ISSN 2277-3061
Volume 15 Number 13
INTERNATIONAL JOURNAL OF COMPUTERS &TECHNOLOGY

ENCRYPTION METHOD USING PASCAL'S TRIANGLE BASED SUBSTITUTION AND SIERPINSKI TRIANGLE BASED PERMUTATION

[1]Sivakumar T, [2]Pauvithraa K.T, [3]Durga Devi V
[1]Assistant Professor
sk@ity.psgtech.ac.in
[2,3] Final Year B.Tech IT
[2]pauvithraa@gmail.com,[3]durgadevibtech13@gmail.com
Department of Information Technology
PSG College of Technology, Tamilnadu, India.

ABSTRACT

Text messages are often created, shared and a person sends at least ten messages a day. Because of its frequent usage those messages are not been encrypted. Thus it is unable to send confidential messages via SMS service. In this paper, we develop a new encryption technique using the notions of Pascal's Triangle and Sierpinski Triangle. The proposed method uses the Pascal's triangle for substitution and Sierpinski triangle for permutation. The method is simple and easy to implement in real time. It is difficult for the attackers to predict the original message contained in the ciphertext. The proposed method is not much vulnerable to brute force and letter frequency attacks.

Keywords

Cryptography, Substitution, Permutation, Pascal's triangle, Sierpinski triangle

1. INTRODUCTION

Due to the availability and abundant use of technology, sending of short text messages between the communicating users has increased in domain such as social media, messaging apps, e-mails. Some messages in those domains are confidential and sensitive for the communicating persons. Hence, providing confidential to those messages is important. Confidential service can be provided by mechanisms like encipherment. Transposition and Substitution methods are used to encrypt and decrypt text messages [15]. In this paper, a new substitution and permutation based technique to encrypt/decrypt text messages using the concept of Pascal and Sierpinski triangle is proposed. The notion of Pascal triangle is used to perform XOR operation on the characters of plaintext message in a particular pattern and then permutation is done to get the ciphertext.

2. Literature survey

In this section, brief descriptions of the few existing classical and modern encryption techniques data are provided. Encrypting text messages using various simple methods have been introduced by various researchers [5, 7-9, 12, 13].

2.1 Classical Ciphers

The Caesar cipher is one of the earliest known and simplest ciphers. The method is named after Julius Caesar, who apparently used it to communicate with his generals. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. The Caesar cipher offers essentially no communication security, and it can be easily broken even by hand. The encryption and decryption process are carried using the Equations (1) and (2) [15].

- Encryption : $C = (P+K) \bmod 26$ (1)
- Decryption : $P = (C-K) \bmod 26$ (2)

The Playfair cipher is a polygraphic cipher which enciphers two letters at a time. The encryption and decryption process are carried out by using a 5x5 matrix. The technique encrypts pairs of letters, instead of single letters as in the simple substitution cipher. The Playfair is significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. Frequency analysis can still be undertaken, but on the 25x25=625 possible digraphs rather than the 25 possible monographs [15].

Vigenere cipher is poly-alphabetic substitution cipher in which a single plain text letter can be converted into multiple cipher text letters. This conversion depends on the position of the letter in the plaintext. The Vigenere cipher makes use of Vigenere table of size 26x26 [15].

Rail fencing technique involves, writing plaintext message as a sequence of diagonal and reading it as a sequence of row to produce ciphertext. In a Rail Fence cipher, after removing the spaces from the original message, write the characters in the message in the zig-zag pattern. The key for the Rail Fence cipher is just the number of rails [15].

In Hill cipher, the concept of matrix multiplication is used for encryption. Plaintext is divided to sub texts based on the key size and each sub text matrix is multiplied with key matrix to get the cipher text matrix [15]. The encryption and decryption processes are done using the Equations (3) and (4).

- Encryption: $C=PK \bmod 26$ (3)
- Decryption: $P=CK^{-1} \bmod 26$ (4)

where, C is ciphertext P is Plaintext, and K is the Key matrix.

2.1 Text Message Encryption Methods

Acharya et al [1] presented an image encryption method using the concept of matrix transformation. Cooper et al [2] introduced an efficient public-key cryptosystem using the Pascal triangle. Dinesh P. Baviskar et al [3] developed an Android based message encryption/decryption method using matrix. Cryptographic algorithms play a vital role in securing confidential data from the attackers. The algorithms consume significant amount of computing resources like CPU time, memory, and encryption time [6]. The concept of matrix reordering is applied to encrypt digital images in the paper [10]. In [11], the authors developed a new symmetric cryptosystem using the key derived from the randomized parameters of SHA-512 and MD5 hash functions. In [14], a new encryption technique using the Pascal triangle is introduced to encrypt/decrypt digital images.

3. THE PROPOSED ENCRYPTION METHOD

The proposed encryption method uses the Pascal's triangle concept as substitution and Sierpinski triangle concept as permutation to encrypt the data. Initially, the characters of the plaintext are arranged in triangle format. Then by using the Pascal principle the characters are XORed bitwise to get a new cipher character. Subsequently permutation technique is applied using sierpinski triangle to get the final encrypted message.

3.1 Pascal triangle

Pascal's triangle is a triangular array of the binomial coefficients. The entries in each row are numbered from the left beginning with $k = 0$ and are usually staggered relative to the numbers in the adjacent rows. Having the indices of both rows and columns start at zero makes it possible to state that the binomial coefficient (n_k) appears in the nth row and kth column of Pascal's triangle. This construction is related to the binomial coefficients by Pascal's rule, which says that if [4]

$$(x + y)^n = \sum_{k=0} (n_k)\, x^{n-k} y^k \quad (5)$$

then

$$(n_k) = (n\text{-}1_{k-1}) + (n\text{-}1_k) \quad (6)$$

A sample Pascal's triangle is shown in Figure 1.

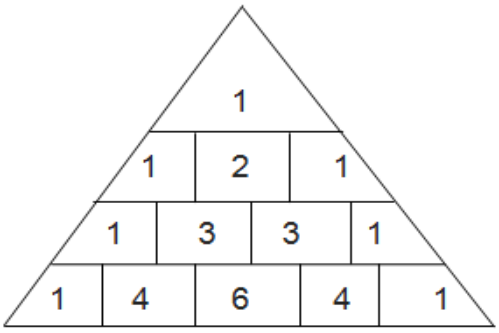

Fig 1: Sample Pascal triangle

3.2 Sierpinski Triangle

The Sierpinski triangle may be constructed from an equilateral triangle by repeated removal of triangular subsets as given below:

(a) Start with an equilateral triangle.

(b) Subdivide it into four smaller congruent equilateral triangles and remove the central one.

(c) Repeat step (b) with each of the remaining smaller triangles

A sample of formation equilateral triangle is shown in Figure 2.

Fig 2: Sample forms of Sierpinski triangle

Based on the above said concepts, the proposed encryption method is divided into two phases such as Phase-I (substitution using Pascal triangle) and Phase-II (permutation using sierpinski triangle).

3.3 Phase I: (Substitution using Pascal triangle)

At sender side, the characters of the plain text are arranged row wise in the triangular pattern (Triangle-1). Based on the above formulae (5) and (6), the characters are XORed with the help of starting character of the plaintext (Triangle-2). Then add these two triangles to get the substituted text message. The following example illustrates the Phase-I of proposed encryption process.

Let us take the plaintext message “meet me at party”. The Triangle-1 after placing the characters of plaintext message is shown in Figure 3. Padding character, in this case x’ is appended at the end to complete the triangle.

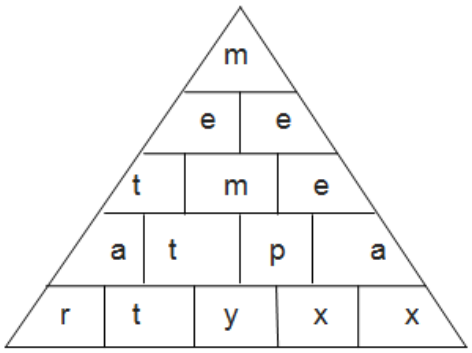

Fig 3: Triangle-1

The Triangle-2 after applying the proposed substitution using the concept of Pascal triangle is shown in Figure 4.

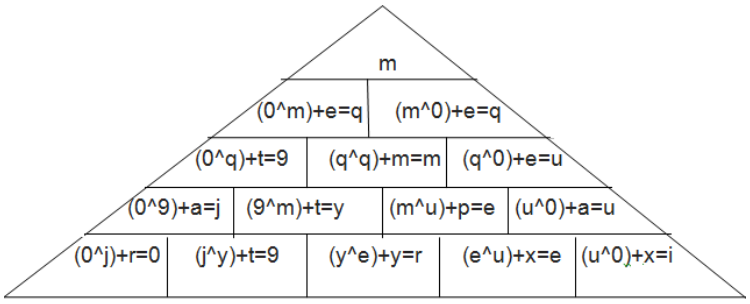

Fig 4: Triangle-2

The obtained substituted text by using Triangle-1 and Triangle-2 is shown in Figure 5.

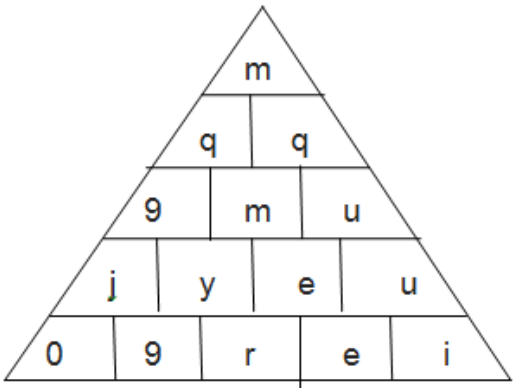

Fig 5: Triangle-3

Hence, the plaintext message after applying the proposed substitution becomes “MQQ9MUJYEU09REI”.

3.4 Phase II: (Permutation using Sierpinski triangle)

In Sierpinski triangle, the characters at the odd positions are written first and then the even position characters. A sample of Sierpinski triangle is shown in Figure 7.

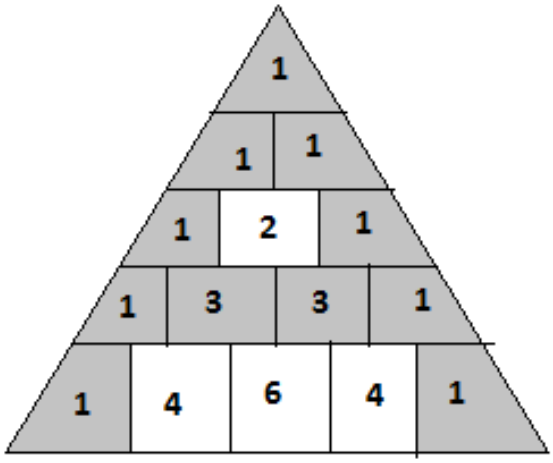

Fig 7: Sierpinski triangle

The result of phase-I is given as input to the phase-II to get the final ciphertext. First, the result of phase-I is arranged as shown in Figure 8 and the characters are read as per the concept of sierpinski triangle.

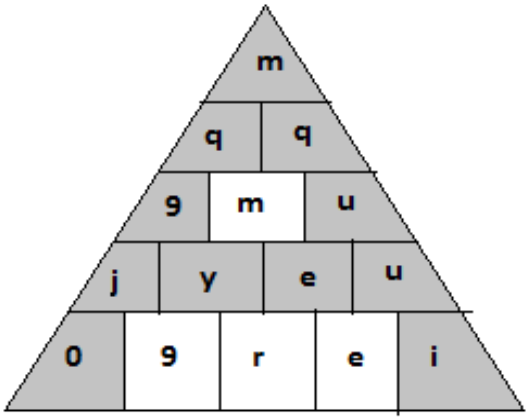

Fig 8: Permutation using sierpinski triangle

Thus, the final encrypted message corresponding to the plaintext “meet me at party” is “MQQ9UJYEU0IM9RE”.

3.5 Encryption Algorithm

Input: Plaintext Output: Ciphertext

Step 1: Let the message to be encrypted in the matrix[m, m] as triangle 1.

Step 2: Develop another triangle, triangle 2, based on the concept of Pascal triangle.

i.e., the corner characters are XORed with 0 and the middle characters are XORed with the neighbouring characters.

Step 3: Add characters in triangle 1 with triangle 2 for substitution.

Step 4: Repeat step 3 until all the characters in the matrix are processed.

Step 5: Read the characters based on the concept of sierpinski triangle to accomplish permutation.

Step 6: Store the encrypted text.

4. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed method is experimented using Java language and the system configuration is Processor Intel i5-5200U, Clock speed 2.2 GHz, RAM 4GB and the operating system is Windows. The proposed encryption method is tested with different plaintext messages of various sizes. The characters of plaintext messages are substituted based on Pascal triangle and the result is given Table 1.The repeated characters of plaintext message are mapped into different characters in the ciphertext using the proposed substitution method. The Hamming distance is computed between the plaintext and the encrypted text to quantity the bit difference.

Table 1. Experimental result of proposed method (Substitution)

S.No.	Plaintext	Encrypted Message	Hamming Distance
1.	attack at dawn 2pm	ATTTC3TA83666GF	32
2.	meet me at party	MQQ9MUJYEU09REI	35
3.	stop the enemy	SB6QAXUUA15YJYY	28

The encrypted messages with proposed substitution and permutation are given in Table 2. The characters of plaintext messages are randomly shuffled and located in various locations in the encrypted message. The Hamming distance is computed between the plaintext and encrypted text and it is observed that the bit difference has been increased.

Table 2. Experimental result of proposed method (Permutation & Substitution)

S.No.	Plaintext	Encrypted message	Hamming Distance
1.	attack at dawn 2pm	ATTT3TA836FC66G	34
2.	meet me at party	MQQ9UJYEU0IM9RE	37
3.	stop the enemy	SB6QXUUA15YAYJY	32

The performance of the proposed method is enhanced after applying both substitution and permutation. The result shows that the repeated characters in the plaintext message are mapped to different cipher characters in the encrypted message. Hence, the ciphertext is not much vulnerable to cryptanalysis and letter frequency attack.

5. CONCLUSION

In this paper, a new cryptosystem to encrypt/decrypt text messages by using Pascal and Serpienski triangles is developed. The method is very simple and easy to implement because it involves permutation and substitution techniques for encryption. The characters of the plaintext are transformed to random characters after substitution and the ciphertext are randomly shuffled by using permutation. The proposed encryption method satisfies both confusion and diffusion properties significantly. The messages encrypted using the proposed method is not much vulnerable to cryptanalysis and letter frequency attacks.

REFERENCES

1. Acharya B, Patra S, and Panda G, “Image encryption by novel cryptosystem using matrix transformation”, Emerging Trends in Engineering and Technology, 2008.
2. Cooper R.H, Fredericton NB, Hunter-Duvar R and Patterson W, “A more efficient public-key cryptosystem using the Pascal triangle”, World Prosperity Through Communications, IEEE International Conference, 1989, vol.3, pp.1165 – 1169.
3. Dinesh P. Baviskar, Sidhhant N. Patil and Onkar K. Pawar, “Android based message encryption/decryption using matrix”, International Journal of Research in Engineering and Technology, Vol. 4, Iss. 1, Jan-2015.
4. Edwards A.W.F, “Pascal’s Arithmetical Triangle: The Story of a Mathematical Idea”.
5. Hazem M. El bakry, Ali E. Taki El Deen and Ahmed Hussein Ali El Tengy, “A New Mobile Application for Encrypting SMS/Multimedia Messages on Android”, International Journal of Scientific & Engineering Research, Vol. 4, Iss. 12, 2013.
6. Himani Agarwal and Monisha Sharma, “A Review of Text Encryption Techniques”, Asian Journal of Computer Science and Information Technology, Vol. 4, No. 5, pp. 47-54, 2014.
7. Punam V. Maitri, Rekha V. Sarawade, Mayuri P. Patil and Sarika T. Deokate, “MSC: Mobile Secure Communication Using SMS in Network Security: A Survey”, International Journal of Engineering Research & Technology, Vol. 2, No. 11, 2013.
8. Rohan Rayarikar, Sanket Upadhyay and Priyanka Pimpale , “SMS Encryption using AES Algorithm on Android”, International Journal of Computer Applications (0975–8887) , Vol. 50, No.19, July 2012.
9. Shobha Jha P U. Dutta P and Priyankgupta P , “SMS Encryption using NTRU Algorithms on Android Application”, International Journal of Scientific Engineering and Applied Science, Vol. 2, No. 1, January 2016.

10. Sivakumar T and Venkatesan R, “A Novel Image Encryption Approach using Matrix Reordering”, WSEAS Transactions on Computers, Vol. 12, No. 11, 2013.
11. Sivakumar T and Anusha T, “A New Symmetric Cryptosystem using Randomized Parameters of SHA-512 and MD5 Hash Functions”, International Journal of Innovations in Engineering and Technology, Vol. 6, No. 4, May 2016.
12. Smile Markovski, Aleksandra Kuzmanovska, and Milivoj Simeonovsk, “A Protocol for Secure SMS Communication for Android OS”, ICT Innovations 2011, Vol. 150, Advances in Intelligent and Soft Computing, pp. 171-178, 2011.
13. Sri Rangarajan, Sai Ram N and Vamshi Krishna N, “Securing SMS using Cryptography”, International Journal of Computer Science and Information Technologies, Vol. 4, No.2 , pp. 285–288, 2013.
14. Sugapriya K, Kishorekumar K and Anitha Kumari K, “A Novel Encryption Technique using Pascal Triangle for Image Cryptosystem”, National Conference on Research and Challenges in IT, April 22 - 23, 2016, PSG College of Technology, Coimbatore.
15. William Stallings, “Cryptography and Network Security-Principles and Practice”, Pearson Education, New Delhi, 2013.

Authors Profile:

Dr.T.Sivakumar was born in Tamilnadu, India, in 1978. He received his B.Sc degree in Mathematics from ManonmaniamSundaranar University in 1998, and M.C.A degree from Bharathidasan University in 2002. He received his master degree M.E in Computer Science and Engineering from Anna University in 2009. He was awarded with Ph.D from Anna University, Chennai in 2016. He is currently working as an Assistant Professor in the Department of Information Technology, PSG College of Technology, Coimbatore-641004, India. His research interests include data & network security and cryptography.

Ms.Pauvithraa K.T and **Ms.Durga Devi V** are the final year students of B.Tech-Information Technology, in the Department of Information Technology, PSG College of Technology, Coimbatore-641004, India. We erudite Object Oriented Programming, Cryptography and Network Security subjects from Dr.T.Sivakumar.