**CIS 3362 Test #1: Classical Cryptographic Schemes**

**Date: 9/19/2011**

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

1) (10 pts) Encrypt “KNIGHTS” using the affine cipher with the encryption function f(x) = (17x + 13) mod 26.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2) (15 pts) Consider an affine cipher for a language with 50 letters. If an encryption function for this alphabet is g(x) = (37x + 20) mod 50, what is the corresponding decryption function?

3) (20 pts) Consider an alphabet with the letters a1, a2, a3, …, an. Let the set A comprised of these letters contain exactly k copies of the letter ak, for all k, 1 ≤ k ≤ n. What is the index of coincidence of the set A? (Hint: $\sum\_{i=1}^{n}i=\frac{n(n+1)}{2}$, $\sum\_{i=1}^{n}\left(i\left(i-1\right)\right)=\frac{\left(n+1\right)n(n-1)}{3}$.) Express your answer as a fraction in terms of n. For full credit, simplify your fraction completely.

4) (10 pts) Explain how keys were used in the Enigma system. (Credit will be awarded based on the accuracy of the details given.)

5) (8 pts) Which of the following are valid keys for the Hill cipher?

 $\left[\begin{matrix}15&3\\7&8\end{matrix}\right]$, $\left[\begin{matrix}6&2\\19&17\end{matrix}\right]$, $\left[\begin{matrix}9&11\\3&8\end{matrix}\right]$, $\left[\begin{matrix}5&10\\2&15\end{matrix}\right]$

6) (10 pts) A cipher text created by the Vigenere cipher is “QJTPMTUUBG”. If the keyword was “CUP” what is the corresponding plaintext?

7) (12 pts) Encrypt the phrase “TENNESSEE” using the Playfair cipher using the padding character “Q” and the keyword, “RANDOMIZE.”

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8) (12 pts) The cipher text “OCEMOTRTMEHAWKNTEO” was encrypted using the permutation cipher. What is the plaintext?

9) (3 pts) In the game of football, what is the chief task of a running back? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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