IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN APPROACH TO MESSAGE ENCRYPTION AND DECRYPTION USING PASCAL'S TRAINGLE

[1]S. Uma, [2*] Dr. K. Rajendran, [3] Mr. P. Mohan,

[1] M.Phil. Scholar, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), India

[2*] Associate Professor, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), India.

[3] Assistant Professor, Department of Mathematics, SRM Arts and Science College, Kattankulathur, Tamilnadu.

ABSTRACT:

Nowadays message encryption techniques are the most necessary to impervious our message and information, encryption techniques are hastily multiplied presently through the growing utilization of internet and web communications. Sharing important data, personal messages from one character to another over an unsecured channel is made a way for attacking, or hacking the information. In order to eliminate this terminology and to provide efficient security, the cryptographic methods are performing the most important vital role. We have many kinds of symmetric encryption techniques like Caesar, Atbash, Playfair, Hill Ciphers, etc. In this paper we are implementing the new enciphering technique for message encryption and decryption using Pascal's triangles to provide more security and resist against stealing the information, it is a simple and easy symmetric encryption technique for both encryption and decryption.

1. Introduction

Cryptography is one of the mathematical strategies which are used to shield our messages, information's, pictures, files from hackers and it facilitates us to growth the safety of the information transfers, cryptography is the take a look at or the method of changing simple texts or messages into an unreadable disguised format in order that the intentional recipients can do away with the hidden form or conceal and examine the authentic message the intermediates doesn't identify. The message we had is known as simple textual content or plaintext and the disguised message is what known as the encrypted textual content or ciphertext content. The simple textual contents and cipher text content each are written in the form of alphabets, each aren't even identical alphabets. In certain cases, the letters or the messages are written within the form of a few unique characters like punctuation marks, numerals and blanks or other unique characters which might be agreed through each the sender and receiver.

If we accomplish that, we will be capable of lessening the opportunity of stealing or hacking. The method of changing a plaintext or authentic message into an unreadable shape, ciphertext is known as enciphering or encryption, and the opposite method this is the method of changing ciphertext into plaintext is known as decoding or decryption. The transformation from plaintext into ciphertext is a characteristic or it's miles a map h from the set M the set of all feasible plaintext message units to the set C of all feasible ciphertext messages, we recognize that this characteristic h is one to one that is, for a given ciphertext message unit there's one and only one plaintext message unit and vice versa.

In cryptography, a key is the variable or the parameter that assists us to transform the given plain textual content messages into cipher textual content messages and vice versa. The length of the key or the hardness of the computing key defines how hard the method of decrypting the plaintext content in authentic message. There are two kinds of cryptography we've they're symmetric key cryptography or personal key cryptography (each the sender and receiver need to use the identical key) and asymmetric key cryptography or public key cryptography (Two distinctive keys are used one is personal key for both and another one is a public key).

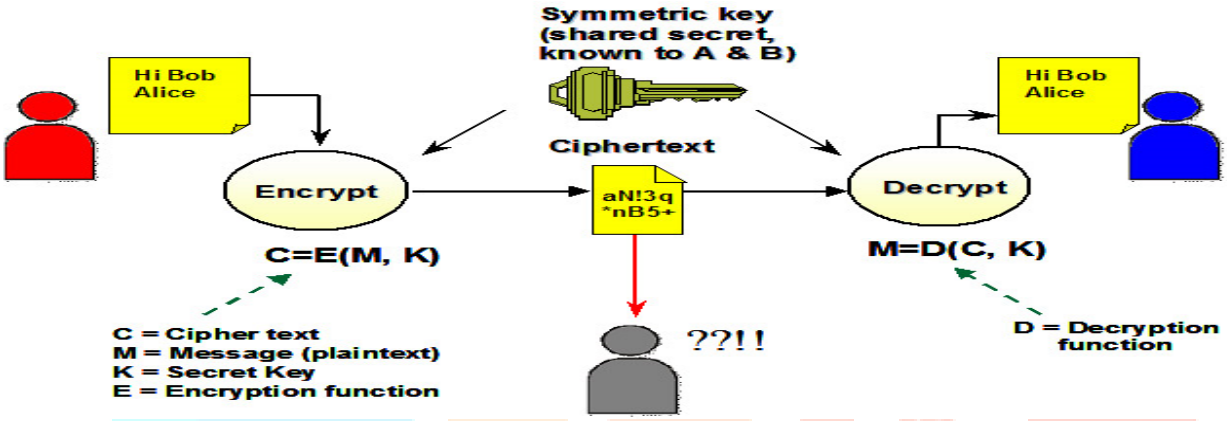

Figure 1.0. Symmetric Cryptosystem

In cryptography, maximum of the symmetric encryption techniques like Caesar cipher, Atbash cipher, etc, are makes use of the easy and equal key for encryption and decryption, it's far too clean to interrupt as soon as the intermediates understand the approach or the uses frequency analysis, this means that the hackers or intermediates can effortlessly discover the unique message with the assist of maximum happening letters withinside the given format, In order to reduce this and deliver greater safety we've proposed the new enciphering approach in this article that uses of Pascal's triangle.

A new method that has been proposed in this paper is made up with the aid of using an acting encryption method and with the use of Pascal triangle to reinforce the safety and convey a new and easy method. This new method doesn't require any key for encryption or decryption. All we need is to recognize the shape of Pascal's triangle and a few simple terminologies of encryption and decryption like changing the given alphabets into their numerical equal values, addition modulo, etc.

The new approach is made by firstly the sender should convert given message units into values and formed it as a triangle form, then the given number units are added with the number units in the Pascal's triangle, taking addition modulo we will get the cipher text and then this ciphertext will send to the receiver and the receiver should use the reversing procedure of this then the receiver is able to identify the original message. The relaxation of this paper is described as follows: an advent to Pascal's Triangle is supplied in Section 2. Given alphabets and their numerical equivalent values become brought in Section 3. Section 4 explains the new proposed approach, in Section 5 the implementation instance might be given. Security evaluation might be given in Section 6. Finally, the Conclusion was given in Section 7.

2. Pascal's Triangle

It is the triangular array of the binomial coefficients; it is a triangle wherein each row has one greater element than the preceding row, every and each row starts and ends with 1. Starting with an countless infinite row of zeros and a unique one in the middle (…, 0, 0, 0, 1, 0, 0, 0, …), new row of numbers are constructed by adding the two numbers above it (0+1 =1, 1+0 = 1, that's the subsequent row entries), similarly the other rows also. Pascal triangle is the set of non-zero numbers that is shown below

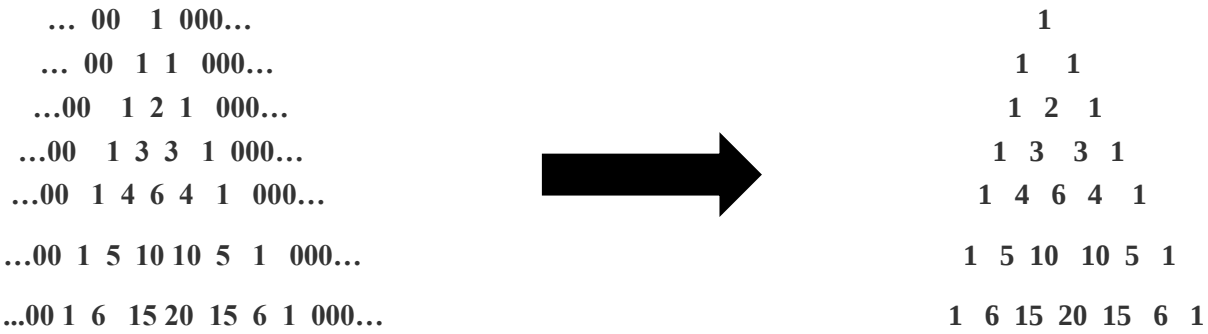

Figure 2.0 Pascal's triangle

3. Alphabets and their numerical equivalent values.

In cryptography, every alphabet can be changed into their numerical equivalent values as numbers for performing arithmetic operations (basically modular arithmetic) in order to perform encryption and decryption. Mathematically we can define if we have alphabets A to Z with labeling their numerical equivalent values 0-25 that is $A \to 0, B \to 1, \dots, Z \to 25$ and blank as 26 which is shown in the below table.

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

Table1.0. Alphabets and their numerical equivalent values.

4. The proposed cryptosystem

The proposed approach of encryption using Pascal's triangle has been introduced in this section. Suppose the sender (User A) wants to send a message to the receiver (User B) over an insecure channel:

Initially, they should agree on Pascal's triangle and use the following procedure; The sender should convert given message units into their numerical equivalent values with the help of Table 1.0 and then the converted message units are now formed in the form of triangle format (it equivalent to Pascal's triangle structure) then the given number units are added with the number units in the Pascal's triangle, finally the resultant number we can perform addition modulo 26 (since there are 26 alphabets in Table 1.0). after taking addition modulo 26 we can convert their numerical equivalent values and then this ciphertext will be send to the receiver over any kind of unsecured channel. If necessary, we can add some dummy letters or blanks at the end.

Decryption is done by reversing the process of the encryption, the receiver should convert the received cipher text message units into their numerical equivalent values using Table 1.0 and then converts it in the form of triangle then subtract the given triangle shaped value with original Pascal's triangle values and take addition modulo 26 then the resultant numbers are now converted into their numerical equivalent values with the help of Table 1.0, then the receiver is now able to read the original message.

5. Implementation Example

Assume that User A (the sender) wants to send a message "MEET YOU AT TODAY MORNING" to User B (the receiver) using Pascal's triangle encryption technique. That is the procedure of encryption using Pascal's triangle which was introduced in Section 4.

Encryption - User A (The sender): Encryption is done by the following five steps.

Step1: First the sender should convert the given message units "MEET YOU AT TODAY MORNING" into their numerical equivalent values with the help of Table 1.0 i.e., $M \to 12, E \to 4, E \to 4, T \to 19, Y \to 24, O \to 14, U \to 20, A \to 0, T \to 19, T \to 19, O \to 14, D \to 3, A \to 0, Y \to 24, M \to 12, O \to 14, R \to 17, N \to 13, I \to 8, N \to 13, G \to 6.$

"MEET YOU AT TODAY MORNING" → "12 4 4 19 24 14 20 0 19 19 14 3 0 24 12 14 17 13 8 13 6"

Step2: The above numbers are now converted in the form of triangle that is, in the form of Pascal's Triangle format

12

4 4

19 24 14

20 0 19 19

14 3 0 24 12

14 17 13 8 13 6

Step3: The above triangle is now added with original Pascal's Triangle as follows,

12 **1** **13**

4 4 **1 1** **5 5**

19 24 14 **1 2 1** **20 26 15**

20 0 19 19 ✚ **1 3 3 1** → **21 3 22 20**

14 3 0 24 12 **1 4 6 4 1** **15 7 6 28 13**

14 17 13 8 13 6 **1 5 10 10 5 1** **15 22 23 18 18 7**

The resultant number is 13 5 5 20 26 15 21 3 22 20 15 7 6 28 13 15 22 23 18 18 7.

Step4: Now we perform addition modulo 26 to the above resultant numbers we get

13(mod 26) = 13	5(mod 26) = 5	5(mod 26) = 5	20(mod 26) = 20	26(mod 26) = 0	15(mod 26) = 15	21(mod 26) = 21
3(mod 26) = 3	22(mod 26) = 22	20(mod 26) = 20	15(mod 26) = 15	7(mod 26) = 7	6(mod 26) = 6	28(mod 26) = 2
13(mod 26) = 13	15(mod 26) = 15	22(mod 26) = 22	23(mod 26) = 23	18(mod 26) = 18	18(mod 26) = 18	7(mod 26) = 7

Table 2.0 Addition modulo 26 (Encryption)

After performing addition modulo 26 we get 13 5 5 20 0 15 21 3 22 20 15 7 6 2 13 15 22 23 18 18 7.

Step5: Now finally the above numbers are now converted into their numerical equivalent values using Table1. $13 \rightarrow N, 5 \rightarrow F, 5 \rightarrow F, 20 \rightarrow U, 0 \rightarrow A, 15 \rightarrow P, 21 \rightarrow V, 3 \rightarrow D, 22 \rightarrow W, 20 \rightarrow U, 15 \rightarrow P, 7 \rightarrow H, 6 \rightarrow G, 2 \rightarrow C, 13 \rightarrow N, 15 \rightarrow P, 22 \rightarrow W, 23 \rightarrow X, 18 \rightarrow S, 18 \rightarrow S, 7 \rightarrow H.$

"13 5 5 20 0 15 21 3 22 20 15 7 6 2 13 15 22 23 18 18 7" → "NFFU APV DW UPHGC NPWXSSH"

Hence the cipher text for "MEET YOU AT TODAY MORNING" is "NFFU APV DW UPHGC NPWXSSH" which is now sent to the receiver over an unsecure channel.

Decryption - User B (The receiver): Decryption is the reverse process of encryption which is done by the following five steps.

Step1: The receiver, receives cipher text as " NFFU APV DW UPHGC NPWXSSH" this should converted into their numerical equivalent values with the help of Table1 i.e., $N \rightarrow 13, F \rightarrow 5, F \rightarrow 5, U \rightarrow 20, A \rightarrow 0, P \rightarrow 15, V \rightarrow 21, D \rightarrow 3, W \rightarrow 22, U \rightarrow 20, P \rightarrow 15, H \rightarrow 7, G \rightarrow 6, C \rightarrow 2, N \rightarrow 13, P \rightarrow 15, W \rightarrow 22, X \rightarrow 23, S \rightarrow 18, S \rightarrow 18, H \rightarrow 7.$

"NFFU APV DW UPHGC NPWXSSH" → **"13 5 5 20 0 15 21 3 22 20 15 7 6 2 13 15 22 23 18 18 7"**

Step2: The above numbers are now formed in the form of triangle as in the form of Pascal's Triangle format

13

5 5

20 0 15

21 3 22 20

15 7 6 2 13

15 22 23 18 18 7

Step3: The above triangle is now subtracted with original Pascal's Triangle that is

13	**1**	**12**
5 5	**1 1**	**4 4**
20 0 15	**1 2 1**	**19 -2 14**
21 3 22 20	**1 3 3 1**	**20 0 19 19**
15 7 6 2 13	**1 4 6 4 1**	**14 3 0 -2 12**
15 22 23 18 18 7	**1 5 10 10 5 1**	**14 17 13 8 13 6**

The resultant number is 12 4 4 19 -2 14 20 0 19 19 14 3 0 -2 12 14 17 13 8 13 6.

Step4: Now we perform addition modulo 26 to the above resultant numbers we get

12(mod 26) = 12	4(mod 26) = 4	4(mod 26) = 4	19(mod 26) = 19	-2(mod 26) = 24	14(mod 26) = 14	20(mod 26) = 20
0(mod 26) = 0	19(mod 26) = 19	19(mod 26) = 19	14(mod 26) = 14	3(mod 26) = 3	0(mod 26) = 0	-2(mod 26) = 24
12(mod 26) = 12	14(mod 26) = 14	17(mod 26) = 17	13(mod 26) = 13	8(mod 26) = 8	13(mod 26) = 13	6(mod 26) = 6

Table 3.0 Addition modulo 26(Decryption)

After performing addition modulo 26 we get 12 4 4 19 24 14 20 0 19 19 14 3 0 24 12 14 17 13 8 13 6.

Step5: Now finally the above numbers are now converted into their numerical equivalent values using Table 1.0.

$12 \to M, 4 \to E, 4 \to E, 19 \to T, 24 \to Y, 14 \to O, 20 \to U, 0 \to A, 19 \to T, 19 \to T, 14 \to O, 3 \to D, 0 \to A, 24 \to Y, 12 \to M, 14 \to O, 17 \to R, 13 \to N, 8 \to I, 13 \to N, 6 \to G.$

"12 4 4 19 24 14 20 0 19 19 14 3 0 24 12 14 1713 8 13 6" → "MEET YOU AT TODAY MORNING"

Hence the decryption for "NFFU APV DW UPHGC NPWXSSH" is "MEET YOU AT TODAY MORNING".

Hence the original message is "MEET YOU AT TODAY MORNING".

6. Security analysis:

Since the proposed technique that has high security than the other private key techniques. Suppose an intermediate has the final ciphertext message unit for example "NFFU APV DW UPHGC NPWXSSH" which was encrypted and send by the User A to User B over an unsecured channel, the intendent people try to break the cipher text message units with the help of Caesar Cipher means he get the output as "NFFU APV DW UPHGC NPWXSSH" → "KCCR XMS AT RMDZ KMTUPPE", using Atbash Cipher means "NFFU APV DW UPHGC NPWXSSH" → "MUUF ZKE WD FKSTX MKDCHHS" and using Affine Cipher means "NFFU APV DW UPHGC NPWXSSH" →"VHHE IFJ XO EFRMS VFOTUUR" in all the cases the hacker will get some other message that is an unreadable form that is not the original message, the hacker didn't crack the original message units. Suppose someone has used frequency analysis means also the original message cannot be braked, our cipher text is "NFFU APV DW UPHGC NPWXSSH" in this the most occurring character is P using frequency analysis means one can relate the most frequency letter with the alphabet character E and the second most frequency letter with I, if do so means also they cannot get the original message. So, the security analysis under this technique is higher than the existing symmetric encryption techniques.

7. Conclusion

Nowadays protecting information is one of the most essential issues, encryption techniques give us protection for our data, messages and private details. A new approach to cryptosystem that has been proposed in this paper is encryption, decryption using Pascal's triangle to boost the safety of our messages than the existing cipher techniques. The proposed approach is more efficient and resists against different breakup techniques some of them are discussed in Section 6. The proposed method may be used successfully in wireless communications also and it's an easy and rapid encryption/decryption method with higher protection. In this paper, we carried out the new method of message encryption, decryption. In the future, this method may be changed and used it for other data encryption and decryption.

References

- Arumugam S, Ramachandran S, Invitation to Graph theory, Scitech Publications, (2015).
- Diffie, W., Hellman, M., New directions in Cryptography, IEEE Trans. Inf. Theory 22 (6), 644 – 654, 1976.
- Joseph H. Silverman, An Introduction to the Theory of Elliptic Curve, University of Wyoming, 2014.
- Mohan. P, Rajendran. K, Rajesh. A, An Encryption Technique using a Complete graph with a Self-invertible matrix, Journal of Algebraic statistics, Volume 13. No 3, (2022), https://publishoa.com/index.php/journal/article/view/816, pp.1821-1826.
- Mohan P, Rajendran K, Rajesh A. A Hamiltonian Path-Based Enciphering Technique with the use of a Self-Invertible Key Matrix, Indian Journal of Science and Technology, 15(44) (2022), pp.2351-2355.

- Mohan P, Rajendran K, Rajesh A. An encryption Technique using the adjacency matrices of certain graphs with a self-invertible key matrix, E3S Web of Conf, Volume 376, 01108(2023) https://doi.org/10.1051/e3sconf/202337601108

- Mohan P, Rajendran K, Rajesh A. Enhancing Computational Performance of Minimal Spanning Tree of Certain Graphs Based Enciphering Technique Using Self-Invertible Key Matrix, Journal of Aeronautical Materials(1005-5053), Vol 43, Issue-01(2023), pp 359-371, https://www.hkclxb.cn/article/view/2023/359.html.

- Neal Koblitz, A course in Number Theory and Cryptography, second edition, Springer, 2014.