CIS 3362 Final Exam
12/4/2013

Name: _____

1) (10 pts) Since the use of letter frequencies was known to aid in breaking substitution ciphers, code makers in the Renaissance added "twists" to the standard substitution cipher to make it more difficult to break. Describe four of these twists and why the code makers expected these twists to thwart attacks that made use of letter frequency information.

2) (10 pts) Show each calculation in the Miller-Rabin primality test if we test n = 49 for primality using the random integer a = 3. In particular, the algorithm calculates various values of the form $a^x \bmod n$. Show which values of x the algorithm tries, what answer it gives for these values of x, and how the algorithm proceeds at each step.

3) (10 pts) Consider a language with four letters: A, B, C, and D that has the following letter frequencies: 45% A, 5% B, 15% C, and 35% D. You are decrypting a ciphertext that was encrypted using the Vigenere cipher and have determined the keyword length to be 6. Given the ciphertext below, set up four mutual index of coincidence tests to determine the most likely choice for the first letter of the keyword used to create the following ciphertext:

```
c b d b b b a b a b a b c d d d a b d a d c b d c a c c a b
d a d c a a d a a a d b b b c d b a a b d b a a b b d c b c
b a d c a c d b d c a c d b a b a c c a a b a a d a a a a b
d b b b d c b b d c d b d b c c a c c b d c b b c b d c b c
d a d a b b c c a b d c c b d a b c d b c b a c d a a c b c
b b d c a b d b a d b c c d b c d c d b d a b c c d b a a b
c d c b b b d b d c d b d a a c b c d a a b c c c a a b a b
c a d b d a c a a a b c d d a b a b d d d b a a b a a c b c
```

Note: For convenience, the ciphertext has been arranged with 30 characters per row.
Hint: In all of your MIC tests, one set of frequencies will stay the same, and that set will be the letter frequencies provided for you above for the language given.

Note: In order to get full credit for this question, you have to both set up the correct MIC tests and obtain the correct results for all four.

4) (10 pts) If the 48 bit input to the S-boxes in DES is 3A29B1234FE6, what is the 32 bit output, expressed in hexadecimal? Put a box around your final answer.

5) (10 pts) Consider an AES plaintext of all 1's with the key (in HEX) of 13579bdf02468ace13579bdf02468ace. Show the state matrix after the shift rows step in round 1. (Note: Remember that in AES, we read through the state matrix in order of columns, not rows.)

6) (10 pts) Consider an RSA system with p = 17 and q = 29. If e = 125, what is d?

7) (10 pts) Consider an El Gamal system with q = 31 and $\alpha = 3$. Let Alice choose $X_A = 17$. Let Bob, who is sending M = 12 to Alice choose the random integer k = 3. Calculate the following values: Y_A, Alice's public key, as well as K, C_1 and C_2, all of which Bob calculates. To aid in calculation, a few powers of 3 mod 31 are provided below:

3^4 mod 31	3^8 mod 31	3^{12} mod 31	3^{16} mod 31	3^{20} mod 31	3^{24} mod 31	3^{28} mod 31
19	20	8	28	5	2	7

8) (10 pts) Consider the elliptic curve $E_{37}(4, 5)$. This curve contains points P = (10, 3) and Q = (14, 17). Determine P + Q.

9) (10 pts) Keys 'R Us randomly generates keys for their suitcases by setting each of 10 ordered notches to one of four particular settings. In order for a key to match, each of the 10 notches must be at the appropriate setting. If 100 passengers are picking up suitcases with keys designed by Keys 'R Us, one suitcase per passenger, what is the probability that at least one pair of passengers can open each other's suitcases? Express your answer using the appropriate mathematical notation.

10) (9 pts) Consider a Group Diffie-Hellman set-up with four users, M_1, M_2, M_3 and M_4 with the public keys p = 29 and g = 8. Let M_1 and M_2 share group key K_1. Let users M_3 and M_4 share group key K_2 and let all four share group key K_0. Let the secret keys for these four users be a_1 = 6, a_2 = 16, a_3 = 8, a_4 = 22. Determine K_0, K_1 and K_2.

11) (1 pt) In a game of battleship, what objects does one place on a 10 x 10 grid, with the goal of hiding them from their opponent?

_____

Scratch Page - Please clearly mark any work on this page you would like graded.