 5 corrente, al Comando del Gruppo di Combat-
 timento "Mantova" n. 10 copie del cifrario "O.P." per l'adde-
 stramento del personale dipendente.

d'ordine

IL TEN. COL. VICE CAPO UFFICIO

F/to Renato De Francesco

STATO MAGGIORE R. ESERCITO - UFF. C.A. =

N. 305082/C.A.

Roma, 10¹⁴ aprile 1945 2813

ALLA LAND FORCES SUB COMMISSION A.C. (M.M.I.A.)

ROMA

....per conoscenza in esito al foglio S/X502/1 in data 8 aprile 1945.-

Please translate
 & return to Signal
 HQ 1945.


 IL GENERALE ADDETTO
 (Giorgio Liuzzi)



48
CONFIDENTIAL

Subject:- Italian Training Cipher.

Land Forces Sub Com A.C.
(M.M.I.A.)
S/X502/1

8 Apr 45

MINISTRY OF WAR.

Copy to: S.C.R.Sigs,
56 B.L.U.

Mantova Group have informed this H.Q. that the Italian Training Cipher which has been requested from you has not been received.

Please ensure that this Cipher is forwarded to Mantova Group as soon as possible, as it is urgently required for training purposes.

Calverley

W. CALVERLEY, Major,
for Major General,
M. M. I. A.

2842

CONFIDENTIALSubject :- Italian Training Cipher.56 BLU
3 Sigs

5 Apr 45

SO R Sigs,
MMIA.

Cpl. C
Write message
ask them to send
pl

Reference conversation Major CALVELEY - Capt PILKINGTON.

1. This Combat Group has at present NO Training Cipher. It has been requested from SMRE but has not yet been received.
2. Since Training Cipher is essential for full scale Signal Exercises may the matter please be taken up with SMRE.

In the Field.
IDRP/ec

John J. Valerius
Lt-Col.
GS.

2841

RI/1p.

STATO MAGGIORE GENERALE
Ufficio "I" - 4^a Sezione

N. *1491* 14^a/Cif. di prot.

P.M. 3.800, 11 19/2/1945

O G G E T T O : cifrario O.P. per i Gruppi di Combattimento italiani.

AL SIGNOR MAGGIORE C A L V E L E Y

- S.O.R. Sigs II - Floor 7 - stanza 54 - A.C. -

SEGRETO

1°) Vi informiamo che i Gruppi di Combattimento italiani hanno in distribuzione per le :

a) comunicazioni esterne in cifra il cifrario O.P. - serie "C", "D" e "E" con i relativi blocchi tabelle di sopracifratura della durata di tre mesi ciascuno;

b) comunicazioni interne in cifra il predetto cifrario O.P. - serie "C" - "D" e "E" con blocchi tabelle di sopracifratura della durata di 31 giorni ciascuno.

2°) La diramazione dei blocchi tabelle di sopracifratura per le comunicazioni interne di ciascun Gruppo di Combattimento è estesa fino ai Comandi dei battaglioni dipendenti.

(Traslation on the back)

P. IL CAPO SEZIONE a.p.s.
(Ten.Col.P. Ducros)

AL SIGNOR MAGGIORE CALVELLEY

- S.O.R. Sigs II - Floor 7 - stanza 54 - A.C. -

SEGRETO

1°) Vi informiamo che i Gruppi di Combattimento italiani hanno in distribuzione per le :

a) comunicazioni esterne in cifra il cifrario O.P. - serie "C", "D" e "E" con i relativi blocchi tabelle di sopracifratura della durata di tre mesi ciascuno;

b) comunicazioni interne in cifra il predetto cifrario O.P. - serie "C" - "D" e "E" con blocchi tabelle di sopracifratura della durata di 31 giorni ciascuno.

2°) La diramazione dei blocchi tabelle di sopracifratura per le comunicazioni interne di ciascun Gruppo di Combattimento è estesa fino ai Comandi dei battaglioni dipendenti.

(Translation on the back)

p. IL CAPO SEZIONE a.p.s.
(Ten.Col.P. Ducros)



Gen. Col. P. Ducros

GENERAL STAFF

I.A.I. and S.P.U. - Section 4

SUBJECT : O.P. cipher for Italian combat groups.

To - Major CALVELEY

S.O.R. - Sigs II - Floor 7 - room 54 - A.C.

1°) We inform you that Italian combat groups have :

- a) for external communications in cipher, the O.P. cipher - series "C", "D", "E" each with reciphering sheets pads for 3 months;
- b) for internal communications in cipher, the same O.P. series "C", "D", "E" each with reciphering sheets pads for 31 days.

2°) Distribution of reciphering sheets pads for internal communications of each combat group is extended down to battalion H.Q.

SECTION CHIEF
Lt. col. P. Ducros

CONFIDENTIAL

Subject:- Communications.

Land Forces Sub Commission A.C.
(M.M.I.A.)
X/502/1

29. Nov 44.

Signal Officer 51 B.L.U.

1. Reference your X1 of 27 Nov 44.

The fact that you hold only one book of cipher is well known to this H.Q. For the purpose of working the existing link a special three-leg O/T pad was obtained from A.F.H.Q. for each station NOT B.L.U.

2. Definite instructions were given and understood by all, to the effect that the cipher would pass with the operating of the station. Even in the absence of instructions this procedure should have been obvious.

Considerable trouble and inconvenience has been caused by failure to appreciate this fact and comply with the instructions.

3. The H.C.O. i/c Signals at this H.Q. is considered to have in no way shown a lack of initiative.


W. GAINSBURY, Major,
For Major General,
M. M. I. A.

2829

Subject :- Communications

To :-
Sigs Officer HQ MIIA

From :-
Sigs Officer
51 British Liaison Unit

51 British Liaison Unit

X 1

- 1 Recently the wireless set from 50 ELU was transferred to 51 ELU.
- 2 The cypher at 51 ELU is being done by my section who at the moment hold only 1 Book. This book was issued by AFHQ, who stated that this was the only cypher we needed.
- 3 The first day the set opened up we received two O messages in cypher that we do not hold. I immediately sent back a message to this effect, stating at the same time that the messages could not be deciphered, and also informing you of the type of cypher we held.
- 4 I consider that your signals should have immediately repeated the two O messages in the cypher we held. This was not done and in fact no action whatsoever was taken.
- 5 I did in actual fact manage to have the messages translated by going to 50 ELU and making them unpack all their cypher. But this does not detract from the fact that a certain lack of initiative was shown by the Sigs NCO of HQ MIIA.
- 6 Up to date no O T P have been received.

Field
27 Nov 44
ANA/ECT

C. W. W. W. W.
Capt
SO R-Sigs

2838

Subject:- ACC Classified Telegrams

Army Sub Commission (MIA)
HQ ACC
ROME
X 17
25 Jul 44

The Executive Commissioner,
HQ ACC

Reference Communications Sub Commission letter
CS/4/18/76 of 22 July.

1. There is no precedent for the use of Italian Cipher personnel using Allied Ciphers but this is not the intention. The proposal is to use the Italian Military Cipher recently approved by the Allies.
2. I see no reason why this plan should not be approved and I suggest you submit to AAI a resume of the situation showing the need for these personnel, together with a suggested War Establishment for an Italian Cipher Section, asking for approval and inclusion in the programme of Italian Troops working for the Allies.

gah

R. Browning
Maj Gen
Army Sub Commission

2827

SECRET.

Subject:--Cipher Communication REGGIO - CATANZARO.

From:--Chief Cipher Officer,
No. I District. ---

To:--Lt. Col. H.A.C. HOWARD,
I.C., Army Sub-Commission, (ACC).,
XXI Italian Corps,
Ponte Grande-CATANZARO. ---

As requested, I have investigated the difficulties in clearing traffic deciphered at REGGIO to CATANZARO.

The cipher detachment at CATANZARO have NOT at present a comon holding with REGGIO but it is understood that they will shortly be in possession of equipment which will enable them to communicate with REGGIO.

As present system of delivering deciphered messages from REGGIO i.e. by train, causes delay it is suggested that the detachment at CATANZARO should be issued with this equipment as soon as possible and advise REGGIO when they are in possession of it.

Field,
27 May 44.

Copy to:--Army Sub-Commission, ACC.,
Main H.Q., (M.M.I.A.).,
LEQUILLE. (IECCE).

Chief Cipher Officer,
No. I District.

2896

SUBJECT:- Cip. rs for Italian Army

BRITISH NO. SECRET - US SYSTEM
File
19
Army Sub Commission A.C.C.
Main H.Q. (MMIA)
LEQUILE (LECCE)

X 17
17 Mar 44

Telecommis Branch
Main H.Q., A.C.C.

Copy to: CSO Allied Armies in Italy

Attached is AAI (ACMF) letter 2783/1/X of 10 Mar 44.

This is fwd to you as you have previously been dealing with the matter and hold all relevant correspondence.

ABC

Bo
Brigadier,
Army Sub Comm A.C.C.

2835

Subject: Ciphers for Italian Army

Army Sub Commission ACC

Main HQ (MILA)

LEWIS (ISSE)

X 17

7 Mar 44

ACC (2 copies)
ACC (Telecoms) for info

Ref your 2783/1/X of 19 Feb

1. This letter has been passed to the Telecoms Branch of the ACC who have handled all questions of Ciphers with the Italian Forces and Government in the past and have all the relevant correspondence.
2. Telecoms Branch ACC agreed that in order to maintain the continuity of contact and correspondence they will deal with this question.

GH

Brig
Army Sub Com ACC

2824

0 8 9 2
X 17
17
BRITISH SECRET = U.S. SECRET.

Subject: Ciphers for Italian Army.

HQ ACTF

MILITARY MISSION

2783/1/X

M.M.I.A.

Date 21/1/44. 19 Feb 44.

Copy to: G (I) to ITALIAN ARMY.

1. In the event of permission being given for the opening up of wireless communications by the Italian Army, either in emergency, or in connection with internal security plans, certain ciphers have been approved for use by Italian personnel.
2. These ciphers are among those submitted to this HQ by Lt.Col. Ducros on 7 Dec 43. They have been subjected to expert examination, and have been classified as follows:
 - (a) The system designated ALPHA may NOT be used.
 - (b) Those designated BETA, GAMMA, and CALMA BIS may be used for administrative traffic, and in emergency.
 - (c) The ciphers themselves are cumbersome, and are NOT suitable for operational use.
3. In view of para 2 (c) above, care will be taken that, should the need for these ciphers arise, their use is limited to that prescribed in Para 2 (b) above.

The question of ciphers for operational use will be examined as and when the need arises.

4. Arrangements should be made forthwith for the training of a sufficient number of Italian personnel in the use of the ciphers mentioned in Para 2 (b) above.

Such training will be strictly limited to the enciphering and deciphering of typical administrative messages. The training of any particular section of operators will be confined to the office in which they are being trained. In no circumstances will a message enciphered in one office, be transmitted to another office for deciphering.

5. Six copies of all keys and basic documents, together with a list of holders, will be forwarded to the following:

in connection with internal security plans, certain ciphers have been approved for use by Italian personnel.

2. These ciphers are among those submitted to this HQ by Lt. Col. Ducros on 7 Dec 43. They have been subjected to expert examination, and have been classified as follows:

- (a) The system designated ALPHA may NOT be used.
 - (b) Those designated BETA, GAMMA, and GAMMA BIS may be used for administrative traffic, and in emergency.
 - (c) The ciphers themselves are cumbersome, and are NOT suitable for operational use.
3. In view of para 2 (c) above, care will be taken that, should the need for these ciphers arise, their use is limited ^{to} that prescribed in Para 2 (b) above.

The question of ciphers for operational use will be examined as and when the need arises.

4. Arrangements should be made forthwith for the training of a sufficient number of Italian personnel in the use of the ciphers mentioned in Para 2 (b) above.

Such training will be strictly limited to the enciphering and deciphering of typical administrative messages. The training of any particular section of operators will be confined to the office in which they are being trained. In no circumstances will a message enciphered in one office, be transmitted to another office for deciphering.

5. Six copies of all keys and basic documents, together with a list of holders, will be forwarded to HQ, ACMF., before any of the above ciphers are brought into use.

WCH: Gajt.

Brigadier
Brigadier,
Chief Signal Officer.

MILITARY MISSION.

Date _____

to

BRITISH SECRET = U.S. SECRET.

ITALIAN ARMY.

Subject: Italian Cipher.HQ 15 Army Group
C.M.F.2783/1/XM.M.I.A. ✓

11 Jan 44.

Ref your X 17 of Jan 7th 44.

1. The cipher referred to has been specially authorized for communication between the Italian Government, Brindisi, and the Italian Consul, Madrid, via cable and land line.
2. It is further stated by AFHQ that this cipher is not suitable for tactical use.
3. It is regretted, therefore, that its use between SENSE and NAPLES cannot be authorized.

WCH: Majt

for *RHO Taylor Col*
Brigadier,
Chief Signal Officer.

282

SUBJECT: Ital a Cipher

Military Mission
to ITALIAN ARMY
X 17
7 Jan 44

15 Army Gp

Copy to: Allied Control Commission

Reference Allied Control Commission TC/8/1 of 4 Jan.

May permission be given for this cipher to be used
for Most Secret messages from SMRE to NAPLES.

ABC

[Signature]
Brig
Comd

061345A

5 JAN 1944

X 17

KWS/nms

In reply
refer to: TO/8/1

4 January 1944

SUBJECT: Italian Cipher.

TO : , GSC., 15 Army Group.

A double transposition type Italian cipher has been authorized for general use by Italians, in a message from AFHQ number 10418 of 6 December 1943. Copies are held at AFHQ. You may wish to know the position.

The cipher will be used on authorized circuits, the only one of which, so far as A.C.C. is concerned, is the Italy - Malta - Gibraltar submarine cable link to Madrid, for diplomatic messages.

Ellery W. Stone
ELLERY W. STONE
Captain, USNR
Communications Section

Copy to: British Military Mission to Italian Army
with reference to memo. no. x/12 of 28 October 1943.

2821

SUBJECT: Italian Ciphers

CSO 15 ARMY GP

MOST SECRET

Military Mission
to ITALIAN ARMY

X/17

22 Nov 43

Further to our X/14 of 17 Nov and reference para 6 of your questionnaire, enclosed are 4 copies of a translation of 7 Army letter 4/1837/OM of 16 Nov and enclosure (Italian Cipher LMT2) together with one copy of "Flowering in the wilderness" by John Galsworthy.

This is the only cipher the Italian Army have at the moment and is intended for use over SMIS, Army and Corps links. There are other ciphers in course of preparation details of which will be sent to you as soon as they are complete.

Please return "Flowering in the wilderness" as it is the only copy 7 Italian Army hold.

ABC

R. H.
Brig
Comm

28-3

TRANSLATIONSubject:- Wireless Messages to XXXI CorpsRef: 4/1637/OM
16 Nov 43

To :- B M M (official)

From:- GHQ 7 Army

With ref to your X/12 of 28 Oct(para 3) we have the pleasure of enclosing herewith:-

Copy of cipher code to be used at this HQ (from the novel
"Flowering Wilderness" : Linda in Flare of John Galsworthy)

Copy of instructions for use of ciphers.

Copy of code numbers allotted to this HQ and different units ~~also~~
attached, for the period from 11 Nov 43 to 31 Dec 43.

This being the only copy in our possession kindly return it as
soon as possible.

Signed: Brig Gen R PELLIGRA
Chief of Staff

2829

DC/om

COMANDO DELLA 7^a ARMATA
Stato Maggiore = Ufficio Ordinamento

N° 4/1837/O.M. di prot.

P.M. 107, li 16 novembre 1943

O G G E T T O : comunicazioni radio con il XXXI S.A.--

ALLA MISSIONE MILITARE BRITANNICA (a mezzo ufficiale)

LEQUILE

In relazione alla richiesta formulata da codesta Missione
col comma 3° del foglio X/12 in data 28 ottobre u.s. si trasmette:

- la copia del cifrario in uso presso questo Comando. (Romano "Landa in fiore" di John Galzworthy);
- copia delle istruzioni per l'uso del cifrario;
- copia della tabella dei numeri personali assegnati a questo Comando, ed agli enti dipendenti, per il periodo dall'11 novembre 1943 al 31 dicembre 1943.

Trattandosi di unica copia in possesso di questo Comando
si prega codesta Missione di valerne curare la restituzione al più presto.--



d'ordine
IL GENERALE DI DIVISIONE CAPO DI S.M.
(Raffaele Pelligrà)

2828

SEGRETISSIMO

CIPRARIO L M T 2

-METOF- DEL LIBRO-

- I°) - Il corrispondente è provvisto di una rivista od altro libro e di un numero personale composto di 4 cifre.

OPERAZIONI DI CIFRATURAFRASE CHIAVE

- II°) - Per cifrare un messaggio è necessario in primo luogo scegliere una frase chiave dal libro. Questa frase dev'essere costituita dalle prime parole di una riga dalle prime 99 pagine e la lettera finale della frase chiave dev'essere l'ultima lettera della parola contenente la quindicesima lettera.

ESEMPIO: Pag. 37, linea 5 della prestabilita lettura del libro :
 "COSI' TACENDO CAMMINAVA VERSO LA...." ecc. La parola CAMMINAVA contiene la quindicesima lettera della linea in modo che la frase chiave sarà:
 "COSI' TACENDO CAMMINAVA" che ha 20 lettere.

- III°) - Le lettere della frase chiave devono quindi essere numerate nel loro ordine alfabetico. Quando una lettera ricorre più volte nella frase la numerazione è continuata da sinistra a destra come nel caso di "A" e "C" sotto descritti:

C O S I T A C E N D O C A M M I N A V A
 5 16 18 10 19 1 6 9 14 8 17 7 2 12 13 11 15 3 20 4

Il messaggio dovrà quindi essere cifrato con una doppia trasposizione in uno schema costruito come più appresso indicato.

- IV°) - I messaggi nel cifrario di cui trattasi devono, per sicurezza, essere non minori di 150 lettere e non devono essere superiori a 500 lettere in lunghezza. Le frasi usuali devono essere evitate. La fine del messaggio dev'essere indicata con una frase come "arrivederci", "ciao" etc.

- V°) - Per procedere alla trasposizione di cui sopra bisogna trascrivere il messaggio fra due gruppi di lettere di sicurezza. Questi gruppi devono essere costituiti almeno di 5 lettere senza significato comune, e devono essere posti in principio ed in fine del testo. Quello scritto alla fine deve contenere lettere diverse da quelle del gruppo scritto al principio. Non devono essere usate lettere poco correnti. Tali gruppi devono contenere un numero di lettere tale che: a) il totale delle lettere del messaggio sia multiplo di 5, b) ci sia una buona proporzione fra le lettere e gli spazi vuoti nell'ultima linea dello schema. Questa linea non deve essere mai riempita.

ESEMPIO:

"ETIANH" Giunto qui la scorsa settimana, punto Bene ricevuto dagli amici che voi sapete e ospite di essi attualmente punto Info-rmatemi se riceverete questo messaggio e fatemi avere ordini al più presto arrivederci "SRETMOE"

2827

- 2 -

PRIMO SCHEMA

Il messaggio con le sue lettere di sicurezza deve quindi essere scritto orizzontalmente sotto i numeri della frase chiave come qui di seguito:

C O S I T A C E N D O C A M M I N A V A
 5 16 18 10 19 1 6 9 14 8 17 7 2 12 13 11 15 3 20 4

E T I A N H G I U N T O Q U I L A S C O
 R S A S E T T I M A N A P U N T O B E N
 E R I C E V U T O D A G L I A M I C I C
 H E V O I S A P E T E E D S P I E D I
 E S S I A T T U A L M E N T E F U N T O
 I N F O R M A T E M I S E R I C E V E R
 E T E Q U E S T O M E S S A G G I O E F
 A T E M I A V E R R E O R D I N I A L P I
 U F R E S T O A R R I V E D E R C I S R
 E T N O E

SECONDO SCHEMA

Fatto il primo schema si proceda al secondo schema che è costruito con la medesima intestazione numerica delle colonne del primo. La prima trasposizione è effettuata leggendo verso il basso le colonne nell'ordine dei numeri posti in testa e scrivendo le lettere orizzontalmente lungo le linee del secondo schema, per esempio le lettere della colonna intestata col numero 1 sono scritte lungo la prima linea del secondo schema continuando, se necessario, nella seconda; le lettere della colonna 2 seguono, e così avanti finché la totalità delle lettere del primo schema sia trasposta nel secondo schema, come qui di seguito:

5 16 18 10 19 1 6 9 14 8 17 7 2 12 13 11 15 3 20 4

H T V S T M E A T Q P L O N E S D E S B
 C E N V O L I O N C I O R F I R E R E H
 E I E A U E G T U A T A S V O O A G E E
 S S R V N A D T L M M E R I I T P U T T
 E A A S C O I O Q M E O L T M I P O G I
 R U U I S T R A I D I N A T E I G N E U
 M O E A E O R R A O I T U E I A C T S R
 E S N T T P T T N A E M I E O I I A I V
 S F E E R N N E E I A R U I S E C E I D
 T E E P S

TRASPOSIZIONE FINALE

VIII°)-La trasposizione finale è effettuata leggendo verso il basso le colonne del secondo schema nell'ordine in cui sono numerate e scrivendo le lettere in gruppi di cinque pronte per la trasmissione.

GRUPPO INDICATORE

IX°)-Il messaggio viene individuato con gruppo indicatore di quattro cifre. Questo è costruito come segue:

- a) Le prime due cifre rappresentano il numero della pagina dalla quale è stata tolta la frase chiave;

...//...

- 3 -

- b)- Le due ultime cifre rappresentano il numero della riga dalla quale la frase chiave è stata tolta.
Al gruppo di quattro cifre così ottenute devono essere sommate, senza riporto, le cifre del numero personale. Il risultato è il gruppo indicatore.

ESEMPIO

Perciò.....	3705
più numero personale.....	2845
	5540

Questo gruppo indicatore deve essere posto all'inizio del messaggio cifrato. Alla fine del messaggio deve essere posto il numero delle lettere del messaggio cifrato seguito dalla ripetizione del gruppo indicatore.

MESSAGGIO CIFRATO

- X°)-Pertanto il messaggio cifrato da trasmettere viene ad essere:

5540	MLEAO	TOPNO	RSRLA	UIUER	GUCNT	AEBHE	TIURV	DHCES
	ERMES	TEIGD	IRRTN	LOAEO	NTBRO	CAMMD	CAIAO	TTOAR
	VSIAT	EPSRO	TIIAI	ENFVI	TPEEI	EIOIM	EIOST	NULQT
	APPGG	ICTEI	SAUOS	FRPIT	MEIIE	AVNER	AUENE	ETOUN
	3SEET	GESII	175	5540				CSETR

- XI°)-Bisogna tener sempre norma dei gruppi indicatori usati e nessun gruppo indicatore può essere usato due volte. Le frasi chiave usate dovranno essere di varie lunghezze il più spesso possibile.

OPERAZIONI DI DECIFRATURA

- XII°)-Per decifrare, le operazioni sono inverse di quelle per cifrare.

FRASE CHIAVE

- XIII°)-La frase chiave viene ricostruita sottraendo senza riporto il numero personale dal gruppo indicatore ed estraendo dal libro la frase chiave indicata dal risultante gruppo di 4 cifre.

Le lettere della frase chiave devono essere allora numerate nello stesso senso di quando si cifra. La misura dello schema richiesto è calcolata dividendo il numero delle lettere del messaggio per il numero delle lettere della frase chiave.

SCHEMA

- XIV°)-Quindi nell'esempio di cui sopra:

Indicatore.....	5540
meno numero personale.....	2845
	resta.....
	3705

(I° esempio pag. 37 linea 05) "COSI' TACENDO CAMMINAVA". Lo schema ha quindi 20 colonne dato che la frase chiave è composta di 20 lettere. Poichè il numero delle lettere del messaggio è 185, il numero delle linee richieste è: 185 diviso per 20 cioè 9 linee più 5 lettere. Pertanto lo schema è disegnato con dieci linee, delle quali gli ultimi quadranti sono depennati perchè devono restare vuoti?

2815

...//...

- 4 -

XV°) - Le lettere del messaggio cifrato devono essere quindi poste nello schema cominciando a scrivere verticalmente nella colonna intestata con n° 1 poi nella colonna intestata col n° 2 e così via. Quando si è ultimata la scrittura delle lettere, tutti i quadratini dello schema devono essere occupati ad eccezione degli spazi vuoti nell'ultima linea.

XVI°) - Dopo bisogna disegnare un secondo schema identico al primo. Le lettere del primo schema devono essere trasportati nelle caselle del secondo schema leggendo orizzontalmente lungo le linee del primo e scrivendo verticalmente nelle colonne del secondo, seguendo l'ordine delle cifre scritte in testa alle colonne (come per il primo schema)

TESTO

XVII°) - Il messaggio originale è ora ottenuto leggendo orizzontalmente lungo le linee di questo schema e non tenendo conto delle lettere di sicurezza poste al principio ed alla fine.



28.4

COMANDO SUPREMO

Ufficio "I" - Sez. Organizzazione

allegato al foglio 26/D/Cif.in data 1° novembre 1943

NUMERI PERSONALI

assegnati ai Comandi di G.U. della 7^a Armata

COMANDO	dall'11 al 20 novembre	Dal 21 al 30 novembre	Dal 1 al 10 dicembre	Dall'11 al 20 dicembre	Dal 21 al 31 dicembre
Comando 7 ^a Armata	3902	7543	5280	9451	1545
Comando IX C.A.	8122	4926	2295	5738	1210
Comando XXXI C.A.	5875	6230	3490	2813	7948
Comando LI C.A.	1308	9271	4238	6542	3496
~~~~~					
Per le radiotrasmissioni circolari sarà adoperato il numero unico	4385	5972	1576	8641	9468

valevole per tutte le unità in indirizzo.-

In tal caso ogni trasmissione sarà preceduta dalla sigla

"cir" che dovrà essere interposta al numero chiave del testo cifrato.-





0905