Test I
Math 105: Topics in Mathematics
Cryptology, the Science of Secret Writing
Rhodes College
13 February 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. (28 points) Short answer.

   (a) Find the least nonnegative solution of the congruence $x \equiv -87 \pmod{5}$.

   (b) Evaluate $421 \mod 34$

   (c) Solve the congruence $137x \equiv 1 \pmod{138}$.

   (d) Let f be the function given by the table

x	1	2	3	4	5	6
$f(x)$	4	6	3	1	2	5

   Find $f(4)$, $f(f(5))$, and $f^{-1}(6)$.

   (e) If $f(x)$ is the function that performs a 4-shift on the string x, find $f^{-1}(\texttt{LSAHC})$.

   (f) In a monoalphabetic ciphertext of 100 letters of English, the letter `Q` is the most common. What are the eight plaintext letters that most likley correspond to ciphertext `Q`? Explain.

   (g) Encipher `GOOD` using the Vigenère autokey method with priming key `J`.

2. (18 points)

   (a) Use the affine cipher given by $E(x) = (21x + 8) \mod 26$ to encipher the message `FAME`.

   (b) Find the decipherment formula.

   (c) Use the decipherment formula to decipher `RIFK`.

3. (18 points) Suppose that an affine cipher $E(x) = (ax + b) \mod 26$ was used to encipher a plaintext. If Eve knows that plaintext `I` enciphers as `F` and plaintext `U` enciphers as `L`, she can determine the coefficients a and b in the encipherment formula. Find these values for her.

4. (18 points) Suppose that a Vigenère encipherment produced the ciphertext `PKSFIH QDNB` when the three-letter key string `XV_` was used (the last letter is not known yet).

   (a) Decipher as much of the plaintext as possible.

   (b) Based on the plaintext you obtain, determine the missing plaintext letters and the third letter of the key string.

5. (18 points) Shown here is the ciphertext resulting from a keyword columnar transposition.

```
VIKTF CNEMA ONAOE SEIOT NRTMO RI
```

   (a) If the word `MISTAKE` was part of the original plaintext and the keyword had fewer letters than this, determine the length of the keyword.

   (b) List the columns in the original message.

   (c) Decipher.

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