**CIS 3362 Final Exam**

**Date: 12/5/2012**

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

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

1) (12 pts) Recall that the φ(n) is defined as the number of values in the set {1, 2, ..., n} relatively prime to n. Define a function β such that β(n) equals the number of values in the set {1, 2, ..., n} that are NOT relatively prime to n. Determine β(paqb), where p and q are distinct prime numbers and a and b are positive integers. Leave your answer in terms of p, q, a and b, in factorized form.

2) (6 pts) Determine the mutual index of coincidence between the two following sets of letters:

Set 1: 18 As, 16 Bs, 13 Cs, 3 Ds, 80 Es

Set 2: 6 As, 7 Bs, 27 Cs, 15 Ds, 25 Es

3) (9 pts) Encrypt the plaintext "CIPHER" using the Hill cipher with the encryption key $\left(\begin{matrix}3&1\\7&8\end{matrix}\right)$.

4) (10 pts) In an RSA system with p = 17, q = 29, and e = 25, what is d?

5) (9 pts) Decrypt the cipher text "SERRRSPYDOELTECNQGRTFEJGDLB" that was created with the Vigenere cipher with the encryption key "MAYANS"

6) (12 pts) Let the 32 bit input to the Expansion matrix E in DES be 4F69C57B, in hex. What is the 48 bit output? Express your answer in hex.

7) (12 pts) Assume that the state matrix right BEFORE the Mix Columns step in AES is $\left[\begin{matrix}\begin{matrix}19&A5\\2B&69\end{matrix}&\begin{matrix}87&C3\\41&95\end{matrix}\\\begin{matrix}88&F3\\59&30\end{matrix}&\begin{matrix}EE&D7\\C3&E0\end{matrix}\end{matrix}\right]$. What is the entry in row 0, column 3 (top right) of the state matrix right AFTER the Mix Columns step? (Note: The fixed matrix used in encryption in the Mix Column step in AES is $\left[\begin{matrix}\begin{matrix}02&03\\01&02\end{matrix}&\begin{matrix}01&01\\03&01\end{matrix}\\\begin{matrix}01&01\\03&01\end{matrix}&\begin{matrix}02&03\\01&02\end{matrix}\end{matrix}\right]$.)

8) (12 pts) Consider the Elliptic Curve E31(2, 6) and the point P = (13, 20) on this curve. First, show that P is on the curve. Then, determine 2P.

9) (7 pts) A hash function has a 24 bit output. Steve has randomly generated 1024 distinct passwords. Assuming that the hash function is an ideal one, what is the probability that at least 2 of the passwords he has generated produce the same hash value? Please use the product symbol (Π) to succinctly represent your answer.

10) (10 pts) Use the Fermat Factoring method to factor 143369. Create a chart showing each value of x that you try. Once you determine a valid x and y, then clearly state the factorization.

11) (1 pt) What common breakfast food does Dunkin Donuts sell? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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