CIS 3362 Test #1: Classical Cryptographic Schemes

Date: 9/13/2013

Name : ____

1) (10 pts) Use the shift cipher to encrypt the plaintext "CRYPTOGRAPHY" with a key of 9.

____

2) (10 pts) The set of letters S consists of 4 A, 19 Bs, 6 Cs, 8 Ds, and 13 Es. What is the index of coincidence of the set S? **Leave your answer as a fraction in lowest terms.**

____

3) (20 pts) Consider an affine cipher for a language with 54 letters. If an encryption function for this alphabet is $g(x) = (35x + 16) \bmod 54$, what is the corresponding decryption function? (Your function must be of the form $g^{-1}(x) = (ax + b) \bmod 54$, where a and b are in between 0 and 53, inclusive.)

4) (8 pts) Of the following, which are valid keys for the Hill cipher? (a) $\begin{pmatrix} 3 & 7 \\ 8 & 6 \end{pmatrix}$, (b) $\begin{pmatrix} 4 & 5 \\ 3 & 7 \end{pmatrix}$, (c) $\begin{pmatrix} 5 & 2 \\ 11 & 5 \end{pmatrix}$, and (d) $\begin{pmatrix} 15 & 8 \\ 14 & 19 \end{pmatrix}$

List the letters for the valid choices: ____ , ____ , ____ , ____ (all slots may not be used)

5) (12 pts) Prove that for the encryption key $\begin{pmatrix} 2 & 17 \\ 3 & 12 \end{pmatrix}$ for the Hill cipher, $\begin{pmatrix} 14 & 17 \\ 3 & 24 \end{pmatrix}$ is the corresponding decryption key.

6) (12 pts) You have intercepted a message encrypted with Vigenere and have managed to determine the corresponding plaintext. The ciphertext is “`kcszjwvfabdlzgzslsygym`” and the corresponding plaintext is “`sallywenttotheseashore`”. What is the key?

____

7) (12 pts) Decrypt the message, “`iyqsoacahfna`”, which was enciphered using the Playfair cipher with the key “RYANTANNENHILL”. Note: The padding character used was “Q”.

____

8) (15 pts) Encrypt the message “TOMORROWUCFPLAYSPENNSTATEINFOOTBALL” using the column permutation cipher with the keyword “RUNBACK”.

____

9) (1 pt) What type of meat is Outback Steakhouse’s specialty? ___________________________

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