DISCRETE MATHEMATICS PROJECT

Assigned By : Professor Manish K. Gupta
Course : SC 205
DA-IICT
GANDHINAGAR

Made By:

UTPAL BUSA (202101193)
SMIT RUPAPARA (202101075)
HIMANSHU AMBANI (202101255)
KRUSHANG BHORANIYA (202101175)
PAL BHESDADIYA (202101261)

CRYPTOGRAPHY IN SECURE COMMUNICATION

STUDENTS OF DA-IICT,
GANDHINAGAR,
INDIA

June 29, 2022

Abstract

This model gives a brief introduction about how cryptography used in data transfer and communication.One such model We dicussed below,which is about communication between two person.

1 INTRODUCTION

In banks , industry and many other places they have to keep their data and information safe and confidential. And if they want to send their information or data to someone else and they want keep their data and information to be secure and private and no third party can read the message.So,this kind of problem can be solved using cryptography.

Here We will discuss about a secure communication problem.

2 A FORMAL STATEMENT OF THE PROBLEM [2]

Suppose, two person want to communicate each other but they want that their message should be safe and private and no one can read their message then they can do like below,

1. Do encryption: convert This plain text into ciphertext(data into a different form which is incomprehensible).

2. Do decryption: convert received ciphertext into plain text.

3 AN ANALYTICAL SOLUTION OF PROBLEM

Suppose, we want to send the message:

"DISCRETE MATHS".

Let's first encrypt this message :

First we denote numbers to each alphabet :
If it is space then take space = 0 ,
otherwise take it's ASCII value and minus 64, - - (1)
Like A = (ASCII value of A) – 64 = 65 – 64 = 1.

So, from above our message "DISCRETE MATHS" become :

" 4 9 19 3 18 5 20 5 0 13 1 20 8 19 " - - - (2)

Take our **public key n = 27** and private key as 2x2 matrix.

$$\textbf{private key} = \begin{bmatrix} 1 & 0 \\ 3 & 2 \end{bmatrix}$$

now, convert result-(2) in matrix whose column is 2.
So we get,

$$\mathbf{A} = \begin{bmatrix} 4 & 9 \\ 19 & 3 \\ 18 & 5 \\ 20 & 5 \\ 0 & 13 \\ 1 & 20 \\ 8 & 19 \end{bmatrix}$$

By multiply A with key, we get like this ,

$$\mathbf{A\ x\ key} = \begin{bmatrix} 4 & 9 \\ 19 & 3 \\ 18 & 5 \\ 20 & 5 \\ 0 & 13 \\ 1 & 20 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 3 & 2 \end{bmatrix}$$

$$\mathbf{A\ x\ key} = \begin{bmatrix} 31 & 18 \\ 28 & 6 \\ 33 & 10 \\ 35 & 10 \\ 39 & 26 \\ 61 & 40 \\ 65 & 38 \end{bmatrix}$$

Now, divide all numbers of this matrix with n so we get,

Reminder : 4 18 1 6 6 10 8 10 12 26 7 13 11 11

Quotient : 1 0 1 0 1 0 1 0 1 0 2 1 2 1.

Now, convert all the Reminders in alphabet using result-(1)

Like : 4 + 64 = 68 = D(ASCII value OF D = 68) so we get:

"DRAFFJHJLZGMKK" - - - (3)

Now, we use **playfair cipher [1]** to encrypt result-(3) and for that we create a 5x5 grid table of alphabets such that each of 25 alphabets must be unique and Y is omitted. The sender and the receiver decide a particular

key, say ‘ TUTORIALS ’. In a key table, the first characters are the phrase, excluding the duplicate letters.The rest of the table will be filled with the remaining letters of the alphabet, in natural order.
If text contains Y then keep Y as it is.
The key table works out to be-

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
J	K	M	N	P
Q	V	W	X	Z

First, message is split into pair of two letters.

“ DR AF FJ HJ LZ GM KK ”

If there are odd number of letters then Z is added to the last.

The rules of encryption :

1. If both the letters are in the same column,then take the letter below each one (going back to the top if at the bottom) and replace it.
Eg. AJ -> DQ.

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
J	K	M	N	P
Q	V	W	X	Z

2. If both letters are in the same row,then take the letter to the right of each one (going back to the left if at the farthest right) and replace it.
Eg. LC -> SA.

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
J	K	M	N	P
Q	V	W	X	Z

3. If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle and replace it.
Eg. LP -> CK.

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
J	K	M	N	P
Q	V	W	X	Z

4. If both letters are same then keep them as it is.
Eg. KK -> KK.

So, the final message is look like,

“ GT SD DM DP CV FN KK ” - - (4)

Send this above message(result-(4)) and quotient to the receiver.
Now decrypting the Playfair cipher is as simple as doing the same process in reverse order. Receiver has the same key so, he/she can create the same key table and then decrypt messages(result-(4)) using that key and rules.

After decrypting playfair cipher(result-(4)), receiver get this message " DRAFFJHJLZGMKK " and quotient.

First, convert this alphabet into numbers using result-(1).

We get,

4 18 1 6 6 10 8 10 12 26 7 13 11 11

Take multiplication of quotient's each number with n and add reminder in it. like below,

1st number we get is $Y1 = 27 \times 1 + 4 = 31$.
then $Y2 = 27 \times 0 + 18 = 18$.
Like this,$Y4 = 27 \times 0 + 6 = 6$.
upto $Y14 = 27 \times 1 + 11 = 38$.

So we get,

31 18 28 6 33 10 35 10 39 26 61 40 65 38.

Convert these numbers in matrix whose column is 2.

$$\mathbf{B} = \begin{bmatrix} 31 & 18 \\ 28 & 6 \\ 33 & 10 \\ 35 & 10 \\ 39 & 26 \\ 61 & 40 \\ 65 & 38 \end{bmatrix}$$

Now multiply B with key^{-1}
So, we get our original matrix.
Here,

$$\mathbf{key} = \begin{bmatrix} 1 & 0 \\ 3 & 2 \end{bmatrix}$$

So,

$$key^{-1} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ -3 & 1 \end{bmatrix}$$

Now,

$$\mathbf{Y} = B \times key^{-1}$$

$$\mathbf{Y} = \begin{bmatrix} 31 & 18 \\ 28 & 6 \\ 33 & 10 \\ 35 & 10 \\ 39 & 26 \\ 61 & 40 \\ 65 & 38 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 2 & 0 \\ -3 & 1 \end{bmatrix}$$

$$\mathbf{Y} = \begin{bmatrix} 4 & 9 \\ 19 & 3 \\ 18 & 5 \\ 20 & 5 \\ 0 & 13 \\ 1 & 20 \\ 8 & 19 \end{bmatrix}$$

Now convert Y's each number in alphabet.

So,we get : **"DISCRETE MATHS"**
This is our original message.

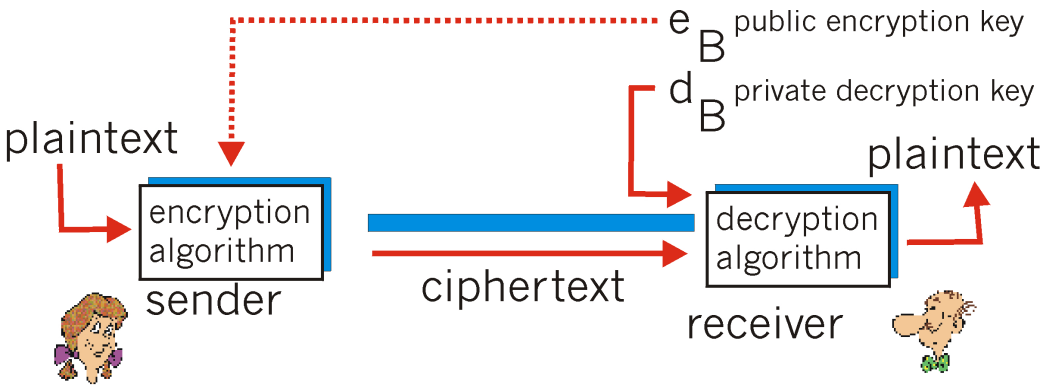

Figure 1: Process of encryption and decryption

So,we encrypt our message securely and decrypt using some particular method so that only receiver can read the message.

4 APPLICATION OF THIS MODEL [3]

This technique is helpful for communicating covertly since it allows the recipient to see the encrypted message in case someone is listening in but prevents them from understanding the actual message. It can only be read by the intended recipient.

There are many more benefits of this model which describes below :

[1]. This technique can be used almost exclusively in security related areas. It can limit only approved people to access secret data.

[2]. This technique can be used in Securely storing data on your computer, like your password keeper.

[3]. This technique can be used in financial, government, medical, software developer, even multiplayer games to secure data and information.

References

[1] tutorialspoint. URL: https://www.tutorialspoint.com/cryptography/traditional_ciphers.htm.

[2] Abdulaziz B.M.Hame and Ibrahim O.A. Albudawe. *Problem*. ajer, 2017. URL: http://ajer.org/papers/v6(06)/ZB0606212217.pdf.

[3] Paul M Watt. quora, 2018. URL: https://www.quora.com/Where-is-cryptography-typically-used.