

A Detailed Analysis on Encryption of Messages Using Cryptographic Model with Matrices

Kalluri Prasanthi

*III - B.TECH, CSE and Section - I, Vignan's Institute of Information Technology,
Visakhapatnam, India
kalluriprasanthi99@gmail.com*

Abstract

The simpler concept of Mathematics which helps to protect the data with methodology called Cryptography. In this a most simple form of Cryptography with matrices one can add a coding matrix for the coding matrix, and so on. With the more levels added, the more secure the message will be. In this a message is taken and encrypted it into a string of numbers via Matrix Multiplication. Then numbers at output are decrypted back into a written message by Inverse Matrix Multiplication.

Keywords: *Cryptography, Decryption, Encryption, Invertible matrix, Matrix multiplication*

1. Introduction

Cryptology is defined as “the science of making communication incomprehensible to everyone (i.e. making the communication Un-understandable to everyone) except to those who are having the authority to read it and understand it” [1]. Also it describes cryptography as “The Study Of Mathematical Methodology” which is with respect to securing the information as like the confidential information, data integrity, entry authenticating and data origin base authenticating Cryptography, the art of encrypting and decrypting, has a crucial role in different Cellular communications, like the e-commerce, sensitive passwords, pay-Bills, sending of emails, the ATM cards, privacy, transmission of fund, and the digital signatures [2]. Presently this symmetric cryptography and asymmetric cryptography are the two classifications in cryptography. In the symmetric cryptography, the sending person or the sender and the person on the other end i.e. receiver both of them shall be using one single key for encrypting and decrypting whereas in the asymmetric cryptography, there will be two randomly generated keys which are different are said to be used. These two cryptosystems have their own pros as well as cons. This study of cryptology contains two parts, as cryptography deals with the confidentiality in systems and their designing where as cryptanalysis is mainly concerned about how system privacy can be broken [3][4]. Majority of the concepts in this cryptography are applied widely in military wars, the secret agents. This area is having large - scale use of this cryptography. Some of the types of cryptography can also use hash functions to decrease complexity.

2. Mathematical modelling

Article history:

Received (January 8, 2020), Review Result (February 12, 2020), Accepted (April 1, 2020)

To encrypt any message (generally a plaintext), we break that message into definite set of consecutive letters to form a matrix (here we take a set of 3 consecutive letters) [5][6]. Now we convert these characters into appropriate numeric vectored value and multiply the key matrix with the numeric vectored matrix of characters made modulo with 27, (since we have 26 alphabets we make modulo with 27, so that modulo result lies in between 0-26) which results column matrices containing numeric values that get transformed into their corresponding characters (i.e. mapped into corresponding characters) to obtain the cipher text. For decrypting the cipher text into the form of plaintext or the original form, we use the same process as in done above as like above encrypting process along with the inverse of matrix in place of the actual matrix [7]. In [Figure.1], the architecture model considered or working model of the entire process had discussed and given in detail. The model gives us the idea that a plaintext was being sending from a sender to a receiver with encryption and the same plain text message is being decrypting at the receiver end. At first a plain text message is being sent from the sender to the receiver [8]. Then the cipher text key is being added to the encryption process and then the message is being received by the receiver. Thereafter at the receiver end, the message is being decrypted and the message with the plain text is being used by the actual user who is sitting r waiting at the receiver end of the application.

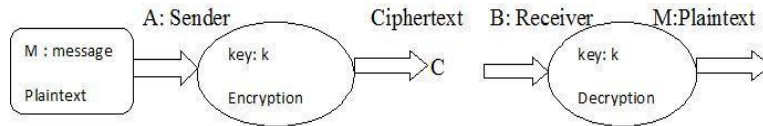


Figure 1. Proposed working model

Table 1. Illustrates English alphabets and their appropriate numerical value with “modulo 27”

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

$$a \times a^{-1} = 1 \pmod{m}$$

Table 2. Demonstration of inverse of those values made that modulo 27 satisfy

Number	2	4	5	7	8	10	11	13	14
Inverse	14	7	11	4	17	19	5	25	2
Number	16	17	19	20	22	23	25	26	
Inverse	22	8	10	23	16	20	13	26	

Now say we are having key matrix,

$$B = \begin{bmatrix} d11 & d12 & d13 \\ d21 & d22 & d23 \\ d31 & d32 & d33 \end{bmatrix}$$

where B is an Invertible Matrix which means that B^{-1} is also existing.

In this method of approach, the general message is splitted into 3 vector columns of characters. Now we multiply it with key matrix to obtain the Following linear system of expressions:

$$\begin{aligned}
 F1 &= P1d11 + P2d12 + P2d13 \\
 F2 &= P1d21 + P2d22 + P2d22 \\
 F3 &= P1d31 + P2d32 + P2d32
 \end{aligned} \tag{1}$$

We also get the expression for multiplication of these matrices:

$$\begin{bmatrix} E1 \\ E2 \\ E3 \end{bmatrix} = \begin{bmatrix} d11 & d12 & d13 \\ d21 & d22 & d23 \\ d31 & d32 & d33 \end{bmatrix} \begin{bmatrix} Q1 \\ Q2 \\ Q3 \end{bmatrix} = C = BP \tag{2}$$

where P and C are the column vector each having length three, which represent plain text and cipher text and B is a 3×3 matrix, that is already given to receiver and sender to decode while decryption.

We use the key matrix We use the key matrix as,

$$A = \begin{bmatrix} 2 & 5 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix}$$

Let the message we are encrypting be “HELP ME PLEASE”. So now let’s first initially break the plaintext (given message) into three consecutive letters and break the message as below:

“HEL” “P_M” “E_P” “LEA” “SE_”.

Now let’s convert each of the character into corresponding numerical vector values, as given below:

$$HEL = \begin{bmatrix} 8 \\ 5 \\ 12 \end{bmatrix},$$

$$P_M = \begin{bmatrix} 16 \\ 0 \\ 13 \end{bmatrix},$$

$$E_P = \begin{bmatrix} 5 \\ 0 \\ 16 \end{bmatrix}$$

$$LEA = \begin{bmatrix} 12 \\ 5 \\ 1 \end{bmatrix}$$

$$SE = \begin{bmatrix} 19 \\ 5 \\ 0 \end{bmatrix} \tag{3}$$

After multiplication of key matrix with column vectored matrix. Numerical vector value, which can be converted into appropriate cipher texts.

$$\begin{aligned}
 \begin{bmatrix} 2 & 5 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix} \begin{bmatrix} 19 \\ 5 \\ 0 \end{bmatrix} \text{mod}27 &\equiv \begin{bmatrix} 9 \\ 8 \\ 2 \end{bmatrix} = IHB \\
 \begin{bmatrix} 2 & 5 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix} \begin{bmatrix} 8 \\ 5 \\ 12 \end{bmatrix} \text{mod}27 &\equiv \begin{bmatrix} 23 \\ 26 \\ 23 \end{bmatrix} = WZC \\
 \begin{bmatrix} 2 & 5 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix} \begin{bmatrix} 5 \\ 5 \\ 16 \end{bmatrix} \text{mod}27 &\equiv \begin{bmatrix} 4 \\ 20 \\ 21 \end{bmatrix} = DTU
 \end{aligned} \tag{4}$$

Finally cipher text “WZCQTBTDUYPWIHB” is been decrypted into user understandable meaning full format “HELP ME PLEASE”, by using the inverse of the key matrices [7][8].

3. Simulation results

In order to verify the performance of the considered model with assumptions and expectations, the simulation had been conducted for the analysis and for the better understanding of the model. The detailed working mechanism had discussed and shown in the following figures as follows,

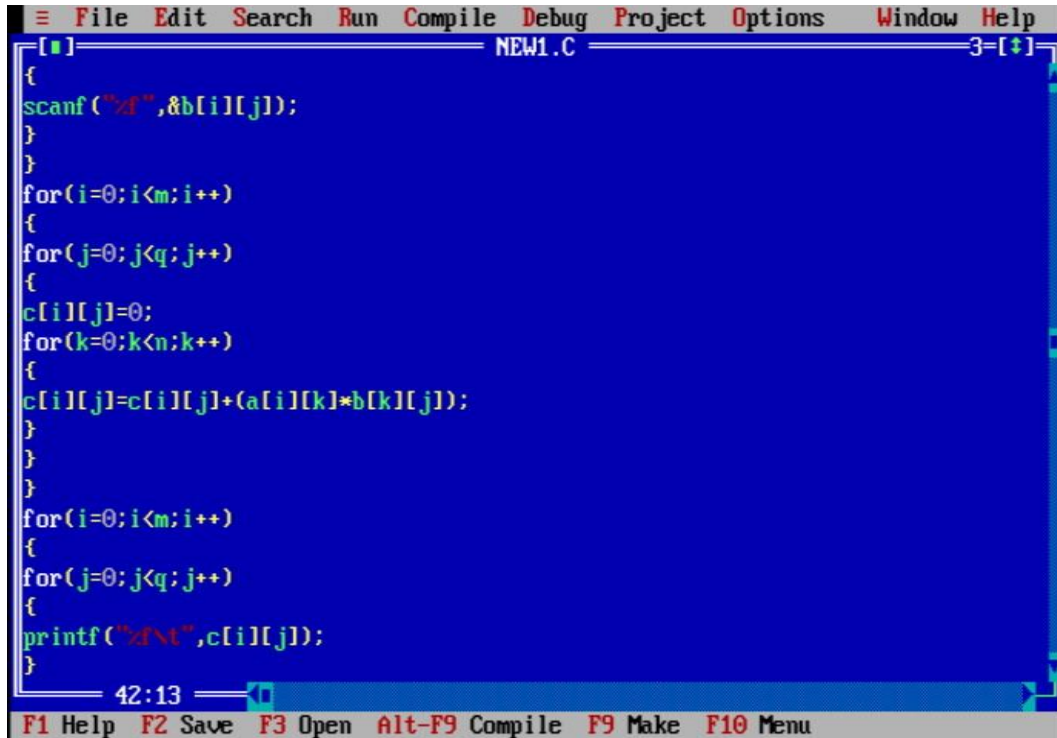
```

≡ File Edit Search Run Compile Debug Project Options Window Help
NEW1.C 3=1+
#include<stdio.h>
#include<conio.h>
void main()
{
float a[5][5],b[5][5],c[5][5];
int i,j,k,n,m,q,p;
clrscr();
printf("enter the no of rows and columns in matrix a,b\n");
scanf("%d%d%d", &m, &n, &p, &q);
printf("enter the values of matrix a\n");
for(i=0; i<m; i++)
{
for(j=0; j<n; j++)
{
scanf("%f", &a[i][j]);
}
}
printf("enter the values of b matrix\n");
for(i=0; i<p; i++)
{
for(j=0; j<q; j++)

```

Figure 2. Multiplication of data matrix and key matrix

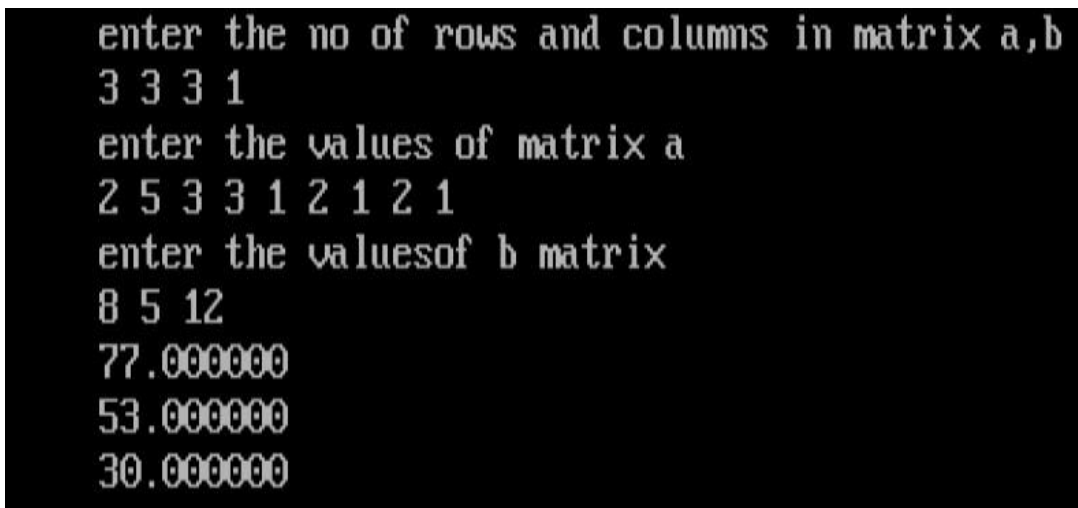
In the above [Figure 2], it is observed that the multiplication of data matrix with the key matrix was shown in detail in the program written and been shown above.



```
File Edit Search Run Compile Debug Project Options Window Help
NEW1.C
{
scanf("%d",&b[i][j]);
}
}
for(i=0;i<m;i++)
{
for(j=0;j<q;j++)
{
c[i][j]=0;
for(k=0;k<n;k++)
{
c[i][j]=c[i][j]+(a[i][k]*b[k][j]);
}
}
}
for(i=0;i<m;i++)
{
for(j=0;j<q;j++)
{
printf("%f\n",c[i][j]);
}
}
42:13
F1 Help F2 Save F3 Open Alt-F9 Compile F9 Make F10 Menu
```

Figure 3. Multiplication of data matrix and key matrix

In the above [Figure 3], it is observed that the multiplication of data matrix with the key matrix was shown in detail in the program written and been shown above is being continued from the next image.



```
enter the no of rows and columns in matrix a,b
3 3 3 1
enter the values of matrix a
2 5 3 3 1 2 1 2 1
enter the values of b matrix
8 5 12
77.000000
53.000000
30.000000
```

Figure 4. Encoded matrix

The details about the matrix values and the details about the rows and columns of the matrix and the details were being selected and given in detail in the above [Figure 4]. The values were

being calculated and were observed as output forms the calculation of the matrix was being generated and can be observed clearly in the above [Figure 4].

```

int mat[3][3],i,j;
float det=0;
clrscr();
printf("enter the elements of matrix\n");
for(i=0;i<3;i++)
{
for(j=0;j<3;j++)
scanf("%d",&mat[i][j]);
}
for(i=0;i<3;i++)
det=det+(mat[0][i]*(mat[1][(i+1)%3]*mat[2][(i+2)%3]-mat[1][(i+2)%3]*mat[2][(i+
printf("determinant-%f\n",det);
printf("\ninverse of t he  matrix is:\n");
for(i=0;i<3;i++)
{
for(j=0;j<3;j++)
printf("%.2f\t",((mat[(j+1)%3][(i+1)%3]*mat[(j+2)%3][(i+2)%3])-(mat[(j+1)%3][(
printf("\n");
}
}
getch();
}
    
```

Figure 5. Finding the inverse of key matrix

In the above [Figure 5], the inverse of the key matrix considered above was being generated and the programming written for such calculation can be shown or can be observed clearly in the above [Figure 5].

```

enter the elements of matrix
2 5 3 3 1 2 1 2 1
determinant-4.000000

inverse of t he  matrix is:
-0.75  0.25  1.75
-0.25  -0.25  1.25
1.25   0.25  -3.25
    
```

Figure 6. Key matrix after inversion

The inversion of the key value must be done such that to identify or to calculate the product value or the detailed values for the cipher text. The value which was being considered and the value being calculated had been discussed and shown clearly in the above [Figure 6].

```
enter the no of rows and columns in matrix a,b
3 3 3 1
enter the values of matrix a
-.75 .25 1.75 -.25 -.25 1.25 1.25 .25 -3.25
enter the values of b matrix
77 53 30
8.000000
5.000000
12.000000
```

Figure 7. Result after multiplying inverted key matrix and cipher text to get the decoded message

In the above text image, it is shown that the result that was being generated and being calculated after following the process and being calculated was the multiplication of inverted key matrix and the cipher text being used and being generated and also the decoded final message after receiving to the receiver can also be shown or noted at the above [Figure 7].

4. Results

In the current work, we have utilized some matrices as keys that are invertible keys by using inverse method, which introduce Hill Cipher order of encrypting and decrypting messages. There are mathematical relations that are logically executed for making the information's and data secured from their partners. Here we can observe that we initially took a message encoded that to numeric values and gave that as input to the program to multiply with key matrix. The output is given as input for multiplying with invertible matrix to decrypt to the original message

5. Conclusion

This study introduces cryptography with messages by using non singular matrices which have keys made modulo with 27, which is already made available to both Receiver i.e. the ally and sender. However, some techniques in mathematics are applied to the positive as well as the negative numeric values equivalent to appropriate character in English alphabets is obtained.

Using 2×2 and 3×3 matrices we had already coded and decoded the messages using invertible matrices making modulo 27. Time being, security to data is obtained by using above method and the message and data of information could be sent and received safely.

Messages and this text cannot be decrypted without having key matrix and the congruency relations.

References

- [1] Neha Sharma and Sachin Chirgaiya, "A novel approach to hill cipher", International Journal of Computer Applications, vol.108, no.11, pp.34-37, (2014)
- [2] Wissam Raji, "An introductory course in elementary number theory," Publisher Saylor Foundation, (2016)
- [3] Muhammad Donni Lesmana Siahaan et. al., "Application of hill cipher algorithm in securing text messages," International Journal of Innovative Research in Advanced Engineering, vol.12, no.2, pp.13-18, (2018) DOI: 10.31227/osf.io/n2kdb
- [4] P. Shanmugam and C. Loganathan, "Involuntary matrix in cryptography", IJRR, vol.6, no.4, March,

- pp.10-16, **(2011)**
- [5] Salman A. Khan, "Design and analysis of playfair ciphers with different matrix sizes," International Journal of Computing and Network Technology, vol.3, no.3, pp.117-123, **(2015)** DOI: <http://dx.doi.org/10.12785/IJCNT/030305>
 - [6] Dr. JyotiShinde et. Al., "A method for encryption and decryption of large messages by using matrices," International Journal of Latest Engineering Research and Applications, vol.2, pp.61-66, **(2017)**
 - [7] K Thiagarajan et. Al., "Encryption and decryption algorithm using algebraic matrix approach," National Conference on Mathematical Techniques and its Applications, pp.1-7, **(2018)**
 - [8] Sani Isa and Abdulaziz B. M. Hamed, "Cryptography using congruence modulo relations", American Journal of Engineering Research, vol.6, no.3, pp.156-160, **(2016)**