Journal of Physics: Conference Series

Encryption and decryption algorithm using algebraic matrix approach

IOP Conf. Series: Journal of Physics: Conf. Series **1000** (2018) 012148 doi:10.1088/1742-6596/1000/1/012148

Encryption and decryption algorithm using algebraic matrix approach

K Thiagarajan[1*], P Balasubramanian[2], J Nagaraj[3], J Padmashree[4]

[1] Department of Mathematics, P.S.N.A. College of Engineering and Technology, Dindigul, Tamilnadu, India.
[2] Department of Mathematics, Bharathiar University, Coimbatore, Tamilnadu, India
[3] Department of Applied Mathematics & Computational Sciences, PSG College of Technology, Coimbatore, Tamilnadu, India.
[4]Department of Mathematics, Research Scholar, Bharathiar University, Coimbatore, Tamilnadu, India.

vidhyamannan@yahoo.com

Abstract. Cryptographic algorithms provide security of data against attacks during encryption and decryption. However, they are computationally intensive process which consume large amount of CPU time and space at time of encryption and decryption. The goal of this paper is to study the encryption and decryption algorithm and to find space complexity of the encrypted and decrypted data by using of algorithm. In this paper, we encrypt and decrypt the message using key with the help of cyclic square matrix provides the approach applicable for any number of words having more number of characters and longest word. Also we discussed about the time complexity of the algorithm. The proposed algorithm is simple but difficult to break the process.

1. Introduction

In network security, cryptography has a long history by provides a way to store confidential information or send it to recipient across insecure networks (i.e. the Internet) so that transmitted information cannot be viewed or read by anyone except the intended sender and receiver, where the cryptosystem is a set of algorithms applied with secured secret keys to convert the original message to encrypted message and convert it back in the intended recipient side to the original message [1]. The first model proposed by Shannon on the cryptosystem is shown in figure 1 [2].

In computer systems, the algorithm consists set of complex mathematical formulas that indictate the rules of conversion of plain text to cipher text and vice versa combined with the secured key. However, algorithmic procedure for encryption and decryption use the same key (i.e. sender, and receiver). And in other encryption and decryption algorithms they use different keys which must be related. The major issue is to design any algorithmic procedure for encryption and decryption to improve the secure level. Therefore, this paper aims to propose a new algorithm to improve the secure level and increase the performance by minimizing a significant amount of delay time to maintain the security of the information [3].

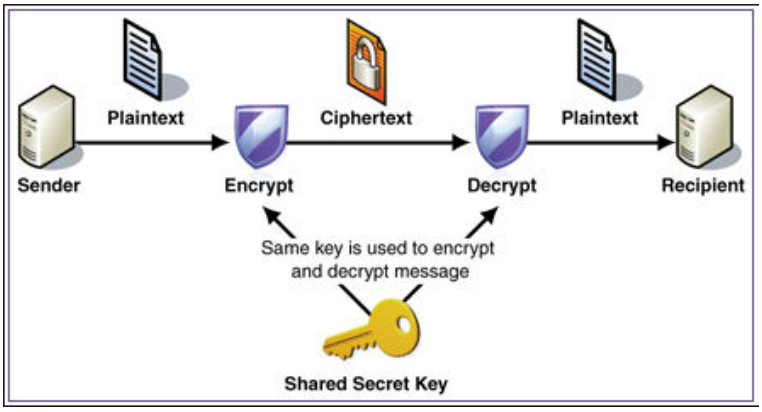

Figure 1: Cryptosystem

This paper is structured as follows: Proposed Algorithm, Basics of Applying algorithm and Encryption and Decryption is done to one of the longest word using the proposed algorithm and conclusion.

2. Proposed Algorithm to Encrypt and Decrypt message

2.1. Steps to Encrypt the message :

1. Assign the value of alphabets as A =-1, B =-2, ..., M =-13 and N=13, O=12, ..., Z=1.
2. Get the message for Encryption. Let the message be $W_1, W_2, ..., W_n$ where n is a number of words in the message.
3. Use Step 1, assign each character in $W_1, W_2, ..., W_n$ to digits separated by spaces between characters and words.
4. Draw Cyclic Square Matrix with characters in W_i for each i =1, 2, ... n
5. Calculate the number of characters in a word, $\eta(W_i)$ for each i =1, 2, ..., n
6. Calculate $E(\eta(W_i)) = \begin{cases} k_i = \frac{j+1}{2} \text{ if } \eta(W_i) = j \text{ is odd}, k = 1,2,...n \ \& \ i, j = 1,2,.. \\ k_i = \frac{j}{2} \text{ if } \eta(W_i) = j \text{ is even}, k = 1,2,...n \ \& \ i, j = 1,2,.. \end{cases}$
7. Choose k_i^{th} (i =1, 2, ..., n) column along the word W_i
8. Set $A_m = (a_{ij})$, i=1 and j, m =1, 2, ..., $\eta(W_i)$
9. Construct diagonal matrix, $D(A_m)$, m = 1, 2, ..., i with A_m values along diagonals and find $D(A_m) - \eta(W_i)I_{\eta(Wi)}$ for all i =1, 2, ..., n and m = 1, 2, ..., i
10. The key is $D(A_m) - \eta(W_i) I_{\eta(Wi))}$ for all i =1, 2, ..., n and m = 1, 2, ..., i separated by commas.

2.2. Steps to Decrypt the message :

1. Get the decryption key $D(A_m) - \eta(W_i) I_{\eta(Wi))}$ for all i =1, 2, ..., n and m = 1, 2, ..., i separated by commas.
2. Assign $B_i = D(A_m) - \eta(W_i) I_{\eta(Wi))}$ for all i =1, 2, ..., n and m = 1, 2, ..., i
3. Compute $E(\eta(B_i)) = \begin{cases} k_i = \frac{j+1}{2} \text{ if } \eta(B_i) = j \text{ is odd}, k = 1,2,...,n \ \& \ i, j = 1,2,.. \\ k_i = \frac{j}{2} \text{ if } \eta(B_i) = j \text{ is even}, k = 1,2,...,n \ \& \ i, j = 1,2,.. \end{cases}$ $C_i = D(B_i) + \eta(B_i) I_{\eta(Bi))}$ for all i =1, 2, ..., n
4. Compute

The value k_i implies the first digit of B_i is the k_i^{th} character of the i^{th} word of the decryption key.

5. Align C_i , i = 1, 2, ... , n in cyclic order along the value k_i^{th} order and rephrase to the order from 1^{st} to i^{th} digits.
6. Use Step 1 in the Encryption algorithm and assign digits to each character.
7. The decrypted value is obtained.

3. Preliminaries

Associate each number to each alphabets as mentioned below,

A	B	C	D	E	F	G	H	I	J	K	L	M
-1	-2	-3	-4	-5	-6	-7	-8	-9	-10	-11	-12	-13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	12	11	10	9	8	7	6	5	4	3	2	1

3.1. Basics :

Consider the message: **GOOD MORNING**

3.1.1. Encryption:

Word 1 (W_1) **Word 2 (W_2)**

G O O D M O R N I N G

-7 12 12 -4 -13 12 9 13 -9 13 -7

Now frame the cyclic square matrix for both Word 1 and Word 2 as below,

W_1

-7	12	12	-4
12	12	-4	-7
12	-4	-7	12
-4	-7	12	12

W_2

-13	12	9	13	-9	13	-7
12	9	13	-9	13	-7	-13
9	13	-9	13	-7	-13	12
13	-9	13	-7	-13	12	9
-9	13	-7	-13	12	9	13
13	-7	-13	12	9	13	-9
-7	-13	12	9	13	-9	13

Then for W_1 and W_2, $\eta(W_1) = 4$, $E(\eta(W_1)) = 4/2 = 2$ and $\eta(W_2) = 7$, $E(\eta(W_2)) = (7+1)/2 = 4$

$E(\eta(W_1)) = 2$ implies that 2^{nd} column values along the word W_1

$E(\eta(W_2)) = 4$ implies that 4^{th} column values along the word W_2

So, assign each columns values as matrices to A_1 and A_2.

Thus A_1 = (12 12 -4 -7) and A_2 = (13 -9 13 -7 -13 12 9)

Compute $D(A_1) - 4I_4 = D(8\ 8\ -8\ 11)$ and $D(A_2) - 7I_7 = D(6\ -16\ 6\ -14\ -20\ 5\ 2)$

where $D(A_1)$ and $D(A_2)$ are diagonal matrices with values of $A_1$and A_2 along diagonal in the matrices respectively.

Hence the encrypted key is **8 8 -8 11 , 6 -16 6 -14 -20 5 2**

3.1.2. Decryption:

The encrypted Key is **8 8 -8 11 , 6 -16 6 -14 -20 5 2** (Seperated by comma are words.)

And on split up, B_1= 8 8 -8 11 and B_2= 6 -16 6 -14 -20 5 2

Compute,

$C_1 = D(B_1)+4I_4 = D(12\ 12\ -4\ -7)$ and

$C_2 = D(B_2)+7I_7 = D(13\ -9\ 13\ -7\ -13\ 12\ 9)$

Then $\eta(B_1) = 4$, $E(\eta(B_1)) = 4/2 = 2$ and $\eta(B_2) = 7$, $E(\eta(B_2)) = (7+1)/2 = 4$

Thus $\eta(B_1) = 2$ implies that the first digit of B_1 is the 2^{nd} character of the first word of the decrypted key and $\eta(B_2) = 4$ implies that the first digitof B_2 is the 4^{th} character of the second word of the decrypted key.

Let C_1= 12 12 -4 -7

2^{nd} 3^{rd} 4^{th} 1^{st}

Rephrasing to the order from 1^{st} to 4^{th} , -7 12 12 -4 which is **GOOD**

Let C_2= 13 -9 13 -7 -13 12 9

4^{th} 5^{th} 6^{th} 7^{th} 1^{st} 2^{nd} 3^{rd}

Rephrasing to the order from 1^{st} to 7^{th} , -13 12 9 13 -9 13 -7 which is MORNING.

4. Encryption and Decryption of the longest word:

One of the longest word containing 45 character in the English language is PNEUMONOULTRAMICROSCOPICSILICOVOLCANOCONIOSIS

4.1. Applying Algorithm to the longest word :

4.1.1. Encryption :.

1. Assign W_1 as PNEUMONOULTRAMICROSCOPICSILICOVOLCANOCONIOSIS
2. Assign each character to digits,

P	N	E	U	M	O	N	O	U	L
11	13	-5	6	-13	12	13	12	6	-12
T	R	A	M	I	C	R	O	S	C
7	9	-1	-13	-9	-3	9	12	8	-3
O	P	I	C	S	I	L	I	C	O
12	11	-9	-3	8	-9	-12	-9	-3	12
V	O	L	C	A	N	O	C	O	N
5	12	-12	-3	-1	13	12	-3	12	13
I	O	S	I	S					
-9	12	8	-9	8					

3. Form Cycle Square Matrix: (45×45) [see Appendix 1(a) and 1(b)]

4. Then for W_1, $\eta(W_1) = 45$, $E(\eta(W_1)) = (45+1)/2 = 23$
5. Thus $E(\eta(W_1)) = 23$ implies the 23^{nd} column values along the word W_1[See appendix 1(a)].
6. Let $A_1 = (a_{ij})$, i = 23, j =1, 2, ..., 45
7. Compute $D(A_1) - 45I_{45}$ =D(-54-48-37-54-57-54-48-33-40-33-57-48-46-32-33-48-33-32-54-33-37 -54-37-34-32-50-39-58-33-32-33-39-57-38-36-46-58-54-48-36-33-37-48-33-34)
8. The encrypted key is -54-48-37-54-57-54-48-33-40-33-57-48-46-32-33-48-33-32-54-33-37-54-37 -34-32-50-39-58-33-32-33-39-57-38-36-46-58-54-48-36-33-37-48-33-34

4.1.2. Decryption :

1. Let $B_1 = D(A_1) - 45I_{45}$ = -54-48-37-54-57-54-48-33-40-33-57-48-46-32-33-48-33-32-54-33-37-54 -37-34-32-50-39-58-33-32-33-39-57-38-36-46-58-54-48-36-33-37-48-33-34
2. Compute $C_1 = D(B_1) + 45\ I_{45}$ = -9 -3 8 -9 -12 -9 -3 12 5 12 -12 -3 -1 13 12 -3 12 13 -9 12 8 -9 8 11 13 -5 6 -13 12 13 12 6 -12 7 9 -1 -13 -9 -3 9 12 8 -3 12 11
3. $E(\eta(B_1)) = 23$ implies that the 23^{nd} column values along the word W_1
4. Thus C_1 = 11 13 -5 6 -13 12 13 12 6 -12 7 9 -1 -13 -9 -3 9 12 8 -3 12 11 -9 -3 8 -9 -12 -9 -3 12 5 12 -12 -3 -1 13 12 -3 12 13 -9 12 8 -9 8

Hence The Message is PNEUMONOULTRAMICROSCOPICSILICOVOLCANOCONIOSIS

5. Time Complexity of the Algorithm:

There are three major components of the proposed algorithm are framing Cycle Square Matrix, Addition, Multiplicaton and Subtraction. The proposed encryption and decryption algorithm is simple, easy and comfortable to be used by all range of target users. For checking of complexity of time, the application was tested with longest word "PNEUMONOULTRAMICROSCOPICSILICOVOLCAN-OCONIOSIS" and the performance of the algorithm was rated by computing the time required for encryption and decryption of the word. Time Complexity of the proposed algorithm depends on the framing Cycle Square Matrix, Addition and Subtraction. Considering the number of character in the word as 'N'. On finding the cycle square matrix, it requires $\boldsymbol{O}(N^2)$. On adding or subtraction the matrix with n^2 values requires $\boldsymbol{O}(N^2)$. Thus overall time complexity of the key generation algorithm will be $\boldsymbol{O}(N^2)$. Also, the reliability of the algorithm was examined by the success rate of encryption and decryption. A successful execution means an encrypted word is understood by others; also successful execution means a decrypted file was obtained using a key and an encrypted file.

6. Conclusion:

In this paper, we have proposed an efficient data encryption and data decryption algorithm to protect the message with the help of key passed between Sender and Receiver. Also Message with any number of words having any number of character can be encrypt and decrypt by Sender and Receiver. With data encryption, data owner can utilize the benefits of Message splitting to number of words such that to reduce storage and computational overheads. The encryption and decryption algorithms developed and described in this paper might not be comparable to well-known encryption algorithms but its simplicity and availability proves that tools can be developed without resorting to purchasing expensive software from the market.

Acknowledgements

The authors would like to pay special thankfulness to Dr. Ponnammal Natarajan, Former Director – Research and Development, Anna University- Chennai, India who supported us to make this research article in successful manner and her constant motivation & encourage us to cherish our goal.

Appendix

1. The first (45× 23) and second(45× 22) diagram indicates the cyclic square matrices of 45× 45.

a. 45× 23

b. 45× 22

a.

11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9
13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3
-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8
6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9
-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12
12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9
13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3
12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12
6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5
-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12
7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12
9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3
-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1
-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13
-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12
-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3
9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12
12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13
8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9
-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12
12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8
11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9
-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8
-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11
8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13
-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5
-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6
-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13
-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12
12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13
5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12
12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6
-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12
-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7
-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9
13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1
12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13
-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9
12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3
13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9
-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12
12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8
8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3
-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12
8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11

b.

-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8
8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11
-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13
-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5
-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6
-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13
12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12
5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13
12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12
-12	-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6
-3	-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12
-1	13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7
13	12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9
12	-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1
-3	12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13
12	13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9
13	-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3
-9	12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9
12	8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12
8	-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8
-9	8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3
8	11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12
11	13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11
13	-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9
-5	6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3
6	-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8
-13	12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9
12	13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12
13	12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9
12	6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3
6	-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12
-12	7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5
7	9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12
9	-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12
-1	-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3
-13	-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1
-9	-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13
-3	9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12
9	12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3
12	8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12
8	-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13
-3	12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9
12	11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12
11	-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8
-9	-3	8	-9	-12	-9	-3	12	5	12	-12	-3	-1	13	12	-3	12	13	-9	12	8	-9

References

[1] P. Zimmerman, "An Introduction to Cryptography", Doubleday & Company, Inc., United State of America, USA, 1999.

[2] C. Shannon, “Communication Theory of Secrecy Systems”, Bell Systems Technical Journal, MD Computing, vol. 15, pp. 57-64, 1998.

[3] H. Mohan, and R. Raji. "Performance Analysis of AES and MARS Encryption Algorithms". International Journal of Computer Science Issues (IJCSI), Vol. 8, issue 4. 2011.