~~SECRET NATO~~

NATO UNCLASSIFIED

COPY NO. 53

S.G. 171/4

18 August 1952

Pages 1 - 18, incl.

REPORT BY THE COMMUNICATIONS-ELECTRONICS COORDINATION SECTION

to the

STANDING GROUP

on

PLAN FOR THE EMPLOYMENT OF THE COMBINED CIPHER MACHINE
(CECS 15/6)

THE PROBLEM

1. To enhance the security of the Combined Cipher Machine in general and in particular to provide means for the encypherment of TOP SECRET traffic.

FACTS BEARING ON THE PROBLEM

2. The United States and the United Kingdom have now completed a further study of the problem of increasing the security of the Combined Cipher Machine and have agreed upon:

a. An electro/mechanical modification to the maze which can easily be made to both C.C.M. Mk II and C.C.M. Mk III. This modification is known as HERMES and details of it and of the procedure for its introduction are given at Enclosure "A".

b. Procedural changes as described in Enclosure "B". These entail the preparation, production and distribution of key lists of a new type.

c. The increase from ten to twenty of the number of rotors in a set.

d. The design of a rotor which will permit rotation of the notch rings.

3. The United States and the United Kingdom have agreed it will be possible:

a. To introduce HERMES for NATO Communications on 1 October 1952.

b. To prepare, produce and distribute selected key lists reflecting the procedural changes by 1 October 1952.

c. To start the introduction of rotors with rotatable notch rings on 1 May 1953, issuing sets of 10 such rotars for use in conjunction with the sets of 10 then in force.

4. A plan for the employment of the Combined Cipher Machine which implements the measures described above is attached at Enclosure "C".

CONCLUSIONS

5. It is concluded that:

a. The "HERMES" modification described in Enclosure "A" should be made to all CCM's used for NATO Communications effective 1 October 1952.

b. The procedural changes described in Enclosure "B" should be introduced for all NATO CCM cryptochannels effective 1 October 1952.

c. 20-rotor sets should replace 10-rotor sets on all NATO CCM crypto channels as soon and as far as procuction of the equipment allows.

d. Rotors with rotatable notch rings should be introduced on all NATO CCM crypto channels as soon and as far as production of the equipment allows.

RECOMMENDATIONS

6. It is recommended that:

a. The above conclusions be approved.

b. The United States and the United Kingdom be asked to undertake urgently the provision of:

(1) The necessary kits to modify in accordance with Enclosure "A" the CCM's Mk III held by NATO forces.

(2) The necessary instructions to promulgate the procedural changes described in Enclosure "B".

(3) The necessary rotors and key lists to implement the plan detailed in Enclosure "C".

c. Member Nations and Supreme Commanders, on receipt of the modification kits for CCMs Mk III, take steps to ensure that all CCM's, both Mk II and Mk III, held by forces under their command are modified in accordance with Enclosure "A".

d. A memorandum substantially as in Enclosure "D" hereto be issued.

ENCLOSURE "A"

C.C.M. (HERMES) MODIFICATION

1. The CCM Mark III Adaptor (BID/08/3A) is to be modified by fitting two new pawl assemblies designed to change the order of rotation of the rotors. This modification, known as the HERMES modification, will be achieved by means of a kit of machine parts which will be supplied to holders on a scale of one per machine. After the modification has been carried out the short title of the C.C.M. Adaptor will be amended to BID/08/3D. C.C.M.'s Mark II (SIGROD or CSP 1700) will also be modified.

2. The C.C.M. Mark III Adaptor modification kit will be supplied in a carton containing:

2 new pawl assemblies
4 springs
1 gauge
1 ivorine label
1 instruction sheet (BID/08/3D drawing)
1 modification certificate

The modification kits will be treated as secret registered cryptographic items. Each kit will bear a serial number which will also appear on the modification instructions. After the modification has been carried out, the ivorine label is to be fixed to the adaptor, instructions must be destroyed, and the modification certificate completed and returned to the Distributing Authority. The modification certificate will be in the following form:

"It is hereby certified that BID/08/3A Serial Number.....
has to-day been modified to BID/08/3D Serial Number.....
BID/08/3D Drawing Copy No.....has been destroyed."

3. Modification of the C.C.M. Adaptor is a simple operation and can be carried out by a mechanic in less than one hour. After modification has been carried out and before the Adaptor is used for encrypting live traffic cryptographic personnel must carry out a test routine. Details of the tests to be made are given in Appendix "A".

4. Modification of the C.C.M. Mark II (SIGROD or C.S.P. 1700) involves changing some electrical circuits. Details of these changes

are given in Appendix "B". The tests to be carried out by the cryptographic personnel are the same as those for the C.C.M. Adaptor Mark III in Appendix "A". After modification the short titles of the C.S.P. 1700's thus modified will be changed to AFSAM 25, the short titles of the SIGRODS to AFSAM 25A by affixing to the machines new nameplates which have been provided separately. A modification certificate in the following form will be submitted to the Distribution Authority:

> "It is hereby certified that C.S.P. 1700, (or SIGROD), register number.....has today been modified to AFSAM 25 (or AFSAM 25A) register number....."

5. Once the C.C.M. has been modified for HERMES working it cannot be used for encrypting or decrypting messages in the old C.C.M. cryptosystem. In order to minimize the dislocation of traffic, arrangements should be made with originators to delay whenever possible sending traffic in the old C.C.M. cryptosystem during the last 12 hours of 30th September, 1952 unless it is certain that the addressees have more than one C.C.M. available. Otherwise, traffic should be held over until it can be encrypted in the HERMES cryptosystem using the key for 1st October, 1952, or the message may be encrypted in the NATO General Cipher System. No cryptograms bearing the date 1st October, 1952, will be transmitted before the day. If the originators date-time group differs from that of the key list, it will be encrypted and an appropriate date-time group will be used on the cryptogram as transmitted.

6. After 0001Z hrs. 1st October 1952, no traffic will be encrypted in the old C.C.M. cryptosystem.

7. Posts with more than one C.C.M. available should modify and test one or more equipments on 30th September, 1952, so that the changeover to HERMES can be effected without delay. The remaining equipments should be modified and tested as early as possible on 1st October, 1952, except that at least one equipment should be left

unmodified for not more than three days to cater for incoming traffic in the old C.C.M. cryptosystem.

8. Posts with only one C.C.M. available should carry out the modification as soon as possible after 0001Z hrs. 1st October, 1952. Should any traffic encrypted in the old C.C.M. be received after the modification has been carried out, an encrypted request will be made for a repeat in the HERMES cryptosystem. Cryptocentres receiving such a request will re-encrypt the message using the key for the day on which the re-encryption is carried out and giving the message an appropriate external date-time group. The true originator's date-time group will be encrypted and care will be taken to ensure that the point of bisection used for the second encryption differs from that used for the first encryption.

APPENDIX "A" TO ENCLOSURE "A"

C.C.M. (HERMES) ADAPTOR

TEST ROUTINE

1. This test routine is to be carried out on every Combined Cipher Machine modified for HERMES working before any live message is encrypted on the machine. CCBP 0311 rotors are to be used for all tests for CCM Mark III; AFSAR 3910 rotors will be used for tests on the CCM Mark II, other than those held by submarines. Rotors CSP 2811 will be used for tests of the CCM's held by submarines.

2. For each test:

a. Place the rotors in the machine in accordance with the rotor arrangement given.

b. Set the rotors to the rotor alignment given.

c. Set the machine to ENCIPHER or DECIPHER as appropriate.

d. Set the counter to zero.

e. For tests 1 and 2,

(1) Operate the "Run-out" (Blank and Repeat) key until the counter gives the appropriate reading.

(2) Check the alignment of the rotors on the machine with that given in the test data.

f. For test 3, check that the resultant plain language is identical with that given in the test data.

3. a. Test 1. (Machine at ENCIPHER)

Rotor Arrangement	-	1	2R	3	4R	5
Rotor Alignment	-	A	B	C	D	E
Counter Reading	-			750		
Resultant Rotor Alignment:						
Using CCBP 0311, AFSAR 3910	-	R	D	G	X	D
Using CSP 2811	-	Z	Y	G	C	B

b. Test 2. (Machine at ENCIPHER)

Rotor Arrangement	-	6R	7	8R	9	10R
Rotor Alignment	-	W	X	Y	Z	V
Counter Reading	-			1000		
Resultant Rotor Alignment:						
Using CCBP 0311, AFSAR 3910	-	G	D	K	G	I
Using CSP 2811	-	T	D	K	F	G

* c. Test 3. (Machine at DECIPHER)

Rotor Arrangement - 5 2R 7 1R 8R
Rotor Alignment - P N T V A
Decipher the following groups--

(1) Using CCBP o311, AFSAR 3910:

XIPVF YMPSI HGMEP AGHWQ ZQKGC JFHPM BQDQW MXOIQ WBEPW
BEWWT JIUFB WSVJE BWTBR GJYCW AMMIY VTEIS TLFEI IZSMB
EJVEM

(2) Using CSP 2811:

YIHHH NOZIQ NVEZP BNEPI CSBVV JSCPF
QGMFB QMYAX GCZGT PHOCZ MAWFT MZAOF
KJBEC QOAIV BINTH JEBOC PGYPK MSRGU
QLCOV

Resultant Plain Language -

THIS IS A TEST MESSAGE TO CHECK THE ACCURACY OF THE
MODIFIED ADAPTOR ABCDEFGHIJKLMNOPQRSTUVWXYZ

*When carrying out Test 3 with C.C.M. Mark II, blank once before decrypting.

APPENDIX "B" TO ENCLOSURE "A"

C.C.M. MARK II

WIRING MODIFICATION FOR CSP 1700 AND SIGROD

1. General - The purpose of this modification is to change the rotor stepping pattern so that the No. 1 rotor stepping contact (operated by rotor No. 2) will control the stepping of rotor No. 5, and the No. 4 rotor stepping contact (operated by rotor No. 4) will control the stepping of rotor No. 1.

2. Modification Procedure for CSP 1700 - The following changes are to be made in the wiring at the rotor stepping contact terminal block (see actual wiring diagram and plate 4-1 in CSP 1802 B or ACP 233).

a. Remove YE wire from terminal 1 (reading from left to right) and connect it to terminal 5.

b. Remove the WH wire from terminal 5 (reading from left to right). Splice, solder, and tape a 2-1/2 inch piece of 24 gauge wire to the WH wire. Strip 1/2 inch of insulation from the free end of the wire, tin it, and connect it to terminal 1.

3. Modification Procedure for SIGROD - The following wiring changes are to be made at the rotor stepping contact terminal block (see actual wiring diagram for SIGROD and figure 14 in SIGLIL-1 or ACP 234).

a. Remove OR wire from the right-hand side of terminal 2 (reading from front to rear) and connect it to the right-hand side of terminal 5.

b. Remove the BL wire from the right-hand side of terminal 5 (reading from front to rear) and connect it to terminal 2.

ENCLOSURE "B"

SIMPLEX PROCEDURE FOR C.C.M.

1. General

Two procedures are herein described. The first procedure, described in paragraph 4 below, is to be used for the encipherment of RESTRICTED, CONFIDENTIAL and SECRET messages. The first procedure entails only one encipherment of each message. The second procedure, described in paragraph 5 below, is to be used only for the encipherment of TOP SECRET messages. The second procedure entails super-encryption of each message.

2. Keying Material

The Key list contains the following data:

a. Two TOP SECRET and five SECURE - and - below system indicators which remain in force for the life of the Key list (i.e. one month).

b. A daily rotor arrangement.

c. A 26-30 letter check group for the above.

d. Two 10-letter random groups for each day.

e. Two rotor-setting tables, each effective for the life of the Key list (i.e. one month).

(1) Table 1 contains a rotor number and an alignment letter in each cell.

(2) Table 2 contains an alignment letter in each cell.

3. The appearance of the above data in a C.C.M. Key list is as follows:

SYSTEM INDICATORS FOR SECRET-AND-BELOW MESSAGES.	FOR TOP SECRET MESSAGES.
XNABU	
RXLBA	TTWHL
PFBUC	UAIBG
LOJFX	
ZKOSE	

DATE	DAILY ROTOR ARRANGEMENT	26-30 LTRCK	RANDOM GROUPS No. 1	No. 2
1	5 4R 2 1 6R	LXLOA	VKIGT/TYOBK	KPQSF/RCKNF
2	2R 3R 7R 4 9	COCTP	AWNIW/MHSOE	AISTQ/MKWPH

TABLE 1

SECOND LETTER

FIRST LETTER

	A	B	C	D	E	F	G	H	I	J	etc.
A	2 O	9R B	5 E	8 S	9 Q						
B	8 D	5 M	1R X	6 A	8 T						
C	2 R	7R R	3R U	9 1	4 P						
D	4 A	Ø E	7R Q	6 1							
etc	6 H	7R 1	6 C	1 N							

TABLE 2

(For use in super encryption only)

SECOND LETTER

FIRST LETTER

	A	B	C	D	E	F	etc.
A	G	O	U	E	P		
B	D	B	H	V	L		
C	I	M	N	K			
D	Q	J	W	F			
E	C	G	A	N			
etc							

3. System Indicator

The system indicators identify:

a. The specific CCM cryptosystem used for encipherment and

b. The procedure used in encipherment.

For each message classified SECRET-and-below, and therefore enciphered using the first procedure, a system indicator is selected at random from the fice groups listed under "SECRET-AND-BELOW". For each message classified TOP SECRET, and therefore encrypted using the second procedure, either of the two groups listed under TOP SECRET is selected. The system indicator is transmitted as the first and last groups of the message.

4. First Procedure. Method of Encipherment of Messages Classified SECRET CONFIDENTIAL or RESTRICTED

a. Five letters are chosen at random. They should not form a word or a recognized abbreviation. This group is known as the message indicator and is phoneticized and transmitted in clear as the second to sixth groups of the message.

b. The rotors are arranged according to the daily rotor arrangement. (This arrangement can be checked by the 26-30 letter check.)

c. The rotors are aligned to the letters of the message indicator.

*d. The daily 10-letter Random Group No. 1 is enciphered. The resultant 10 letters are known as the intermediate sequence.

e. The intermediate sequence is formed into five digraphs by pairing the 1st letter with the 6th, the 2nd with the 7th, the 3rd with the 8th, the 4th with the 9th and the 5th with the 10th.

f. The cell corresponding to each digraph is located in rotor-setting Table No. 1, the first letter of the digraph designating the row and the second the column, and the rotor numbers and alignments found in the cells are recorded. If a rotor number found in a cell is one that has been found in a cell that has already been recorded, the next cell to the right, which contains an available rotor number, is used. If the end of the row is reached, the first cell in the same row is resorted to.

*When C.C.M. Mk II is in use, before encipherment is commenced, the rotors must be advanced once by use of the "BLANK" Key with the function controller turned to "R".

*g. The rotors are rearranged and aligned according to the arrangement and alignment thus recorded from Table I. This is the message rotor arrangement and message rotor alignment on which the message is then enciphered.

5. Second Procedure. Method of Encipherment of Messages Classified TOP SECRET

a. Five letters are chosen at random. They should not form a word or a recognized abbreviation. This group is known as the message indicator and is phoneticized and transmitted in clear as the second to sixth groups of the message.

b. The rotors are arranged according to the daily rotor arrangement. (This arrangement can be checked by the 26-30 letter check.)

c. The rotors are aligned to the letters of the message indicator.

*d. Both the 10-letter random groups No. 1 and No. 2 are enciphered. The resultant 20 letters are the intermediate sequence.

e. The first ten letters of the intermediate sequence are formed into five digraphs by pairing the 1st with the 6th, the 2nd with the 7th, the 3rd with the 8th, the 4th with the 9th, the 5th with the 10th.

f. The cell corresponding to each digraph is located in rotor-setting Table No. 1, the first letter of the digraph designating the row and the second the column, and the rotor numbers and alignments found in the cells are recorded. If a rotor number found in a cell is one that has been found in a cell that has already been recorded, the next cell to the right, which contains an available rotor number, is used. If the end of the row is reached, the first cell in the same row is resorted to.

*When C.C.M. Mk II is in use, before encipherment is commenced, the rotors must be advanced once by use of the "BLANK" Key with the function controller turned to "R".

*g. The rotors are rearranged and aligned according to the arrangement and alignment thus recorded from Table 1 and the message is enciphered. The result is known as the intermediate cipher text.

h. The second ten letters of the intermediate sequence are formed into five digraphs by the 11th with the 16th, the 12th with the 17th, the 13th with the 18th, the 14th with the 19th and the 15th with the 20th.

i. The cell corresponding to each digraph is located in rotor-setting Table No. 2, the first letter of the digraph designating the row and the second the column, and the letters found in the cells are recorded, regardless of repeats.

j. The rotors are realigned to the letters thus recorded but they are not rearranged.

k. The intermediate cipher text is enciphered preceded by the 11th to the 15th letters of the intermediate sequence and followed by the 16th to the 20th. These groups are enciphered in these positions to provide a check to the deciphering operator who, on recognizing them as part of the intermediate sequence, is assured that the first phase of decipherment has been accomplished correctly. During this encipherment of the intermediate text, when the CCM Mk. II is in use, the space bar is used for encrypting the letter Z; when the CCM Mk. III is in use, the Z Kay is used for encrypting the letter X and the space bar is used for encrypting the letter Z.

l. The spaces between the groups of the intermediate cipher text are not enciphered.

5. Length of Message

The length of messages or the cryptoparts will be limited to 300 groups, the maximum number which may be encrypted using any one message indicator. The same message indicator must never be used for more than one message.

*When C.C.M. Mk II is in use, before encipherment is commenced, the rotors must be advanced once by use of the "BLANK" Key with the function controller turned to "R".

6. Bisection

Bisection will be employed.

7. Variable Spacing

Variable spacing will not be employed.

8. Encipherment of Message Classification

The classification of a message which is SECRET, CONFIDENTIAL or RESTRICTED must be enciphered immediately after the bisection group. The classification of TOP SECRET messages need not be enciphered since it is indicated by the system indicator.

9. Decipherment

Decipherment is merely a matter of reversing the above procedures but it should be noted that in the case of the TOP SECRET procedure after the first process of decipherment has been performed any spaces which appear in the intermediate cipher text should be filled in with Z and so decrypted.

ENCLOSURE "C"

PLAN FOR THE EMPLOYMENT OF THE C.C.M.

1. Machines

All C.C.M. Machines, both Mark II (CSP 1700 and SIGROD) and Mark III, will be modified to HERMES on 1 October 1952.

2. Key Lists

a. The following Key Lists are effective now and will remain so until further notice.

ACP's 228, 229, 235.

b. The following Key Lists are effective now but will be temporarily suspended on 1 October 1952. They will be reintroduced as soon as production facilities permit.

ACP's 236, 252, 253.

c. The following Key List is effective now but will be discontinued on 1 October 1952.

ACP's 237.

d. The following Key Lists will be prepared for use as soon as production facilities permit.

ACP's 247, 254.

e. The following Key Lists will be prepared for retention as war reserve as soon as production facilities permit.

ACP's 244 - 246.

f. The following Key Lists will no longer be held as war reserve in view of the introduction of NATO General Cipher.

ACP's 238 - 243.

3. Rotors

a.	Rotors	CCBP 0311 or AFSAR 3910
	Period	now until 30 April 53
	ACP's	228, 229, 236, 252
b.	Rotors	CCBP 0311 plus CCBP 0311-1 (rotatable notch rings) or AFSAR 3910 plus AFSAR 3910-1 (rotatable notch rings)
	Period	1 May 1953 until further notice
	ACP's	228, 229, 236, 252

c.	Rotors	CCBP 0211 or CSP 2811
	Period	now until 30 June 53*
	ACP's	235, 244-246
d.	Rotors	CCBP 0211 plus CCBP 0211-1 (rotatable notch rings) or CSP 2811 plus AFSAR 3914-1 (rotatable notch rings)
	Period	1 July 1953* until further notice.
	ACP's	235, 244-246
e.	Rotors	CCBP 0213 or CSP 2813
	Period	Now until further notice
	ACP's	253

A decision will be made regarding the rotors to be used with ACP's 247 and 254 when these Key Lists are available for issue.

---

* Or earlier if rotor production permits

ENCLOSURE "D"

MEMORANDUM FOR: All Member Nations except Iceland and Luxembourg
SACEUR
SACLANT
CinC CHANNEL
EMCCC

SUBJECT: Plan for the Employment of the Combined Cipher Machine

1. In order to enhance the security of the Combined Cipher Machine in general and in particular to provide means for the encipherment of TOP SECRET traffic, on _____ the Standing Group approved that:

a. The "HERMES" modification described in Enclosure "A" should be made to all CCM's used for NATO Communications effective 1 October 1952.

b. The procedural changes described in Enclosure "B" should be introduced for all NATO CCM cryptochannels effective 1 October 1952.

c. 20-rotor sets should replace 10-rotor sets on all NATO CCM cryptochannels as soon and as far as production of the equipment allows.

d. Rotors with rotatable notch rings should be introduced on all NATO CCM cryptochannels as soon and as far as production of the equipment allows.

2. The United States and the United Kingdom are requested to undertake urgently the provision of:

a. the necessary kits to modify in accordance with Enclosure "A" the CCM's Mk III held by NATO forces.

b. The necessary instructions to promulgate the procedural changes described in Enclosure "B".

c. the necessary rotors and key lists to implement the plan detailed in Enclosure "C".

3. Member Nations and Supreme Commanders, on receipt of the modification kits for CCM's Mk III, are requested to ensure that all CCM's both Mk II and Mk III held by forces under their command are modified in accordance with Enclosure "A".

~~SECRET NATO~~

19 August 1952

NATO UNCLASSIFIED

COPY NO. 53

NOTE BY THE SECRETARY

to the

HOLDERS OF S.G. 171/4

CORRIGENDUM

Holders of S.G. 171/4 (Plan for the Employment of the Combined Cipher Machine (CECS 15/6)) are requested to replace page 1 with the enclosed page 1 and to destroy the removed page by burning.

Corrected 8/21/52 gcl

3/11

S.G. 171/4

18 June 1952

Pages 1 - 18 inc.

REPORT BY THE COMMUNICATIONS ELECTRONICS COORDINATION SECTION

to the

STANDING GROUP

on

PLAN FOR THE EMPLOYMENT OF THE COMBINED CIPHER MACHINE (CECS 15/6)

THE PROBLEM

1. To enhance the security of the Combined Cipher Machine in general and in particular to provide means for the encypherment of TOP SECRET traffic.

FACTS BEARING ON THE PROBLEM

2. The United States and the United Kingdom have now completed a further study of the problem of increasing the security of the Combined Cipher Machine and have agreed upon:

a. An electro/mechanical modification to the maze which can easily be made to both C.C.M. Mk II and C.C.M. Mk III. This modification is known as HERMES and details of it and of the procedure for its introduction are given at Enclosure "A".

b. Procedural changes as described in Enclosure "B". These entail the preparation, production and distribution of key lists of a new type.

c. The increase from ten to twenty of the number of rotors in a set.

d. The design of a rotor which will permit rotation of the notch rings.

3. The United States and the United Kingdom have agreed it will be possible:

a. To introduce HERMES for NATO Communications on 1 October 1952.