Linear Algebra: Applications of Linear Algebra in Image Processing & Cryptography

Due on September 22, 2019

Professor MacArthur

Nathan Gordon, Katerine Metcalf & Carson Storm

Math

Problem 1

You intercept the message "SONAFQCHMWPTVEVY", which you know was enciphered using a Hill 2-cipher. An earlier statistical analysis of a long string of intercepted cipher-text revealed that the most frequently occurring cipher-text digraphs were "KH" and "XW" in that order. You take a guess that those digraphs correspond to "TH" and "HE", respectively, since those are the most frequently occurring digraphs in most long plaintext messages on the subject you think is being discussed. Find the deciphering matrix and state what the message is supposed to be

Solution:

Using the assumption that "KH" decrypts to "TH" and "XW" decrypts to "HE", we can assume that the message "KHXW" should decrypt to "THHE" to find a decryption key by finding the modular multiplicative inverse of the encrypted message and multiply it with the decrypted message to find the decryption key.

$$\textit{let } K \text{ be the decryption key} \tag{1}$$

$$\textit{let } P \text{ be the encrypted message} = \begin{bmatrix} K & X \\ H & W \end{bmatrix} = \begin{bmatrix} 10 & 23 \\ 7 & 22 \end{bmatrix} \tag{2}$$

$$\textit{let } Q \text{ be the decrypted message} = \begin{bmatrix} T & H \\ H & E \end{bmatrix} = \begin{bmatrix} 19 & 7 \\ 7 & 4 \end{bmatrix} \tag{3}$$

To find the decryption key, K, we can use the equation $KP = Q \pmod{26}$, since we know that the product of the decryption key and the encrypted message show be equal to the decrypted message.

$$KP = Q \pmod{26} \tag{4}$$

$$KP \cdot P^{-1} = Q \cdot P^{-1} \pmod{26} \tag{5}$$

$$K = Q \cdot P^{-1} \pmod{26} \tag{6}$$

In order to find K, we must find the modular multiplicative inverse of P since we know that $P \cdot P^{-1} = I \pmod{26}$, we can use the inverse formula $P^{-1} = d^{-1} \cdot \text{adj}(P)$, where d^{-1} is the modular multiplicative inverse of the determinate of P.

$$P^{-1} = d^{-1} \cdot \text{adj}(P) \tag{7}$$

$$d \cdot d^{-1} = 1 \pmod{26} \tag{8}$$

$$59 \cdot d^{-1} = 1 \pmod{26} \tag{9}$$

$$d^{-1} = 15 \tag{10}$$

$$\text{adj}(P) = \begin{bmatrix} 22 & -23 \\ -7 & 10 \end{bmatrix} \tag{11}$$

$$P^{-1} = 15 \cdot \begin{bmatrix} 22 & -23 \\ -7 & 10 \end{bmatrix} \tag{12}$$

$$P^{-1} = \begin{bmatrix} 330 & -345 \\ -105 & 150 \end{bmatrix} \tag{13}$$

$$P^{-1} \pmod{26} = \begin{bmatrix} 18 & 19 \\ 25 & 20 \end{bmatrix} \tag{14}$$

Now, we can find the value of K, using the values of Q and P^{-1}

$$K = QP^{-1} \pmod{26} \tag{15}$$

$$K = \begin{bmatrix} 19 & 7 \\ 7 & 4 \end{bmatrix} \begin{bmatrix} 18 & 19 \\ 25 & 20 \end{bmatrix} \tag{16}$$

$$K = \begin{bmatrix} 517 & 501 \\ 266 & 213 \end{bmatrix} \tag{17}$$

Now that we have found the decryption key, we can use it to decrypt the message by multiplying the matrix that represents the message "SONAFQCHMWPTVEVY" with the decryption

key to find the decrypted message.

$$let\ P = \begin{bmatrix} S & N & F & C & M & P & V & V \\ O & A & Q & H & W & T & E & Y \end{bmatrix} = \begin{bmatrix} 18 & 13 & 5 & 2 & 12 & 15 & 21 & 21 \\ 14 & 0 & 16 & 7 & 22 & 19 & 4 & 24 \end{bmatrix} \quad (18)$$

$$KP = Q \pmod{26} \quad (19)$$

$$KP = \begin{bmatrix} 517 & 501 \\ 266 & 213 \end{bmatrix} \begin{bmatrix} 18 & 13 & 5 & 2 & 12 & 15 & 21 & 21 \\ 14 & 0 & 16 & 7 & 22 & 19 & 4 & 24 \end{bmatrix} = Q \pmod{26} \quad (20)$$

$$Q \pmod{26} = \begin{bmatrix} 18 & 13 & 19 & 17 & 14 & 10 & 17 & 1 \\ 4 & 0 & 14 & 19 & 14 & 1 & 8 & 4 \end{bmatrix} \pmod{26} \quad (21)$$

$$Q \pmod{26} = \begin{bmatrix} S & N & T & R & O & K & R & O \\ E & A & O & T & O & B & I & E \end{bmatrix} \quad (22)$$

The decrypted message is "SENATORTOOKBRIBE" or "Senator took bribe".

Problem 2

In order to increase the difficulty of breaking your crypto-system, you decide to encipher your messages using a Hill 2-cipher by first applying the matrix $\begin{bmatrix} 3 & 11 \\ 4 & 15 \end{bmatrix}$ working modulo 26 and then applying the matrix $\begin{bmatrix} 10 & 15 \\ 5 & 9 \end{bmatrix}$ working modulo 29. Thus, while your plain-texts are in the usual 26 letter alphabet, your cipher-texts will be in the alphabet with 0-25 as usual and blank=26, ?=27, and !=28.

a) Encipher the message "THIS IS A FUN PROJECT".

b) Describe how to decipher a cipher-text by applying two matrices in succession, and decipher "ZMOY".

c) Under what conditions is a matrix with entries module 29 invertible modulo 29?