Tanner Krebs, Gerardo Lopez, William Thornton
Math 314
9/14/17

COSC/MATH - 314

Assignment 2

Problem 1: Exercise 10, page 56 (to convert to numbers, use a=0, b=1). Suppose there is a language that has only the letters a and b. The frequency of the letter a is .1 and the frequency of 6 is .9. A message is encrypted using a Vigenere cipher (working mod 2 instead of mod 26). The ciphertext is BABABAAABA.

(a.) Show that the key length is probably 2.

(b.) Using the information on the frequencies of the letters, determine the key and decrypt the message.

Solution:

Problem 2: Exercise 13, page 56 (if you want to compute the inverse of the matrix, see section 3.8). The ciphertext YIFZM A was encrypted by a Hill cipher with the matrix

$$\begin{bmatrix} 9 & 13 \\ 2 & 3 \end{bmatrix}$$

Find the plaintext.

Solution:

Problem 3: Exercise 14, page 56 . (Note: The matrix M has 4 entries, so there are 4 unknowns, and to determine them you need 4 equations.) Since the given cipher-text/plaintext pair has 6 letters, you can form 6 equations. You need to choose 4 of them, so that the system that results can be solved.) The ciphertext text GEZXDS was encrypted by a Hill cipher with a 2 x 2 matrix. The plaintext is solved. Find the encryption matrix M .

Solution:

Problem 4: The following ciphertext has been obtained by Vigenere encryption.

ocwyikoooniwugpmxwktzdwgtssayjzwyemdlbnqaaavsuwdvbrflauplooubfgq
hgcscmgzlatoedcsdeidpbhtmuovpiekifpimfnoamvlpqfxejsmxmpgkccaykwfzp
yuavtelwhrhmwkbbvgtguvtefjlodfefkvpxsgrsorvgtajbsauhzrzalkwuowhgedef
nswmrciwcpaaavogpdnfpktdbalsisurlnpsjyeatcuceesohhdarkhwotikbroqrdfm
zghgucebvgwcdqxgpbgqwlpbdaylooqdmuhbdqgmyweuik

(a.) Use displacement of 5 and 6. Which displacement produces the largest number of coincidences?

(b.) Find the key.

(c.) Find the plaintext.

Solution: