NATIONAL SECURITY AGENCY
Washington 25, D. C.

PROBLEMS IN THE CRYPTANALYSIS OF THE ZEN-40 CIPHER MACHINE

Training Division
14 June 1954

PROBLEMS IN THE CRYPTANALYSIS OF THE ZEN-40 CIPHER MACHINE

* * * * * * *

1. The five following messages, enciphered on the Aggressor ZEN-40 machine, were intercepted on 16 December. Solve the texts and recover the alphabets employed.

a. BABAX HYNVG RCWTL HCLSU JFSVX
BJZPW HYQTY MPPER VMAUN XMZXX
RRZPW HMKCE AJGAJ TAEHI DXZKC
DBSIP GGDCT AXGSS MNMTD WMZER
UWCZP QBNNP PPFHO MDTLD YUXBC
VDVGT MCWUP ERNDR BYJUF TRJNZ
DDTLW HBDVE MVXQR MUKSZ QDZYO
BPRYX GHZAN MYBIG BCPSP GPZIM
QTPPW JCUSS MLZVZ GTCCR XOSAX
RKZRZ ZBJIN EPZVZ GICQN XOYNL
LLSRW DBJVN XSLUZ BUKSZ QLOOG
LXTWP HMKRA URNZC QYAHX TRIBQ
LXTRK MAYMF BDGTD HJEMD VCKZZ
NRRHT KWZGP IYLUO YWNJF WHZIR
DYZYU GDZAS FOPWY FXNMU JCPAO
XKLQG VAQCA PTXNG BSKJD DCFVC
XZGMD

b. VEVEX OSELD LVQUX HYVGG GKMYT
IESUJ FSVXG LGBUR YPXNF PGTDQ
NEIHI

c. JUJUX LHCLS UYCHT LOJZH VJYLV

AUVWT WSYLV OTLDA CXWRO MRQDN

PPPFH OMDTL DCLJS NLXSI YVAZM

FBDNI HQIEX TQDYB LHDVQ GLTHK

d. PEPEX GTDHJ EMNXN ZXUYL TMKMY

DWMUV WTWSY LBOPN YERTJ VQWJA

QSNMV VVOAY KQYKV FZXLP GKKZH

JCWRN LAGAM MZLWZ DHGEH

e. NONOX LUAEZ IBVSN KKLWZ QRTVI

EAPOI RPJDX NKGWO QJDBC TGROB

MLCHB

2. Solution of ZEN-40 traffic on 17 December yielded the following enciphering matrix. In this matrix, Alphabet 1 is the alphabet used to encipher the 1st, 26th, 51st,... letters of each BABAX message of the day. Discover the relationships between the matrices of 16 and 17 December, give a graphic representation of the relationships in as concise a manner as possible, and complete the matrix of 16 December.

Plain	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	P		P	P	L	I	R	I		Y	T	L	U	M	F	Y	X	Y		W	Y		M	D	Y
B	X			I	P		Y	M	I	W					X	P	I	L		Q				U	P
C	F	W	I	Q	Y		U		T	I		Y		I	D	L				P	F		U		
D	H	E		S					Z		S	S	N		C			S		Z	N	J	G	A	J
E	Q	D	X		X	R	T	X		F	I		L	W	U	F	U	Q	Q	I	P	U	X	I	L
F	C		G	O	G	G				E		H		K	A	E	N	V	V	J	C			K	
G	M	M	F	R	F	F	W		M	X								M	R		W		D		U
H	D	Q			R	L	L		U	U	R	F	I	X	L	I	L				M	I	Y		
I			C	B	K	A	V	A	B	C	E	N	H	C	J	H	B	K		E	K	H	V	E	
J	U	L	L			M				R	P	T			I	U			T	F		D	T	T	D
K					I								R	F	T		W	I	U	R	I			F	
L		J	J		A	H	H	S		S	O	A	E	S	H	C	H	B	N			S	Z	O	E
M	G	G	N			J	N	B	G	N	Z		V	A	Z	O	Z	G	S	N	H		A	S	O
N	Y	T	M	T	U		M	U	Q	M	Q	I	D	T	R	X	F		L	M	D	X	R	Q	W
O		X		F		Q		R	W	Q	L	X	W	P	P	M	P	R	Y	U	U	Q		L	M
P	A		A	A	B		Z			Z	J			O	O	B	O		Z	C	E		S	V	B
Q	E	H		C		O	S		N	O	N							E	E	B		O		N	
R	S	S		G	H	E	A	O	S	J	H	V	K	V	N	S		O	G	K	Z	V	N		
S	R	R		D	W	Y	Q	L	R	L	D	D	T	L		R	T	D	M			L	P	M	
T		N		N		Z	E	Z	C		A	J	S	N	K		S		J				J	J	Z
U	J	Z	V		N		C	N	H	H			A		E	J	E		K	O	O	E	C	B	G
V		Y	U				I		X			R	M	R				F	F			R	I	P	
W		C			S		G		O	B			O	E			K			A	G			Z	N
X	B	O	E	Z	E			E	V	G		O		H	B	N	A					N	E		
Y	N	V			C	S	B			A		C				A		A	O		A		H		A
Z		U		X		T	P	T	D	P	M				M		M		P	D	R		L	W	T

3. On 18 December there was intercepted the following message, suspected to begin with the words REQUEST CONCURRENCE. Solve the text, and reconstruct the diagrammatic representation of the relationships between the matrix for this date and that of 16 December.

BABAX SOOJS QIKTW KVIIV ETHQW

KYEQB ZSSGD RLMQX ECRUQ XVUVV

URQRC FAQYF RQSKV OBZHV RQHYJ

TGSXT VMSLS TRSKI DRHIY CUUHZ

CUSNN

4. On 19 December the following message was intercepted. It is suspected that the message has a stereotyped beginning of the form "TO COMMANDING OFFICER number REGIMENT", where the regiment involved is one of the first 20 regiments, from FIRST to TWENTIETH inclusive. First place the correct full crib, then solve the remainder of the text and reconstruct the diagrammatic representation of the relationships between the matrix for this date and that of 16 December.

K I K I X Z N D E U A Y V N M O F N A W N I O V N

V G C N O H Z L J W J C I Z E X H I E S V B O V A

N B F J D Y Z U P M A I G W Y C H I G W N Z O I S

A H W J G S F U B T B X K P O O I N P V E P K T W