instructions in BSG/01/IA and B with particular reference to the possible necessity for paraphrasing

Form Z. 43
Declassified by ASD - 17/11/2021
Information removed for national security and/or personal sensitivities

## MESSAGE

Precedence		DSB F	1 / -	Cy. Ser. No.	1
PRICALLY .		 193	FROM	Circuit	2
DSB MELBOURNE	LONDON	W.	G.C.O.		

Classification TOP SECRET FROTH

FROM BOTTERILL

RETURNED TO

FROM

THURSDAY MORNING. FOLLOWING ARE MAIN

POINTS ARISING FROM VISIT. WRITTEN REPORT WILL FOLLOW

2. THERE IS NO BACKLOG OF UNTRANSLATED DOCUMENTS EITHER IN CYPHER OR

IN PLAIN TEXT AT THE

(HEREAFTER REFERRED TO AS

)

ALL CODES AND CYPHERS USED TO DATE HAVE BEEN SOLVED BY THE EXPERT (HEREAFTER REFERRED TO AS THE GENERAL)

- 2. M.C.P. CRYPTOGRAPHY.
- (A) ALL MCP CYPHER SEEN SO FAR HAS BEEN INTERSPERSED WITH PLAIN TEXT
- (B) JUDGING FROM BOTH CAPTURED AND SOLVED CYPHER MATERIALS MCP CRYPTOGRAPHY HAS BEEN FAIRLY SOPHISTICATED IN THE NORTH

BUT VERY ELEMENTARY IN THE CENTRE AND SOUTH. NO OBVIOUS EVIDENCE
OF EITHER INTERNAL V COORDINATION OR OUTSIDE INFLUENCE
(C) TYPICAL NORTHERN SYSTEM CONSISTS OF CODE BOOK OF 40 TO 60 PAGES
OF SINGLE CHARACTERS ARRANGED IN EITHER RADICAL OR

ORDER, FOLLOWED BY SEVERAL HANDWRITTEN PAGES CONTAINING NUMERALS DATES, PLACE NAMES, COMMON COMPOUNDS ETC. THERE IS NORMALLY SPACE FOR THREE SETS OF PAGE NUMBERS AND ROW/COLUMN CO-ORDINATES (ALWAYS FILLED IN BY HAND AND APPARENTLY IN MOST CASES HUMAN RANDOM). EACH USER OF THE BOOK WOULD BE ALLOTTED A CERTAIN SET FOR HIS USE ONLY.

ML	MLD	МН	MHR	MS	MSC	MSO	MSS	MQ	МТ	MZ	MZC	suko	FUS	MP	SIG	SIG I	SIG
1		X		х										Х		A STATE OF THE PARTY OF THE PAR	
	1				Турес	by				Time	Турес				Syst	em Indi	cator
X	4/54	1				H.C.			- 1	64	1245	52/4/	54			No. of London	
	\			V X	X X	V X X	X X Typed by	X X Typed by	X X Typed by	Typed by	Typed by Time	Typed by Time Typed System	Typed by Time Typed System Indi				

t' message has to be re-encrypted, attention is ca' to the instructions in BSG/01/IA and B with particular reference to the possible necessity for paraphrasing

Form Z. 43
Declassified by ASD - 17/11/2021
Information removed for national security and/or personal sensitivities

## MESSAGE

Precedence PRIORITY	DSB File		Cy. Ser. No.	
6	* J 5*	FROM	Circuit	-
· · · · · · · · · · · · · · · · · · ·				

Classification TOP SECRET FROTH ... 2...

(D) FOR THE REST TYPICAL SYSTEMS ARE LETTER FIGURE, SUBSTITUTION OF CTC OR OF REFERENCE NUMBERS IN DICTIONARY, OFTEN WITH DUMMIES INSERTED, DICTIONARY CODES ETC.

- 3. SPENT A CONSIDERABLE AMOUNT OF TIME WITH THE GENERAL WHOM I FOUND EXTREMELY LIKEABLE AND INTELLIGENT. I FURTHER FORMED A HIGH OPINION BOTH OF HIS ABILITY AND HIS INTEGRITY (POWER OF SELF CRITICISM) IN THE CRYPT WORK HE HAS DONE.
- A. IN VIEW OF PARA 2 (A), THE GENERALS LINE OF ATTACK HAS BEEN BY
  PRAPSING FOLLOWED UP BY ATTEMPTING TO FIT THE PRAPSES TO A KNOWN
  DICTIONARY OR CODE. IN THIS HE HAS BEEN MOST SUCCESSFUL AND THERE
  WAS LITTLE IMPROVEMENT I COULD OFFER ON HIS TECHNIQUE. DID HOWEVER
  GIVE HIM SOME IDEAS OF THE USE OF FREQUENCY COUNTS IN SOLVING SIMPLE
  RECYPHERMENTS OF C.T. ETC AT

  REQUEST ADVISED THE GENERAL
  ON A SYSTEM OF KEEPING CRYPT RECORDS BASED MORE OR LESS ON OUR OWN.
  6. LEFT WITH

  A LIST OF (A) OUR PRESENT REQUIREMENTS MAINLY
  COPIES OF CODE BOOKS ETC. (I HAVE SOME ORIGINALS WITH ME, THE OTHERS
  TO BE PHOTOGRAPHED AND SENT ON IN DUE COURSE).
- (B) OUR FUTURE REQUIREMENTS, SPECIFYING THE TYPE OF CRYPT INFORMATION WE REQUIRE AND THE FORM IT SHOULD TAKE (C) WAYS IN WHICH WE MIGHT BE ABLE TO HELP. THE MOST LIKELY SEEMED TO BE THE CASE OF A MESSAGE ENTIRELY IN CYPHER WITH NO PLAIN TEXT. SUGGESTED THAT IF WE WERE

SUCCESSFUL ON ANY OF THEIR MATERIAL WE MIGHT FORWARD SOME NOTES TO THE

R ML MLD MH MHR MS MSC MSO MSS MQ MT MZ MZC SUKO FUS SIG SIG I SIG

ΣTG	Typed by	Time Typed	System Indicato

3005 52/4/54

Decrypted By Registered By File

s message has to be re-encrypted, attention is c d to the instructions in BSG/01/IA and B with particular reference to the possible necessity for paraphrasing

Form Z. 43
Declassified by ASD - 17/11/2021
Information removed for national
security and/or personal
sensitivities

## MESSAGE

D.4784/7.51—68 Precedence	PRIORITY	DSB File		Cy. Ser. No.	
TO	1		FROM	Circuit	-
	y to the see		* 1		

Classification TOP SECRET FROTH ... 3 ...

GENERAL ON METHODS OF SOLUTION. OFFERED HELP ON ANY CYPHER WITH WHICH THEY WERE HAVING DIFFICULTY.

- 7. CHANNEL OF COMMUNICATION TO CONTINUE TO BE VIA S.L.O. PRESENT SLO, MARTIN, PARTICULARLY SUITED FOR THIS IN VIEW OF HIS PREVIOUS CONTACTS WITH SIGINT.
- 8. INTERPRETATION OF MCP DOCUMENTS. THOUGH AGREEING THAT TRANSLATION
  OF MCP DOCUMENTS INVOLVES MANY DIFFICULT QUESTIONS OF INTERPRETATION
  AND THOUGH CERTAINLY IMPLYING NO CRITICISM OF TRANS-LATIONS MADE
  BY STILL DO NOT FEEL THAT THE PROBLEM IS SOMETHING PECULIAR TO
  THE MCP AND CONSIDER THAT GIVEN ADEQUATE COLLATERAL AND BACKGROUND
  INFORMATION (MCP ORGANISATION HISORY ETC.) AND EXPERIENCED REPEAT
  EXPERIENCED SIGINT TRANSLATOR COULD HANDLE OUR OWN MATERIAL
  SATISFACORILY.

UNFORTUNATELY AM SURE STILL NOT CONVINCED OF THIS. OF COURSE, SECURITY FACTORS PERMITTING, CO-OPERATION WOULD BE TO GREAT MUTUAL ADVANTAGE SINCE ADMITTEDLY MUCH USEFUL BACKGROUND INFORMATION ONLY EXISTS IN THE GENERALS HEAD.

9. VALUE OF VISIT. IN SPITE OF MISUNDERSTANDING OVER PARA 1. CONSIDER VISIT WORTHWHILE (A) KNOWLEDGE OF CRYPTOGRAPHY OBTAINED WOULD BE IN-VALUABLE IN THE EVENT OF ANY SUCCESS IN INTERCEPTION OF MCP MATERIAL.

(B) IT WAS POSSIBLE TO GIVE A CERTAIN AMOUNT OF ASSISTANCE, ADVICE

AND ENCOURAGEMENT TO THE GENERAL. MSC MSO MQ MZC SUKO FUS MHR MSS MT MZ SIG SIG I MLD MH DIR ML DTG System Indicate Typed by Time Typed

3005 52/4/54

 is message has to be re-encrypted, attention is indicate to the instructions in BSG/01/1A and B with particular reference to the possible necessity for paraphrasing

IN	
	MESSAGE

Precedence PRIORITY	DSB File		Cy. Ser. No.	).
ТО	×	FROM	Circuit	

Classification

-TOP-SECRET-FROTH- ... 4..

9. CON. (C) PRESENT AND FUTURE PROBLEMS, REQUIREMENTS AND POSSIBLE FIELDS OF MUTUAL AID BETWEEN THE FEDERATION AND SIGINT HAVE BEEN CLARIFIED. (D) A HARMONIOUS RELATIONSHIP HAS I HOPE BEEN ESTABLISHED 10. SECURITY COVER USED WAS SIMPLY THAT I WAS A CYPHER EXPERT FROM S.I.F.E. NO COMPLICATIONS AROSE.

11. THE FULLEST COOPERATION AND ASSISTANCE WAS GIVEN BY ALL FEDERATION AUTHORITIES CONCERNED.

DIR	ML	MLD	MH	MHR	MS	MSC	MSO	MSS	MQ	МТ	MZ	MZC	SUKO	FUS		S	SIG I	SIG 2
						4				-		8						
DTG		0.05	57/	1. 151.		Туреф	by				Time	Туреб			1	Syst	em Indi	cator
		Ву	1261	<i>⊾ 15 L</i>	C	ackad	D.,			Į		No. of the last of				5.1		; <del>4</del>