Math 135 Prelim #2 – July 24, 2006

This exam has 6 problems and 7 numbered pages.

Name: _____ Instructor: Michael Kozdron

*You have **75** minutes to complete this exam. Show all work neatly and in order, and clearly indicate your final answers. Answers must be justified whenever possible in order to earn full credit.*

Unless otherwise specified, no credit will be given for unsupported answers, even if your final answer is correct. *Points will be deducted for incoherent, incorrect, and/or irrelevant statements. A formula page will be provided, and calculators are permitted, but no other aids are allowed.*

You are allowed to use standard notation. However, any new notation or abbreviations that you introduce must be clearly defined.

*This examination consists of **6** problems and is worth **100** total points. You must answer all of the questions in the space provided.*

Good luck!

Problem	Score
1	
2	
3	
4	
5	
6	

TOTAL: _____

Formula Page

The numerical equivalents of the letters are as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\det(A) = ad - bc$$

$$A^{-1} = \det(A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$I = \frac{n_0(n_0 - 1) + \cdots + n_{25}(n_{25} - 1)}{n(n-1)}$$

$$k = \frac{0.0265n}{(0.065 - I) + n(I - 0.0385)}$$

$$\#\text{ digits in binary representation of } x = \left\lfloor \frac{\ln x}{\ln 2} \right\rfloor + 1$$

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

1. (*16 points*) Suppose that $A = \begin{bmatrix} -2 & 1 \\ -3 & 2 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 2 \\ 3 & 3 \end{bmatrix}$.

(a) Compute $AB \mod 26$.

(b) Let $C = AB \mod 26$ be the matrix that you computed in **(a)**. Determine $C^{-1} \mod 26$.

(continued)

2. (*16 points*)

(a) Convert the number with base twenty-six representation `ELVES` to decimal (base ten).

(b) Convert the number with binary (base two) representation 11011001 to decimal.

(c) Convert the number with decimal representation 123 to octal (base eight).

(d) Let $a = 110110$ and $b = 10101$ be two binary numbers. Compute the binary numbers $a + b$ and $a - b$.

(continued)

3. (*16 points*)

(a) Encipher the message `GANDALF THE GREY` using the Vigenère method with the keyword `BILBO`.

(b) Suppose that the Vigenère encipherment produced the ciphertext `PKSFIH QDNB` when the three-letter key string `XV_` was used. (The last letter of the key string is not yet known.) Decipher as much of the plaintext as possible, and based on the plaintext you obtain, determine the missing plaintext letters and the third letter of the key string.

(continued)

4. (*16 points*)

(a) The ciphertext `ELPF` resulted from a Hill encipherment with the key matrix $A = \begin{bmatrix} 4 & 3 \\ 3 & 1 \end{bmatrix}$. Decipher the message.

(b) The ciphertext `BAOI` resulted from a Hill encipherment of the plaintext `BASE`. Based on this information, determine the key matrix A.

(continued)

5. (*20 points*) A message was enciphered using the Vigenère method with a keyword of a certain length. The ciphertext is shown below, and certain repeated letter groups are underlined.

YYFHS WZBJG KFFWV JVZYS SBWQU XLBGS WKVHG PPGHJ
JETRF YYSGK FITOC WUGLB YYSLF MRZOG TWGWC SVBLB
JWCUA TIHDZ RVBGC TDSGH TUWHC SVTRF YYSGO WBZRF
IFBKW XUOUY YYFRB JZBWV JCOQR TWARF IFFZV JISWV
JJVDR TNGOW JFBHF NEUWC WLZHH MVADZ QFBHF NEUWC
KZBGH MVARB JIWQU YFPUW SXHKS RRZOO SUWQH MVRDF
PESVG GZBGH MVALB YYSOO SUCIA TIRRF BYSUS YYSVV
FUCZG QZS

(a) From the spacing between the repeated letter groups, use Kasiski's test to estimate the length of the keyword.

(continued)

The distribution (i.e., letter counts) of the 288 characters in the ciphertext is as follows.

A	B	C	D	E	F	G	H	I	J	K	L	M
6	18	10	5	4	21	17	14	8	12	6	6	5
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	10	4	6	15	21	10	14	17	21	3	18	14

(b) Suppose that 4 letters from this ciphertext are picked at random. Write down (but do not evaluate) an expression to represent the probability that these 4 letters are identical.

(c) Suppose that 4 letters from this ciphertext are picked at random. Write down (but do not evaluate) an expression to represent the probability that either "a pair of A's and a pair of B's" is drawn or "three J's and one K" is drawn.

(continued)

6. (*16 points*) Consider the 5-bit linear feedback shift register given by

$$\begin{aligned} b_1' &\leftarrow b_2 \\ b_2' &\leftarrow b_3 \\ b_3' &\leftarrow b_4 \\ b_4' &\leftarrow b_5 \\ b_5' &\leftarrow b_3 + b_2 + b_1 \end{aligned}$$

with initial values $b_5 = 1$, $b_4 = 0$, $b_3 = 0$, $b_2 = 1$, $b_1 = 0$. Compute the first 8 values of b_1, and use them to do a binary Vigenère encipherment of the plaintext 11101101.

(The End.)