Hill Ciphers

JONAKI B GHOSH

Introduction

Cryptography is the science of making and breaking codes. It is the practice and study of techniques for secure communication. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

This article is a sequel to an article which appeared in the November 2014 issue of *At Right Angles* in which we had described an interesting cryptography method known as the *Hill Cipher*. (See http://www.teachersofindia.org/en/article/hill-ciphers.) The Hill Cipher method is based on matrices and modular arithmetic. As in the previous article, we will explore the method using the spreadsheet MS Excel in which we will perform operations on matrices.

Keywords: *Cryptography, cipher, matrix, augmented, inverse, identity, multiplication, transformation, plaintext, encoding, decoding, modular*

Hill Ciphers

We had described in the previous article that Hill ciphers are an application of matrices to cryptography. Ciphers are methods for transforming a given message, the *plaintext*, into a new form that is unintelligible to anyone who does not know the key (the transformation used to convert the plaintext). In a cipher the key transforms the plaintext letters to other characters known as the *ciphertext*. The secret rule, that is, the inverse key, is required to reverse the transformation in order to recover the original message. To use the key to transform plaintext into ciphertext is to *encipher* the plaintext. To use the inverse key to transform the ciphertext back into plaintext is to *decipher* the ciphertext.

In order to understand Hill ciphers, we need to understand modular arithmetic, and be able to multiply and invert matrices. We would urge the reader to refer to the article in the November 2014 issue. However, we shall mention some important definitions here.

Definition 1: An arbitrary Hill n-cipher has as its key a given $n \times n$ invertible matrix whose entries are non-negative integers from among $0, 1, \ldots, m-1$, where m is the number of characters used for the encoding process. Suppose we wish to use all the 26 alphabets from A to Z and three more characters, say ‘.’, ‘–‘ and ‘?’. This means we will have 29 characters with which we can write our plaintext. These have been shown in the given substitution table where the 29 characters have been numbered from 0 to 28.

Let us recall the encryption method by applying this to an example of a Hill 2-cipher corresponding to the substitution table (Table 1) with 29 characters. Let the key be the invertible 2 × 2 matrix

$$\mathrm{E} = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$$

We can also refer to E as the ‘encoding matrix’. We will use E to encipher groups of two consecutive characters. Suppose we have to encipher the word **HI**. The alphabets H and I correspond to the numbers 7 and 8, respectively, from the above substitution table. We shall represent it as a 2 × 1 matrix.

$$\begin{bmatrix} 7 \\ 8 \end{bmatrix}$$

To encipher **HI**, we shall pre-multiply this matrix by the encoding matrix E.

$$\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 38 \\ 68 \end{bmatrix}$$

The product is a 2 × 1 matrix with entries 38 and 68. But what characters do the numbers 38 and 68 represent? These are not in our substitution table! What we shall do is as follows:

We will divide these numbers by 29 and consider their respective remainders after the division process is done. Thus when we divide 38 by 29, the remainder is 9 and when we divide 68 by 29, the remainder is 10.

To express this in the language of *modular arithmetic*, we write

$$38 \equiv 9 \pmod{29} \text{ and } 68 \equiv 10 \pmod{29}$$

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25
.	**_**	**?**										
26	27	28										

Table 1. The substitution table for the Hill Cipher

Definition 2: Given an integer $m > 1$, called the *modulus*, we say that the two integers a and b are *congruent* to one another *modulo m* and we write

$$a \equiv b \,(\text{mod}\; m) \quad \text{(we read this as '}a\text{ is congruent to }b\text{ modulo }m\text{')}$$

This means that the difference $a - b$ is an integral multiple of m. In other words, $a \equiv b \pmod{m}$ when $a = b + km$ for some integer k (positive, negative or zero)

For our Hill 2-cipher, we have

$$38 \equiv 9 \pmod{29} \text{ and } 68 \equiv 10 \pmod{29}$$

Note that 38 = 9 + 1 × 29 and 68 = 10 + 2 × 29.

The numbers 9 and 10 correspond to the alphabets J and K respectively from our substitution table.

Thus the word **HI** is enciphered to **JK**!

In order to use this method of sending secret messages, the sender has to encrypt the plaintext (the original message) **HI** and send the encrypted form **JK** to the receiver. The secret key, that is, the encoding matrix E is known only to the sender and the receiver. Now let us see how the receiver can decipher what **JK** stands for.

In order to decipher **JK**, we begin by looking for the numbers corresponding to **J** and **K** in our substitution table. These are 9 and 10 respectively. We represent this in the form of a 2 × 1 matrix

$$\begin{bmatrix} 9 \\ 10 \end{bmatrix}$$

In the previous article we had used the matrix $\begin{bmatrix} 1 & 4 \\ 2 & 9 \end{bmatrix}$ as our encoding matrix. Note that we have to use the inverse of the encoding matrix to decipher the ciphertext. Thus we had used its inverse $\begin{bmatrix} 9 & -4 \\ -2 & 1 \end{bmatrix}$ to decrypt the ciphertext. Note that $\begin{bmatrix} 1 & 4 \\ 2 & 9 \end{bmatrix}$ has a determinant equal to 1. Thus the decryption was simple as we needed to multiply the inverse matrix with the message matrix (refer to pages 67-68 in the November 2014 issue). However this method is likely to pose a difficulty if the determinant of the encoding matrix is any value other than 1. This means that the inverse matrix, that is, the inverse key will comprise fractional entries. How will we then decode the encrypted text or ciphertext?

Thus, if the determinant of the encoding matrix is not equal to 1, as in the case of $E = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$ (the determinant is equal to -2), we will need to find the inverse of the matrix in Z_{29}, the set of integers modulo 29. Note that the actual inverse is $E^{-1} = \frac{1}{-2}\begin{bmatrix} 5 & -3 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} -5/2 & 3/2 \\ 2 & -1 \end{bmatrix}$ but this will not be helpful as two entries in the matrix are fractions. However, when we find the inverse in Z_{29}, all entries will be integers from 0 to 28 which will certainly serve our purpose. Note that the set $\{0, 1, 2, 3, \ldots, n-1\}$ is referred to as the *set of integers modulo n* and is represented as Z_n.

To find the inverse of a matrix in Z_{29}:

We shall now demonstrate the method of finding the inverse of a 2 × 2 matrix in $Z_{29.}$ First we shall augment the matrix E with the 2 × 2 identity matrix, I, to its right, and obtain$[E|\,I]$. Further we shall apply elementary row operations till we obtain $[I|\,E^{-1}]$.

Now,

$$[E|\,I] = \left[\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 4 & 5 & 0 & 1 \end{array}\right]$$

Our aim is to convert E to I, using elementary row transformations. At the end of the process, I will be automatically converted to E^{-1}. In general we will perform row operations so that 2 gets converted to 1, 4 to 0, 5 to 1 and 3 to 0 (in that order). We shall refer to the first row of the augmented matrix as $R_1$and the second row as R_2.

To begin the process we need to find the multiplicative inverse of 2 in Z_{29}. We shall thus multiply R_1 by 15 since 15 is the multiplicative inverse of 2 in Z_{29}. Note that $2 \times 15 = 30 \equiv 1 \pmod{29}$. In Table 2 we have included the multiplicative inverses of all integers in Z_{29} (in blue). The reader is urged to verify these values and use them as a reference for the remaining calculations.

Thus, performing the row operation $R_1 \rightarrow 15\, R_1$ on $[E|I]$ and reducing it modulo 29, we get

$$\left[\begin{array}{cc|cc} 30 & 45 & 15 & 0 \\ 4 & 5 & 0 & 1 \end{array}\right] \approx \left[\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 4 & 5 & 0 & 1 \end{array}\right] (\text{mod } 29)$$

Note that 2 in the original augmented matrix has been replaced by 1.

In order to convert 4 to 0 (in the reduced matrix), we need to perform the row operation $R_2 \rightarrow R_2 - 4 \times R_1$. This gives

$$\left[\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 0 & -59 & -60 & 1 \end{array}\right] \approx \left[\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 0 & 28 & 27 & 1 \end{array}\right] (\text{mod } 29)$$

Now, to convert 28 to 1, we need to multiply 28 by its inverse in Z_{29}, that is, perform the row operation $R_2 \rightarrow 28\, R_2$. Note that 28 is its own inverse in Z_{29}, as $28 \times 28 = 784 \equiv 1 \pmod{29}$.We now get:

$$\left[\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 0 & 784 & 756 & 28 \end{array}\right] \approx \left[\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 0 & 1 & 2 & 28 \end{array}\right] (\text{mod } 29)$$

Finally, to convert 16 to 0, we need to perform the row operation $R_1 \rightarrow R_1 - 16 \times R_2$. This gives us:

$$\left[\begin{array}{cc|cc} 1 & 0 & -17 & -448 \\ 0 & 1 & 2 & 28 \end{array}\right] \approx \left[\begin{array}{cc|cc} 1 & 0 & 12 & 16 \\ 0 & 1 & 2 & 28 \end{array}\right] (\text{mod } 29)$$

We have now succeeded in converting the segmented matrix $[E|I]$ to $[I|E^{-1}]$.

Thus, the inverse of E = $\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$ in Z_{29} is $E^{-1} = \begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix}$.

Now, to decrypt **JK** we need to perform the multiplication

$$\begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix}\begin{bmatrix} 9 \\ 10 \end{bmatrix} \text{ and reduce it modulo 29.}$$

Thus,

$$\begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix}\begin{bmatrix} 9 \\ 10 \end{bmatrix} = \begin{bmatrix} 268 \\ 298 \end{bmatrix} \approx \begin{bmatrix} 7 \\ 8 \end{bmatrix} (\text{mod } 29)$$

7 and 8 can be traced back to the alphabets H and I and hence the plaintext message **HI**!

In the previous article, we had encrypted the plaintext **MATH_IS_FUN.** using the matrix $\begin{bmatrix} 1 & 4 \\ 2 & 9 \end{bmatrix}$. Let us now encrypt the same using the matrix $\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	15	10	22	6	5	25	11	3	3	8	17	9	27
15	16	17	18	19	20	21	22	23	24	25	26	27	28
2	20	12	21	26	16	18	4	24	23	7	19	14	28

Table 2.

The steps are indicated below. For matrix computations we use MS Excel. In Excel, the commands for multiplying matrices and finding the inverse of a matrix are MMULT and MINVERSE respectively. For reducing a number modulo a divisor the required command is MOD.

Encoding or enciphering the plaintext: The steps

Step 1: Convert the plaintext **MATH_IS_FUN.** to the corresponding substitution values from the substitution table. The values are

$$12 \quad 0 \quad 19 \quad 7 \quad 27 \quad 8 \quad 18 \quad 27 \quad 5 \quad 20 \quad 13 \quad 26$$

We need to make a 2 × n matrix using these values

Step 2: Form pairs of these numbers as follows

$$12 \quad 0 \qquad 19 \quad 7 \qquad 27 \quad 8 \qquad 18 \quad 27 \qquad 5 \quad 20 \qquad 13 \quad 26$$

Each pair will form a column of a 2 × 6 matrix (since there are 6 pairs). Let us call this matrix P (the plaintext matrix)

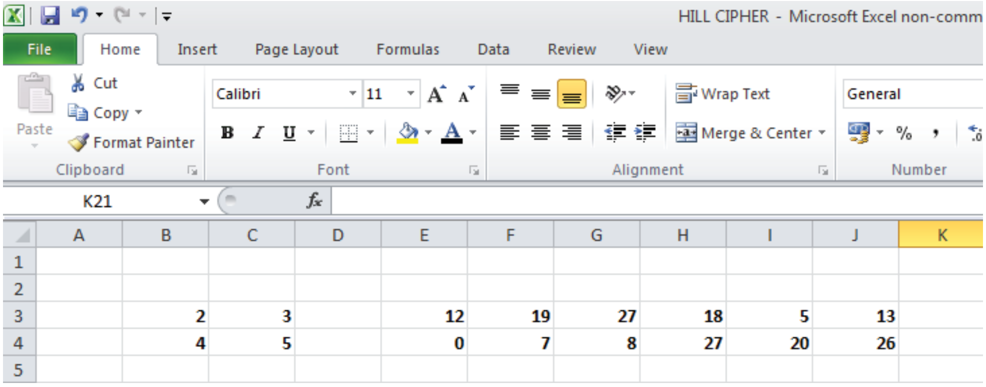
$$P = \begin{bmatrix} 12 & 19 & 27 & 18 & 5 & 13 \\ 0 & 7 & 8 & 27 & 20 & 26 \end{bmatrix}$$

Step 3: Compute the product EP

$$EP = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 12 & 19 & 27 & 18 & 5 & 13 \\ 0 & 7 & 8 & 27 & 20 & 26 \end{bmatrix} = \begin{bmatrix} 24 & 59 & 78 & 117 & 70 & 101 \\ 48 & 111 & 148 & 207 & 120 & 177 \end{bmatrix}$$

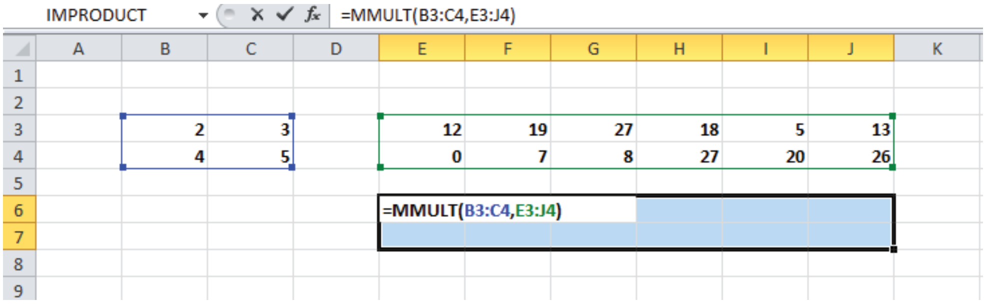
In order to perform this computation in Excel, we proceed as follows:

Enter the 2 × 2 matrix E and the 2 × 6 matrix P as separate arrays as shown. Each entry of a matrix may be entered by typing a number in a cell and pressing Enter. The arrow keys may be used to move to the next appropriate cell.



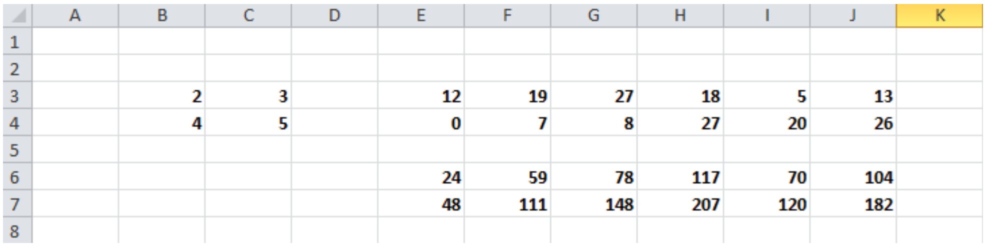
	A	B	C	D	E	F	G	H	I	J	K
1											
2											
3		2	3		12	19	27	18	5	13	
4		4	5		0	7	8	27	20	26	
5											

To obtain the product, select a blank 2 × 6 array and type **=MMULT(** in the top leftmost cell of the chosen array. Within the parentheses, first select the array for matrix E and then the array for matrix P separated by a comma. Press **Crtl + Shift** followed by **Enter** to obtain the product. (Note that you need to press **Crtl** and **Shift** simultaneously and then press **Enter**.)



=MMULT(B3:C4,E3:J4)

	A	B	C	D	E	F	G	H	I	J	K
1											
2											
3		2	3		12	19	27	18	5	13	
4		4	5		0	7	8	27	20	26	
5											
6					=MMULT(B3:C4,E3:J4)						
7											
8											
9											



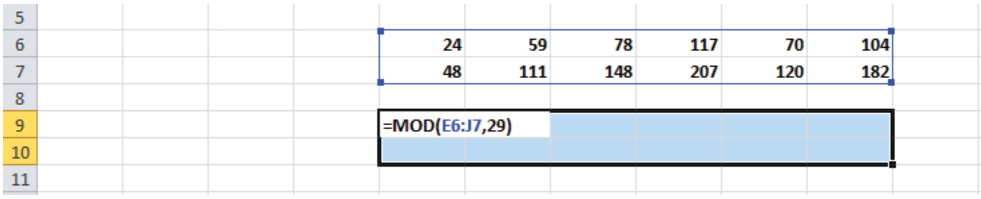
	A	B	C	D	E	F	G	H	I	J	K
1											
2											
3		2	3		12	19	27	18	5	13	
4		4	5		0	7	8	27	20	26	
5											
6					24	59	78	117	70	104	
7					48	111	148	207	120	182	
8											

Step 4: Reduce the product modulo 29 to obtain the Hill 2-cipher values. This means we have to divide each number by 29 and find the remainder. In Excel we can reduce the entire matrix modulo 29 in one go!

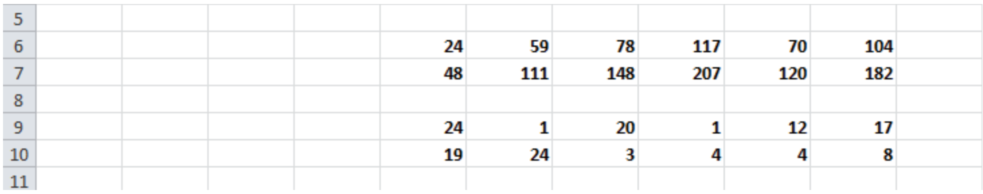
$$EP = \begin{bmatrix} 24 & 59 & 78 & 117 & 70 & 104 \\ 48 & 111 & 148 & 207 & 120 & 182 \end{bmatrix} \approx \begin{bmatrix} 24 & 1 & 20 & 1 & 12 & 17 \\ 19 & 24 & 3 & 4 & 4 & 8 \end{bmatrix} \pmod{29}$$

To do this in Excel proceed as follows

Select a blank 2 × 6 array and type **=MOD(** in the top leftmost cell of the array. Within the parentheses, select the array of the product matrix EP and type 29 for the divisor.



5											
6					24	59	78	117	70	104	
7					48	111	148	207	120	182	
8											
9					=MOD(E6:J7,29)						
10											
11											



5											
6					24	59	78	117	70	104	
7					48	111	148	207	120	182	
8											
9					24	1	20	1	12	17	
10					19	24	3	4	4	8	
11											

Step 5: Write out the columns of the matrix in a sequence

$$\begin{bmatrix} 24 & 1 & 20 & 1 & 12 & 17 \\ 19 & 24 & 3 & 4 & 4 & 8 \end{bmatrix}$$

These are

$$24 \quad 19 \quad 1 \quad 24 \quad 20 \quad 3 \quad 1 \quad 4 \quad 12 \quad 4 \quad 17 \quad 8$$

Replace these values by the characters from the substitution table to which these values correspond.

The encrypted message or ciphertext is **MTBYUDBEMERI**.

Decoding or deciphering the ciphertext: The steps

In this section we will try to decipher the ciphertext **MTBYUDBEMERI**

Step 1: Convert the characters to their respective Hill-2-cipher values from the substitution table

$$24 \quad 19 \quad 1 \quad 24 \quad 20 \quad 3 \quad 1 \quad 4 \quad 12 \quad 4 \quad 17 \quad 8$$

Form a 2 × 6 matrix using these values. Make pairs of these numbers as follows

$$24 \quad 19 \qquad 1 \quad 24 \qquad 20 \quad 3 \qquad 1 \quad 4 \qquad 12 \quad 4 \qquad 17 \quad 8$$

Each pair will form a column of a 2 × 6 matrix (since there are 6 pairs). Let us call this matrix C (the ciphertext matrix)

$$\mathrm{C} = \begin{bmatrix} 24 & 1 & 20 & 1 & 12 & 17 \\ 19 & 24 & 3 & 4 & 4 & 8 \end{bmatrix}$$

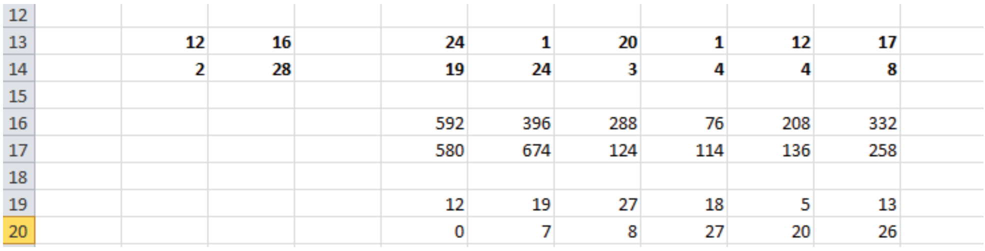
Step 2: Compute the product E^{-1} C

$$E^{-1}C = \begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix} \begin{bmatrix} 24 & 1 & 20 & 1 & 12 & 17 \\ 19 & 24 & 3 & 4 & 4 & 8 \end{bmatrix} = \begin{bmatrix} 592 & 396 & 288 & 76 & 208 & 332 \\ 580 & 674 & 124 & 114 & 136 & 258 \end{bmatrix}$$

Step 3: Reduce the product modulo 29 to obtain the substitution values.

$$\begin{bmatrix} 592 & 396 & 288 & 76 & 208 & 332 \\ 580 & 674 & 124 & 114 & 136 & 258 \end{bmatrix} \approx \begin{bmatrix} 12 & 19 & 27 & 18 & 5 & 13 \\ 0 & 7 & 8 & 27 & 20 & 26 \end{bmatrix} (\mathrm{mod}\ 29)$$

The reader may perform these computations using Excel. The screenshot of the Excel sheet is as follows.



12										
13		12	16		24	1	20	1	12	17
14		2	28		19	24	3	4	4	8
15										
16					592	396	288	76	208	332
17					580	674	124	114	136	258
18										
19					12	19	27	18	5	13
20					0	7	8	27	20	26

Step 4: Write out the columns of the matrix in a sequence

$$\begin{bmatrix} 12 & 19 & 27 & 18 & 5 & 13 \\ 0 & 7 & 8 & 27 & 20 & 26 \end{bmatrix}$$

These are

12 0 19 7 27 8 18 27 5 20 13 26

Replace these values by the characters from the substitution table to which these values correspond.

The decrypted message or plaintext is **MATH_IS_FUN.**

So far we have learnt how to encrypt a plaintext using a Hill 2-cipher. This means that our encoding matrix is a 2 × 2 matrix. If we choose a 3 × 3 matrix, the plaintext will have to be converted to a 3 × n matrix (here the number of columns 'n' depends on the length of the message).

The reader is urged to try to decode the messages in the next few exercises to practice the method. All computations may be done on Excel. Note that the substitution table remains the same as before.

Exercises

(1) Decode the secret message **O? ZR ZV OW MK AC GM KX** which was encrypted using the encoding matrix

$$E = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$$

(2) Decode the secret message **SA_ NCN PIB WNF PRU JRP RII** which was encrypted using the encoding matrix

$$E = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 4 & 5 \\ 1 & 2 & 3 \end{bmatrix}$$

This is an example of a Hill 3-cipher.

Hint: The first step is to find the inverse of the matrix E in Z_{29}. The method described in the article for a 2×2 matrix may be followed. Note that the augmented matrix $[E|\,I]$ is the matrix

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 4 & 5 & 0 & 1 & 0 \\ 1 & 2 & 3 & 0 & 0 & 1 \end{array}\right].$$

Conclusion

The Hill Cipher presents an interesting application of matrices and number theory to cryptography. It is open to exploration and students find it exciting to use this method. This is an example of a practical situation where performing matrix operations such as matrix multiplication and finding the inverse are actually required. It helps the student to understand the need and importance of matrix operations and also explore the method by using different keys (that is, encoding matrices). Any computing tool which can perform matrix operations, will be helpful, as the computations may be tedious and time consuming (especially when the plaintext or ciphertext is lengthy). In this article we have discussed a more general form of the method where any invertible square matrix may be chosen as the key.

References

1. http://en.wikipedia.org/wiki/Hill_cipher
2. http://practicalcryptography.com/ciphers/hill-cipher/
3. http://www.pstcc.edu/math/_files/pdf/augment.pdf (for information about the augmented matrix)

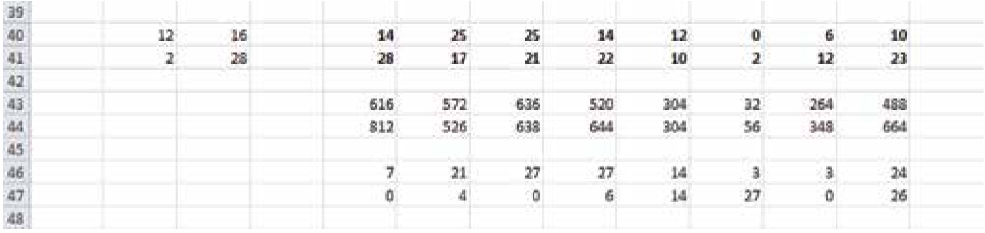
Solutions to exercises

Exercise 1:

The ciphertext **O? ZR ZV OW MK AC GM KX** converts to the hill – 2 – cipher matrix

$$\begin{bmatrix} 14 & 25 & 25 & 14 & 12 & 0 & 6 & 10 \\ 28 & 17 & 21 & 22 & 10 & 2 & 12 & 23 \end{bmatrix}$$

We pre-multiply this matrix using the inverse of the matrix $\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$ in Z_{29}, which is $\begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix}$. Further we reduce the product modulo 29 to obtain the original values which correspond to alphabets from the substitution table. The computations are shown in MS Excel.



39												
40		12	16		14	25	25	14	12	0	6	10
41		2	28		28	17	21	22	10	2	12	23
42												
43					616	572	636	520	304	32	264	488
44					812	526	638	644	304	56	348	664
45												
46					7	21	27	27	14	3	3	24
47					0	4	0	6	14	27	0	26
48												

The values (taken column-wise) are as follows

7 0 21 4 27 0 27 6 14 14 3 27 3 0 24 26

These translate to the message

HAVE_A_GOOD_DAY.

Exercise 2:

The inverse of the matrix $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 4 & 5 \\ 1 & 2 & 3 \end{bmatrix}$ in Z_{29} is $\begin{bmatrix} 28 & 28 & 2 \\ 12 & 28 & 17 \\ 2 & 1 & 27 \end{bmatrix}$ which may be obtained as follows.

Consider the augmented matrix $[E|\,I] = \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 4 & 5 & 0 & 1 & 0 \\ 1 & 2 & 3 & 0 & 0 & 1 \end{array}\right]$.

We need to perform elementary row transformations so that E gets transformed to I, the 3 × 3 identity matrix, which is $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

We begin by performing the row operation $R_3 \rightarrow R_3$ - R_1 on $[E|\,I]$. Reducing the product modulo 29, we get

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 4 & 5 & 0 & 1 & 0 \\ 0 & 2 & 2 & -1 & 0 & 1 \end{array}\right] \approx \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 4 & 5 & 0 & 1 & 0 \\ 0 & 2 & 2 & 28 & 0 & 1 \end{array}\right] (\text{mod } 29)$$

Note that the first 1 in R_3 in the original augmented matrix has been replaced by 0. In order to convert 4 to 1 (in the reduced matrix), we need to multiply it by its inverse which is 22 and perform the row operation $R_2 \rightarrow 22 \times R_2$. This gives

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 88 & 110 & 0 & 22 & 0 \\ 0 & 2 & 2 & 28 & 0 & 1 \end{array}\right] \approx \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 23 & 0 & 22 & 0 \\ 0 & 2 & 2 & 28 & 0 & 1 \end{array}\right] (\text{mod } 29)$$

Now, to convert the first 2 in R_3 to 0, we need to perform the row operation $R_3 \rightarrow R_3$ - 2× R_2. We now get,

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 23 & 0 & 22 & 0 \\ 0 & 0 & -44 & 28 & -44 & 1 \end{array}\right] \approx \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 23 & 0 & 22 & 0 \\ 0 & 0 & 14 & 28 & 14 & 1 \end{array}\right] (\text{mod } 29)$$

In order to convert the first 14 of R_3 to 1 (in the reduced matrix), we need to multiply it by its inverse which is 27 and perform the row operation $R_3 \rightarrow 27 \times R_3$ and reduce it modulo 29. This gives

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 23 & 0 & 22 & 0 \\ 0 & 0 & 378 & 756 & 378 & 27 \end{array}\right] \approx \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 23 & 0 & 22 & 0 \\ 0 & 0 & 1 & 2 & 1 & 27 \end{array}\right] (\text{mod } 29)$$

To convert 23 in R_2 to 0, we need to perform the row operation $R_2 \rightarrow R_2 - 23 \times R_2$. This gives us,

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & -46 & -1 & -621 \\ 0 & 0 & 1 & 2 & 1 & 27 \end{array}\right] \approx \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 12 & 28 & 17 \\ 0 & 0 & 1 & 2 & 1 & 27 \end{array}\right] (\text{mod } 29)$$

The last step is to perform the row operation $R_1 \rightarrow R_1 - R_3$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & -1 & -27 \\ 0 & 1 & 0 & 12 & 28 & 17 \\ 0 & 0 & 1 & 2 & 1 & 27 \end{array}\right] \approx \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 28 & 28 & 2 \\ 0 & 1 & 0 & 12 & 28 & 17 \\ 0 & 0 & 1 & 2 & 1 & 27 \end{array}\right] (\text{mod } 29)$$

We have now succeeded in converting the augmented matrix $[E|\,I]$ to $\left[I|\,E^{-1}\right]$.

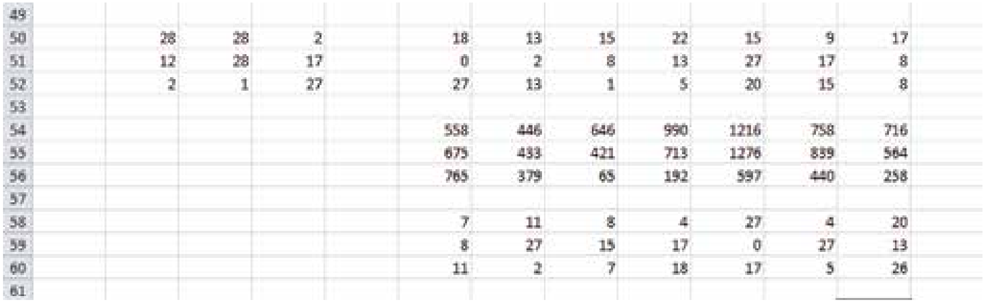
Thus, the inverse of E = $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 4 & 5 \\ 1 & 2 & 3 \end{bmatrix}$ in Z_{29} is E^{-1} =. $\begin{bmatrix} 28 & 28 & 2 \\ 12 & 28 & 17 \\ 2 & 1 & 27 \end{bmatrix}$

We can now use the matrix E^{-1} to decipher the secret message.

The ciphertext **SA_ NCN PIB WNF PRU JRP RII** converts to the hill – 3 – cipher matrix

$$\begin{bmatrix} 18 & 13 & 15 & 22 & 15 & 9 & 17 \\ 0 & 2 & 8 & 13 & 27 & 17 & 8 \\ 27 & 13 & 1 & 5 & 20 & 15 & 8 \end{bmatrix}$$

We pre-multiply this matrix using the inverse of the matrix $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 4 & 5 \\ 1 & 2 & 3 \end{bmatrix}$ in Z_{29}, which is $\begin{bmatrix} 28 & 28 & 2 \\ 12 & 28 & 17 \\ 2 & 1 & 27 \end{bmatrix}$.
Further we reduce the product modulo 29 to obtain the original values which correspond to alphabets from the substitution table. The computations are shown in MS Excel.



49												
50		28	28	2		18	13	15	22	15	9	17
51		12	28	17		0	2	8	13	27	17	8
52		2	1	27		27	13	1	5	20	15	8
53												
54						558	446	646	990	1216	758	716
55						675	433	421	713	1276	839	564
56						765	379	65	192	597	440	258
57												
58						7	11	8	4	27	4	20
59						8	27	15	17	0	27	13
60						11	2	7	18	17	5	26
61												

The values (taken column-wise) are as follows

7 8 11 11 27 2 8 15 7 4 17 18 27 0 17 4 27 5 20 13 26

These translate to the message

HILL_CIPHERS_ARE_FUN.

JONAKI GHOSH is an Assistant Professor in the Dept. of Elementary Education, Lady Sri Ram College, University of Delhi where she teaches courses related to math education. She obtained her Ph.D. in Applied Mathematics from Jamia Milia Islamia University, New Delhi, and her M.Sc. from IIT Kanpur. She has taught mathematics at the Delhi Public School, R K Puram, where she set up the Math Laboratory & Technology Centre. She has started a Foundation through which she conducts professional development programmes for math teachers. Her primary area of research interest is in the use of technology in mathematics instruction. She is a member of the Indo Swedish Working Group on Mathematics Education. She regularly participates in national and international conferences. She has published articles in journals and authored books for school students. She may be contacted at jonakibghosh@gmail.com.