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

**Date: 9/17/2012**

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

1) (12 pts) Encrypt “FOOTBALL” using the affine cipher with the following encryption function: f(x) = (7x + 14) mod 26.

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

2) (10 pts) The set of letters S consists of 1 A, 3 Bs, 5 Cs, 7 Ds, and 9 Es. What is the index of coincidence of the set S?

3) (15 pts) Consider an affine cipher for a language with 48 letters. If an encryption function for this alphabet is g(x) = (17x + 20) mod 48, what is the corresponding decryption function?

4) (7 pts) How long would a message have to be in number of letters before it was guaranteed that the Enigma would encrypt two letters in that message with the exact same substitution?

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

5) (12 pts) What is the corresponding decryption key for the encryption key for the Hill cipher with an alphabet of size 26?

6) (12 pts) Encrypt the phrase, “FOXJUMPSOVERLAZYDOG” using the Vigenere Cipher with the key “SOCCER”.

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

7) (12 pts) Decrypt the following phrase that was encrypted with the Playfair cipher with the key, “PEZDISPENSER”: “CPAVBVVZBQFDARWZ”

8) (15 pts) Decrypt the following message:

“OSBETHNYTSEHAYTSMVNCOAPRTWSADEENHIDIEEEIMX”

The message was encrypted using transposition with the keyword, “KERMIT”.

9) (5 pts) Name one type of food sold at the restaurant chain, “Noodles and Company.”

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

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