Addendum to Hill Ciphers

KUMAR GANDHARV MISHRA

The Hill Cipher method in cryptography has been described in detail in earlier issues of *At Right Angles* [1] [2]. Through those articles, the reader will be familiar with the art of encryption and decryption of messages using matrices and modular arithmetic. The Hill Cipher method requires a substitution table comprising letters and numerals, and a fixed key invertible matrix that is used to encrypt the plain text into the cipher text. Further, the inverse of the key matrix is used to decrypt the cipher text back to the plain text. A substitution table must comprise of the characters and their corresponding numerical values. Table 1 with 29 characters (numbered from 0 to 28) is a particular choice, which we will use in this article.

The process of encryption and decryption requires the plaintext to be converted to a matrix using the numerals from the substitution table. Further, the plaintext matrix is to be pre multiplied or post multiplied by the key matrix to obtain a matrix that leads to the cipher text. When the values of numerals in this product matrix exceed 28, modular arithmetic is used, i.e., the product matrix is reduced modulo 29. This requires knowledge and understanding of modular arithmetic and Ghosh has shown how modular arithmetic can also be performed with technical tools like MS-Excel.

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

Table 1. Substitution Table[a]

[a] '0' represents a blank space

Keywords: Cryptography, Hill cipher, code, substitution, matrix

However, lack of familiarity with technology and absence of topics like 'modular arithmetic' at school level pose a challenge in introducing 'Cryptography' to students. In this article we introduce an alternative technique by *faking* numerical values which are either negative or greater than 28. The reader is requested to refer to the previous articles on Hill Ciphers to recall the original method. In this article, we illustrate the cases when the matrix of ciphertext has negative elements or elements greater than 28, i.e., $c_{ij} > 28$ or $c_{ij} < 0$.

Let's try this:

Suppose you wish to send the message '**HELLO HOW R U?**' to your friend.

Choose an invertible 3 by 3 matrix K as the key and share it with your friend. The sender and the receiver are required to know the key but it is to be kept secret from others. Let us choose K as follows

$$K = \begin{bmatrix} 1 & 0 & -2 \\ 2 & -1 & 1 \\ 3 & -2 & 1 \end{bmatrix}$$

The message - **HELLO HOW R U?** has 14 characters including spaces. We would form our message matrix based on the key matrix. As the key matrix is of order 3 by 3, the message matrix must be either a 3 by 5 or 5 by 3 matrix.

Note: The order of the message matrix M will depend on the order of the key matrix K. To get a new matrix C (for ciphertext), we will need to pre-multiply or post-multiply M by K (depending on the order of the message matrix M created by the sender of the message). For example, if M is of order 3 by 4 then we need to compute KM = C whereas if M is of order 4 by 3 we will compute MK = C.

Part I – ENCRYPTION

The process of encryption is as follows:

Step 1: In **HELLO HOW R U?** each character is replaced with its corresponding number from Table 1. We obtain the following string of numbers.

10_7_14_14_17_0_10_17_25_0_20_0_23_2

Step 2: Since the key matrix K is of order 3 by 3, we may create a message matrix M of order 3 by 5. The elements in the string will be positioned in M row wise and then the remaining empty positions can be filled with '0'.

$$M = \begin{bmatrix} 10 & 7 & 14 & 14 & 17 \\ 0 & 10 & 17 & 25 & 0 \\ 20 & 0 & 23 & 2 & 0 \end{bmatrix}$$

Step 3: We need to pre-multiply M by K to get the matrix for obtaining ciphertext.

Thus C = KM

$$\begin{bmatrix} 1 & 0 & -2 \\ 2 & -1 & 1 \\ 3 & -2 & 1 \end{bmatrix} \begin{bmatrix} 10 & 7 & 14 & 14 & 17 \\ 0 & 10 & 17 & 25 & 0 \\ 20 & 0 & 23 & 2 & 0 \end{bmatrix} = \begin{bmatrix} -30 & 7 & -32 & 10 & 17 \\ 40 & 4 & 34 & 5 & 34 \\ 50 & 1 & 31 & -6 & 51 \end{bmatrix}$$

Step 4: The values obtained can be arranged as a new string:

$$-30\_7\_-32\_10\_17\_40\_4\_34\_5\_34\_50\_1\_31\_-6\_51$$

Note that some of the elements in the string are greater than 28 and some are even negative integers. These values are not in Table 1. How will you proceed? Well, the idea is to convert (fake) these values in terms of a numeral in Table 1 and substitute with corresponding letters but your friend should be aware of the method of making these conversions and be able to retrieve the characters from Table 1.

Let's see how:

Rule of conversion while sending ciphertext:

i. **If $C_{ij} > 28$**	ii. **If $C_{ij} < 0$**
• Divide C_{ij} by 28, and then find the quotient and remainder For example, in the numeral string take '50' $50 = 1.28 + 22, q = 1, r = 22$ • Represent the new element as $r^{q+} = 22^{1+}$ Similarly $31 = 3^{1+}, 34 = 6^{1+}, 40 = 12^{1+}$, $51 = 23^{1+}$	• Find difference between 28 and C_{ij} For example, in the numeral string take '–32' Difference: $28 - (-32) = 60$ Divide the difference obtained by 28 $60 = 2.28 + 4, q = 2, r = 4$ Represent the new element for '–32' as $r^{q-} = 4^{2-}$ Similarly $-30 = 2^{2-}, -6 = 6^{1-}$

Table 2

The sender can now use the following new string of numerals:

2^{2-}_7_4^{2-}_10_17_12^{1+}_4_6^{1+}_5_6^{1+}_22^{1+}_1_3^{1+}_6^{1-}_23^{1+}
for − 30_7_ − 32_10_17_40_4_34_5_34_50_1_31_ − 6_51

Using Table 1, the obtained letter string would be:

$?^{2-}$_E_B^{2-}_H_O_J^{1+}_B_D^{1+}_C_D^{1+}_T^{1+}_._A^{1+}_D^{1-}_U^{1+}

You will send this modified letter (the cipher text) string to your friend

$?^{2-}$_E_B^{2-}_H_O_J^{1+}_B_D^{1+}_C_D^{1+}_T^{1+}_._A^{1+}_D^{1-}_U^{1+}

Part II – DECRYPTION

Step 1: When your friend receives the cipher text, he/she will be required to convert the letter string to a numeral string using Table 1 as follows

2^{2-}_7_4^{2-}_10_17_12^{1+}_4_6^{1+}_5_6^{1+}_22^{1+}_1_3^{1+}_6^{1-}_23^{1+}

Step 2: Note that within this string of characters, some elements are different from others as these have superscripts. These are converted (fake) numerals which need to be reconverted to their original values.

Rule of conversion after cipher text has been received

r^{q+}	r^{q-}
• When the superscript is q+, he/she understands that the original numerals are greater than these converted numerals. • To retrieve these, he/she simply adds q times 28 to r. For example: $23^{1+} = 1.28 + 23 = 51$ Similarly, $22^{1+} = 50, 12^{1+} = 40, 6^{1+} = 34, 3^{1+} = 31$	• When the superscript is q^-, he/she understands that the original numerals are negative integers. • To retrieve these he/she adds q times 28 to r and further subtracts this result from 28. For example: $6^{1-} = 28 - (1.28 + 6) = 28 - 34 = -6$ Similarly, $4^{2-} = -32, 2^{2-} = -30$

Table 3

In this way, your friend converts the received letter string

$$\mathbf{?^{2-}\_E\_B^{2-}\_H\_O\_J^{1+}\_B\_D^{1+}\_C\_D^{1+}\_T^{1+}\_.\_A^{1+}\_D^{1-}\_U^{1+}}$$

$$-30\_7\_-32\_10\_17\_40\_4\_34\_5\_34\_50\_1\_31\_-6\_51$$

Step 3: It should be kept in mind that Matrix C was generated by pre-multiplication of M by K. For obtaining M, C needs to be pre multiplied by K^{-1}. In other words, C must be of order 3 by *m*. The elements of this string fit into a 3 by 5 matrix C and Matrix M is obtained.

$$M = (K)^{-1}C = \begin{bmatrix} 1/3 & 4/3 & -2/3 \\ 1/3 & 7/3 & -5/3 \\ -1/3 & 2/3 & -1/3 \end{bmatrix} \begin{bmatrix} -30 & 7 & -32 & 10 & 17 \\ 40 & 4 & 34 & 5 & 34 \\ 50 & 1 & 31 & -6 & 51 \end{bmatrix}$$

$$M = \begin{bmatrix} 10 & 7 & 14 & 14 & 17 \\ 0 & 10 & 17 & 25 & 0 \\ 20 & 0 & 23 & 2 & 0 \end{bmatrix}$$

Step 4: The final numeral string obtained from this matrix is

*10_7_14_14_17_0_10_17_25_0_20_0_23_2_*0

Using Table 1, the message is decrypted as:

HELLO HOW R U?

In the above example, we have pre-multiplied M by K. We can also generate the new matrix for ciphertext by post-multiplying M by K, i.e., C = MK. In that case, M will be of order 5 by 3.The reader is urged to try this as an exercise.

As Table1 has 29 values, we can also use 29 in place of 28 during the conversion process (Table 2 and Table 3). For convenience, we chose 28 as it is the largest numerical value which appears here, but it is not necessary. Any number can be chosen for this conversion. It will only change the ciphertext, not the final result. The number chosen for conversion (28, 29 or any other number) must be pre-known and private

between the sender and receiver. Here, apart from the key matrix (private) we have also involved a 'number' as our private element.

Points to be kept in mind:

i. The key matrix should be a non- singular matrix.

ii. The order of multiplying message matrix by key matrix, i.e., pre multiplication or post multiplication by key matrix must be pre decided between the sender and the receiver.

iii. If the elements (letters) of message are fewer than the number of elements of matrix M, then fill the vacant positions with '0'.

iv. Symbols of (+) and (−) in r^{q+} and r^{q-} respectively can be replaced by new ones which both sender and receiver can decide (denoting addition and subtraction respectively).

v. Larger sentences may be fragmented into groups of three letters such as **HEL, LOH, OWR, U?**. Each group may be treated as a 1 by 3 or 3 by 1 matrix, which may be multiplied with key matrix and then cipher matrix for each group may be obtained separately. In the same way inverse of each cipher matrix may also be obtained separately.

References

1. Ghosh, J. B. (2014, November). Hill Ciphers. *At Right Angles, 3*(3), pp. 60-67. http://www.teachersofindia.org/en/periodicals/right-angles-november-2014

2. Ghosh, J. B. (2015, November). Hill Ciphers. *At Right Angles, 4*(3). http://teachersofindia.org/en/ebook/hill-cipher-ii

KUMAR GANDHARV MISHRA is an independent researcher and practitioner in Mathematics Education. He has completed his Masters in Mathematics Education – M.Sc. (Mathematics Education) from Cluster Innovation Centre, University of Delhi. His research interests lies in Undergraduate Mathematics, Mathematics & Music, Social and Cultural aspects of Mathematics Education. He also writes on mathematics and mathematics education in popular newspapers and magazines. He can be reached at mishrakumargandharv@gmail.com.