Final Exam
Math 105: Topics in Mathematics
Cryptology, the Science of Secret Writing
Rhodes College
Tuesday, 30 April 2002
8:30 – 11:00 a.m.

Instructions: Please be as neat as possible (use a pencil), and show your work. A correct answer with no work shown may not receive full credit. Start each numbered question on a new page. Unless otherwise indicated, use your calculator only to do basic arithmetic and function evaluation. Turn in your test sheets along with those containing your work.

---

1. (15 points) For each of the following indicate whether the statement is true or false.

   (a) If the greatest common divisor of integers a and b is 1, then either a or b is prime.

   (b) A scytale is a device that implements a type of polyalphabetic substitution.

   (c) A principle of cryptography is that the security of a ciphersystem resides in the key information.

   (d) In a substitution cipher, the letters in the plaintext message are rearranged.

   (e) If Alice and Bob have exchanged a great deal of Vigenère key data and they use this method, alway using a key as long as the plaintext and never re-using a key, then Eve, attempting a ciphertext-only attack and knowing that the underlying plaintext is English, will do no better than guessing at the plaintext.

   (f) If an English plaintext is enciphered using the Vigenère method with a long random keyword, then the index of coincidence of the resulting ciphertext will be close to 1/26.

   (g) A 6-bit linear shift register generates a sequence of 0's and 1's that never repeats .

   (h) In any sample of ordinary English text, the letter `E` will be the most frequent.

(i) If an efficient method for factoring very large numbers is found, then RSA would no longer be a secure means of encryption.

(j) The number with base twenty-six representation `EXAM` is 85865.

(k) A principle of cryptography is that the security of a cipher system rests on keeping the method of encipherment secret.

(l) $3^{3079} \equiv 20 \pmod{3079}$.

(m) RSA has been proven unbreakable.

(n) Public key cryptosystems tend to run on computers more slowly than secret-key systems.

2. (8 points) Decipher `NOCJUT`, which was enciphered with the affine encipherment function $E(x) = (21x + 1) \bmod 26$.

3. (8 points) Decipher `FCUWPZ`, which was enciphered using the Hill cipher matrix $A = \begin{bmatrix} 11 & 18 \\ 12 & 17 \end{bmatrix}$.

4. (8 points) Decipher `TETST WTUEA HTEOU RTRRA OBTON U`, which was enciphered with a keyword columnar transposition using the keyword `URGENT`.

5. (8 points) Decipher `FOYNIIOYSJRJ` which was enciphered using the Vigenère method with keyword `NUMBER`.

6. (8 points) Decipher 00101101, which was enciphered using the binary Vigenère method with the key stream generated by the LFSR $b_5 \leftarrow b_3 + b_1 \bmod 2$ with initial bit values $b_5b_4b_3b_2b_1 = 10001$.

7. (9 points)

   (a) Find the greatest common divisor of 4961 and 4235.

   (b) The number 1074967 is a product of two distinct primes. At most how many trial divisions by primes will be required to find these primes (see the prime table)?

   (c) Use the corollary to Fermat's little theorem to help to compute $3^{147} \bmod 95$.

8. (10 points) Suppose that Alicia is implementing RSA with primes $p = 53$, $q = 31$, and public exponent $e = 17$.

(a) Explain what she does to set up for receiving encrypted messages and calculate all of the numbers that she will use with these choices of p, q, and e.

(b) If Roberto wants to send Alicia the message $x = 24$ encrypted using her public key, determine the ciphertext he produces.

(c) Suppose Alicia receives the encrypted message $y = 775$. Write down the expression she will need to evaluate in order to decrypt. (Do not actually evaluate this expression.)

9. (9 points) Explain briefly but completely what is involved in a cryptanalysis of the Vigenere cipher. Mention the various techniques we have used.

10. (9 points) Shown here are letter distributions for three different ciphertexts, one from a monoalphabetic substitution, one from a polyalphabetic substitution, and one from a transposition.

(i)	*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*
	7	6	9	3	5	6	8	3	4	7	13	10	7	0	1	5	3	6	8	5	4	8	4	8	5	5
(ii)	*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*
	22	4	12	14	41	10	7	16	29	1	1	6	14	25	21	7	1	15	18	32	0	4	5	0	5	0
(iii)	*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*
	3	0	3	6	17	1	0	1	5	1	8	6	2	7	0	4	1	5	0	1	4	1	13	1	0	9

(a) Indicate which distribution corresponds to which cipher. Explain.

(b) For the polyalphabetic one, compute the index of coincidence.

(c) Assuming encipherment by the Vigenère method with a keyword, use the Friedman test to estimate the keyword length.

11. (9 points) Alice and Bob are going to use the Diffie-Hellman key agreement protocol. If the public prime modulus is $p = 53$ and the public base is $s = 5$, Alice generates the number $a = 10$, and Bob generates $b = 13$. Determine the key on which they agree.

---

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

Primes

2	179	419	661	947	1229	1523	1823	2131	2437	2749
3	181	421	673	953	1231	1531	1831	2137	2441	2753
5	191	431	677	967	1237	1543	1847	2141	2447	2767
7	193	433	683	971	1249	1549	1861	2143	2459	2777
11	197	439	691	977	1259	1553	1867	2153	2467	2789
13	199	443	701	983	1277	1559	1871	2161	2473	2791
17	211	449	709	991	1279	1567	1873	2179	2477	2797
19	223	457	719	997	1283	1571	1877	2203	2503	2801
23	227	461	727	1009	1289	1579	1879	2207	2521	2803
29	229	463	733	1013	1291	1583	1889	2213	2531	2819
31	233	467	739	1019	1297	1597	1901	2221	2539	2833
37	239	479	743	1021	1301	1601	1907	2237	2543	2837
41	241	487	751	1031	1303	1607	1913	2239	2549	2843
43	251	491	757	1033	1307	1609	1931	2243	2551	2851
47	257	499	761	1039	1319	1613	1933	2251	2557	2857
53	263	503	769	1049	1321	1619	1949	2267	2579	2861
59	269	509	773	1051	1327	1621	1951	2269	2591	2879
61	271	521	787	1061	1361	1627	1973	2273	2593	2887
67	277	523	797	1063	1367	1637	1979	2281	2609	2897
71	281	541	809	1069	1373	1657	1987	2287	2617	2903
73	283	547	811	1087	1381	1663	1993	2293	2621	2909
79	293	557	821	1091	1399	1667	1997	2297	2633	2917
83	307	563	823	1093	1409	1669	1999	2309	2647	2927
89	311	569	827	1097	1423	1693	2003	2311	2657	2939
97	313	571	829	1103	1427	1697	2011	2333	2659	2953
101	317	577	839	1109	1429	1699	2017	2339	2663	2957
103	331	587	853	1117	1433	1709	2027	2341	2671	2963
107	337	593	857	1123	1439	1721	2029	2347	2677	2969
109	347	599	859	1129	1447	1723	2039	2351	2683	2971
113	349	601	863	1151	1451	1733	2053	2357	2687	2999
127	353	607	877	1153	1453	1741	2063	2371	2689	3001
131	359	613	881	1163	1459	1747	2069	2377	2693	3011
137	367	617	883	1171	1471	1753	2081	2381	2699	3019
139	373	619	887	1181	1481	1759	2083	2383	2707	3023
149	379	631	907	1187	1483	1777	2087	2389	2711	3037