**CIS 3362 Final Exam**

**Date: 12/7/2011**

**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Note: For questions with numeric answers, put a box around your final answer.**

**For each step plugged into a calculator, please write (CALC) in parentheses by the step.**

1) (5 pts) What is the prime factorization of 28140000?

2) (10 pts) The following chart shows how many of each dollar bill Alice and Bob have:

|  |  |  |
| --- | --- | --- |
| Dollar Bill | Alice (quantity) | Bob (quantity) |
| 1 | 5 | 40 |
| 5 | 15 | 30 |
| 10 | 35 | 40 |
| 20 | 50 | 10 |
| 100 | 55 | 50 |

If we randomly select a dollar bill from Alice and one from Bob, what is the probability that the value of both bills will be the same? Express your answer as a fraction in lowest terms or a decimal rounded to the nearest thousandth.

3) (10 pts) In an RSA system, p = 29, q = 37 and e = 715. What is d?

4) (10 pts) Alice and Bob are trying to arrive at a secret key using quantum cryptography using the scheme discussed in class. As a test run, Alice has sent Bob 100 bits. Of these, Bob used the correct reader for 47 of them. Of those 47, Alice and Bob decide to compare answers on 15 of the bits, leaving 32 to use for their key if no eavesdropping was detected. What is the probability that Eve was listening but goes undetected in their test of 15 bits? (Please use the probabilities discussed in class. Namely, Eve guesses the correct reader half the time, and half the time she uses the incorrect reader, the data remain unchanged.)

7) (10 pts) Each year Topps makes a set of 792 baseball cards. Many copies of each card exist. Roger has bought four packs of 15 cards each. Assuming that each pack has a completely random selection of cards (meaning that a single pack could have two of the same card), what is the probability that Roger has at least two copies of some card. Please give an expression for the answer, but do not calculate it. Your expression should have exponents and either factorials or permutations in it.

5) (10 pts) Consider the elliptic curve E37(3, 7), as defined in the class textbook. Let P = (2, 13). P is on the given elliptic curve. Calculate 2P.

6) (12 pts) Consider an ElGamal system with the global public elements q = 19, α = 10. Let Alice select the private key XA = 12. What is the public key YA? Now, let Bob send a message, M = 7 to Alice by selecting a random integer k = 4. What are the two values, C1 and C2 that Bob sends to Alice?

8) (10 pts) Encrypt the plaintext "POOL" using the Hill cipher and the encryption matrix $\left(\begin{matrix}5&17\\6&13\end{matrix}\right)$.

9) (8 pts) Let the input to the 8 S-boxes in DES be 48 1s (in HEX it would be 0xffffffffffff). What is the output in HEX?

10) (10 pts) Let the state matrix for AES right before a round starts be $\left[\begin{matrix}\begin{matrix}3E&F8\\95&44\end{matrix}&\begin{matrix}CA&0D\\26&75\end{matrix}\\\begin{matrix}B1&8E\\66&8A\end{matrix}&\begin{matrix}34&9B\\C7&FF\end{matrix}\end{matrix}\right]$. What does the state matrix look like during that round right after the ShiftRows step? (This is right before the MixColumns step.)

11) (5 pts) In which state did the first California Pizza Kitchen appear? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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