

~~RESTRICTED~~Security InformationNATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE Military Cryptanalysis, Part I
 LESSON 5 Polygraphic substitution: four-square and two-square matrices
 TEXT ASSIGNMENT Section IX

1. Construct a digraphic distribution for the cryptogram below.
 Solve the cryptogram, and recover all keys.

	5					10					15				
A	MH	EA	XP	SO	ZP	LM	HT	XN	PR	QU	EH	HG	<u>RH</u>	<u>GR</u>	<u>LC</u>
B	<u>HU</u>	<u>ZW</u>	<u>VA</u>	BD	MD	WO	HU	<u>ZB</u>	<u>XR</u>	DD	DU	<u>RH</u>	<u>GR</u>	<u>CG</u>	<u>HO</u>
C	<u>SO</u>	<u>ZB</u>	<u>XN</u>	<u>WS</u>	<u>ZO</u>	RG	BL	PC	SO	ZP	ZC	OC	BL	BT	QL
D	CP	GR	CC	LU	SD	WS	PR	PX	MD	YG	AM	DF	MH	IL	QH
E	<u>CQ</u>	<u>YO</u>	<u>IQ</u>	<u>PF</u>	<u>GF</u>	ND	BI	PF	CC	VA	<u>LF</u>	CC	<u>CQ</u>	<u>YO</u>	OZ
F	RT	OQ	VH	CG	IQ	KP	DL	IY	<u>AO</u>	<u>HA</u>	<u>CG</u>	<u>HO</u>	<u>PF</u>	<u>GF</u>	TD
G	<u>CP</u>	<u>AO</u>	<u>HA</u>	<u>CV</u>	<u>LF</u>	CC	<u>CQ</u>	<u>YO</u>	QU	OD	CN	OG	CN	WA	QC
H	HT	MH	KQ	ZG	<u>LC</u>	<u>HU</u>	PB	GT	ID	WQ	OF	WG	ZO	LG	KG
J	DL	<u>ZW</u>	<u>VA</u>	<u>ZB</u>	<u>XR</u>	AU	VA	DH	PF	MH	FF	ZB	OH	WL	<u>CG</u>
K	<u>HO</u>	LZ	<u>SO</u>	<u>ZB</u>	<u>XN</u>	<u>WS</u>	<u>ZO</u>	IU	TA	AO	GA	HA	<u>EU</u>	<u>MH</u>	YO
L	LF	<u>EU</u>	<u>MH</u>	HU	LV	WQ	MZ	YT	ZT	<u>ZO</u>	<u>YG</u>	SO	LZ	CP	EU
M	ON	MU	WG	RT	<u>CG</u>	<u>HO</u>	<u>MH</u>	<u>MS</u>	<u>PR</u>	OT	MF	LF	CP	KS	RO
N	WZ	MN	QU	<u>CP</u>	<u>AO</u>	<u>HA</u>	<u>CV</u>	CO	MH	DT	DU	<u>PF</u>	<u>GF</u>	NQ	YG
O	QD	EB	WS	<u>ZO</u>	<u>YG</u>	BB	YO	ZN	XR	LW	HU	IQ	WS	<u>QD</u>	<u>DC</u>
P	ZB	IB	RM	SO	EN	IA	RU	DW	GR	<u>CG</u>	<u>HO</u>	<u>MH</u>	<u>MS</u>	<u>PR</u>	<u>QD</u>
Q	<u>DC</u>	LZ	TN	WL	KN	PF	XD	UT	WA	ZO					

~~RESTRICTED~~

~~RESTRICTED~~

2. The following cryptogram is suspected to contain the probable word REQUISITIONS. Solve it and recover all keys.

	5					10					15				
A	<u>DI</u>	<u>AF</u>	<u>IQ</u>	GY	II	KG	IT	GC	QC	OV	DE	KU	DM	RI	RN
B	<u>RO</u>	<u>NK</u>	<u>UN</u>	KP	DH	CU	RH	PA	<u>QQ</u>	<u>PL</u>	OD	CM	YB	HE	MR
C	QQ	EG	LP	QC	IP	OP	LN	SN	DT	DP	UT	RS	EM	RN	OA
D	QL	OD	DA	QL	EL	EM	WK	NK	DC	XP	RK	HT	HE	QR	QU
E	BP	LP	LK	NQ	LE	SR	HF	SQ	SO	QR	CM	QL	HL	AC	TX
F	GK	KF	CM	TT	QB	RP	IT	BK	MP	HL	BC	IU	MT	ZF	RW
G	ZR	CK	CM	DC	VC	OA	UA	QP	RR	IV	RQ	PK	TP	CE	QH
H	KP	UC	<u>RO</u>	<u>NK</u>	HO	<u>QQ</u>	<u>PL</u>	OD	CM	YB	HE	MR	<u>DI</u>	<u>AF</u>	<u>IQ</u>
J	IT	IW	SO	EM	DM	QT	RQ	BK	IG	TB	CE	AY	IU	IK	NX

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

$\phi_p^2=125$ $\phi_r^2=27$ $\phi_o^2=106$

~~RESTRICTED~~

~~RESTRICTED~~

3. The following cryptogram was enciphered by means of an inverse four-square matrix, wherein the cipher sections are normal alphabets (I=J) inscribed in straight horizontals. Solve it and recover all keys.

				5					10					15	
A	QU	KF	FF	TO	IP	KI	GB	AD	ES	FQ	HD	GL	AG	KI	EE
B	TO	RD	GH	SO	RH	FO	FV	KI	GO	RH	HD	GU	UU	IP	WF
C	ON	MD	RI	HB	ME	SO	BU	MO	FF	UK	GI	GL	AG	OO	MI
D	GH	PQ	GI	FG	ER	GI	UO	NL	QD	FQ	QK	HD	WG	FG	FG
E	NU	TO	MH	LP	OK	GG	QX	<u>AH</u>	<u>GQ</u>	PY	KT	PZ	KT	LP	FV
F	KY	KT	NE	RT	UQ	IT	HK	FG	DN	US	ID	LU	PD	HA	KB
G	OD	GT	FZ	IA	FQ	FF	ZD	HI	GH	RI	QC	FQ	<u>AH</u>	<u>GQ</u>	MT
H	FU	<u>AH</u>	<u>GQ</u>	FD	DP	TY	EP	EQ	AN	SD	RT	TL	LC	KI	KA
J	RI	DC	TO	LU	FA	RF	UC	TO	WF						

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

$\phi_p^2 = 116$ $\phi_r^2 = 25$ $\phi_o^2 = 126$

~~RESTRICTED~~

~~RESTRICTED~~

5. The following two messages were intercepted on the same radio link half an hour apart, message "B" being in answer to a request for a service. Solve the texts, recover all keys, and determine the cause of the cryptographic error involved.

MESSAGE "A"

	5					10					15				
A	DS	ZM	<u>CM</u>	GI	QM	<u>AB</u>	<u>VG</u>	<u>ED</u>	SU	XI	TO	<u>SQ</u>	OR	NR	SB
B	<u>PN</u>	QO	HN	TB	LL	QN	QS	SI	CR	YU	TQ	CC	KG	AT	FN
C	YF	<u>VG</u>	<u>ED</u>	CG	NU	MO	LL	NP	SO	SB	NP	<u>SQ</u>	OR	NR	SB
D	<u>PN</u>	CM	MB	RP	OG	LL	YX	<u>CM</u>	GI	QM	<u>AB</u>	SO	NQ	LZ	IC
E	FD	YR	VI	OR	SB										

MESSAGE "B"

	5					10					15				
A	OY	RU	<u>PU</u>	KV	TU	<u>WO</u>	<u>IW</u>	LL	NR	EV	VD	<u>NB</u>	BZ	YZ	NO
B	<u>AS</u>	TD	HS	VO	DE	TS	TY	NV	PZ	SR	VB	PM	FW	WQ	XS
C	SK	<u>IW</u>	<u>LL</u>	PW	YR	CD	DE	YC	ND	NO	YC	<u>NB</u>	BZ	YZ	NO
D	<u>AS</u>	PU	CO	UC	BW	DE	SF	<u>PU</u>	KV	TU	<u>WO</u>	ND	YB	DI	DM
E	XL	SZ	IV	BZ	NO										

~~RESTRICTED~~

~~RESTRICTED~~

6. The following cryptogram, suspected to begin with the words AIR RECONNAISSANCE REPORTS, was enciphered by means of a four-square matrix with four different keyword-mixed sections. Solve it and recover all keys.

	5					10					15				
A	IC	RO	IK	HC	AA	OU	TC	IH	BO	NR	RD	TT	CD	FI	LP
B	MS	TD	XA	LB	<u>EA</u>	<u>OY</u>	TI	PC	<u>PF</u>	<u>HC</u>	QC	RD	TM	XB	US
C	CD	MO	EB	IV	<u>HE</u>	<u>GG</u>	LB	XA	ND	US	KC	SF	<u>EA</u>	<u>OY</u>	KC
D	PL	HC	US	LO	BT	NK	NL	IG	<u>PF</u>	<u>HC</u>	ND	GC	IX	YF	RR
E	<u>HE</u>	<u>GG</u>	OW	IR	QI	IL	IR	NB	TT	HG	TM	OU	SC	BT	RD
F	<u>US</u>	<u>HS</u>	<u>LB</u>	<u>SO</u>	<u>AR</u>	UF	CS	CA	EH	<u>CF</u>	<u>TS</u>	<u>OE</u>	<u>AQ</u>	HC	TM
G	AR	NR	OS	RU	<u>OE</u>	<u>AQ</u>	LA	DB	XA	IA	CT	NK	OG	SF	UI
H	OE	CB	TY	<u>US</u>	<u>HS</u>	AS	TD	HC	AS	<u>CF</u>	<u>TS</u>	<u>OE</u>	<u>AQ</u>	BD	IK
J	CS	QI	BR	NK	<u>LB</u>	<u>SO</u>	<u>AR</u>	PN	QE	ME	NR	RD	UF	AR	NB
K	UT	RS	GC	SC	GC	NL	SO	BD	SF	OR	<u>US</u>	<u>HS</u>	KG	IH	AS
L	SF	CK	HD	BD	TY										

(See distribution on following page)

~~RESTRICTED~~

RESTRICTED

(Frequency distribution for Problem 6)

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

$\phi_p^2=165$ $\phi_r^2=36$ $\phi_o^2=228$

RESTRICTED

~~RESTRICTED~~

(BLANK)

~~RESTRICTED~~

~~RESTRICTED~~Security InformationNATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE

Military Cryptanalysis, Part I

LESSON 6

Polygraphic substitution: Play-
fair cipher systems

TEXT ASSIGNMENT

Section IX

1. Solve the following cryptogram and recover all keys:

	5	10	15
A	UA SK UA SP KM MR IO OR IX YR OR OS <u>MS SD</u> UA →		
B	← <u>RH LV</u> BR SA AK SW AX SA BG CW PN CW <u>XS AU</u> BS →		
C	← <u>NA NM SM VU YN AR OR HG RA</u> RL SA YN UK SA OR		
D	MY IA AU BF <u>MS SD</u> UN WC AS EN CA HN DR FB NL		
E	AS PU RF VU RO MW BE RP NY IA CU GR WO SR <u>XS</u> →		
F	← <u>AU BU LB UG DM KS MR</u> GN HQ DM DU HU SB WC AS		
G	UB EO AS AD WB NO DK AD FB RH SP RW HO UC AD		
H	FT NO SB AU RD OT <u>MS SD</u> UN XB VL UA KS HQ <u>KS</u> →		
J	← <u>MR UA RH</u> LV CU CW FB NL QO <u>AR OR HG RA</u> LV AL		
K	UB UA CE RB AD EQ YX OE XH UM SW PR FS ON UK		
L	GN DR UP UR XW RW QH FR SD AS NO AD UA WB NO		
M	WS IG FS LR UB CA UO RP AS SB NW BH NP <u>BS NA</u>		
N	UA OE RB RB RZ RO KR OR VR NU US DR SR SP RW		
O	FR DA		

(For distribution, see page 2)

~~RESTRICTED~~

(Frequency distribution for Problem 1)

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

$\phi_p^2=266$

$\phi_r^2=58$

$\phi_o^2=316$

~~RESTRICTED~~

2. The following cryptogram is suspected to contain the word DIVISION. Solve it and recover all keys.

	5					10					15				
A	MP	<u>QK</u>	<u>KA</u>	SZ	<u>QK</u>	<u>KA</u>	HX	<u>EH</u>	<u>LK</u>	<u>YS</u>	<u>ND</u>	<u>TP</u>	<u>CQ</u>	OL	NP
B	RC	AH	<u>IM</u>	<u>SK</u>	<u>ND</u>	YG	<u>QK</u>	<u>DU</u>	<u>RF</u>	<u>QK</u>	<u>EH</u>	<u>LK</u>	<u>YS</u>	<u>ND</u>	<u>TP</u>
C	SA	OE	SY	FR	QP	FE	YS	MO	FD	AF	RJ	RS	<u>DU</u>	<u>RF</u>	RN
D	<u>TP</u>	<u>CQ</u>	<u>UL</u>	<u>IM</u>	<u>SK</u>	<u>ND</u>	UD	FM	JE	HR	VN	<u>QK</u>	<u>UD</u>	<u>EC</u>	<u>LF</u>
E	AK	BH	IY	QV	SM	FO	SY	DY							

3. Solve the following cryptogram and recover all keys. It is suspected that this message is signed "WINTHROP COL INF."

	5					10					15				
A	4L	65	4L	C3	<u>1V</u>	PV	7W	XV	ZX	<u>B1</u>	DS	07	L4	CW	4K
B	OF	RT	<u>4L</u>	<u>79</u>	<u>OL</u>	<u>HR</u>	YN	MR	RM	DQ	QV	9R	6M	CX	4K
C	QF	4N	<u>4L</u>	<u>79</u>	<u>OL</u>	<u>HR</u>	OP	E4	NR	QB	4M	XS	WN	<u>ØE</u>	NU
D	GC	QX	4K	<u>ØD</u>	<u>51</u>	NP	Z5	4R	L4	VQ	PF	HN	<u>4L</u>	<u>79</u>	<u>OL</u>
E	<u>HR</u>	EM	8X	<u>41</u>	ND	AP	<u>Z1</u>	4N	XC	M4	RT	P6	4M	5H	FZ
F	C3	R9	Q4	CI	2H	XZ	48	<u>1Ø</u>	L4	YN	PQ	LM	HR	T4	PQ
G	BQ	RM	D3												

~~RESTRICTED~~

~~RESTRICTED~~

4. Solve the following cryptogram and recover all keys:

XVDQG	YUUSD	FSRAZ	WMDYY	WUQBL	YUZRB
YPBYU	KCKFU	OSRZK	FXZRK	DYEUE	GQZRB
MDCOL	VZRAG	HGQRS	KVING	BQKBY	RBFXD
YDFVZ	BCGBB	MDCYW	UQBLY	UZREQ	NAZRV
QACQP	HQBUW	TXJYE	UHXQN	GPDQL	UIRSK
CGKOF	LKVZI	OBAXI	TCUQH	LGHAR	DFKHK
QUSPV	LHXQY	VKFGH	ARZAU	YPYHQ	MBTWE
PVKTO	YRBPU	BFGKF	UOSRO	KKXSR	XFYEW
QSRBU	OZEUQ	GPYRS	VPQUK	OQFRG	XISRZ
KBZWG	OXVDV	DRPVZ	VKBYD	FJXVD	QGYUU
SABVD	EQTBV	KBMVZ	UYPYH	QBMDC	OLKLB
ULPIP	THBLV	HRZBX	QXSRM	KVKSR	MGZRK
JVUUY	BSUZK	VAUVD	PDIQE	CIPTF	QVTMR
WKVBA	RVBBQ	KQVHG	JXRIX		

~~RESTRICTED~~

~~RESTRICTED~~

5. The following cryptogram is suspected to contain the signature "CLINTON COURTNEY COL INF." Solve it and recover all keys.

```

LHQEF IPXOE OPYQE NCOPC MAGZH EFQEL
MCOBY FMEBO DKDYS YFQEL EFD FH EFQET
OLIEG GYHLO SLMLQ LBPJZ SPTFA OFQRL
DQELN HQEFF MIBTZ OFGWJ FOSLM DPYFQ
ELBLY BYFQE LYFQE LLMSX LEBIF EFD MQ
ECFZN LQEMF XSLMT OLIDY OADSF EOSQE
MLEFQ RQILU BPSTL MFHLM FIKQE FFYFQ
ELTOL LGDYD TLQLB PKFAO FQROT PCQEM
OSQEM LMBLY BGC'GZ FQRWO OLSAP SKLLM
ESZQR LKMOE SPSRN

```

6. The following cryptogram is suspected to contain the probable beginning "PART ONE OF THREE PARTS." Solve it and recover all keys.

```

NBBVC QKVHI EBMMN BBVII BDLBK LSF XV
RKCBV MKRYF QTBVR HVIYP YBVHB ODBFT
XEGRR LWYBV FYIIK TUCPH MWPYF YWRQA
IBLHZ VGYUU YCAVE GHIRW UVHPK RBDDI
SYEAI ZNTIQ NYMWP YFYIK KTSYU EQVXP
UVPTF MRWIP YCVDD RFYGB SMYCA VEGHI
KGNYN LTBI V KRHFG LFLFG ABYDP TIQNY
YFQTB VIKNY CMVHP BPTLP IZYUK IEGUU
TQFYB CYDPB NRVYV AYGOZ

```

~~RESTRICTED~~

~~RESTRICTED~~

(BLANK)

~~RESTRICTED~~

~~RESTRICTED~~Security InformationNATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE	Military Cryptanalysis, Part I
LESSON 7	Polygraphic substitution: large tables
TEXT ASSIGNMENT	Section IX

1. The following cryptogram is suspected to contain the probable word "RECONNAISSANCE." Solve it and recover all keys.

	5					10					15				
A	SA	<u>CJ</u>	<u>JY</u>	RO	HT	KP	LP	DO	CV	PS	LN	PE	GN	RP	SP
B	FP	LU	<u>QT</u>	<u>LW</u>	PR	<u>CJ</u>	KL	RN	QE	RO	CV	MF	SE	LZ	QZ
C	RR	AO	TH	SQ	PG	TL	GL	NR	QS	UZ	KK	<u>KK</u>	<u>JE</u>	MV	NL
D	LU	AR	QE	SA	MW	KK	LP	SL	AP	PZ	QV	KK	PB	<u>CJ</u>	<u>JY</u>
E	RL	CJ	HA	CO	AR	BH	LL	JH	QT	RP	AS	SL	RP	SL	NL
F	<u>QJ</u>	<u>QT</u>	<u>AJ</u>	NL	IG	NR	WX	AI	HI	YD	<u>KK</u>	<u>JE</u>	CP	YO	SP
G	KO	FB	QT	QP	YP	NZ	SO	AM	DZ	KR	FP	SX	PK	FJ	PR
H	OE	AK	CE	AS	LP	DO	PB	SI	AX	SX	PB	LP	HT	WX	RF
J	GZ	<u>QT</u>	<u>LW</u>	PR	<u>CJ</u>	<u>JY</u>	AK	HT	JY	AA	NN	SX	CB	RO	WE
K	SA	RD	LL	ML	AX	AF	YU	NC	PK	MS	NE	<u>QJ</u>	<u>QT</u>	<u>AJ</u>	

(For distribution, see next page)

~~RESTRICTED~~

~~RESTRICTED~~

(Frequency distribution for Problem 1)

	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	
A	1	-	-	-	1	-	-	1	2	2	-	1	-	1	1	-	2	2	-	-	-	-	2	-	-	-	16
B	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
C	-	1	-	-	1	-	-	-	-	5	-	-	-	-	1	1	-	-	-	-	-	2	-	-	-	-	11
D	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	1	3
E	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
F	-	1	-	-	-	-	-	-	-	1	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	-	4
G	-	-	-	-	-	-	-	-	-	-	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	1	3
H	1	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	3	-	-	-	-	-	-	-	5
I	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
J	-	-	-	2	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	-	7	
K	-	-	-	-	-	-	-	-	-	5	1	-	-	1	1	-	1	-	-	-	-	-	-	-	-	-	9
L	-	-	-	-	-	-	-	-	-	2	1	4	-	-	-	-	-	-	2	2	-	-	-	1	-	12	
M	-	-	-	-	1	-	-	-	-	1	-	-	-	-	-	-	-	1	-	1	1	-	-	-	-	5	
N	-	-	1	1	-	-	-	-	-	3	1	-	-	-	2	-	-	-	-	-	-	-	-	-	1	9	
O	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	
P	-	3	-	-	1	1	-	-	2	-	-	-	-	-	-	-	-	3	1	-	-	-	-	-	1	12	
Q	-	-	-	2	-	-	-	2	-	-	-	-	-	-	1	-	-	1	6	1	-	-	-	-	1	14	
R	-	-	-	1	1	-	-	-	1	1	3	3	-	1	-	-	-	1	-	-	-	-	-	-	-	-	11
S	3	-	-	-	1	-	-	1	-	3	-	1	2	1	-	-	-	-	-	-	-	-	3	-	-	15	
T	-	-	-	-	-	-	1	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	
U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	
V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
W	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	3	
X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Y	-	-	-	1	-	-	-	-	-	-	-	-	-	1	1	-	-	-	-	-	1	-	-	-	-	-	4
Z	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
	5	5	1	2	10	3	2	3	3	10	9	13	1	4	10	16	1	9	5	9	3	4	3	7	4	7	

Digraphic phi data

$\phi_p^2 = 152$ $\phi_r^2 = 33$ $\phi_o^2 = 184$

Monographic phi data

$\phi_p = 1471$ $\phi_r = 849$
 Initial ltrs: $\phi_o = 1386$ Final ltrs: $\phi_o = 1096$

~~RESTRICTED~~

~~RESTRICTED~~

2. The following cryptogram is suspected to begin with the opening words "WEATHER FORECAST FOR WEDNESDAY ONE THREE SEPTEMBER." Solve it and recover all keys.

	5					10					15				
A	OL	TS	HM	XD	AW	AU	ST	ZF	AW	OL	QJ	WD	EM	KB	SA
B	OD	WE	WD	TG	YG	KC	VE	<u>JY</u>	<u>DY</u>	QG	EX	FE	KK	FP	OR
C	IF	OD	RD	MJ	OB	MH	HG	SK	VQ	VQ	OD	QL	AW	WR	US
D	KK	DO	CA	US	VQ	OD	DO	<u>YD</u>	<u>VE</u>	<u>MY</u>	<u>MH</u>	<u>JY</u>	<u>DY</u>	MY	HX
E	HM	ST	YG	EI	VU	VQ	VC	TS	KX	XD	MX	DO	CK	SK	LX
F	US	MH	BZ	LU	CF	<u>XW</u>	<u>BQ</u>	VJ	OU	JD	IW	QF	UO	US	NO
G	LH	EC	WD	XJ	JM	VQ	AI	<u>YD</u>	<u>VE</u>	<u>MY</u>	<u>MF</u>	VR	VE	AP	VQ
H	ZE	HT	KW	CK	<u>XW</u>	<u>BQ</u>	HZ	BR	HP	CJ	FS	TW	OG	ZX	IZ
J	AM	AG	JD	YG	FE	MH	ER	VE	OU	TW	WD	<u>JY</u>	<u>DY</u>	RK	RG
K	WF	TG	AW	QW	DO	OD	VE	JY	TS	WP	OZ	NT	IW	HX	YJ
L	BZ	KW	CK	DQ	AM										

~~RESTRICTED~~

3. The following two messages, intercepted on links known to be passing traffic enciphered by means of random digraphic tables, are believed to be isologs containing the probable signature "MAJ GEN CARTER WORTHINGTON". Solve the texts and reconstruct the fragmentary table.

Message "A"

	5					10					15				
A	<u>CX</u>	<u>JI</u>	<u>GO</u>	<u>NB</u>	<u>XJ</u>	<u>LV</u>	<u>OP</u>	<u>LD</u>	<u>XG</u>	<u>OI</u>	UT	LI	ZV	<u>DM</u>	<u>DE</u>
B	<u>AY</u>	AM	CX	BD	DZ	JX	VK	DQ	<u>IY</u>	<u>IG</u>	JO	KW	DE	IG	JX
C	BR	OU	LN	SR	<u>SC</u>	<u>DE</u>	<u>UW</u>	<u>QK</u>	<u>VN</u>	<u>LN</u>	<u>ZH</u>	<u>YM</u>	IQ	DW	KS
D	ER	AV	ZH	LD	RD	DE	IQ	<u>OF</u>	<u>QQ</u>	HT	OF	VB	DE	PC	JI
E	GS	<u>XJ</u>	<u>NZ</u>	<u>NN</u>	<u>IG</u>	OF	NB	SR	ZH	JU	TI	AA	GP	DZ	GP
F	XF	DE	KW	FH	WX	ML	PY	RN	AY	AM	<u>ER</u>	<u>AJ</u>	UI	SX	OW
G	<u>UW</u>	<u>QK</u>	<u>VN</u>	<u>LN</u>	<u>ZH</u>	<u>YM</u>	AV	HW	OW	SC	JX	<u>OF</u>	<u>QQ</u>	<u>MO</u>	<u>SR</u>
H	<u>AY</u>	<u>NR</u>	DZ	CO	IS	SR	ZH	HT	VF	IQ	VN	FH	TQ	UT	HT
J	EX	EV	XG	<u>IY</u>	<u>IG</u>	OF	YR	<u>JL</u>	<u>OF</u>	OF	IA	IG	BT	<u>MO</u>	<u>SR</u>
K	<u>AY</u>	<u>NR</u>	HF	WX	GD	PX	OL	CO	EN	SG	SL	MG	CX	ID	VM
L	OP	IH	<u>LN</u>	<u>ZH</u>	TM	SL	SC	OF	GL	IG					

Message "B"

	5					10					15				
A	<u>CX</u>	<u>JI</u>	<u>GO</u>	<u>NB</u>	<u>XJ</u>	<u>LV</u>	<u>OP</u>	<u>LD</u>	<u>XG</u>	<u>OI</u>	UI	SC	<u>XJ</u>	<u>NZ</u>	<u>NN</u>
B	<u>IG</u>	<u>ER</u>	<u>AJ</u>	OF	ZH	WC	PM	<u>SR</u>	<u>AY</u>	NR	KQ	RI	BR	LD	YM
C	JO	ED	XG	TI	CO	VU	<u>QF</u>	<u>UO</u>	<u>KM</u>	<u>LI</u>	<u>JX</u>	EN	MX	QF	NE
D	SC	SR	WX	LH	HK	EN	FW	DT	SL	DR	LV	CO	WG	ZT	IG
E	NU	<u>DM</u>	<u>DE</u>	<u>AY</u>	PS	XQ	XQ	TI	LH	YO	CX	VF	OF	<u>JL</u>	<u>OF</u>
F	CO	HI	IQ	PC	DZ	CH	NN	<u>IY</u>	<u>IG</u>	WG	CX	BD	KC	UT	FJ
G	<u>QF</u>	<u>UO</u>	<u>KM</u>	<u>LI</u>	<u>JX</u>	VU	IN	XS	LI	UW	RI	DT	SL	<u>VF</u>	<u>IY</u>
H	<u>IG</u>	IG	<u>SC</u>	<u>DE</u>	VF	TI	JX	FL	LN	KJ	RT	ER	SX	OW	JI
J	AJ	JX	<u>SR</u>	<u>AY</u>	PS	NR	QV	GP	PS	IV	JI	DT	EE	<u>VF</u>	<u>IY</u>
K	<u>IG</u>	SL	DJ	PS	KS	JO	<u>SC</u>	<u>DE</u>	IQ	CH	LI	<u>ER</u>	<u>AJ</u>	VF	TF
L	WX	ZZ	<u>LI</u>	<u>JX</u>	FG	LI	CO	LV	CX	CC					

~~RESTRICTED~~

4. Solve the following cryptogram and recover all keys:

	1	2	3	4	5	6	7	8	9	10
A	003	<u>315</u>	<u>097</u>	114	347	261	067	217	314	241
B	195	062	350	115	006	451	062	<u>141</u>	<u>072</u>	472
C	189	192	018	400	189	067	<u>315</u>	<u>097</u>	530	403
D	<u>115</u>	<u>393</u>	262	609	192	356	115	186	122	467
E	212	071	074	237	235	114	416	<u>115</u>	<u>393</u>	271
F	055	293	186	552	009	062	471	141	150	193
G	186	516	184	266	274	470	002	238	053	186
H	<u>141</u>	<u>072</u>	236	516	189	004	195	191	479	067
J	008	397	080	137	105	189	391	262	343	408
K	133	273	071	084	274	400	367	223	403	186
L	211	524	008	292	011	122	393	284		

~~RESTRICTED~~

~~RESTRICTED~~

5. The cryptogram below is suspected to begin with the stereotype "REFERRING TO YOUR MESSAGE" or "REFERENCE YOUR MESSAGE." Solve the text and recover all keys.

	1	2	3	4	5	6	7	8	9	10
A	MRA	DMT	<u>GCI</u>	YIY	MFG	NNL	SRK	QFB	<u>DMD</u>	WII
B	DSZ	GNM	IJA	GOO	<u>LGI</u>	DEV	LTD	<u>GCI</u>	IYD	LCI
C	MMT	JIU	PNM	VZP	<u>LGI</u>	DMY	ITI	<u>POV</u>	<u>GIP</u>	TGO
D	PLM	MCH	JPB	MRC	<u>DGK</u>	<u>FWJ</u>	IHC	EEF	MDO	DSZ
E	TEN	<u>DGK</u>	<u>FWI</u>	NNM	LEV	EZF	TAS	DIP	HMT	TDL
F	GTR	QMD	MZU	ROD	NPC	JNJ	<u>GCI</u>	<u>IQM</u>	UZK	LIY
G	NJN	CWQ	MZF	VOD	NWG	PRG	NLC	URP	MIA	DGI
H	VRG	NRF	URV	PIF	DUJ	TDL	POJ	VRT	DAZ	MRI
J	IFX	DGG	DHV	<u>VZP</u>	<u>IQM</u>	<u>EMF</u>	<u>JPC</u>	<u>SMK</u>	<u>JLM</u>	MND
K	PQW	YZB	OZN	IJY	IPJ	DMD	YJP	NIP	<u>EMF</u>	<u>JPC</u>
L	<u>SMK</u>	<u>JLF</u>	ENG	NFW	FNV	FJJ	LWI	GTT	MOT	EOW
M	CRV	WLF	ELE	TSZ	TNM	VRS	MTR	TEQ	VRV	QJQ
N	MRV	<u>NOV</u>	<u>GIP</u>	RMT	KQX	GCJ	ELC	MZH	PRT	LNM
P	LCR	IYR	CZY	GPW	XPA					

θ^1 : 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 $\phi = 1094$

θ^2 : 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 $\phi = 981$

θ^3 : 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 $\phi = 794$

$E(\phi_p) = 1207$

$E(\phi_r) = 696$

~~RESTRICTED~~

~~RESTRICTED~~

6. The following cryptogram is suspected to contain the probable word "AIRCRAFT." The encipherment is believed to involve a tetranome trigraphic system employing a matrix similar to that illustrated in Fig. 59 of the text, the ciphertext sections being composed of the dinomes 00-99 inscribed in the normal manner of writing, but the plaintext sections consisting of keyword-mixed sequences which differ from those in the text example. Solve the cryptogram and recover all keys.

	1	2	3	4	5	6	7	8	9	10
A	0601	7849	4912	<u>2533</u>	<u>1747</u>	6031	4270	8240	1877	6111
B	0240	1245	4827	1236	5681	6831	<u>4214</u>	9945	1875	8917
C	3309	4143	8843	5342	7719	1517	2774	3249	4507	4872
D	6011	1266	4145	7327	6760	5345	7619	5945	7349	3043
E	7709	2819	4322	0129	3875	2713	3046	9040	0775	6561
F	2911	2507	3576	1505	<u>4214</u>	9875	3570	0208	6583	6161
G	3247	2107	1777	3918	<u>2533</u>	<u>1747</u>	0264	1956	1242	4707
H	7772	3296	3491	0576	0779	5514	1145	3143	8569	2871

~~RESTRICTED~~

~~RESTRICTED~~

(BLANK)

~~RESTRICTED~~