Simple CRYPTOGRAPHY

MEGHRAJ BHATT

This is in reference to the articles [1], [2] and [3] published in At Right Angles. All of them explain clearly the basic mechanism of the science of cryptography for those who have studied Matrices and Modulo arithmetic. What about a student of secondary level?

To answer this question, let us try to develop a simple cryptogram which does not use matrix algebra but uses a simple linear function and a simplified version of modulo arithmetic. We need to prepare a table to convert the letters of the alphabet to numerals and vice-versa. We will use the same conversion table as used in [3]. It is as follows:

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

Table I

Now let us take a linear algebraic function, say $y = 2x + 3$ … (1).

The person who is sending the message in encrypted form and the person who has to decrypt the message must know the above table, the function given by (1) and the transformation rule (explained in step 3 ahead).

Now, let the message be: "**MATHEMATICS IS EASY.**"

Keywords: Cryptography, coding, encryption, functions

ENCRYPTION

Step 1

Replace all the letters in the message by the corresponding numbers from Table I. The space between the words will be replaced by 0 (zero) and full stop by 1. So, 'M' will be replaced by 15, 'A' by 3, 'T' by 22 and so on. We will insert '–' (dash) between two numbers to separate them. The whole message will be converted to:

15 – 3 – 22 – 10 – 7 – 15 – 3 – 22 – 11 – 5 – 21 – 0 – 11 – 21 – 0 – 7 – 3 – 21 – 27 – 1 … (2)

Step 2

Now, take these numbers as values of x in the function $y = 2x + 3$ and calculate the corresponding values of y, e.g. for x = 15, $y = 2(15) + 3 = 33$; for x=3, y = 9, etc. So the whole message in (2) will be converted into a new string of numbers (i.e. values of y) as follows: **33 – 9 – 47 – 23 – 17 – 33 – 9 – 47 – 25 – 13 – 45 – 3 – 25 – 45 – 3 – 17 – 9 – 45 – 57 – 5 … (3)**

Step 3: Transformation Rule

In string (3), we see that all the numbers are odd numbers (because of the nature of the function (1)). We also observe that there are two types of numbers: (a) less than or equal to 28 and (b) greater than 28.

(a) For numbers less than or equal to 28, we can use Table I directly; e. g. for the second number 9, we can replace it with G; we can replace 23 with U, etc.

(b) For numbers greater than 28, we will follow this rule: "If 'n' is the number ($n > 28$) find 'r' ($1 \le r \le 28$) such that $n = 28\ (p) + r$, $p \in N$ and replace 'n' by the letter corresponding to 'r' from Table I. But this letter will have superscript '$+p$' over it; e.g. (i) for the first number 33, we get 33 = 28(1) + 5; hence p = 1 and r = 5. Hence we will look in the table for 5 and we get 'C '. So in the encryption, we will replace 33 by C^{+1}. (ii) For the number 57, we get 57 = 28(2) + 1; hence, p = 2 , r =1 . Table shows '.' for 1 and so we will write '.$^{+2}$' for 57.

So, the **encrypted** script will be:

$C^{+1}\ G\ Q^{+1}\ U\ O\ C^{+1}\ G\ Q^{+1}\ W\ K\ O^{+1}$
$A\ W\ O^{+1}\ A\ O\ G\ O^{+1}\ .^{+2}\ C$ … (*A*)

We will send this text to the receiver.

DECRYPTION

The person receiving the above encrypted message must know

i. Table 1,

ii. The function and

iii. The transformation rule.

First of all, he has to find the inverse function of the function given in (1). It means that, for decryption, he has to use the function $x = \frac{y-3}{2}$ … (4)

Step 4: Transformation Rule (for decryption)

Let us observe the encrypted message carefully. It is made up of two types of letters:

(a) Simple letters like G, U, etc.

(b) Letters having a superscript of the type $+n$ namely, C^{+1}, Q^{+1}, etc.

We decrypt them as follows.

(a) For simple letters, we can use Table I directly to get the value of y; e.g. G = 9, U = 23, etc.

(b) For letters having a superscript $+n$ on it, go to the table and find the number and add $(28*n)$ to it to get the value of y; e.g. C^{+1}: from the table $C = 5$ and hence $y = 5 + 28(1) = 33$ or Q^{+1} : from the table $Q = 19$ and hence $y = 19 + 28(1) = 47$ and in particular, $.^{+2}$: from the table . = 1 and hence $y = 1 + 28(2) = 57$. This will give us any number greater than 28. Now

replace all letters by these numbers obtained by (a) or (b) and find a string of y values as follows:

33 – 9 – 47 – 23 – 17 – 33 – 9 – 47 – 25 – 13 – 45 – 3 – 25 – 45 – 3 – 17 – 9 – 45 – 57 – 5 … (5)

Step 5

The above string represents y. Now put these values of y in the function $\mathbf{x} = \frac{y-3}{2}$ and get the corresponding values of x. So the string of x values will be:

15 – 3 – 22 – 10 – 7 – 15 – 3 – 22 – 11 – 5 – 21 – 0 – 11 – 21 – 0 – 7 – 3 – 21 – 27 – 1 …(6)

Step 6

At the end, again use Table I and write the proper letter or space or symbol to decrypt and get the original message. It will read: MATHEMATICS IS EASY.

Closing remarks

Here are some points which may enhance the understanding of the procedure.

1. One can choose any linear function which is easy to invert and for which calculations become easy. We want to avoid negative numbers.
2. Table I may be changed to include more punctuation marks. We can even avoid coding all punctuation marks. In that case, they will not be encrypted and will be shown in the encrypted script as they are.
3. One can assign the numbers to letters in any random manner.
4. If the greatest number assigned is different from 28, one has to modify the encryption / decryption rules suitably.
5. If numerals are present in the original message, one has to extend the table and set some other trick for encryption. The simple way is to not encrypt the numerals!
6. The whole work provides exercises in algebra and students will enjoy doing it in a play way method.
7. A teacher can modify this according to his/ her requirement.

References

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

[3] Mishra, K.G. (2019, March), Addendum to Hill Ciphers, *At Right Angles*, pp 23-27.

MEGHRAJ J. BHATT is from Valsad, Gujarat. He taught Mathematics at Pre-University level for 35 years and is associated with Gujarat Ganit Mandal, The AMTI, AIMER. He is a text book writer for Gujarat state, who works to popularize Mathematics among students/parents and conducts workshops and seminars. He has a special interest in ancient Indian Mathematics. Mr. Bhatt may be contacted at mjbhatt9@yahoo.com