TEXT MESSAGE ENCRYPTION METHOD USING HILBERT CURVE BASED PERMUTATION AND CIRCULAR SHIFT OPERATION

[1]Sivakumar T, [2]Gayathri S, [3]Pauvithraa K.T

[1]Assistant Professor, [2,3]Final Year Students,

[1,2,3]Department of Information Technology, PSG College of Technology, Coimbatore, Tamil Nadu

ABSTRACT

Storage and transmission of digital data has been increased due to communication technique development. Information security is becoming more important as the amount of text messages and sensitivity of messages being exchanged on the Internet increases. Therefore, data confidentiality and integrity are required to protect data against unauthorized disclosure and modification. This has resulted in the explosive growth of information security. Cryptography is the art of achieving security by encrypting messages to make them non-readable at the sender's side and decrypting the messages at the receiver's end to obtain the original information. In this paper, a simple encryption algorithm using HilbertCurve based permutation and substitution using circular shift operation is proposed. The proposed encryption method satisfies both confusion and diffusion properties.

Keywords: Cryptography, Text Encryption, Hilbert Curve, Permutation, Substitution

I. INTRODUCTION

Due to the availability and abundant use of technology, sending of short text messages between the communicating persons has increased in domain such as social media, messaging apps and e-mails. Some messages in those domains are sensitive and hence confidential for the communicating persons. Hence, providing confidentiality service to those messages is an important requirement. Confidential service can be provided by mechanisms like encipherment. Security is required to transmit confidential information over the network. Cryptographic algorithms play a vital role in providing the data security against malicious attacks. But they consume significant amount of computing resources like CPU time, memory and encryption time [1]. Transposition and substitution are two methods used to encrypt and decrypt text messages.

In this paper, a simple encryption method for text messagesusing the concept of HilbertCurveand circular shift operation is proposed. Hilbert curve is a kind of space filling curves which is being currently used in compression techniques. Here, HilbertCurve is adapted to develop a new permutation based encryption algorithm for text messages. Detailed discussion of Hilbert Curve is provided in Section 3.1.

1.1 About Text Encryption

Text encryption is needed for communicating sensitive information through public networks and Internet. Encryption assumes that no other third-party is able to crack the code of private conversations. Text encryption is perfect for high-level discussion of enterprise products coming to market, exchanging files containing private financial data, or sending personal family information you wouldn't want getting out in the world.Encryption protects data in personal computers, laptops, data centers, and it protects it when it's being transmitted around the Internet. Several encryption methods have been introduced by various authors exclusively to encrypt/decrypt text messages [1, 3, 4, 6-8, 10, 12-14].

II. LITERATURE SURVEY

Encrypting and decrypting data is investigated and developed because there is a demand for a stronger encryption and decryption which is very hard to crack. Most of the existing algorithms have several weaknesses either caused by low security level or increase the delay time due the design of the algorithm itself [8].The Caesar cipher, Playfair cipher and Hill cipher are the basic encryption methods used in earlier days to encrypt/decrypt important messages.

Forwarding an SMS is one of the cheapest, fastest and simple methods.The SMS information is already gathered in the system of the network operator and this data can be easily perceived by their personnel [12]. Due this problem encryption is important for every SMS which is being delegate through the network operator. Sometimes we transfer the private information like password, banking details to service provider through a SMS. But traditional message applications do not give encryption to the data contained in the SMS before its transmission [12].The SMS communication is insecure and the message information can be viewed of many interested parties [14].

IBM introduced Data Encryption Standard (DES) which was initially used for the encryption of electronic data and it is now considered to be insecure because of brute force attack. It has a block size of 64-bits and key size is 56-bits. The Advanced Encryption Standard (AES) proposed by Daemen and Rijmen is a symmetric key algorithm. It has a fixed block size of 128-bits and key size of 128,192 or 256 bits [18].

In this paper, a simple and secure encryption method to protect text messages ispresented using the notion of Hilbert Curve and Circular shift operation.

III. PROPOSED ENCRYPTION METHOD

In this section, the overall working model of the proposed encryption method is presented. At sender side, the characters of the plaintext are arranged column wise in an NxN matrix. Based on the length of the plaint text messages the N value is chosen as 4 or 8. For arranging the plaintext charactersthe permutation key is derived from the primitive root of a prime number concept used in the Diffie-Hellman algorithm.Then the characters of the matrix are given to HilbertCurve for further permutationto get the permuted text message.

Further substitution is performed using circular shift operation. For substitution, the elementary operation, $ROTR^n(x)$, of SHA-512 hash function is used. At the receiver side, the substitution and then Hilbert Curve based inverse permutation are performed to get the intermediate text message.

Then the characters are rearranged as per the key derived from the primitive root of a prime number. The overall working model of proposed encryption method is shown in Figure1.

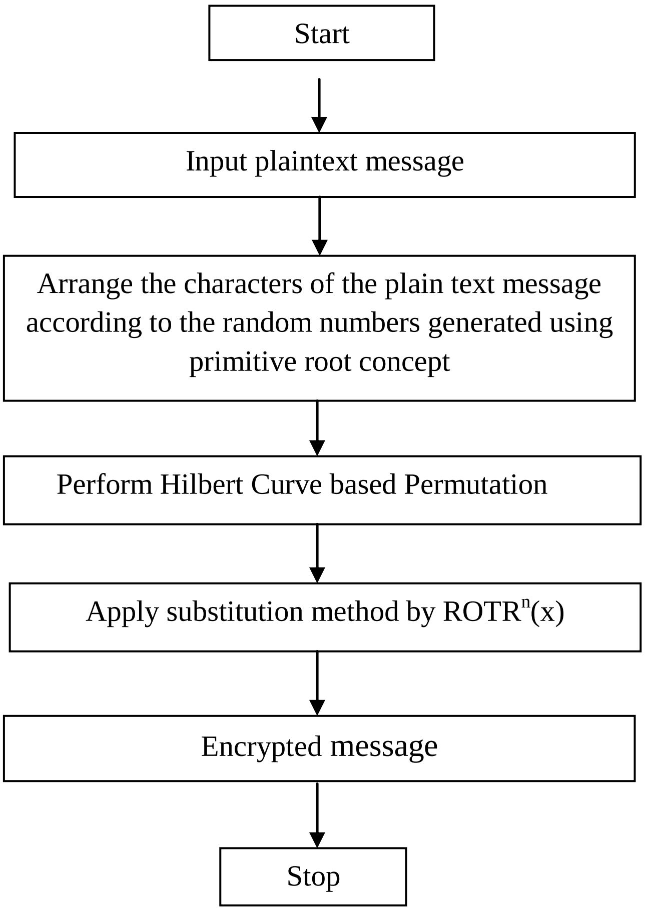

Start
Input plaintext message
Arrange the characters of the plain text message according to the random numbers generated using primitive root concept
Perform Hilbert Curve based Permutation
Apply substitution method by ROTR^n(x)
Encrypted message
Stop

Figure 1. Overall Working Model of Proposed Encryption Method

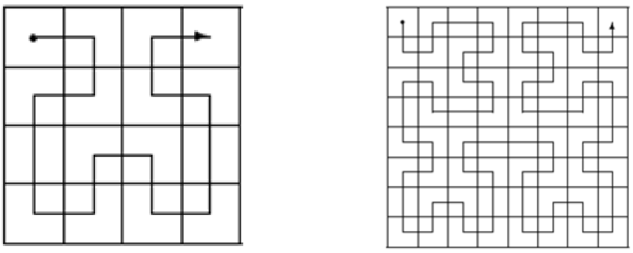
The meaning of ROTR^n(x) is circular right shift of the argument ‘x’ by ‘n’ bits.The permutation key derived from the primitive root of a prime number is utilized as ‘n’ to accomplish circular shift. If the length of the plain text message is less than or equal to 16 then N is 4, else N is 8. If the plain text message contains more than 64 characters then the entire process is repeated for the remaining characters. During decryption ROTL^n(x), circular left shift of the argument x by n bits, is used.

3.1 Notion of Hilbert Curve

A Hilbert space-filling curve is a curve of $2^n \times 2^n$ two-dimensional space that it visits neighboring points consecutively without crossing itself. The Hilbert Curve (HC) has been applied for indexing regions and for spatial data and to rearrange image pixels in order to enhance pixel locality [6].

Tropf[2] presented the application of space-filling curves, and related curves sharing some of the characteristics of space-filling curves, to the storage and retrieval of multi-dimensional point data. Lawder& King [5] presented a radically different approach to multi-dimensional indexing based on the concept of Hilbert Curve.In storage and retrieval of multi-dimensional data, the concept of Hilbert Curve has been used for generating the sequence of one-dimensional numbers for indexing and this is often referenced by one-dimensional sequence numbers. The concept of Hilbert Curve (HC) is used in spatial, text, and multimedia databases to implement one-dimensional index and search on multi-dimensional data. Liang et al [6] studied and implemented the Hilbert space filling curves for lossless medical image compression.

The structure of Hilbertcurves using first, second and third orders are shown in the Figure2. There are four possible coordinates such as Left Bottom (LB), Left Top (LT), Right Bottom (RB), and Right Top (RT) to start the permutation process in a Hilbert Curve.



(b)Second order Hilbert curve **(c)Third order Hilbert curve**

Figure 2. Structure of Hilbert Curve

3.2 Illustrative for Hilbert Curve based Permutation

In this section the working model of proposed encryption method is illustrated with a sample plaintext message. Let us consider the plain text message as "**attack at dawn 2 pm**".

Shuffle the characters of the plaintext based on the key obtained by using the primitive root of 17. Using this permutation table is constructed and this is shown in Figure 3.

3	9	10	13
5	15	11	16
14	8	7	4
12	2	6	1

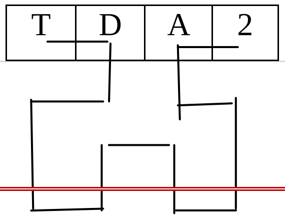
Figure 3.Definition of IP Table using Primitive root of 17

The characters of the plaintext message are arranged in a matrix as per the IP definition and the result is shown in Figure 4.

T	D	A	2
C	M	W	X
P	T	A	A
N	T	K	A

Figure 4. Arrangement of Plain Text message

Further Hilbert Curve(HC) based permutation is applied and the result is shown in Figure 5.



C	M	W	X
P	T	A	A
N	T	K	A

Figure 5.Hilbert Curve based Permutation

The encrypted message obtained using the proposed method without substitution is TDMCPNTTAKAAXWA2. Further substitution is performed using circular right shift operator. That is, the ASCII value of character is rotated right according to the permutation key generated by using the primitive root of a prime number, which is already shown in Figure 3. This is demonstrated for the first three characters as follows.

T=01110100=>$ROTR^3$(T) =>10001110 =>10001110 XOR 00000011 =>10001101=>141

D=01100100 =>$ROTR^9$(D) =>00110010 =>00110010 XOR 00001001=>00111011=>59

M=01101101 =>$ROTR^{10}$(M)=>01011011=>01011011 XOR 00001010 =>01010001=>81

Thus, the cipher text corresponding to the letters "TDM" is "É; Q". This process is repeated for the remaining letters.

3.3 Architecture of Proposed Encryption Method

In this section, the architecture design of proposed encryption method is briefly presented. This is useful to understand the various stages of the proposed encryption/decryption processes. The architectural design of the proposed method is shown in Figure 6.

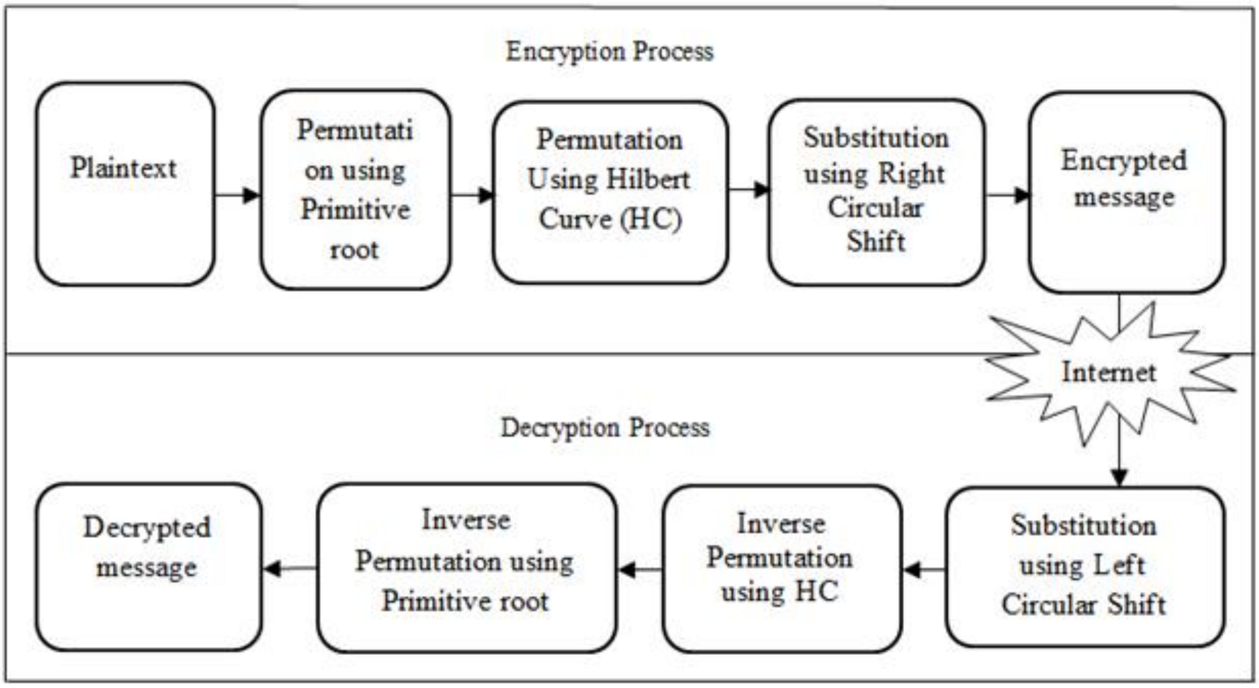

Encryption Process
Plaintext
Permutation using Primitive root
Permutation Using Hilbert Curve (HC)
Substitution using Right Circular Shift
Encrypted message
Internet
Decryption Process
Substitution using Left Circular Shift
Inverse Permutation using HC
Inverse Permutation using Primitive root
Decrypted message

Figure 6. Architectural Design of Proposed Method

3.4 Encryption Algorithm

This section gives the sequence of steps used to convert the plaintext message into ciphertext.

Input: Plaintext Message, Prime number and its primitive root

Output: Encrypted Message

Step 1: Start

Step 2: Input plaintext message.

Step 3: Find the length of the plaintext message.

Step 4: If length≤16, then the size of the matrix (W) is 4, Else W=8.

Step 5: Construct the definition of IP table using primitive root of a prime number.

Step 6: Permute the characters of the plaintext based on the definition of IP table.

Step 7: Apply Hilbert Curve based permutation.

Step 8: Apply substitution using circular shift right operator.

Step 8: Store the encrypted message.

Step 9: Stop.

Padding character is appended at the end of the plaintext message, if the plaintext message is not in the multiple of 16 or 64. The decryption process is the inverse of encryption algorithm.However in decryption, the substitution is performed by using circular left shift operator.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed method is experimented using Java language and the system configuration is Processor Intel i5-5200U CPU, 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 obtained result of proposed method for various stages is given Table 1, Table 2, and Table 3.

Table 1 Result after the Initial Permutation

S.No	Plaintext Message	Permuted Message	Hamming Distance
1	attack at dawn 2pm	TDA2CMWXPTAANTKA	40
2	meet after party	ERPTAXAXYETTREFM	42
3	stop the enemy	ONEXTXMXXEEPYTHS	29

Table 2 Resultafter Permutation using Hilbert Curve based Permutation

S.No	Plaintext Message	Permuted Message	Hamming Distance
1	attack at dawn 2pm	TDMCPNTTAKAAXWA2	38
2	meet after party	ERXAYREETENTXAPT	36
3	stop the enemy	ONXTXYTEEHSPXMEX	36

Table 3.Final Result after Permutation and Substitution

S.No	Plaintext Message	Encrypted Message	Hamming Distance
1	attack at dawn 2pm	ì;Q▬ å╙ ìd♫c ♦ ï●▀♠↑	54
2	meet after party	»0¶ɔ╬ δ ºu▀m█C ü ☻ ╟;	69
3	stop the enemy	ε >¶« ╞² àu¢` ß♥ ï Y ô=	56

From the result, it found that 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 to confirm the bit difference between the plaintext and its corresponding ciphertext.

V. CONCLUSION

In this paper, a simple and secure cryptosystem to encrypt/decrypt text messages by using the notion of Hilbert Curve is developed. The method is very simple and effective because it involves the permutation and substitution techniques. The characters of the plaintext are shuffled after permutation and the ciphertext contain arbitrary characters after substitution. The proposed encryption method satisfies both confusion and diffusion properties significantly.

REFERENCES

[1] HimaniAgarwal and Monisha Sharma, A Review of Text Encryption Techniques, *Asian Journal of Computer Science and Information Technology, 4(5)*, 2014, 47-54.

[2] H. Tropf, Database and Method for Organizing Data Elements, US Patent No.7,321,890, 2008.

[3] 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, 4(12),* 2013.

[4] 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, 4(1)*, 2015.

[5] J.K Lawder and P.J King, Using Space-filling Curves for Multi-dimensional Indexing, in Advances in Databases, Springer Berlin Heidelberg, 2000, pp. 20-35.

[6] J.Y Liang, C.S Chen, C.H Huang and L. Liu, Lossless Compression of Medical Images using Hilbert Space-filling Curves, *Computerized Medical Imaging and Graphics, 32(3),* 2008, 174-182.

[7] KundankumarRameshwarSaraf, Vishal PrakashJagtap and Amit Kumar Mishra, Text and Image Encryption Decryption Using Advanced Encryption Standard,*International Journal of Emerging Trends & Technology in Computer Science, 3(3)*, May–2014.

[8] Obaida Mohammad Awad Al-Hazaimeh, A new approach for complex encrypting and decrypting data,*International Journal of Computer Networks & Communications, 5(2)*, 2013.

[9] Puja Padiya and MeghanaMadhusudanan,Study of SMS Encryption Techniques, *International Journal of Computer Applications, International Conference on Advances in Science and Technology 2015* (ICAST 2015).

[10] 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*,*2(11)*,2013.

[11] RohanRayarikar, SanketUpadhyay and PriyankaPimpale ,SMS Encryption using AES Algorithm on Android,*International Journal of Computer Applications, 50(19)*, 2012.

[12] ShitalD.Rautkar and Dr.Prakash S. Prasad, An Overview of Real Time Secure SMS Transmission, *International Journal of Advanced Research in Computer and Communication Engineering, 4(1)*, 2015.

[13] ShobhaJha PU, Dutta P and Priyankgupta P , SMS Encryption using NTRU Algorithms on Android Application,*International Journal of Scientific Engineering and Applied Science, 2(1)*, 2016.

[14] Smile Markovski, Aleksandra Kuzmanovska, and Milivoj Simeonovsk, A Protocol for Secure SMS Communication for Android OS, *ICT Innovations 2011,Advances in Intelligent and Soft Computing, 150*,2011, 171-178.

[15] Sri Rangarajan, N. Sai Ram and N. Vamshi Krishna, Securing SMS using Cryptography, *International Journal of Computer Science and Information Technologies, 4(2)* , 2013 pp. 285–288.

[16] T. Sivakumar and R. Venkatesan, Image Encryption Based on Pixel Shuffling and Random Key Stream, *International Journal of Computer and Information Technology, 3(6)*, 2014, 1468-1476.

[17] T. Sivakumar and T. Anusha, A New Symmetric Cryptosystem using Randomized Parameters of SHA-512 and MD5 Hash Functions, *International Journal of Innovations in Engineering and Technology, 6(4)*, 2016, 600-606.

[18] William Stallings, Cryptography and Network Security-Principles and Practice (Pearson Education, New Delhi, 2013).

AUTHORS PROFILE

Dr. T. Sivakumar was born in Tamil nadu, India, in 1978. He received his B.Sc degree in Mathematics from Manonmaniam Sundaranar 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.Gayathri S and Ms. Pauvithraa K.T are the final year students of B.Tech-Information Technology, in the Department of Information Technology, PSG College of Technology, Coimbatore-641004, India. They are doing the final year project work under the guidance of Dr.T.Sivakumar. We are grateful to our guide Dr.T.Sivakumar, who was very supportive of our ideas and was helpful to us in every possible way.