3rd International Conference on Latest Trends in Engineering, Science, Humanities and Management
(IFUNA) Indian Federation of United Nations Associations, New Delhi (India) (ICLTESHM-17)
8th April 2017, www.conferenceworld.in ISBN: 978-93-86171-23-8

DATA ENCRYPTION USING BINARY TREE TRAVERSAL (DEBTT)

Sivakumar T[1], Humshavarthini K[2], Jayasree M[3], Eswaran M[4]

[1,2,3,4] *Department of Information Technology*

PSG College of Technology, Tamilnadu, (India)

ABSTRACT

In cryptography, encryption is the process of encoding messages in such a way that only authorized parties can read it. The amount of digital data created and shared via internet has been increasing every day. The number of security attacks/threats has also increased due to the vulnerabilities in the network and software. In this paper, a new data encryption and decryption method is proposed using ASCII values of characters in the plaintext and Binary Tree Traversal (BTT). First level encryption uses ASCII values of the plaintext characters to achieve substitution. Then, the binary tree traversal is used as the second level of encryption for achieving permutation. Also, the algorithm does not explicitly use any key to encrypt the data. The algorithm has been verified with experimental results.

Keywords- ASCII,Binary Tree Traversal, Encryption, Decryption, Plaintext

I INTRODUCTION

With the fast progression of digital data exchange in electronic way, Information Security is becoming much more important in data storage and transmission [6]. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary [2]. In network security, cryptography has a long history by providing a way to store sensitive information or transmit it across insecure networks (i.e. the Internet). Cryptographic algorithms ensure that the messages cannot be read by anyone except the intended recipient. Cryptosystem is a set of algorithms combined with keys to convert the original message to encrypted message and convert it back in the intended recipient side to the original [3]. The encryption algorithm performs various substitutions and transformations on the plaintext. Decryption is reverse of encryption process.Plaintext is the intended original message. Cipher text is the coded message [8, 10].There are two classes of encryption in use, which are referred to as i) Symmetric-key encryption using secret keys and ii) Asymmetric-key encryption using public and private keys. Public-key algorithms are slow, whereas Symmetric-key algorithms generally run 1000 times faster [3]. Symmetric key cryptography has been still extensively used to solve the traditional problem of communication over an insecure channel [9]. The first model proposed by Shannon on the cryptosystem is shown in Figure 1 [1].

ISBN: 978-93-86171-23-8

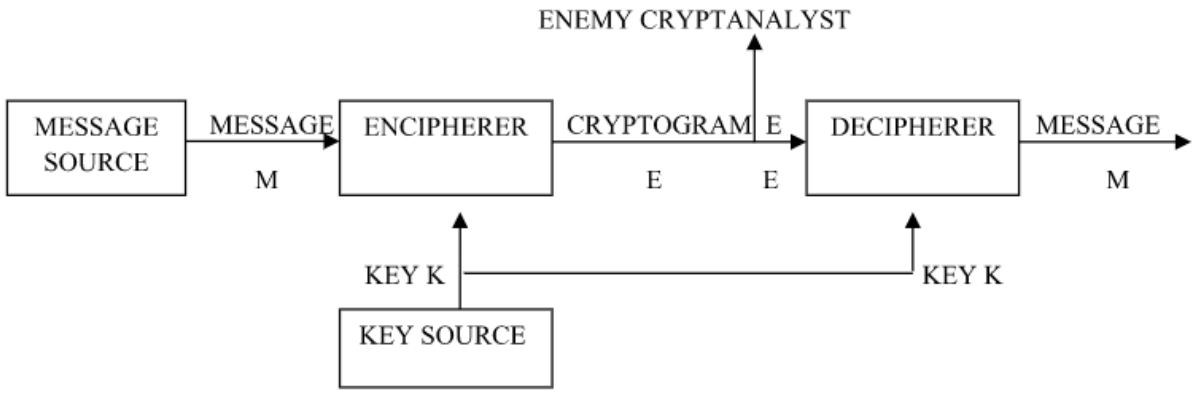

Fig.1Shannon model of cryptosystem

The main goals of cryptography are to provide Authentication, Privacy, Integrity, Non-repudiation and Access Control. Authentication is the assurance that the communicating entity is the one that it claims to be. Data Confidentiality (Privacy) is the protection of data from unauthorized disclosure. Data Integrity is the assurance that data received are exactly as sent by an authorized entity. Non-repudiation provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. Access Control is the prevention of unauthorized use of a resource [10].

ASCII stands for American standard code for information inter change has been adopted by several American computer manufactures as their computer's internal code American standard association developed ASCII. ASCII value of each character is different as A-65, B-66, C-67 or a -97, b-98 and so on [7].

In the proposed method, ASCII values of the characters in the plain text are manipulated to form a set of different cipher characters. Further, binary tree is used for the second level encryption. A binary tree is a tree data structure in which each node has at most two children, which are referred to as the left child and the right child. Reversing the alternate levels of the tree and level order traversal are performed on the tree structure to encrypt the plaintext in the second level.

II LITERATURE SURVEY

Traditional (pre-computer) symmetric ciphers use substitution and/or transposition techniques. Substitution techniques map plaintext elements (characters, bits) into cipher text elements. Transposition techniques systematically transpose the positions of plaintext elements [10]. Each and every algorithm either it may be block cipher or stream cipher or any other cipher types can be easily attacked by performing various cryptanalysis techniques like linear cryptanalysis, n-gram analysis, meet in the middle attack, brute force attack, man in the middle attack etc. [4] The efficiency of the Ciphers that are being used depends mainly on their throughput and memory requirement. Using of large key spaces with huge number of rounds with multiple complex operations may provide security but at the same time affects speed of operation [5]. Both substitution method and transposition method encryption are easily performed with the power of computers. The combination of these two classic techniques provides more secure and strong cipher. The final cipher text is so strong that is very difficult to break [8].

 ISBN: 978-93-86171-23-8

In [6], the authors implemented a text message encryption method using Z-Order Curve (Z-oC) based permutation. In [8], the authors utilized the additive constants generation method used in MD5 and SHA hash functions as random key stream to encrypt/decrypt text messages.

2.1 Substitution Methods of Cryptography

A substitution method is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns. Various substitution methods are Caesar Cipher, Play fair Cipher, Hill Cipher and One time padding[10].The proposed method ASCII values in the first level of encryption to perform substitution.

2.2 Transposition Methods of Cryptography

A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This method is referred to as a transposition cipher.A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. Cryptanalysis is fairly straightforward. The transposition cipher can be made significantly more secure by performing more than one stage of transposition [10]. The second level of encryption in the proposed algorithm uses transposition using binary tree traversal.

III PROPOSED ENCRYPTION METHOD

This section explains the overall working model of the proposed method. The proposed method uses two levels of encryption. The first level encryption is based on substitution using ASCII values and the second level of encryption is based on transposition using binary tree traversal. ASCII values of alphabets in the plaintext are in the range 65-90 as A-65,B-66 and so on. The SPACE between each word in the plain text is also considered as a separate character and converted to the corresponding ASCII value. Two consecutive characters in the plaintext form a pair. If there are odd numbers of characters in the plaintext, then a SPACE character can be used as filler at the end of the plaintext to form a pair. Position value starts from 1. In each pair, the value on the left is calculated to be the sum of the ASCII value of the left character and the position valueof the right character. Similarly, the value on the right is calculated to be the sum ofthe ASCII value of the right character and the position value of the left character. A complete binary tree is constructed in the second level of encryption. Nodes are constructed from left to right in a complete binary tree. After two levels of encryption, receiver receives the encrypted text which is the level order traversal of the complete binary tree. The overall working model of the proposed method is shown in Figure 2.

ISBN: 978-93-86171-23-8

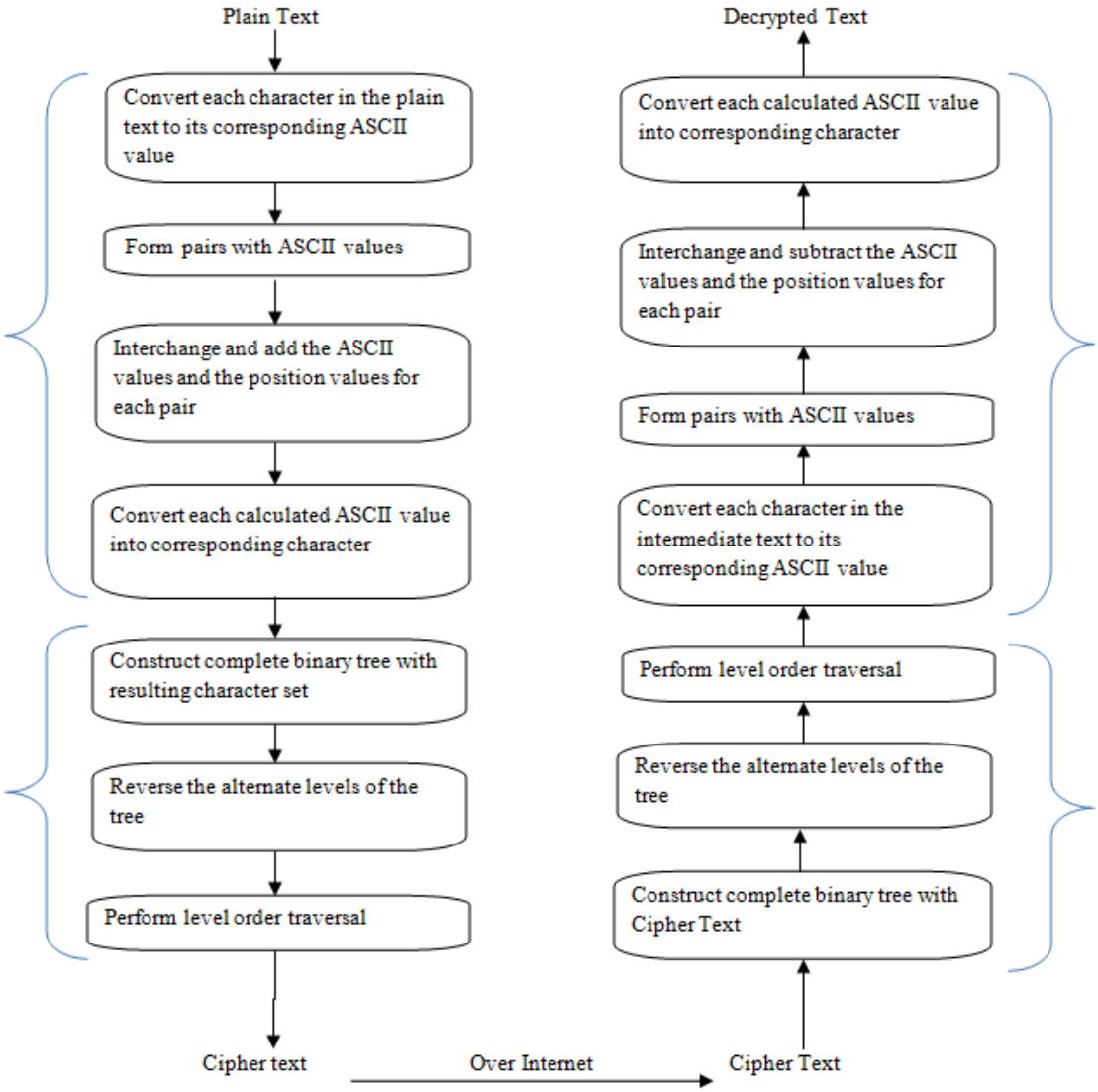

Fig.2 Working model of proposed method

3.1 Illustration of the Proposed Method

In this section, the proposed encryption/decryption method is illustrated with a sample plaintext message.

Plaintext:code red

(a) First Level Encryption

Step 1:Convert the characters in the plaintext to their corresponding ASCII values.

Position	1	2	3	4	5	6	7	8
String	C	O	D	E		R	E	D
ASCII value	67	79	68	69	32	82	69	68

Step 2:Form pairs with the ASCII values.

Position	1	2	3	4	5	6	7	8
ASCII value	67	79	68	69	32	82	69	68

Step 3:Interchange and add the ASCII values.

ISBN: 978-93-86171-23-8

69 80 72 72 38 87 77 75

Step 4:Convert ASCII values back to the corresponding characters.

E P H H & W M K

The obtained intermediate cipher is “EPHH&WMK”.

(b) Second Level Encryption

Input to the second level encryption is “EPHH&WMK”.

Step 1:Construct complete binary tree with the characters in intermediate cipher as shown in Figure 3.

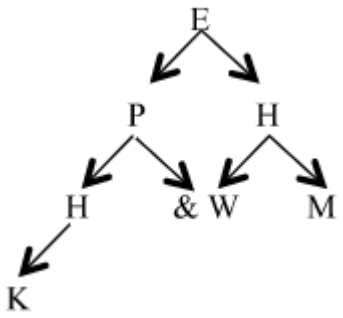

Fig.3Complete binary tree (encryption)

Step 2:Reverse the alternate levels in the complete binary tree as shown in Figure 4.

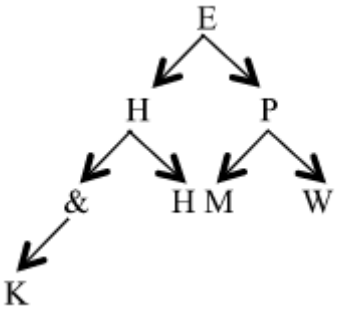

Fig.4Reversing alternate levels (encryption)

Step 3:Perform level order traversal of the resulting tree structure to get the ciphertext.

Thus, the final ciphertext is “EHPH&WMK”.

(a) First Level Decryption

Step 1:Construct a complete binary tree with the characters of the ciphertext as shown in Figure 5.

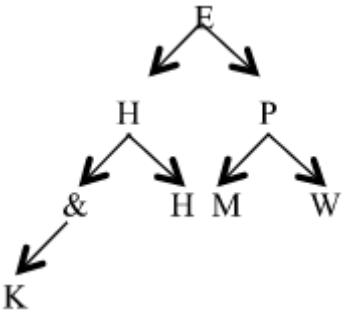

Fig.5Complete binary tree (decryption)

ISBN: 978-93-86171-23-8

Step 2:Reverse the alternate levels of the tree structure as shown in Figure 6.

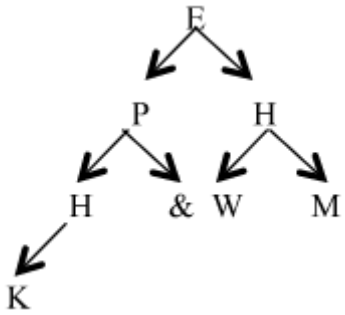

Fig.6Reversing alternate levels (decryption)

Step 3:Perform level order traversal of the resulting tree to get the intermediate text.

Intermediate messageis "EPHH&WMK".

(b) Second Level Decryption

Step 1:Convert the characters of the intermediate message into corresponding ASCII values.

Position	1	2	3	4	5	6	7	8
Intermediate Text	E	P	H	H	&	W	M	K
ASCII value	69	80	72	72	38	87	77	75

Step 2:Form pairs with the ASCII values.

Position	1 2	3 4	5 6	7 8
ASCII value	69 80	72 72	38 87	77 75

Step 3:Interchange and subtract the ASCII values.

	67	79	68	69	32	82	69	68

Step 4:Convert ASCII values back to corresponding characters to obtain the decrypted text.

C	O	D	E	R	E	D

Thus the decrypted message is "code red".

3.2 Encryption Algorithm

In this section, the algorithm for two levels of encryption of proposed method is provided.

3.2.1 First Level Encryption

Input:Plaintext Output:Intermediate Cipher

Step 1: Start

Step2: Convert each character in the plaintext into its corresponding ASCII value

Step 3: Form pairs with the ASCII values of the characters in the plaintext

Step 4: Interchange and add the ASCII values and the position values in each pair

Step5: Convert the calculated ASCII values into the corresponding characters to get the intermediate cipher

Step 6: Stop

3.2.2 Second Level Encryption

Input: Intermediate Cipher Output:Final Cipher

ISBN: 978-93-86171-23-8

Step 1: Start

Step 2:Construct a complete binary tree with the intermediate cipher

Step 3:Reverse the alternate levels in the resultant tree structure

Step 4: Perform level order traversal of the tree to get the final ciphertext

Step 5: Store the ciphertext

Step 6: Stop

3.3 Decryption Algorithm

3.3.1 First Level Decryption

Input: Final Cipher Output:Intermediate Cipher

Step 1: Start

Step 2: Construct a complete binary tree with the ciphertext

Step 3: Reverse the alternate levels of the tree

Step4: Perform level order traversal of the resultant tree to get the intermediate cipher.

Step 5: Stop

3.3.2 Second Level Decryption

Input: Intermediate Cipher Output:Decrypted Text

Step 1: Start

Step 2: Convert the characters in the intermediate cipher to their corresponding ASCII values

Step 3: Form pairs with the ASCII values of the characters in the intermediate cipher

Step 4:Interchange and subtract the ASCII values and the position values in each pair

Step 5:Convert the resultant ASCII values into corresponding characters to get back the decrypted text

Step 6: Store the decrypted message

Step 7: Stop

3.4 Salient features of the proposed method

The following are the salient features of the proposed method:

1. The proposed method uses two levels of encryption which makes it robust against attacks.
2. It makes use of the ASCII values of the characters, swapping, addition, subtraction, construction of a complete binary tree, reversing the alternate levels and level order traversal.
3. It does not use a key explicitly to encrypt and decrypt data.
4. There is no overhead involved in key generation, key distribution/sharing and keeping the key securely.
5. This method is simple and easy to implement.

IV EXPERIMENTAL RESULTS

The proposed method is experimented using C++ language and the system configuration is Processor Intel® Core™ i3 CPU, Clock speed 2.2 GHz, RAM 4GB and the operating system is Windows (64bit). The proposed method is analyzed with various plaintext messages and the corresponding ciphertext messages. The obtained results are tabulated as in Table 1 and Table 2. In Table 1, the obtained results of the first level encryption of the

ISBN: 978-93-86171-23-8

proposed method is given. In Table 2, the obtained result of the first and second level encryption of the proposed method is given.

Table 1 Results of First Level Encryption

S No.	Plaintext Message	Ciphertext
1.	come to graveyard	EPQH&YW'Q[MaSfQaV1
2.	visit us at 3 pm	XJWLZ%]Z*J`+A-`*
3.	george, come soon	IFSUMJ4'MXYP,`_^`1

Table 2 Results of First and Second Level Encryption

S No.	Plaintext	Ciphertext
1.	come to graveyard	EQPH&YWQfSaM[Q'aV1
2.	visit us at 3 pm	XWJLZ%]`-A+`J*Z*
3.	george, come soon	ISFUMJ4_`,PYXM'^`1

The word "COME" appears in the plaintexts 1 and 3. Each occurrence of the word has a different ciphertext based on the position of the word. Similarly, occurrences of the same character in the plaintext also take up different ciphertext character depending on the position of the character. Plaintexts 1 & 3 also have odd number of characters including the space between the words in the plaintext. So, to form a pair, a SPACE has been inserted at the end as filler. Special characters also do appear in the ciphertext which makes the cryptanalysis difficult.

V CONCLUSION

In this paper, a novel encryption method is developed using ASCII values and binary tree traversal. The proposed methodology will give the new area of research on cryptography. This new methodology for encrypting data using ASCII values followed by binary tree traversal is definitely an effective method while compared with other cryptography systems. The proposed method includes both confusion and diffusion properties and resists letter frequency attacks. This method is fast, secure and reliable.

FUTURE SCOPE

In the first level of encryption, other basic arithmetic operations can be used. Operations like mirroring can be implemented on binary tree to further increase the security in the second level encryption.

REFERENCES

[1]. C. Shannon, *"Communication Theory of Secrecy Systems"*, Bell Systems Technical Journal, MD Computing, *Vol. 15*, pp. 57-64, 1998.

[2]. Devendra Kumar Malakar and Prof. Dineshchandra Jain, *"The Problem Analysis on Encryption Techniques in Cryptography", Vol.2,No. 5*, pp.1354-1358, May 2013.

[3]. Obaida Mohammad AwadAlHazaimeh, *"A New Approach For Complex Encrypting And Decrypting Data" in International Journal of Computer Networks & Communications (IJCNC), Vol. 5, No. 2*, pp.95-103, March 2013.

[4]. Sai ram Natarajan,*"A Novel Approach for Data Security Enhancement Using Multi Level Encryption scheme", Vol.2, No. 1*, pp.469-473, 2011.

[5]. S G Srikantaswamy and Dr. H D Phaneendra, *"Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption",* International Journal on Cryptography and Information Security (IJCIS), *Vol. 2, No. 4*, pp.39-49, December 2012.

[6]. Sivakumar T, Keerthana S, and Niveditha A.R, *"A Simple Text Message Encryption Method using Z-Order Curve (Z-oC) Based Permutation",* International Journal of Computer & Mathematical Sciences (IJCMS), *Vol. 5, No. 10*, pp. 37-42, 2016.

[7]. SomdipDey, JoyshreeNath and AshokeNath, *"An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation, Bit Reversal, Modified Caesar Cipher (SD-REE), DJSA method, TTJSA method: SJA-I Algorithm",* International Journal of Computer Applications (IJCA),*Vol. 46, No.20*,pp.46-53, May 2012.

[8]. 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, *Vol. 6, No. 4*, April 2016.

[9]. VineetSukhraliya, Sumit Chaudhary and Sangeeta Solanki, *"Encryption and Decryption Algorithm using ASCII values with substitution array Approach",* International Journal of Advanced Research in Computer and Communication Engineering, *Vol. 2, No. 8*, pp. 3094-3097, August 2013.

[10]. Vinod Saroha, SumanMor and Anurag Dagar, *"Enhancing Security of Caesar Cipher by Double Columnar Transposition Method",* International Journal of Advanced Research in Computer Science and Software Engineering, *Vol. 2, No. 10*, pp.86-88, October 2012.

[11]. Vinod Shokeen and Niranjan Yadav, *"Encryption and Decryption Technique for Message Communication"*,International Journal of Electronics & Communication Technology, *Vol. 2, No. 2*, June 2011.

[12]. William Stallings, *"Cryptography and network security-principles and practice"*Pearson Education, New Delhi, 2013.

ISBN: 978-93-86171-23-8

AUTHORS PROFILE:

Dr.T.Sivakumaris currently working as an Assistant Professor in the Department of Information Technology, PSG College of Technology, Coimbatore-641004,India. His research interests include information security and cryptography.



Ms. Humshavarthini K,**Ms. Jayasree M** and **Mr. Eswaran M** are the final year students of B.Tech-Information Technology, in the Department of Information Technology, PSG College of Technology, Coimbatore-641004, India.