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 b 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: We will start by displaying different levels of displacement in hopes of finding a high number of coincidences.
Displacement of 1: $BABABAAABA$
$BABABAAABA$
Number of coincidences: 2

Displacement of 2: $BABABAAABA$
$BABABAAABA$
Number of coincidences: 7
This is most likely going to be the key length: (Key = 2) due to the high number of frequencies.

Displacement of 3: $BABABAAABA$
$BABABAAABA$
Number of coincidences: 2

So, 7 coincidences will be the highest amount we find. Meaning, we will

further analyze every second letter in the cipher-text, starting at the first letter. With the highest percentage of B(.9) occurring most frequently (4 times) compared to A(.1) occurring **ONCE** we will assume that the first number in our key is 0. Next, analyze every second letter, starting at the second letter. A occurs 5 times and B zero times. We can conclude the second number in the key is 1. So the key is $\{0, 1\}$. The message decrypts to *BBBBBBABBB*.

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: To start, let us find the inverse $[A]^{-1}$ So we get:

$$[A]^{-1} = \begin{bmatrix} 9 & 13 \\ 2 & 3 \end{bmatrix}^{-1} = \frac{1}{9(3) - 13(2)} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \frac{1}{1} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix}$$

If we split the given ciphertext by 2 letters to get smaller matrices we get:

$$\begin{bmatrix} Y & I \end{bmatrix} \begin{bmatrix} F & Z \end{bmatrix} \begin{bmatrix} M & A \end{bmatrix}$$

which correlates to

$$\begin{bmatrix} 24 & 8 \end{bmatrix} \begin{bmatrix} 5 & 25 \end{bmatrix} \begin{bmatrix} 12 & 0 \end{bmatrix}$$

Now we can start getting the plaintext:

$$\begin{bmatrix} Y & I \end{bmatrix} \begin{bmatrix} M^{-1} \end{bmatrix} = \begin{bmatrix} 24 & 8 \end{bmatrix} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} 56 & -240 \end{bmatrix} mod(26) = \begin{bmatrix} 4 & 20 \end{bmatrix}$$

$$\begin{bmatrix} F & Z \end{bmatrix} \begin{bmatrix} M^{-1} \end{bmatrix} = \begin{bmatrix} 5 & 25 \end{bmatrix} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} -35 & 160 \end{bmatrix} mod(26) = \begin{bmatrix} 17 & 4 \end{bmatrix}$$

$$\begin{bmatrix} M & A \end{bmatrix} \begin{bmatrix} M^{-1} \end{bmatrix} = \begin{bmatrix} 12 & 0 \end{bmatrix} \begin{bmatrix} 3 & -13 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} 36 & -156 \end{bmatrix} mod(26) = \begin{bmatrix} 10 & 0 \end{bmatrix}$$

Lastly if we put the results together we get:

$$\begin{bmatrix}4 & 20 & 17 & 4 & 10 & 0\end{bmatrix}$$

which results in the plaintext EUREKA.

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: If we split the ciphertext we get

$$\begin{bmatrix}G & E\end{bmatrix}\begin{bmatrix}Z & X\end{bmatrix}\begin{bmatrix}D & S\end{bmatrix}$$

which translates to

$$\begin{bmatrix}6 & 4\end{bmatrix}\begin{bmatrix}25 & 23\end{bmatrix}\begin{bmatrix}3 & 18\end{bmatrix}$$

If we split the plaintext we get

$$\begin{bmatrix}S & O\end{bmatrix}\begin{bmatrix}L & V\end{bmatrix}\begin{bmatrix}E & D\end{bmatrix}$$

which translates to

$$\begin{bmatrix}18 & 14\end{bmatrix}\begin{bmatrix}11 & 21\end{bmatrix}\begin{bmatrix}4 & 3\end{bmatrix}$$

As a result, we can have 3 different matrices for [A]:

$$[A] = \begin{bmatrix}18 & 14\\ 11 & 21\end{bmatrix} or \begin{bmatrix}18 & 14\\ 4 & 3\end{bmatrix} or \begin{bmatrix}11 & 21\\ 4 & 3\end{bmatrix}$$

In order to figure out what matrix to use, we need to find the determinant

that will give us a result of 1 when we take the GCD between the det(A) and 26. In the first 2 matrices, the GCD between the determinant and 26 was 2 for both, which is incorrect. As a result we tested the last one and the GCD was indeed 1, so we found the correct matrix.

$$[A]^{-1} = \begin{bmatrix} 11 & 21 \\ 4 & 3 \end{bmatrix}^{-1} = \frac{1}{1}\begin{bmatrix} 3 & -21 \\ -4 & 11 \end{bmatrix} = \begin{bmatrix} 3 & -21 \\ -4 & 11 \end{bmatrix} mod(26) = \begin{bmatrix} 3 & 5 \\ 22 & 11 \end{bmatrix}$$

From here we use the general equation: $[A][M] = [B]$ and rearrange it so that we get $[M] = [A]^{-1}[B]$ It is important to note that $[B]$ is found based on the letters from the ciphertext corresponding to the plaintext we chose for $[A]$. Meaning that

$$[B] = \begin{bmatrix} 25 & 23 \\ 3 & 18 \end{bmatrix}$$

since

$$\begin{bmatrix} L & V & E & D \end{bmatrix} -> \begin{bmatrix} Z & X & D & S \end{bmatrix}$$

Now that we have all the missing pieces we can solve for [M]:

$$[M] = [A]^{-1}[B] = \begin{bmatrix} 3 & 5 \\ 22 & 11 \end{bmatrix}\begin{bmatrix} 25 & 23 \\ 3 & 18 \end{bmatrix} = \begin{bmatrix} 90 & 159 \\ 583 & 704 \end{bmatrix} mod(26) = \begin{bmatrix} 12 & 3 \\ 11 & 2 \end{bmatrix}$$

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

ocwyikooooniwugpmxwktzdwgtssayjzwyemdlbnqaaavsuwdvbrflauplooubfgq
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:

Using my program, I found that a displacement of 6 had a greater number of coincidences. so it was assumed to be the key length. To find the key I then used the key length to split the cipher-text into 6 sections and did a frequency attack on each one. The most frequent letters for each section were found to be u, b, d, q, i, and g for each respective section. Assuming each one to correspond to e in the plaintext, the key would be 10, 3, 1, 14, 22, 24. This gives the plaintext:

qxzmecqjrbeowbsatomocrsyvnvoubbrbsivnwqewscqvisvxwuthswkockmdaje
dyenfacrnvwcavengsevrwkhimqqswackaswixpjdardrlilabuhaalymxfoucyacdumc
qwshojmkascdwyupywqwsbbnjgtaxmqsloytnrfryvvmposwccfvsnfziko
jbhraxpnzanukrfdwscqrulvpasypvdvogekwmoblklthopuwxhsogjcgoncjrrhecdmr
envhhcudywxhpryyxgetyrwjesdrwgoudqjtrimjwgecearhiec