techspace

Hill Ciphers: Solutions to the Exercises

Jonaki B Ghosh

1. Using the substitution table the encrypted message (**FY O. KI ZT WA QC**) is converted to the following 2×6 matrix:

$$\begin{bmatrix} 5 & 14 & 10 & 25 & 22 & 16 \\ 24 & 26 & 8 & 19 & 0 & 2 \end{bmatrix}$$

We pre-multiply this with the inverse of the matrix $\begin{bmatrix} 1 & 4 \\ 2 & 9 \end{bmatrix}$ which is $\begin{bmatrix} 9 & -4 \\ -2 & 1 \end{bmatrix}$. Thus:

$$\begin{bmatrix} 9 & -4 \\ -2 & 1 \end{bmatrix}\begin{bmatrix} 5 & 14 & 10 & 25 & 22 & 16 \\ 24 & 26 & 8 & 19 & 0 & 2 \end{bmatrix}$$
$$= \begin{bmatrix} -51 & 22 & 58 & 149 & 198 & 136 \\ 14 & -2 & -12 & -31 & -44 & -30 \end{bmatrix}$$

Reducing the product modulo 29 we get:

$$\begin{bmatrix} 7 & 22 & 0 & 4 & 24 & 20 \\ 14 & 27 & 17 & 27 & 14 & 28 \end{bmatrix}$$

Converting the numbers to characters, column wise, we obtain the original message:

HO W_ AR E_ YO U?

That is: **HOW_ARE_YOU?**

2. The secret message **ITS DGN STX SJK DVO JHE TCB** is first converted to a 3×7 matrix using the substitution table. We get:

$$\begin{bmatrix} 8 & 3 & 18 & 18 & 3 & 9 & 19 \\ 19 & 6 & 19 & 9 & 21 & 7 & 2 \\ 18 & 13 & 23 & 10 & 14 & 4 & 1 \end{bmatrix}$$

We pre-multiply this matrix with the inverse of the encoding matrix $\begin{bmatrix} 0 & 2 & 4 \\ 1 & 4 & 7 \\ 2 & 3 & 6 \end{bmatrix}$ which is $\begin{bmatrix} 3 & -3 & 2 \\ 8 & -6 & 3 \\ -5 & 4 & -2 \end{bmatrix}$. Thus

$$\begin{bmatrix} 3 & -3 & 2 \\ 8 & -6 & 3 \\ -5 & 4 & -2 \end{bmatrix}\begin{bmatrix} 8 & 3 & 18 & 18 & 3 & 9 & 19 \\ 19 & 6 & 19 & 9 & 21 & 7 & 2 \\ 18 & 13 & 23 & 10 & 14 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 17 & 43 & 47 & -26 & 14 & 53 \\ 4 & 27 & 99 & 120 & -60 & 42 & 143 \\ 0 & -17 & -60 & -74 & 41 & -25 & -89 \end{bmatrix}$$

In Excel, the entry in position (3,1) of the matrix is seen to be a very small number. It may be treated as 0. Reducing the matrix modulo 29 we get the following:

$$\begin{bmatrix} 3 & 17 & 14 & 18 & 3 & 14 & 24 \\ 4 & 27 & 12 & 4 & 27 & 13 & 27 \\ 29 & 12 & 27 & 13 & 12 & 4 & 27 \end{bmatrix}$$

(Note that 29 is equivalent to 0 in modulo 29.) We convert the numbers to characters, column wise and obtain the original message: **DEA R_M OM_ SEN D_M ONE Y_ _**

That is: **DEAR_MOM_SEND_MONEY_ _**

Note that the number of characters in the original message is 19, which is not a multiple of 3. Hence two underscores have been added at the end of the message so that the 3×7 matrix could be completed.

3. The same process as shown in Exercise 2 may be used to decode the message. The details are left to the reader. The original message is: **HILL_CIPHERS_ARE_FUN.**

4. Here is a 4×4 matrix whose determinant is equal to 1:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 0 & 2 & 3 \\ 1 & 1 & 4 & 7 \\ 8 & 2 & 3 & 6 \end{bmatrix}$$

There are clearly many more such matrices (in fact, infinitely many).