Register No. 161

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

THE PRINCIPLES OF INDIRECT SYMMETRY OF POSITION IN SECONDARY ALPHABETS AND THEIR APPLICATION IN THE SOLUTION OF POLYALPHABETIC SUBSTITUTION CIPHERS

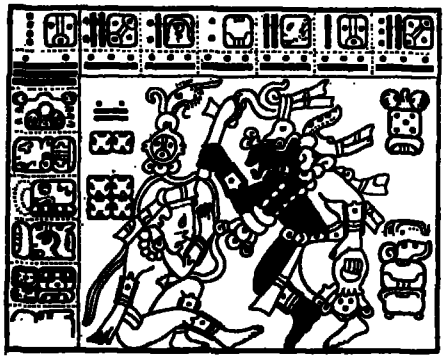
William F. Friedman
Washington
1935

Umol-huun tah-tiyal

William Frederick

yetel

Elizebeth Smith Friedman



Lay ca-huunil kubenbil tech sama.
This our book we entrusted you a while-ago.
Ti manaan apaclam-tz'a lo toon
It not-being you-return-give it us,
Epahal ca-baat tumen ah-men.
Is-being-sharpened our-axe by the expert.

Classification changed to RESTRICTED
By Authority of
HAROLD G. HAYES, Col., Signal Corps
Acting Chief, Army Security Agency

By MASON G. CAMPBELL, 1st Lt., SigC
1 April 1946

NO ACCOUNTING NECESSARY

REGISTRATION CANCELED
by
Authority Hqs, ASA ltr dated 27 Feb 46
2d Ind 11 Mar 46, signed:
HAROLD G. HAYES, Col., Signal Corps
Acting Chief, Army Security Agency

30 April 1959

Paul S. Willard
Colonel, AGC
Adjutant General

555.2

~~Confidential~~

Register No. 161

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

THE PRINCIPLES OF INDIRECT SYMMETRY OF POSITION IN SECONDARY ALPHABETS AND THEIR APPLICATION IN THE SOLUTION OF POLYALPHABETIC SUBSTITUTION CIPHERS

▼

TECHNICAL PAPER

By

WILLIAM F. FRIEDMAN

Cryptanalyst, Chief of Signal Intelligence Section
War Plans and Training Division

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON: 1935

THE PRINCIPLES OF INDIRECT SYMMETRY OF POSITION IN SECONDARY ALPHABETS AND THEIR APPLICATION IN THE SOLUTION OF POLYALPHABETIC SUBSTITUTION CIPHERS

TABLE OF CONTENTS

1. **Preliminary remarks.**—The cipher alphabets of polyalphabetic substitution ciphers are most frequently secondary alphabets resulting from the juxtaposition, at various points of coincidence, of two basic sequences of letters usually termed primary components.[1] One of these components is designated the plain component, being the one in which the plain-text letter to be enciphered is sought; the other component is designated the cipher component, being the one in which the cipher letter is sought, the cipher letter in the cipher component standing in some spatial relation with the plain-text letter in the plain component—usually opposite it as the two components are juxtaposed at the predetermined point of coincidence.

When the plain component is the normal sequence and the cipher component is a mixed sequence, the complete solution and reconstruction of the secondary alphabets, as well as of the mixed primary cipher component, from a few values obtained by the application of the principles of frequency to the cipher text, is a very simple matter and the method to be followed in these processes can be found in various treatises.[2] In such a case the process is termed "*solution and reconstruction by the application of the principles of direct symmetry.*"

When, however, both components of a primary alphabet are unknown sequences which, by juxtaposition at various points of coincidence, are made to yield a series of secondary alphabets employed in polyalphabetic encipherment, the principles of direct symmetry can no longer be applied in an attempt to solve and reconstruct the primary components and the secondary alphabets, given a few values obtained as a result of cryptanalytic solution of fragments of the cipher text. This is because the letters of the cipher components of the secondary alphabets no longer show externally any symmetry of position when written beneath the letters of the plain component (usually the normal alphabet A B C . . . Z).

If the matter be studied with care, however, an internal or *indirect symmetry of position* can be found, the application of the principles of which will very much facilitate the solution of many varied cases. In fact, it has been found in certain difficult cases that solution can be achieved only by a recourse to the principles of indirect symmetry.

[1] See Friedman, William F., *Elements of Cryptanalysis*, Signal Corps Training Pamphlet No. 3, 1924, pp. 34, 35.

[2] Friedman, W. F., loc. cit., pp. 53–63. Hitt, Parker. *Manual for the Solution of Military Ciphers*, For Leavenworth Press, 1916, p. 68. Givierge, M. *Cours de Cryptographie*, Paris, 1925, p. 107.

2. **Simultaneous explanation of principles and application to a concrete case.**—The case described below will serve not only to explain the principles of the method but will at the same time also show how the solution of a single rather difficult polyalphabetic substitution cipher was greatly facilitated by applying these principles. It is realized, of course, that the cryptogram could have been solved by the usual methods of frequency and long, patient experimentation. However, the method to be described was applied and very materially reduced the amount of time and labor actually required for solution.

3. **The cryptogram employed in the demonstration.**—The problem herein described involved an actual cryptogram submitted for solution in connection with a cipher device having two concentric disks upon which the same random mixed alphabet appears, both alphabets progressing in the same direction. This was obtained from a study of the descriptive circular accompanying the cryptogram. By the usual process of factoring, it was determined that the cryptogram involved 10 alphabets. The message as arranged according to its period is shown in figure 1, in which all repetitions of two or more letters are indicated.

The trigraphic frequency tables are given in figure 2. It will be seen that on account of the brevity of the message, considering the number of alphabets involved, the frequency tables do not yield many clues. By a very careful study of the repetitions, tentative individual determinations of values of cipher letters, as illustrated in figures 3, 4, 5, and 6, were made. These are given in sequence and in detail in order to show that there is nothing artificial or arbitrary in the preliminary stages of analysis here set forth.

FIGURE 1

THE CRYPTOGRAM

(Repetitions underlined)

	1	2	3	4	5	6	7	8	9	10
A	W	F	U	P	C	F	O	C	J	Y
B	G	B	Z	D	P	F	B	O	U	O
C	G	R	F	T	Z	M	Q	M	A	V
D	K	Z	U	G	D	Y	F	T	R	W
E	G	J	X	N	L	W	Y	O	U	X
F	I	K	W	E	P	Q	Z	O	K	Z
G	P	R	X	D	W	L	Z	I	C	W
H	G	K	Q	H	O	L	O	D	V	M
I	G	O	X	S	N	Z	H	A	S	E
J	B	B	J	I	P	Q	F	J	H	D
K	Q	C	B	Z	E	X	Q	T	X	Z
L	J	C	Q	R	Q	F	V	M	L	H
M	S	R	Q	E	W	M	L	N	A	E
N	G	S	X	E	R	O	Z	J	S	E
O	G	V	Q	W	E	J	M	K	G	H
P	R	C	V	O	P	N	B	L	C	W
Q	L	Q	Z	A	A	A	M	D	C	H
R	B	Z	Z	C	K	Q	O	I	K	F
S	C	F	B	S	C	V	X	C	H	Q
T	Z	T	Z	S	D	M	X	W	C	M
U	R	K	U	H	E	Q	E	D	G	X
V	F	K	V	H	P	J	J	K	J	Y
W	Y	Q	D	P	C	J	X	L	L	L

	1	2	3	4	5	6	7	8	9	10
X	G	H	X	E	R	O	Q	P	S	E
Y	G	K	B	W	T	L	F	D	U	Z
Z	O	C	D	H	W	M	Z	T	U	Z
AA	K	L	B	P	C	J	O	T	X	E
BB	H	S	P	O	P	N	M	D	L	M
CC	G	C	K	W	D	V	B	L	S	E
DD	G	S	U	G	D	P	O	T	H	X
EE	B	K	D	Z	F	M	T	G	Q	J
FF	L	F	U	Y	D	T	Z	V	H	Q
GG	Z	G	W	N	K	X	J	T	R	N
HH	Y	T	X	C	D	P	M	V	L	W
II	B	G	B	W	W	O	Q	R	G	N
JJ	H	H	V	L	A	Q	Q	V	A	V
KK	J	Q	W	O	O	T	T	N	V	Q
LL	B	K	X	D	S	O	Z	R	S	N
MM	Y	U	X	O	P	P	Y	O	X	Z
NN	H	O	Z	O	W	M	X	C	G	Q
OO	J	J	U	G	D	W	Q	R	V	M
PP	U	K	W	P	E	F	X	E	N	F
QQ	C	C	U	G	D	W	P	E	U	H
RR	Y	B	W	E	W	V	M	D	Y	J
SS	R	Z	X							

FIGURE 2

TRIGRAPHIC FREQUENCY TABLES

I

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	EB	FF			XK	YB	ES	XK	ZC	VZ	WQ			ZC	ZR	DC	HC	HR		MK		-F		YQ	QT
	HZ	FC				OR	NH		VQ	ZL	JF						MK							NT	QG
	XK					WJ	ZO		QJ								JZ							NU	
	WG					WK																		HB	
	QK					MO																			
						ES																			
						EV																			
						LH																			
						EK																			
						MC																			
						ES																			

II

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	GZ	QB			WU	ZW	GX		GX	IW	KB			GX		LZ	GF	GX	ZZ	YX	GQ				KU
	BJ	JQ			CB	BB	HV		JU	GQ				HZ		YD	PX	HP	YX						BZ
	YW	RV			LU					RU						JW	SQ	GU							RH
		OD								FV															
		GK								GB															
		CU								BD															
										BK															
										UW															

III

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	CZ		QP		RT				BI	CW					SO	KH				FP	CO	KE	JN		BD
	FS		CH													CR				ZG	KH	GN	RD		QA
	KW		KZ													RE				KH	HL	QO	OS		ZC
	LP															VW				SG		KP	SE		TS
	GW																			FY		BE	HE		00
																				JG			TC		
																				CG			KD		
																							UO		
																							Z-		

IV

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ZA		ZK	ZP	WP		UD	QO	JP			VA		XL	VP	UC		QQ	XN	FZ			QE		UD	BE
		XD	XW	QW		UD	UE						WK	PP	DC			BC				BT			DF
			XS	XR		UD	VP							WO	BC			ZD				KD			
				XR		UD	DW							XP	WE							BW			
				WW										ZW											

V

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
AA		PF	GY	ZX	ZM					CQ	NW		SZ	HL	DF	RF	EO	DO	WL			DL			TM
LQ		SV	SM	WJ						NX				OT	EQ		EO					EM			
		PJ	WV	HA											IQ							HM			
		PJ	GP	PF											ON							WO			
			VT												HJ							OM			
			CP												ON							EV			
			GW												OP										
			GW																						

VI

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
AM					CO				EM		WZ	ZQ	PB	RZ	DO	PZ			DZ		CX	LY	EQ	DF	NH
					PB				PJ		OO	WL	PM	RQ	DM	PF			OT		DB	DQ	KJ		
					QV				CX		TF	DX		WQ	PY	KO					WM	DP			
					EX				CO			WZ		SZ		EE										
												FT				AQ									
												WX													

VII

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	FO			QD	YT		ZA		JK		MN	JK		FC	WE	MM			MG		FM		VC	WO	QO
	NL				QJ				XT			AD		LD		XT			TN				MW	PO	LI
	VL				LD							ND		QI		OP							JL		OJ
												PV		JT		OR							MC		MT
												VD		PT		QV							FE		TV
																WR									OR

VIII

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
HS		OJ	OV	XN		TQ		ZC	FH	MG	BC	QA	LA	BU	QS		QG		FR		ZH	XC			
		XH	MC	PU				OK	ZS	JJ	XL	VL	TV	YU			ZS		QX		ML				
		XG	EG								BS			ZK			QV		ZU		QA				
			FU											YX					OX						
			ML																OH						
			MY																JR						

IX

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
MV		IW				KH	JD		CY	OZ	MH		EF			GJ	TW	AE		OO	DM		TZ	DJ	
NE		LW				DX	CQ		KY	IF	LL						TN	JE		OX	NQ		TE		
VV		DH				RN	TX				DM							PE		DZ	RM		OZ		
		WM				CQ	VQ				VW							LE		TZ					
																		RN		EH					

X

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
			HQ	SB	KC		LS		QL		LG	VG	RY	UG		HZ					AK	RG	UI	JG	KP
				AG	NC		GR		YR			CR	GH			HZ					AJ	CG	GF	JY	XJ
				SG			CB					LG	SY			VB						CL	HB		UO
				SG			UY					VU				GJ						LB			UK
				XH																					XH
				SG																					

FIGURE 3

INITIAL VALUES FROM ASSUMPTIONS

$^{1}G_c=E_p$; $^{2}K_c=E_p$; $^{3}X_c=E_p$; and $^{5}D_c=E_p$, from frequency tables.

$^{3\,4\,5}UGD=THE$; $^{4\,5\,6}PCJ=THE$; and $^{9\,10\,1}SEG=THE$, from study of repetitions.

	1	2	3	4	5	6	7	8	9	10
A	W	F	U	P	C	F	O	C	J	Y
			T	T	H					
B	G	B	Z	D	P	F	B	Q	U	O
	E									
C	G	R	F	T	Z	M	Q	M	A	V
	E									
D	K	Z	U	G	D	Y	F	T	R	W
			T	H	E					
E	G	J	X	N	L	W	Y	Q	U	X
	E		E							
F	I	K	W	E	P	Q	Z	O	K	Z
		E								
G	P	R	X	D	W	L	Z	I	C	W
			E							
H	G	K	Q	H	O	L	O	D	V	M
	E	E								
I	G	O	X	S	N	Z	H	A	S	E
	E		E						T	H
J	B	B	J	I	P	Q	F	J	H	D
K	Q	C	B	Z	E	X	Q	T	X	Z
L	J	C	Q	R	Q	F	V	M	L	H
M	S	R	Q	E	W	M	L	N	A	E
										H
N	G	S	X	E	R	O	Z	J	S	E
	E		E						T	H
O	G	V	Q	W	E	J	M	K	G	H
	E				E					
P	R	C	V	O	P	N	B	L	C	W
Q	L	Q	Z	A	A	A	M	D	C	H
R	B	Z	Z	C	K	Q	O	I	K	F
S	C	F	B	S	C	V	X	C	H	Q
					H					
T	Z	T	Z	S	D	M	X	W	C	M
					E					
U	R	K	U	H	E	Q	E	D	G	X
		E	T							
V	F	K	V	H	P	J	J	K	J	Y
		E			E					
W	Y	Q	D	P	C	J	X	L	L	L
				T	H	E				

	1	2	3	4	5	6	7	8	9	10
X	G	H	X	E	R	O	Q	P	S	E
		E		E					T	H
Y	G	K	B	W	T	L	F	D	U	Z
	E	E								
Z	O	C	D	H	W	M	Z	T	U	Z
AA	K	L	B	P	C	J	O	T	X	E
				T	H	E				H
BB	H	S	P	O	P	N	M	D	L	M
CC	G	C	K	W	D	V	B	L	S	E
	E				E				T	H
DD	G	S	U	G	D	P	O	T	H	X
	E		T	H	E					
EE	B	K	D	Z	F	M	T	G	Q	J
		E								
FF	L	F	U	Y	D	T	Z	V	H	Q
			T		E					
GG	Z	G	W	N	K	X	J	T	R	N
HH	Y	T	X	C	D	P	M	V	L	W
			E		E					
II	B	G	B	W	W	O	Q	R	G	N
JJ	H	H	V	L	A	Q	Q	V	A	V
KK	J	Q	W	O	O	T	T	N	V	Q
LL	B	K	X	D	S	O	Z	R	S	N
		E	E						T	
MM	Y	U	X	O	P	P	Y	O	X	Z
NN	H	O	Z	O	W	M	X	C	G	Q
OO	J	J	U	G	D	W	Q	R	V	M
			T	H	E					
PP	U	K	W	P	E	F	X	E	N	F
		E		T						
QQ	C	C	U	G	D	W	P	E	U	H
			T	H	E					
RR	Y	B	W	E	W	V	M	D	Y	J
SS	R	Z	X							
			E							

FIGURE 4

ADDITIONAL VALUES FROM ASSUMPTIONS (I)

Refer to line DD in figure 3; $\overset{2}{S}_e$ assumed to be N_p.

Refer to line M in figure 3; $\overset{9}{A}_e$ assumed to be W_p.

Then in lines C–D, $\overset{9}{A}\ \overset{10}{V}\ \overset{1}{K}\ \overset{2}{Z}\ \overset{3}{U}\ \overset{4}{G}\ \overset{5}{D}$ is assumed to be WITH THE.

	1	2	3	4	5	6	7	8	9	10
A	W	F	U	P	C	F	O	C	J	Y
			T	T	H					
B	G	B	Z	D	P	F	B	O	U	O
	E									
C	G	R	F	T	Z	M	Q	M	A	V
	E								W	I
D	K	Z	U	G	D	Y	F	T	R	W
	T	H	T	H	E					
E	G	J	X	N	L	W	Y	O	U	X
	E		E							
F	I	K	W	E	P	Q	Z	O	K	Z
		E								
G	P	R	X	D	W	L	Z	I	C	W
			E							
H	G	K	Q	H	O	L	O	D	V	M
	E	E								
I	G	O	X	S	N	Z	H	A	S	E
	E		E						T	H
J	B	B	J	I	P	Q	F	J	H	D
K	Q	C	B	Z	E	X	Q	T	X	Z
L	J	C	Q	R	Q	F	V	M	L	H
M	S	R	Q	E	W	M	L	N	A	E
									W	H
N	G	S	X	E	R	O	Z	J	S	E
	E	N	E						T	H
O	G	V	Q	W	E	J	M	K	G	H
	E				E					
P	R	C	V	O	P	N	B	L	C	W
Q	L	Q	Z	A	A	A	M	D	C	H
R	B	Z	Z	C	K	Q	O	I	K	F
		H								
S	C	F	B	S	C	V	X	C	H	Q
					H					
T	Z	T	Z	S	D	M	X	W	C	M
					E					
U	R	K	U	H	E	Q	E	D	G	X
		E	T							
V	F	K	V	H	P	J	J	K	J	Y
		E				E				
W	Y	Q	D	P	C	J	X	L	L	L
				T	H	E				

	1	2	3	4	5	6	7	8	9	10
X	G	H	X	E	R	O	Q	P	S	E
			E		E				T	H
Y	G	K	B	W	T	L	F	D	U	Z
	E	E								
Z	O	C	D	H	W	M	Z	T	U	Z
AA	K	L	B	P	C	J	O	T	X	E
	T			T	H	E				H
BB	H	S	P	O	P	N	M	D	L	M
		N								
CC	G	C	K	W	D	V	B	L	S	E
	E				E				T	H
DD	G	S	U	G	D	P	O	T	H	X
	E	N	T	H	E					
EE	B	K	D	Z	F	M	T	G	Q	J
		E								
FF	L	F	U	Y	D	T	Z	V	H	Q
			T		E					
GG	Z	G	W	N	K	X	J	T	R	N
HH	Y	T	X	C	D	P	M	V	L	W
			E		E					
II	B	G	B	W	W	O	Q	R	G	N
JJ	H	H	V	L	A	Q	Q	V	A	V
									W	I
KK	J	Q	W	O	O	T	T	N	V	Q
LL	B	K	X	D	S	O	Z	R	S	N
		E	E						T	
MM	Y	U	X	O	P	P	Y	O	X	Z
NN	H	O	Z	O	W	M	X	C	G	Q
OO	J	J	U	G	D	W	Q	R	V	M
			T	H	E					
PP	U	K	W	P	E	F	X	E	N	F
		E		T						
QQ	C	C	U	G	D	W	P	E	U	H
			T	H	E					
RR	Y	B	W	E	W	V	M	D	Y	J
SS	R	Z	X							
		H	E							

FIGURE 5

ADDITIONAL VALUES FROM ASSUMPTIONS (II)

Refer to figure 4, line A; W F U P C F O C J Y; assume to be BUT THOUGH.
1 2 3 4 5 6 7 8 9 10
– – T T H – – – – –

Refer to figure 4, lines N and X, where repetition XERO occurs; assume EACH.
3 4 5 6
E—

	1	2	3	4	5	6	7	8	9	10
A		F	U	P	C	F	O	C	J	Y
	B	U	T	T	H	O	U	G	H	
B	G	B	Z	D	P	F	B	O	U	O
	E					O				
C	G	R	F	T	Z	M	Q	M	A	V
	E								W	I
D	K	Z	U	G	D	Y	F	T	R	W
	T	H	T	H	E					
E	G	J	X	N	L	W	Y	O	U	X
	E		E							
F	I	K	W	E	P	Q	Z	O	K	Z
		E		A						
G	P	R	X	D	W	L	Z	I	C	W
			E							
H	G	K	Q	H	O	L	O	D	V	M
	E	E					U			
I	G	O	X	S	N	Z	H	A	S	E
	E		E						T	H
J	B	B	J	I	P	Q	F	J	H	D
K	Q	C	B	Z	E	X	Q	T	X	Z
L	J	C	Q	R	Q	F	V	M	L	H
						O				
M	S	R	Q	E	W	M	L	N	A	E
				A					W	H
N	G	S	X	E	R	O	Z	J	S	E
	E	N	E	A	C	H			T	H
O	G	V	Q	W	E	J	M	K	G	H
	E				E					
P	R	C	V	O	P	N	B	L	C	W
Q	L	Q	Z	A	A	A	M	D	C	H
R	B	Z	Z	C	K	Q	O	I	K	F
		H					U			
S	C	F	B	S	C	V	X	C	H	Q
		U			H			G		
T	Z	T	Z	S	D	M	X	W	C	M
					E					
U	R	K	U	H	E	Q	E	D	G	X
		E	T							
V	F	K	V	H	P	J	J	K	J	Y
		E				E			H	
W	Y	Q	D	P	C	J	X	L	L	L
				T	H	E				

	1	2	3	4	5	6	7	8	9	10
X	G	H	X	E	R	O	Q	P	S	E
		E		E	A	C	H		T	H
Y	G	K	B	W	T	L	F	D	U	Z
		E	E							
Z	O	C	D	H	W	M	Z	T	U	Z
AA	K	L	B	P	C	J	O	T	X	E
		T		T	H	E	U			H
BB	H	S	P	O	P	N	M	D	L	M
			N							
CC	G	C	K	W	D	V	B	L	S	E
	E				E				T	H
DD	G	S	U	G	D	P	O	T	H	X
	E	N	T	H	E		U			
EE	B	K	D	Z	F	M	T	G	Q	J
		E								
FF	L	F	U	Y	D	T	Z	V	H	Q
		U	T		E					
GG	Z	G	W	N	K	X	J	T	R	N
HH	Y	T	X	C	D	P	M	V	L	W
			E		E					
II	B	G	B	W	W	O	Q	R	G	N
						H				
JJ	H	H	V	L	A	Q	Q	V	A	V
									W	I
KK	J	Q	W	O	O	T	T	N	V	Q
LL	B	K	X	D	S	O	Z	R	S	N
		E	E			H			T	
MM	Y	U	X	O	P	P	Y	O	X	Z
NN	H	O	Z	O	W	M	X	C	G	Q
								G		
OO	J	J	U	G	D	W	Q	R	V	M
			T	H	E					
PP	U	K	W	P	E	F	X	E	N	F
		E		T		O				
QQ	C	C	U	G	D	W	P	E	U	H
			T	H	E					
RR	Y	B	W	E	W	V	M	D	Y	J
				A						
SS	R	Z	X							
		H	E							

FIGURE 6

ADDITIONAL VALUES FROM ASSUMPTIONS (III)

4 5 6
OPN—assume ING from repetition and frequency.

9 10 1
HQZ—assume ING from repetition and frequency.

	1	2	3	4	5	6	7	8	9	10
A	W	F	U	P	C	F	O	C	J	Y
	B	U	T	T	H	O	U	G	H	
B	G	B	Z	D	P	F	B	O	U	O
	E				N	O				
C	G	R	F	T	Z	M	Q	M	A	V
	E								W	I
D	K	Z	U	G	D	Y	F	T	R	W
	T	H	T	H	E					
E	G	J	X	N	L	W	Y	O	U	X
	E		E							
F	I	K	W	E	P	Q	Z	O	K	Z
		E		A	N					
G	P	R	X	D	W	L	Z	I	C	W
			E							
H	G	K	Q	H	O	L	O	D	V	M
	E	E					U			
I	G	O	X	S	N	Z	H	A	S	E
	E		E						T	H
J	B	B	J	I	P	Q	F	J	H	D
					N				I	
K	Q	C	B	Z	E	X	Q	T	X	Z
L	J	C	Q	R	Q	F	V	M	L	H
						O				
M	S	R	Q	E	W	M	L	N	A	E
				A					W	H
N	G	S	X	E	R	O	Z	J	S	E
	E	N	E	A	C	H			T	H
O	G	V	Q	W	E	J	M	K	G	H
	E				E					
P	R	C	V	O	P	N	B	L	C	W
				I	N	G				
Q	L	Q	Z	A	A	A	M	D	C	H
R	B	Z	Z	C	K	Q	O	I	K	F
		H				U				
S	C	F	B	S	C	V	X	C	H	Q
		U			H			G	I	N
T	Z	T	Z	S	D	M	X	W	C	M
	G				E					
U	R	K	U	H	E	Q	E	D	G	X
		E	T							
V	F	K	V	H	P	J	J	K	J	Y
		E			N	E			H	
W	Y	Q	D	P	C	J	X	L	L	L
				T	H	E				

	1	2	3	4	5	6	7	8	9	10
X	G	H	X	E	R	O	Q	P	S	E
	E		E	A	C	H			T	H
Y	G	K	B	W	T	L	F	D	U	Z
	E	E								
Z	O	C	D	H	W	M	Z	T	U	Z
AA	K	L	B	P	C	J	O	T	X	E
	T			T	H	E	U			H
BB	H	S	P	O	P	N	M	D	L	M
		N		I	N	G				
CC	G	C	K	W	D	V	B	L	S	E
	E				E				T	H
DD	G	S	U	G	D	P	O	T	H	X
	E	N	T	H	E		U		I	
EE	B	K	D	Z	F	M	T	G	Q	J
		E								
FF	L	F	U	Y	D	T	Z	V	H	Q
		U	T		E				I	N
GG	Z	G	W	N	K	X	J	T	R	N
	G									
HH	Y	T	X	C	D	P	M	V	L	W
			E		E					
II	B	G	B	W	W	O	Q	R	G	N
						H				
JJ	H	H	V	L	A	Q	Q	V	A	V
									W	I
KK	J	Q	W	O	O	T	T	N	V	Q
				I						N
LL	B	K	X	D	S	O	Z	R	S	N
		E	E			H			T	
MM	Y	U	X	O	P	P	Y	O	X	Z
				I	N					
NN	H	O	Z	O	W	M	X	C	G	Q
				I				G		N
OO	J	J	U	G	D	W	Q	R	V	M
				T	H	E				
PP	U	K	W	P	E	F	X	E	N	F
		E		T		O				
QQ	C	C	U	G	D	W	P	E	U	H
				T	H	E				
RR	Y	B	W	E	W	V	M	D	Y	J
				A						
SS	R	Z	X							
		H	E							

From the initial and subsequent tentative identifications shown in figures 3, 4, 5, and 6, the values obtained were arranged in the form of the secondary alphabets shown in figure 7.

FIGURE 7

	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	26
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	.	W	.	.	G	.	Z	.	.	.	.	.	.	.	.	.	.	.	.	K	.	.	.	.	.	.
2	.	.	.	.	K	.	.	Z	.	.	.	.	.	S	.	.	.	.	.	.	F	.	.	.	.	.
3	.	.	.	.	X	.	.	.	.	.	.	.	.	.	.	.	.	.	.	U	.	.	.	.	.	.
4	E	.	.	.	.	.	.	G	O	.	.	.	.	.	.	.	.	.	.	P	.	.	.	.	.	.
5	.	.	R	.	D	.	.	C	.	.	.	.	.	P	.	.	.	.	.	.	.	.	.	.	.	.
6	.	.	.	.	J	.	N	O	.	.	.	.	.	.	F	.	.	.	.	.	.	.	.	.	.	.
7	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	O	.	.	.	.	.
8	.	.	.	.	.	.	C	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
9	.	.	.	.	.	.	.	J	H	.	.	.	.	.	.	.	.	.	.	S	.	.	A	.	.	.
10	.	.	.	.	.	.	.	E	V	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

4. **Fundamental theory.**—In paragraph 47c of "Elements of Cryptanalysis" (see footnote 1, page 1), a method of reconstructing primary components from one of the secondary alphabets was given in detail. It is necessary that that method be fully understood before the following steps be studied. It was there shown that the primary component can be one of a series of 26 equivalent primary sequences, all of which will give exactly similar results so far as the secondary alphabets and the cryptographic text are concerned. It is not necessary that the identical or original primary component employed in the cryptographing be reconstructed—any equivalent primary sequence will serve. The whole question is one of establishing a sequence of letters the interval between which is either equal to that in the original primary component or else is an exact constant multiple of the interval separating the letters in the original primary component. For example, suppose K P X N Q forms a sequence in the original primary component. Here the interval between K and P, P and X, X and N, N and Q is one; in an equivalent primary component, say the sequence K..P..X..N..Q, the interval between K and P is three, that between P and X also three, and so on; and the two sequences will yield the same secondary alphabets. So long as the interval between K and P, P and X, X and N, N and Q is a constant one, the sequence will yield the same secondary alphabets as do those of the original primary sequence. However, it is necessary that this interval be an odd number other than 13, as these are the only cases which will yield one unbroken sequence of 26 letters.

Suppose a secondary alphabet to be as follows:

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

We can say that the primary component contains the following sequences:

XN KP NQ PX

These, when united by means of their common letters, yield K P X N Q.

Suppose we had also the following secondary alphabet:

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

Here we get the sequences PN, XQ, KX, and NZ, which when united yield the two sequences KXQ and PNZ.

By a comparison of the sequences K P X N Q, K X Q, and P N Z, we can establish the following:

K P X N Q
K . X . Q
P . N . Z

It follows that we can now add the letter Z to the sequence, making it K P X N Q Z.

The reconstruction of a primary alphabet from one of the secondaries by the process given in "Elements of Cryptanalysis" requires a complete or nearly complete secondary alphabet. This is at hand only *after* a cryptogram has been completely solved. But if we could employ several very scant or skeletonized secondary alphabets simultaneously with the analysis of the cryptogram we could then possibly build up a primary component from fewer data and thus solve the cryptogram much more rapidly than would otherwise be the case. Let us see how.

Suppose we place into juxtaposition only the cipher components of the two secondary alphabets given above. Thus:

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 26
. . . . . X . K N . . . . . P . .
. . . . . P . . X . . . . . K . N

The sequences PX, XN, and KP result, which united yield KPXN as part of the primary sequence. It follows, therefore, that we can employ the *cipher components of secondary alphabets* as sources of independent data to assist in building up the primary sequences. The usefulness of this point will become clearer subsequently.

5. **Application of principles.**—Refer now to figure 7. Hereafter, in order to avoid all ambiguity and for ease in reference, the position of a letter in figure 7 will be indicated by coordinates in parentheses. Thus, N (6—7) refers to the letter N in line 6 and in column 7.

Now, consider the following pairs of letters:

E (0— 5) J (6— 5)
G (0— 7) N (6— 7)
H (0— 8) O (6— 8) } HO+OF=HOF
Q (0—15) F (6—15) }

(We are enabled to use the line marked zero in figure 7 since we have a mixed sequence sliding against *itself*.)

The immediate results of this set of values will now be given. Having HOF as a sequence, with EJ as belonging to the same interval set, suppose we place HOF and EJ into juxtaposition as portions of sliding alphabets. Thus:

Plain text . . . H O F . . .
Cipher . . . E J . . . .

When $H_p=E_c$, then $O_p=J_c$.

Refer now to alphabet 10, figure 7, where it is seen that $H_p=E_c$. *We can immediately insert the derived value, in the same alphabet,* $O_p=J_c$, and substitute in the cryptogram.

Again, GN belongs to the same set of interval values as do EJ and HOF. Hence, by superimposition:

Plain text____ . . . H O F . . .
Cipher_____ . . . G N . . . .

When $H_p=G_c$ then $O_p=N_c$. Therefore, we can insert the value, in alphabet 4, $O_p=N_c$, and also substitute in the cryptogram.

Furthermore, note the corroborations we find from this particular superimposition:

H(0—8)	G(0—7)
O(6—8)	N(6—7)

This checks up the value in alphabet 6, $G_p=N_c$.

Again superimpose HOF and GN:

H O F
G N

Note this corroboration:

O (6— 8)	G (4— 8)
F (6—15)	N (4—15)

which has just been inserted in figure 7, as stated above.

Again using HOF and EJ, but in a different superimposition, we have:

. . . H O F . .
. . E J . . . .

Refer now to H (9—9) J (9—8). Directly under these letters we find V (10—9) E (10—8). Therefore, we can add the V immediately before H O F, making the sequence V H O F.

Now take V H O F and juxtapose it with E J, thus:

V H O F
E J

Refer now to figure 7, and find the following:

V (10—9)	E (10—8)
H (9—9)	J (9—8)
O (4—9)	G (4—8)
I (0—9)	H (0—8)

From the value O G it follows that G can be set next to J in E J. Thus:

V H O F
E J G

But we already have G N as a member of the same interval set as E J. Therefore, we now can combine E J, J G, and G N into one sequence, E J G N; then we have

V H O F
E J G N

Refer now to figure 7.

V (0—22)	E (0—5)
? (1—22)	G (1—5)
? (2—22)	K (2—5)
? (3—22)	X (3—5)
? (5—22)	D (5—5)
? (6—22)	J (6—5)

The only values we can insert are:

O (1—22)	G (1—5)
H (6—22)	J (6—5)

This means that $V_p=O_c$ in alphabet 1 and that $V_p=H_c$ in alphabet 6. There is one O_c in the frequency table for alphabet 1, and no H_c in that for alphabet 6. The frequency table is, therefore corroborative insofar as these values are concerned.

Further, taking E J G N and V H O F, superimpose them thus:

E J G N
V H O F

Refer now to figure 7.

E (0—5)	H (0—8)
G (1—5)	? (1—8)

From the diagram of superimposition we can insert the value G (1—5) F (1—8), which gives us $H_p=F_c$ in alphabet 1.

Again, placing V H O F and E J G N into juxtaposition, we have:

V H O F
E J G N

Refer to figure 7 and find the following:

H (0—8)	G (4—8)
A (0—1)	E (4—1)

This means that we can add A thus:

A V H O F
E J G N

In the set we have also

E (0—5)	G (1—5)
G (0—7)	Z (1—7).

Then in the superimposition

E J G N
E J G N

we can add Z under G, making the sequence E J G N Z.

Then taking

A V H O F
E J G N Z

and referring to figure 7:

H (0—8)	N (0—14)
O (6—8)	? (6—14)

it will be seen that O=Z from superimposition, and hence in alphabet 6, $N_p=Z_c$, an important new value, but occurring only once in the cryptogram. Has an error been made? The work so far seems too corroborative to think so.

We have by no means exhausted the possibilities of the superimposition and sliding of the AVHOF and the EJGNZ sequences, but let us go on a little different trail this time.

E (0—5)	T (0—20)
G (1—5)	K (1—20)
X (3—5)	U (3—20)

Then we have

E J G N Z
T . K

Now refer to the following:

E (0— 5)	K (2— 5)
N (0—14)	S (2—14)

whereupon we can insert the value S:

E J G N Z
T . K . . S

Consider all the values based upon the interval corresponding to JG:

J (6—5) G (1—5)→J (9— 8) G (4— 8)
N (6—7) Z (1—7) H (9— 9) O (4— 9)
S (9—20) P (4—20)→S (2—14) P (5—14)
Z (2— 8) C (5— 8)
K (2— 5) D (5— 5)

Since J and G are sequent in the EJGNZ sequence, we can say that all the letters of the foregoing pairs are also sequent. Hence we have Z C, S P, and K D as new data. Therefore, we have E J G N Z C and T . K D . S P.

From figure 7:

T (0—20)	P (4—20)
A (0— 1)	E (4— 1)
H (0— 8)	G (4— 8)
I (0— 9)	O (4— 9)

1 2 3 4 5 6

Now in the T . K D . S P sequence the interval between T and P is T . . . . . P. Hence the interval between A and E is 6 also. It follows therefore that the sequences A V H O F and E J G N Z C should be united thus:

1 2 3 4 5 6
A V H O F . E J G N Z C

Corroboration is found in the interval between H and G, which is six. The letter I can be placed into position, from the relation I (0—9) O (4—9), thus:

```
                1 2 3 4 5 6
            I . . A V H O F . E J G N Z C
```

From figure 7:

H (0— 8) Z (2— 8)
E (0— 5) K (2— 5)
N (0—14) S (2—14)
U (0—21) F (2—21)

From the I . . A V H O F . E J G N Z C sequence we can write

```
H . . . . . . . Z
E . . . . . . . K
N . . . . . . . S
U . . . . . . . F
  1 2 3 4 5 6 7 8
```

and likewise

Hence we can make the sequence

```
                  1 2 3 4 5 6 7 8
        I . . A V H O F . E J G N Z C . . K
Then    I . . A V H O F . E J G N Z C T . K D . S P
and   U I . . A V H O F . E J G N Z C T . K D . S P
      1 2 3 4 5 6 7 8               1 2 3 4 5 6 7 8
```

Subsequent derivations can be indicated very briefly as follows:

E (0—5) C (0—3)
D (5—5) R (5—3)

```
                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 26
From            U I . . A V H O F . E J G N Z C T . K D . S P . . .
we can write                        E . . . . C
                                    1 2 3 4 5

and                                                         D . . . . R
                                                            1 2 3 4 5
making the sequence U I . . A V H O F . E J G N Z C T . K D . S P . R .
                    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 26
```

U (3—20) T (0—20)
X (3— 5) E (0— 5)

```
                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 26 | 1
From            U I . . A V H O F . E J G N Z C T . K D . S P . R . | U
we can write     U . . . . . . . . . . . . . . . T
and              . . . . . . . . . . E . . . . . . . . . . X . . . . .
making the sequence U I . . A V H O F . E J G N Z C T . K D X S P . R .
                    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 26
```

E (0—5) G (1—5)
B (0—2) W (1—2)

```
From                    E J G
we can write            E . G
and then                B . W
```

There is only one place where B . W can fit, viz, at the end:

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	26
U	I	.	.	A	V	H	O	F	.	E	J	G	N	Z	C	T	.	K	D	X	S	P	B	R	W

Only four letters remain to be placed into the sequence L, M, Q, and Y. They were easily found by application of the primary alphabet to the message. Having the primary component almost fully constructed, decipherment of the cryptogram can be completed with speed and precision. The text is as follows:

FIGURE 8

1	2	3	4	5	6	7	8	9	10
W	F	U	P	C	F	O	C	J	Y
B	U	T	T	H	O	U	G	H	W
G	B	Z	D	P	F	B	O	U	O
E	C	A	N	N	O	T	A	S	Y
G	R	F	T	Z	M	Q	M	A	V
E	T	R	E	V	I	E	W	W	I
K	Z	U	G	D	Y	F	T	R	W
T	H	T	H	E	M	I	N	D	S
G	J	X	N	L	W	Y	O	U	X
E	Y	E	O	U	R	P	A	S	T
I	T	W	E	P	Q	Z	O	K	Z
W	E	C	A	N	T	O	A	N	E
P	R	X	D	W	L	Z	I	C	W
X	T	E	N	T	F	O	R	E	S
G	K	Q	H	O	L	O	D	V	M
E	E	O	U	R	F	U	T	U	R
G	O	X	S	N	Z	H	A	S	E
E	W	E	C	A	N	W	I	T	H
B	B	J	I	P	Q	F	J	H	D
S	C	I	E	N	T	I	F	I	C
Q	C	B	Z	E	X	Q	T	X	Z
C	O	N	F	I	D	E	N	C	E
J	C	Q	R	Q	F	V	M	L	H
L	O	O	K	F	O	R	W	A	R
S	R	Q	E	W	M	L	N	A	E
D	T	O	A	T	I	M	E	W	H
G	S	X	E	R	O	Z	J	S	E
E	N	E	A	C	H	O	F	T	H
G	V	Q	W	E	J	M	K	G	H
E	B	O	D	I	E	S	C	O	M

1	2	3	4	5	6	7	8	9	10
R	C	V	O	P	N	B	L	C	W
P	O	S	I	N	G	T	H	E	S
L	Q	Z	A	A	A	M	D	C	H
O	L	A	R	S	Y	S	T	E	M
B	Z	Z	C	K	Q	O	I	K	F
S	H	A	L	L	T	U	R	N	A
C	F	B	S	C	V	X	C	H	Q
N	U	N	C	H	A	N	G	I	N
Z	T	Z	S	D	M	X	W	C	M
G	F	A	C	E	I	N	P	E	R
R	K	U	H	E	Q	E	D	G	X
P	E	T	U	I	T	Y	T	O	T
F	K	V	H	P	J	J	K	J	Y
H	E	S	U	N	E	A	C	H	W
Y	Q	D	P	C	J	X	L	L	L
I	L	L	T	H	E	N	H	A	V
G	H	X	E	R	O	Q	P	S	E
E	R	E	A	C	H	E	D	T	H
G	K	B	W	T	L	F	D	U	Z
E	E	N	D	O	F	I	T	S	E
O	C	D	H	W	M	Z	T	U	Z
V	O	L	U	T	I	O	N	S	E
K	L	B	P	C	J	O	T	X	E
T	I	N	T	H	E	U	N	C	H
H	S	P	O	P	N	M	D	L	M
A	N	G	I	N	G	S	T	A	R
G	C	K	W	D	V	B	L	S	E
E	O	F	D	E	A	T	H	T	H
G	S	U	G	D	P	O	T	H	X
E	N	T	H	E	S	U	N	I	T

1	2	3	4	5	6	7	8	9	10
B	K	D	Z	F	M	T	G	Q	J
S	E	L	F	W	I	L	L	G	O
L	F	U	Y	D	T	Z	V	H	Q
O	U	T	B	E	C	O	M	I	N
Z	G	W	N	K	X	J	T	R	N
G	A	C	O	L	D	A	N	D	L
Y	T	X	C	D	P	M	V	L	W
I	F	E	L	E	S	S	M	A	S
B	G	B	W	W	O	Q	R	G	N
S	A	N	D	T	H	E	S	O	L
H	H	V	L	A	Q	Q	V	A	V
A	R	S	Y	S	T	E	M	W	I
J	Q	W	O	O	T	T	N	V	Q
L	L	C	I	R	C	L	E	U	N
B	K	X	D	S	O	Z	R	S	N
S	E	E	N	G	H	O	S	T	L
Y	U	X	O	P	P	Y	O	X	Z
I	K	E	I	N	S	P	A	C	E
H	O	Z	O	W	M	X	C	G	Q
A	W	A	I	T	I	N	G	O	N
J	J	U	G	J	W	Q	R	V	M
L	Y	T	H	E	R	E	S	U	R
U	K	W	P	E	F	X	E	N	F
R	E	C	T	I	O	N	O	F	A
C	C	U	G	D	W	P	E	U	H
N	O	T	H	E	R	C	O	S	M
Y	B	W	E	W	V	M	D	Y	J
I	C	C	A	T	A	S	T	R	O
R	Z	X							
P	H	E							

6. **General remarks.**—It is to be stated that the sequence of steps described in this paper corresponds quite closely with that actually followed by the writer in solving the problem. It is also to be pointed out that this method can be used as a control in the early stages of analysis because it will allow the cryptanalyst to check assumptions for values. For example, the very first value derived by the writer in applying the principles of indirect symmetry to the problem herein described was $H_c=A_p$ in alphabet 1. As a matter of fact he had been inclined toward this value, from a study of the frequency and combinations which H_c showed, and when the indirect-symmetry method actually substantiated his tentative hypothesis he immediately proceeded to substitute the value given. If he had assigned a different value to H_c, or if he had assumed a letter other than H_c for A_p in that alphabet, the conclusion would immediately follow that either the assumed value for H_c was erroneous, or that one of the values which led to the derivation of $H_c=A_p$ by indirect symmetry was wrong. Thus, these principles aid not only in the derivation of new values mathematically, and without reference to the actual frequencies of letters, or to tentative hypotheses for plain-text values, but they also assist very materially in serving as a check upon the validity of the assumptions already made.

Furthermore, while the writer has set forth in figure 7 a set of 30 values, before he began to reconstruct the primary component, this was done for purposes of clarity and brevity in exposition of the principles herein described. As a matter of fact, what he did was to watch very carefully, when inserting values in figure 7, to find the very first chance to employ the principles of indirect symmetry; and just as soon as a value could be derived, he actually substituted the value in the cryptographic text, not only to see that no impossible combinations were formed, but also in the expectation that further assumptions for values would suggest themselves, by the addition of the derived values to those previously assumed. Thus, the processes of reconstructing the primary component, and the finding of additional data for the reconstruction, proceed simultaneously in an ever widening circle.

It is worthy of notice that the careful analysis of only a sum total of 30 values in figure 7 results in the derivation of the entire table of secondary alphabets, 676 values in all. And while the description of the method, as is usually the case, seems long and tedious, in its actual application, the results are speedy, accurate, and gratifying in their corroborative effect upon the mental activity of the cryptanalyst.

7. **Concluding remarks.**—The problem here used as an illustrative case is by no means one that most favorably presents the application and value of the method. The writer has applied it to other much more favorable cases. For example, suppose that in a cryptogram of 6 alphabets the equivalents of only THE in all 6 alphabets are fairly certain. As in the previous case, it is supposed that the secondary alphabets are obtained by sliding a mixed alphabet against itself. Suppose the secondary alphabets to be as follows:

FIGURE 9

	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	26
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	.	.	.	.	B	.	.	Q	.	.	.	.	.	.	.	.	.	.	.	E	.	.	.	.	.	.
2	.	.	.	.	C	.	.	L	.	.	.	.	.	.	.	.	.	.	.	X	.	.	.	.	.	.
3	.	.	.	.	I	.	.	V	.	.	.	.	.	.	.	.	.	.	.	C	.	.	.	.	.	.
4	.	.	.	.	N	.	.	P	.	.	.	.	.	.	.	.	.	.	.	B	.	.	.	.	.	.
5	.	.	.	.	X	.	.	O	.	.	.	.	.	.	.	.	.	.	.	P	.	.	.	.	.	.
6	.	.	.	.	T	.	.	Z	.	.	.	.	.	.	.	.	.	.	.	V	.	.	.	.	.	.

Consider the following chain of derivatives:

H (0— 8) O (5— 8)
T (0—20) P (5—20)
E (0— 5) X (5— 5)→E (1—20) X (2—20)
Q (1— 8) L (2— 8)
B (1— 5) C (2— 5)→B (4—20) C (3—20)
N (4— 5) I (3— 5)
P (4— 8) V (3— 8)→

→P (5—20) V (6—20)
O (5— 8) Z (6— 8)
X (5— 5) T (6— 5)→X (2—20) T (0—20)
L (2— 8) H (0— 8)
C (2— 5) E (0— 5)→C (3—20) E (1—20)
V (3— 8) Q (1— 8)
I (3— 5) B (1— 5)

These pairs are manifestly all of the same interval, and therefore unions can be made immediately. The complete list is as follows:

EX	QL	NI	LH
HO	BC	OZ	CE
TP	PV	XT	VQ
			IB

Joining pairs by their common letters, we have

N I B C E X T P V Q L H O Z

With this as a nucleus the cryptogram can be solved speedily and accurately. When it is realized that it is quite often that the cryptanalyst can assume THE's rather readily, the value of this principle becomes apparent. When it is further realized that if a cryptogram has sufficient text to enable the THE's to be found easily, it is usually also possible to assume values for two or three other high-frequency letters, it is clear that the entire primary component can be very rapidly reconstructed.

The foregoing principles of indirect symmetry and the described method of reconstructing primary components were first used by the writer in 1919, in the solution of a much more difficult

problem, and the facts in connection therewith are rather interesting. Credit for the original and independent discovery of the possibility and method of applying the principles of indirect symmetry is due Mr. Paul S. Burdick, formerly second lieutenant, Signal Corps, who was associated with the writer in the Cipher Department, Riverbank Laboratories, Geneva, Ill., and the writer takes this opportunity of acknowledging his indebtedness to Mr. Burdick for the basic idea.

As originally stated by Mr. Burdick, the method only contemplated the insertion of values in the table of secondary alphabets by derivation from indirect symmetry. The writer extended the principles leading to the reconstruction of the primary component, by adding the idea of using partial sequences as sliding alphabets, a procedure which adds very considerably to the method and in fact makes it a most useful instrument in the analysis of cryptograms of this type, and by demonstrating that with but slight modification the basic principles could also be applied to the case where the primary components are not identical mixed sequences. A brief discussion of this point will be of interest.

Not long after Mr. Burdick's original contribution he presented the writer with a set of cryptograms prepared according to a method devised by him and which he claimed were proof against cryptanalysis.

The method of encipherment consisted in the use of two differently mixed primary sliding alphabets without a repeating key; each pair of plain-text letters served as the indicators for the juxtaposition of the sliding alphabets for the encipherment of the next pair of plain-text letters. The initial setting for a message was determined by prearrangement. For example, given the two alphabets below, and the initial key indicators as $\overset{1}{X}\overset{2}{P}$, they would be juxtaposed as follows:

(1)____ K I E Q B V Z Y $\bar{X}$ U P A W J D N S G O M C F T L R H
(2)____ H E R I L D Q Y $\underline{P}$ K G X Z O B S J V A T M F W U C N

Suppose the word WHEN is to be enciphered. The plain-text pair, WH, would be enciphered on alternate alphabets. Thus, W_p in (1)=Z_c, and H_p in (2)=K_c. Hence WH=ZK.

The alphabets are then juxtaposed according to the key letters WH, thus:

(1)____ K I E Q B V Z Y X U P A $\bar{W}$ J D N S G O M C F T L R H
(2)____ B S J V A T M F W U C N $\underline{H}$ E R I L D Q Y P K G X Z O

The next pair of plain-text letters, EN, is enciphered thus: E_p in (1)=J_c; N_p in (2)=A_c. Hence the word WHEN becomes ZKJA.

It is apparent that cryptograms enciphered in such a manner show no periodicity; that all possible secondary alphabets may be used in one and the same cryptogram; and that there are really 52 secondary alphabets instead of the usual number, 26, though, of course, the 52 secondaries consist of two sets of 26 each, which are interrelated in the manner of enciphering-deciphering alphabets.

A set of fifty test messages, each 25 letters in length and beginning at the same initial enciphering juxtaposition, was submitted by Mr. Burdick. By superimposing the messages the writer solved them and completely reconstructed both basic alphabets, *by applying and extending the principles of indirect symmetry of position that were first discovered by Mr. Burdick himself!* It is not often that a cryptanalyst unknowingly discovers the very weapon that deals the deathblow to his own brain-child! The steps in that solution can be briefly indicated. The attack was begun, of course, by superimposing the test messages and making an assault upon

the first few columns by using the simple principles of analysis based upon frequency and repetitions. A few values were tentatively assigned and the writer immediately decided to attempt to apply the principles of indirect symmetry of position. He realized, naturally, that because the primary components were dissimilar the principles would have to be modified somewhat, and he set out to uncover the necessary modification. It was found to be quite simple and consisted in restricting the field for the derivation of values for the *cipher* component to that portion of the table of secondary alphabet equivalents which is below the zero line. For example, if figure 9 applied to a case of dissimilar mixed primary components, we could not consider *all* the letters in columns 5 and 20 as belonging to the same interval in *both* primary components. Only those below the zero line would belong to the same interval in the *cipher* component. Although the pairs E (0–5) T (0–20), B (1–5) E (1–20), and N (4–5) B (4–20) are of similar intervals, the E (0–5) T (0–20) would pertain to the primary *plain* component, the B (1–5) E (1–20) and the N (4–5) B (4–20) would pertain to the primary *cipher* component, so that although we could construct the sequence NBE as applicable to the cipher component, it would be incorrect to add the T to make the sequence NBET. By restricting the selection of letters to those below the zero line in the case of dissimilar primary components, we can reconstruct the cipher component; having the latter, the plain component can then be reconstructed quite readily. For example, suppose in figure 9 that the completed cipher component places the letter N in position 1–1, i.e., directly under A in the zero line. Then we could say that since NBE forms a sequence in the cipher component, the chain ETA forms a sequence in the plain component. Thus, continuing in this manner the entire (equivalent primary) component may be reconstructed.

○