

November 27, 1940

MEMORANDUM FOR: Mr. David A. Salmon, Chief,
Division of Communications and Records
State Department

I am enclosing herewith an original and one carbon of the new permutation table requested by you. It will provide for about 90,000 groups of the type that you want, with 2-letter differential and non-transposability feature.

You will note that certain letters have been omitted from Section 2 in order to bring the total down to around where you wanted it. The omitted letters have been scattered so as not to disturb the natural balance which the table must have if you are going to super-encipher the code. If at any time in the future you need additional groups you can get them merely by adding a few letters here and there in the vacant spaces in Section 2.

I am returning also the master table which you brought with you.

William F. Friedman,
Principal Cryptanalyst.

2 Enclosures
Permutation Tables

SIS

Date.....11/27. Sig.....W.F.S.....

*Table compiled for
State Dept
Oct 30, 1939*

SECTION 1

BA	CA	DA	..	FA	GA	HA	..	JA	KA	LA	MA	NA	..	PA	QA	RA	SA	TA	..	VA	WA	XA	..	ZA	
FE	GE	HE	..	JE	KE	LE	ME	NE	..	PE	QE	RE	SE	TE	..	VE	WE	XE	..	ZE	
JT	KI	LI	MI	NI	..	PI	QI	RI	SI	TI	..	VI	WI	XI	..	ZI	BI	CI	DI	..	FI	GI	HI	
PO	QO	RO	SO	TO	..	VO	WO	XO	..	ZO	BO	DO	DO	..	FO	GO	HO	..	JO	KO	LO	MO	NO		
VU	WU	XU	..	ZU	BU	CU	DU	..	FU	GU	HU	..	JU	KU	LU	MU	NU	..	PU	QU	RU	SU	TU
ZY	BY	CY	DY	..	FY	GY	HY	..	JY	KY	LY	MY	NY	..	PY	QY	RY	SY	TY	..	VY	WY	XY

432

A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G	E
Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A
V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z
R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V
N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R
J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N
F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J
B	.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F
.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B
W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.
S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W
O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S
K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O
G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K
.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G
X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.
T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X
P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T
L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P
H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L
.	.	Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D
Y	W	U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.
U	S	Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y
Q	O	M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U
M	K	I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q
I	G	E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M
E	.	A	.	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	.	Y	W	U	S	Q	O	M	K	I

AV	EZ	UM	YQ
..	OF	UL
AT	UX	..
AS	EW	OD	UJ
AR	EV	IZ	OC	..	YM
AC	OB	UH
..	ET	YK
..	ES	IW	YJ
AN	ER	IV
AM	EQ	UD	YH
AL	..	IT	OZ	UC	..
AK	..	IS	..	UB	YF
AJ	EN	IR
..	EM	IQ	OW	..	YD
..	EL	..	OV	..	YO
..	EK	YB
..	EJ	IN	OT	UZ	..
..	..	IM	OS
AD	EH	IL	OR
AC	..	IK	O, UW
..	EF	IJ	..	UV	..
..	ED	IH	O, UT
..	EC	..	OM	US	YW
..	EB	IF	OL	UR	YV
AZ	OK	U,	..
..	ID	OJ	..
..	IC
AW	IB	OH	UN
				YR	

SECTION 2

SECTION 3

SECTION 1

✓ B A C A D A .. F A G A H A .. J A K A L A M A N A .. P A Q A R A S A T A .. V A W A X A .. Z A
 ✓ F E G E H E .. J E K E L E M E N E .. P E Q E R E S E T E .. V E W E X E .. Z E B E C E D E
 ✓ J I K I L I M I N I .. P I Q I R I S I T I .. V I W I X I .. Z I B I C I D I .. F I G I H I
 ✓ P O Q O R O S O T O .. V O W O X O .. Z O B O C O D O .. F O G O H O .. J O K O L O M O N O
 ✓ V U W U X U .. Z U B U C U D U .. F U G U H U .. J U K U L U M U N U .. P U Q U R U S U T U
 ✓ Z Y B Y C Y D Y .. F Y G Y H Y .. J Y K Y L Y M Y N Y .. P Y Q Y R Y S Y T Y .. V Y W Y X Y

✓ A . Z X V T R P N L J H F D B . . Y W U S Q O M K I G E A V E Z U M Y
 ✓ Z X V T R P N L J H F D B . . Y W U S Q O M K I G E . A O F U L .
 ✓ V T R P N L J H F D B . . Y W U S Q O M K I G E . A . Z A T L K .
 ✓ R P N L J H F D B . . Y W U S Q O M K I G E . A . Z X V A S E W .. O D U T Y
 ✓ N L J H F D B . . Y W U S Q O M K I G E . A . Z X V T R A R E V I Z O C .. Y
 ✓ J H F D B . . Y W U S Q O M K I G E . A . Z X V T R P N A R O B U H Y
 ✓ F D B . . Y W U S Q O M K I G E . A . Z X V T R P N L J " E T Y
 ✓ B . . Y W U S Q O M K I G E . A . Z X V T R P N L J H F " E S I W .. U F Y
 ✓ . Y W U S Q O M K I G E . A . Z X V T R P N L J H F D B A N E R I V
 ✓ W U S Q O M K I G E . A . Z X V T R P N L J H F D B . . A M E Q U D Y
 ✓ S Q O M K I G E . A . Z X V T R P N L J H F D B . . Y W A L .. I T O Z U C .
 ✓ O M K I G E . A . Z X V T R P N L J H F D B . . Y W U S A K .. I S .. U B Y
 ✓ K I G E . A . Z X V T R P N L J H F D B . . Y W U S Q O A T E N I R
 ✓ G E . A . Z X V T R P N L J H F D B . . Y W U S Q O M K " E M I Q O W .. Y
 ✓ . A . Z X V T R P N L J H F D B . . Y W U S Q O M K I G A H E L .. O V .. Y
 ✓ . Z X V T R P N L J H F D B . . Y W U S Q O M K I G E . " E K Y
 ✓ X V T R P N L J H F D B . . Y W U S Q O M K I G E . A . A F E J W O T U Z .
 ✓ T R P N L J H F D B . . Y W U S Q O M K I G E . A . Z X " I M O S
 ✓ P N L J H F D B . . Y W U S Q O M K I G E . A . Z X V T A D E H I L O R
 ✓ L J H F D B . . Y W U S Q O M K I G E . A . Z X V T R P A C .. I K O Q U W ..
 ✓ H F D B . . Y W U S Q O M K I G E . A . Z X V T R P N L " E F I J .. U V ..
 ✓ ~~D B . . Y W U S Q O M K I G E . A . Z X V T R P N L J H~~
 ✓ . Y W U S Q O M K I G E . A . Z X V T R P N L J H F D " E D I H O N U T ..
 ✓ Y W U S Q O M K I G E . A . Z X V T R P N L J H F D B . " E C " O M U S Y
 ✓ U S Q O M K I G E . A . Z X V T R P N L J H F D B . . Y " E B I F O L L R Y
 ✓ Q O M K I G E . A . Z X V T R P N L J H F D B . . Y W U A Z O K L Q .
 ✓ M K I G E . A . Z X V T R P N L J H F D B . . Y W U S Q " I D O T .. Y
 ✓ I G E . A . Z X V T R P N L J H F D B . . Y W U S Q O M " I C Y
 ✓ E . A . Z X V T R P N L J H F D B . . Y W U S Q O M K I A W .. I B O H U W Y

SECTION 2

SECTION 3