**CIS 3362 Final Exam**

**Date: 12/10/2010**

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

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

1) (10 pts) Consider an affine cipher for an alphabet of size 49. Let the encryption function be f(x) = (32x + 21) mod 49. Determine the corresponding decryption function.

2) (10 pts) Encrypt the plaintext “ITISWAYTOOCOLDOUTSIDE” using the Vigenere cipher with the key “FROSTY”.

3) (10 pts) In DES, the 48 bit input into all the s-boxes is 3D8B947F70C5. What is the 32 bit output right after the s-boxes are applied to this input? Express your final answer in 8 HEX characters.

4) (10 pts) You know that the plaintext “ONDECEMBERTHIRTY” matches to the ciphertext “AIEGDGESDSFKKQBX” and that the cipher being used is the Playfair cipher. Try to complete as much of the playfair encryption matrix as possible based on this information. Also, attempt to determine the keyword.

5) (10 pts) Prove that the polynomial x4 + x3 + 1 over the field GF(2) is irreducible.

6) (10 pts) In AES, if the input to the Mix Columns stage is the following state matrix: $\left[\begin{matrix}\begin{matrix}3F&2D\\B2&FF\end{matrix}&\begin{matrix}55&18\\92&22\end{matrix}\\\begin{matrix}78&93\\95&75\end{matrix}&\begin{matrix}B4&31\\C3&45\end{matrix}\end{matrix}\right]$, what is the output in row 2, column 3 of the state matrix, right after the Mix Columns stage is done?

7) (10 pts) Determine the following quantities:

(a) φ(35) (b) φ(1331) (c) φ(559872) (d) φ(105537) (e) φ(4165000)

Hint for (d): 105537 has a prime factor in between 100 and 150.

8) (10 pts) In an RSA system, if n = 851 and e = 25, what is the value of d? (Note: Your answer must be positive and less than φ(n).)

9) (10 pts) A year on an arbitrary planet lasts n days. Imagine that you have a gathering of k people from that planet, where k > 1 and k < n. Write a C function that returns the probability that at least one pair of people from the group of k share the same birthday. (Assume that each possible birthday is equally likely.)

10) (10 pts) Consider the Knapsack Cipher with the private set, {15, 92, 108, 279, 563, 1172, 2243, 4468}. Let w = 2393 and u = 9291 for this set. Calculate the corresponding public set of values and give the ciphertext for the plaintext x = 10110001. (Note: We assume that the left-most bit corresponds to the first item listed in the set, etc.)

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