Test II
Math 105: Topics in Mathematics
Cryptology, the Science of Secret Writing
Rhodes College
20 March 2002

Instructions: Start each numbered problem on a new page. Show your work, explain when requested, and be as neat as possible. Don't spend too much time on any one problem. Turn in your test sheet along with your work, making sure that you have pledged your work.

1. (15 points)

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

   (b) Convert the number with binary representation 11110111 to base ten.

   (c) Convert the number with base ten representation 117 to binary.

2. (12 points) Write down a formula for a Boolean function that produces the following table of values.

$x_1x_2x_3$	$F(x_1x_2x_3)$
000	0
001	1
010	0
011	0
100	0
101	0
110	1
111	0

   Simplify the formula so that it is a sum of products of the x's.

3. (9 points) Decipher the message `FEKYUFBJ` which was enciphered using the Vigenère method using the keyword `MATH`.

4. (18 points) The ciphertext `JZDS` resulted from a Hill encipherment with the key matrix $A = \begin{bmatrix} 3 & 12 \\ 13 & 7 \end{bmatrix}$. Decipher the message.

5. (20 points)

   (a) Josie and Charles are planning a dinner party with eight guests. They will sit at opposite ends of a rectangular table, and their guests will sit four to a side, with assigned seating. In how many different ways can the guests be seated in this way?

   (b) Suppose that in a group of 28 students, 3 were born on a Sunday, 4 were born on a Monday, 2 were born on a Tuesday, 4 were born on a Wednesday, 5 were born on a Thursday, 7 were born on a Friday, and 3 were born on a Saturday. What is the probability that two students selected at random will have been born

      i. on a Friday?

      ii. on the same day of the week?

   (c) Suppose that in another group of 28 students, exactly 4 were born on any given day of the week. What is the probability that two selected at random were born on the same day? Should this probability be higher or lower than for the group in part (b)? Explain.

   (d) Eve is attempting to break into Alice's computer account by guessing Alice's password. If she knows that the password is exactly 5 characters, and each character can be an uppercase or lowercase letter or a digit from 0 to 9, what is the probability that Eve guesses Alice's password on the first try? Suppose that Eve has determined that the first character in the password is a digit in the range 0 to 9. With this information, what is the probability that Eve guesses the password on one try?

6. (9 points) A Vigenère ciphertext is shown here, and certain repeated letter groups are underlined. From the spacing between the recurrence of the respective groups, determine a likely length of the keyword used to do the encipherment.

```
ANNLO QPLQG DHZRJ BDWAV SLYIQ WYPZK WQVZO BTEUR WVSDL
IQWYP ZKWQV ZGAJV RYYLE ETUNQ MXWWA XYHZR XNRFT TIYLR
RHOVN GVWZZ ZRSQR QDWRX WGRWO GAGTC DLXBT PWSWJ EJLYJ
IOQTF QGPAU BNXHR MIRZU KJSNW SQUME LHXZX GEGOI KOKAN
XVPIC IEJKJ YDDNZ MHKVY DLKUA ZWWGH ZNGKF VTWRV ZZQJD
HHFBC KDUAJ QXWSZ LLTGW HRUZE WWFTK BLOQP LQGRU JCMOA
                  LFLCT OXXRY VZEMW
```

7. (17 points) A Viegnère ciphertext had the following counts of letters.

letter	A	B	C	D	E	F	G	H	I	J	K	L	M
count	10	6	5	10	9	6	13	10	8	11	11	16	6
letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
count	10	10	7	16	17	7	11	9	12	23	12	11	19

Use the Friedman index of coincidence to estimate the length of the keyword used for the encipherment.

Bonus: (5 points) An English plaintext has been enciphered in two different ways: with a 2×2 Hill cipher matrix A and with a 2-letter Vigenère keyword. The resulting ciphertexts have been separated into two cosets consisting respectively of the first, third, fifth, ... and the second, fourth, sixth, ... letters, and the two ciphertexts' coset letter counts are shown in the following table.

cipher- text	letter	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	coset 1	0	2	9	9	0	0	3	7	12	21	4	0	5	4	12	5	0	1	0	1	0	10	4	5	4	24
	coset 2	0	9	1	8	5	14	2	8	6	7	0	1	6	7	12	9	0	1	9	17	9	5	0	1	1	4
2	coset 1	3	3	5	5	8	3	10	4	4	6	6	7	8	0	7	2	1	7	2	4	6	3	16	7	13	2
	coset 2	5	3	7	8	1	1	7	6	2	5	8	1	1	16	5	16	9	6	1	0	4	4	14	3	0	9

Identify which ciphertext is from the Hill cipher and which is from the Vigenère. *Explain.*

x	1	3	5	7	9	11	15	17	19	21	23	25
$x^{-1} \pmod{26}$	1	9	21	15	3	19	7	23	11	5	17	25

	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