

MAT 483 – 001

Fall 2007

Do ten problems.

Due no later than W, October 3.

1. Unknown ciphers. One of the following three ciphertext messages was encrypted with a Caesar cipher, one with an affine cipher, one with a keyword cipher, and one with another cipher. Determine which is which. Explain.

Ciphertext number one

JSMZI CTURG IZVUF GCBFS ATJGC HUBIC HHBBH SIJFE
OHFIP UHJBI CFIIC HTZLL PSJTF IJZSL FRMHO UHHER
VJWHS IZFEE ICHDZ UEAFE ICZPV CJIJB PSJSI HEEJV
JMEHB FWHIZ ICZBH DCZGZ BBHBB ICHXH R

Ciphertext number two

IEWIN IGTFR ICOID RTHHT DOMTA EHHAE EOLGU TMTNT
RAGOO DSTIE ESLQE GWNRA ELHIH CBESE USSSI NLSII
QTSRT FNAOR IHAIG YNRHN AUFSM EGQFS ETAGU WUDSH
FNBAH WAPBN YOGNQ MERIE NIDEN EEEAT RGEIE CEFSN SQ

Ciphertext number three

IWTBT GTUPR IIWPI IWTBT HHPVT XHRDC RTPAT SDGHT
RGTIA NRDCK TNTSS DTHCD IBPZT XIPRG NEIDV GPEWD
GRXEW TGIWT BPYDG XINDU HIDGX THSTP AXCVL XIWHT
RGTIR DBBJC XRPIX DCHPG TRDCR TGCTS LXIWI WTPGI
UJACT HHLXI WLWXR WIWTB THHPV TXHRD CRTPA TSDGR
DCKTN TSPCS WPKTC DIWXC VIDSD LXIWI WTRGN EIDVG
PEWHD GRXEW TGH

Ciphertext number four

HJTPQ MCXHF IMLMN TYMLH KHXHY YMCZN BCTET YOIFJ
QHCHJ EMCKH CITEC HCTWF TYSMY EMLZC IFHYH CITEC
HCFRK MZNWM EEMCK BZCLK ZCJQH CHJEM CKTYZ EQMCE
QHYEQ MTCZC LTYHC FKMYK MTYEM WWTOT IWMZY WFEZE
QZKMP ZKKMK KTYOE QMVMF EQMBZ CLTKK ZXMET XMKRK
MLEZL MYZEM EQMJZ XXRYT JHETZ YXHLM

2. Cryptanalyze one of the ciphers in problem 1.
3. Cryptanalyze another of the ciphers in problem 1.
4. Cryptanalyze another of the ciphers in problem 1.
5. Symbols. Cryptanalyze the following message:

☉●✕□☒ ●✕☉●□ ✕□ℳ❖❖ ○✕✕✕ℳ ☒☒●✕○ ❖□✕☉◆
 ☒ℳℳ○◆ □☒●✕ℳ ☉✕❖✕☒ ℳ□✕□☒ ●ℳ◆✕□
 ◆□☒●✕ &❖◆☒□ ✕◆◆er☒ ●✕ℳ□□ ✕ℳℳ□◆
 erer○γ●✕ ✕◆◆✕✕ ☒◆◆□☒ ●✕□☒● ✕○□◆◆ ❖☒ℳ□γ●
 ✕◆er☒● ✕○❖☉◆ ❖□ℳ□✕ ☒●✕◆✕ ❖○◆☒◆ □✕◆◆◆
 er✕✕ℳ□ ○□&☉○ ☒●γ●□ℳ ◆◆○er○ ✕✕□ℳ☒ ✕❖○ℳ
 □ ☒●○◆☉ ℳ◆er◆□ □◆☉✕✕ ✕ℳℳ□◆ ☒●✕❖◆
 erer○γ●✕ □ℳ□ℳ☉ ◆□✕□☒ ●◆☒&● ☒☒◆✕✕ ℳγ●ℳ◆
 □ℳ○□

6. Known plaintext attack. Cryptanalyze the following message. We believe that the word *benediction* appears in the message.

XNFXV JBDZJ EHXVX BLXRS XDXWB VJBED JUXMR LXIMX
 HXIKH FHBIX WJESX JETWB YPEKX LXHJX TTMUR JPEKR
 HXWEB DZPEK RHXVE CCBJJ BDZJH XRIED RDWWE DJJUB
 DAJUR JOKIJ SXVRK IXPEK RHXPE KDZTR WBXIP EKMBT
 TSXJH XIJXW RDPWB YYXHX DJTPJ UXDJU XCXDM UEVEC
 CBJJH XRIED BYPEK XLXHJ XTTMX MBTTI UEEJP EK

7. Known plaintext attack on Playfair cipher. Determine a Playfair square for the following message that was encrypted with a Playfair cipher.

FZTOZ DGRNB ASCOQ YDOBK RZOXX CNTFD ULNZZ
LYZNG HVTZT LUBDY UQOPY DNBQE RPSOK MMZQA
XCIYD OZPCP UOZNO NCIXC QKNVY DFOOH EN

The plaintext message begins “Australian coastwatchers.”

8. Cryptanalyze an aristocrat:

ZIWKDYEHL OESYWC YELZKYGMYFE YL: “Y SF EFM
ZFOEM MIU SWTL FN ZCFOSL WES LIFQUKL; Y FECT
ZFOEM MIU LIYEFEL IFOKL!”

9. Known plaintext attack on the Hill cipher. Find the key for the following ciphertext message that was enciphered with a Hill cipher.

VRAAU OTNLK NJWVJ QJXXY BEOLW CVRYK FOYPQ
TWVMP ALUEA ACWWE GB

The plaintext message begins “The Riddle.”

10. Decrypt a Hill cipher. The following message was encrypted with a Hill cipher with key $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$. Decrypt the message.

ZKYZR QHBDM JMPVX WLCGF MIXGM PKBUZ
FHPCI XZTIW

11. Decrypt a Playfair cipher. The following was encrypted with a Playfair Cipher with keyword *Galois*. Decrypt the message.

AQOUN GCIEY EOKVN GBIME HOTUE UNBCL OKIH

12. Encryption using a new cipher. Here is a four-square cipher. Keywords are used to fill the square in the upper right corner and the lower left corner; traditionally alphabetical order is used for the other two squares. Locate the first letter of each digraph in the upper left square, and locate the second letter of each digraph in the lower right square.

a	b	c	d	e	S	E	A	G	R
f	g	h	i/j	k	V	B	C	D	F
l	m	n	o	p	H	I/J	K	L	M
q	r	s	t	u	N	O	P	Q	T
v	w	x	y	z	U	W	X	Y	Z

P	L	A	Y	F	a	b	c	d	e
I/J	R	B	C	D	f	g	h	i/j	k
E	G	H	K	M	l	m	n	o	p
N	O	Q	S	T	q	r	s	t	u
U	V	W	X	Z	v	w	x	y	z

Use this four-square cipher to encrypt the message:

Trigraphic encipherment is also possible.

The four-square cipher was invented by the French cryptologist Félix Marie Delastelle (1840 – 1902). It occurs in his book *Traité Élémentaire de Cryptographie*, which he completed in 1901.

13. Determine an affine key. An affine cipher was used to encrypt a message. You know that MNB is the encrypted nku. Determine the affine key.

14. Decrypt a keyword cipher. The following message has been enciphered with a keyword cipher with keyword CRYPTOLOGICAL and keyletter e. Decrypt it.

ZTRRT	CPCGG	IVAVA	ZICFG	CPVMC	WCXBI	CRVIB
KHVHX	FSDJB	YFVDP	CFH			