Mathematics 348   Introduction to Cryptography   Spring 2012

REVIEW FINAL EXAMINATION

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*
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
6.6	1.1	1.9	3.6	10	1.7	1.6	5.4	5.6	.08	.66	3.2	2.0	5.5	6.1	1.3	.08	4.5	5.0	7.3	2.2	.88	1.9	0.14	1.6	.05

e t a o i n s r h l d c u m f p g w y b v k x j q z

The letters of the alphabet are replaced by the integers written below them when we wish to represent strings of letters as strings of integers modulo 26. The frequency of the letter in English (as a percentage) is on the third row. The letters ordered by frequency in English text are on the last row.

No books or cellphones
Calculators may NOT be used
Show all of your work and provide explanations

Problem	Score
1	
2	
3	
4	
5	
6	
7	
8	
9	
TOTAL	

NAME ____

1. (24 points)

   a) Encrypt the phrase “cryptography is fun” (translated to numerical equivalents modulo 26 the phrase is “2,17,24,15,19,14,6,17,0,15,7,24,8,18,5,20,13 “) using the Vigenère cipher of period 7 with the key “rutgers”.

   b) Explain how a Vigenère cipher encrypted with a short keyword can be broken.

   c) What happens if the keyword in a Vigenère cipher is as long as the message?

2. (25 points)

The RSA cipher is used with modulus 77 and public key 7. The cipher is used to encrypt the age in years of my cat. The encrypted age of the cat is 57. How old is the cat? You may use that $57^{16} \equiv 2^6 \pmod{77}$ if it is helpful in your calculations.

3. (24 points) Let $p = 2^{16} + 1 = 65537$. This is a prime number (you do not need to prove this).

a) Show that $2^{16} \equiv -1 \pmod{p}$ and determine the smallest positive power of 2 which is congruent to 1 modulo p.

a) Show that 3 a primitive root modulo p. You may use that $3^{(2^{11})} \equiv -8 \pmod{p}$.

c) Let the discrete logarithm $\log_3(2 \pmod{p})$ be noted by l. Show that l is a multiple of 2^{11} (Hint: Raise both sides of the equation defining l to the 32nd power).

4. (21 points)

a) Let p and q be odd primes. State the quadratic reciprocity law for p, q.

b) Use quadratic reciprocity to show that 3 is a square modulo 167

c) Compute all square roots of 3 modulo 167.

5. (21 points) Let N=8911. Here are some true equations modulo N:

$$p^{8910} \equiv 1 \pmod{N} \text{for all primes } p < N \text{ prime to } N,$$

$$2^{4455} \equiv 6364 \pmod{N}, \quad 3^{4455} \equiv -1 \pmod{N}, \quad 5^{4455} \equiv 2813 \pmod{N}.$$

a) Show that N is a Fermat pseudoprime for any base b prime to N).

b) Define what it means for a number M to be an Euler pseudoprime for the base b.

c) Is $N = 8911$ an Euler pseudoprime for base 3? Is N composite or prime? Prove that your answer is correct.

6. (20 points) Find the least positive integer solution x to the simultaneous system of congruences

$$\begin{aligned} 2x &\equiv 8 \pmod{13} \\ x &\equiv 5 \pmod{11} \end{aligned}$$

7. (25 points) Decrypt the following affine substitution cipher by finding the key. (You only need to decrypt the first three words and provide the key to the cipher. Don't bother to decrypt the whole message.):

JZQOU DQGKZ UULYU MKUOX LQJQJ ZQZCW ZQDYU MDXUJ QRJCE
LQEDR CRWGL UUIEJ JZQEP QDEWQ QEDRC RWGCR JZCGK ZEDJJ
ZQYJQ LLJZQ GJUDY

Note: numerical equivalents for the first line of ciphertext are
9,25,16,14,20 3,16,6,10,25 20,20,11,24,20 12,10,20,14,23 11,16,9,16,9
25,16,25,2,22 25,16,3,24,20 12,3,23,20,9

given that the number of each character in the ciphertext is the number following the letter in the table below:

C 6 D 8 E 7 G 5 I 1 J 13 K 3 L 6 M 2 O 2 P 1 Q 15 R 6 U 10 W 4 X 2 Y 4 Z 10

8. (20 points)

a) How many integers in the interval [1,774] are relatively prime to 775?

b) Evaluate $7^{1462} \pmod{22}$, expressing the answer as an integer in the range from 0 to 21.

9. (20 points)

a) Explain how Adam and Betty can securely exchange a secret key by Diffie-Hellman key exchange.

b) Adam and Betty wish to agree on a secret key by Diffie-Hellman key exchange. They agree to use the primitive root 3 modulo 17 for their key exchange. We eavesdrop on their communications and observe Adam transmitting $10 \pmod{17}$ to Betty and Betty transmitting $5 \pmod{17}$ Adam. What will be the key that they have agreed to use?