Indian Journal of Science and Technology, Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/86648, December 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Secure Aware Communication using Novel End To End (ETE) Cipher Algorithm

M. Lavanya[1*], G. Aishwarya[2], S. Keerthana[2], V. Vaithiyanathan[1] and S. Saravanan[1]

[1]School of Computing, SASTRA University, Thanjavur - 613401, Tamil Nadu, India; m_lavanyass@ict.sastra.edu, vvn@it.sastra.edu, saran@core.sastra.edu
[2]Information and Communication Technology, SASTRA University, Thanjavur - 613401, Tamil Nadu, India; ishwaryagunasekeran@gmail.com, keerthisiva.ict@gmail.com

Abstract

This article aims to bring a novel method in cipher algorithm for secure aware communication. This paper proposes a unique scheme and ensures higher security during encryption and decryption process. The Key (ki) is generated for every Plain text pi. Plain text and key are converted to their equivalent ASCII values, by which the scrambled Cipher text (ci) is generated by implementing some of the concepts of the substitution techniques. During Decryption, the corresponding (ki) are used to recover the Plain text pi. It makes sure the need to send the full length key along with the cipher text for decryption process. The suggested method assures the greater security during transmission. There is a practical hindrance in guessing the Number of rounds (N) and the number of bits n shifted, by Cryptanalyst. This method will be more suitable for analyzing the discover key (ki) values from attempting Brute Force technique.

Keywords: Ciper Algorithms, Cryptanalyst, Decryption, Encryption, Secure Communication

1. Introduction

Cryptography becomes essential part of the secure communication. There are two types of Cryptographic algorithm to accomplish these goals: Symmetric Cryptography and Asymmetric Cryptography. The primary message is known as plain text, while scrambled message is known as cipher text. The conversion of plain text to cipher text is known as enciphering or encryption. Recovering the plain text from the scrambled message is known as deciphering or decryption. If both encryption and decryption are performed using the identical key, then the system is referred to as symmetric or single key. If both encryption and decryption uses distinct keys, then the system is referred to as asymmetric or two key. In this paper we introduce an algorithm that is modification to existing Vernam cipher algorithm. This algorithm performs N Number of rounds, and n number of bits shifted, which depends on the key value.

The flawless secrecy of the vernam cryptographic system, commonly called as the One Time Pad (OTP), which is proved by shanon in 1949. From then, it has been trusted that, the random uncompressible OTP is transmitted, which has its length equal to the message.

This paper[1] is based on kerchoff's principle, assuming that opponent knows both the encryption and decryption techniques. This paper uses many classical encryption schemes such as vignrecipher, hillcipher, etc., It is found that the variation of the key used for each plain text to be encrypted ensures higher security. But the negative side is dealing with large amount of keys. This can be overcome by using simple computation for greater security. Keys are generated by using shift and Exor operation.

This paper[2] retains the probity of the network security using several encryption and decryption techniques. Confidentiality of the message should be retained for prosperous transmission.The symmetric key is used by both sender and receiver. This paper encompasses three

*Author for correspondence

layers for encryption and decryption such as transposition, randomization and quadratic encryption and decryption linearly. The probity of the message is conserved by using hash code generation and verification.

This paper[3] formulates a new cryptographic primeval that focused on encryption and decryption of the message to any Unicode language. The encrypted text would be a composition of characters from various languages. Here the algorithm used is magnification of one time pad cipher implementing pseudo random numbers. In this paper[4] they proved that the length of OTP, has necessary information and need not to be compromised, which might be less than the length of message relinquishing without flawless secrecy.

This paper[5] provides distinct way to implement the OTP. In this paper, OTP encryption technique is achieved by using both block cipher and one way hash. Cipher text is obtained by encrypting each bit of the plain text by modular addition with each bit of the confidential random key, whose length is equal to its plain text length. It is very difficult to decrypt/break the cipher text (without having any knowledge about the key) if the key is random and never reused whose length is equal to its plain text, kept secret.

To establish secure channel over the internet, authentication key exchange protocol have been developed. This paper[6] is based on Diffiehellman key exchange using one time-ID. It is an identity of the user, which is used only once. This paper proposes a three party key exchange protocol to overcome the attacks like eavesdropping, impersonation, etc. In this paper[7], authors have proposed two way method named TTSJA. For both encryption and decryption, they have implemented bit manipulation method and randomized key matrix. This presented work introduces vernam cipher in 2 different directions: First, XOR operation is performed between first character to last character and then last to first. In second phase, XOR operation is performed between keypad and encrypted message from the first phase.

The length of the key should be of maximum 16 letters.

This paper[8] implements symmetric key encryption, which uses same pattern of both encryption and decryption. To yield better security, this method implements the generation of internal key at receiver side and uses 512 bits as its key size. The brute force attack is prevented by storing internal key in the sender side database, which is further transformed to the receiver side database through another channel. Stream cipher algorithms are used in different protocols like SSL, Bluetooth etc, which provides data telecommunication security, on the other public algorithm face security problems. This paper[9] proposes a systematic stream cipher algorithm. At each round it produces 23 random bits by random number generator in parallel fashion and also produces initial vector of 115 bits. High speed communication link can be easily implemented by this algorithm.

This paper[10] yields benchmark instruction on protection over short messages using one time pad. This method provides complete message security. If this method is applied properly, then it is mathematically unsustainable to break the decrypted message without the key. This paper[11] presents an enormous number of information security methods. One Time Pad guarantees higher security. There are more cryptographic transformations, which provides guarantee for conditional security but they are not perfect. The basic requirement is key, which should be random in nature. Hardware generator is used to produce keys, which are bit sequence in random fashion. Presently we are provided with electronic device, which produces random sequence in binary at 100Mbit/s. It is capable of constructing systematic key generation, where we require long keys.

The algorithm assures big data security, in group oriented services which requires trusted server. This increases complexity in computation. In this paper[12], they constructed key transfer over group, based on sharing the secret big data. This is based on Diffie Hellman agreement and LSSS.

2. Proposed Technique

Cryptography provides many techniques to provide security to the information transferred over the network. This protection ensures the objectives of preserving the integrity, availability and confidentiality of the plain text. To improve existing environment, we have introduced End to End cipher algorithm, which raises the security level of information. In this proposed method, the length of the key is equal to the plain text.

Both plain text and key are converted to its equivalent ASCII values which are further converted to its corresponding binary values. Before proceeding the N number of rounds in the End to End cipher, preprocessing of the plain text and key are performed. In preprocessing, the binary values of plain text and key are XOR-ed from one end of the plain text to the other end of the key (i.e). XORing the plain text with reversed binary value of that key.

As we said before, Number of rounds N to be performed is based on the Diffie Hellman algorithm. Let n be the number of bits to be shifted right. The value of n is evaluated by dividing the highest ASCII value of the key by 16. The value N is calculated by the following procedure:

- Let prime number u and an integer r, that is a primitive root of u be two publicly known numbers.
- Sender selects a secret number a and sends receiver, Q = (r^amod u).
- Receiver selects number b and sends a sender, S = (r^b mod u).
- Sender computes number of rounds
  N = ((r^b mod u)^a mod u)
  (or) N = ((S)^a mod u).
- Receiver computes
  N = ((r^a mod u)^b mod u)
  (or) N= ((Q)^b mod u).
- Both sender and receiver can use this number as their number of rounds N.

If the value of n has floating number, neglect all the fractional part and take the value of an integer part. In first round, n bits are shifted to the rightmost end of the key. For forthcoming rounds, the same n bits are shifted to the rightmost end of the previous round shifted key values. At each round the shifted key values are reversed and XOR-ed with the results of previous round XOR-ed values. This process is continued up to N rounds. The output of the Nth round is converted to its equivalent decimal values and further converted to its corresponding characters Eg: (0 = A, 1 = B…). This scrambled value is the Cipher text of the proposed End to End cipher algorithm. The sender and receiver shares encryption algorithm, key, Q and S through the Trusted Third Party.

At Decryption side, Cipher text is converted into its integer values (i.e.,) A = 0, B = 1…. The obtained decimal values are converted into its binary values. The rounds to be performed at decryption side is just reverse processperformed during encryption. The plain text can be recovered by converting the binary values of Nth round to its ASCII values, and further to its corresponding character.

3. Block Diagram

The block diagram of End To End cipher algorithm is given below Figure 1. This diagram depicts the process

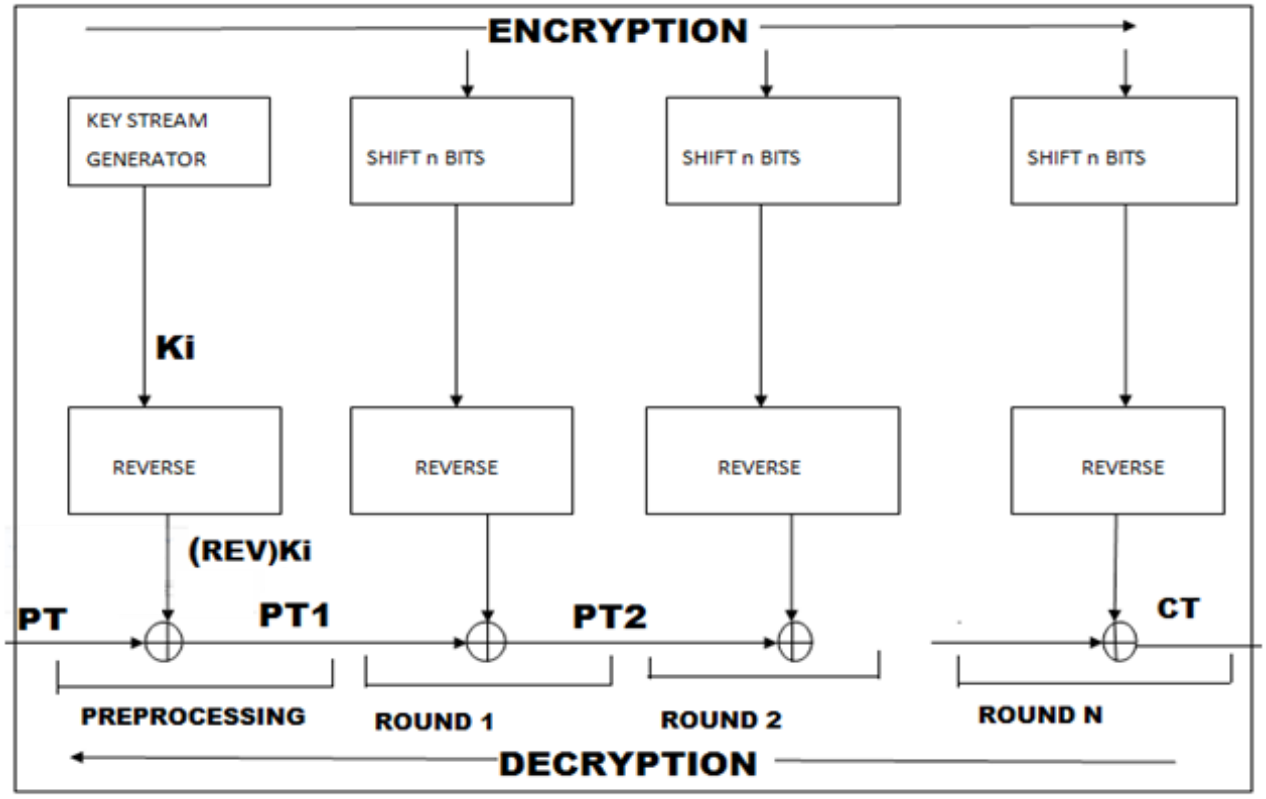

Figure 1. Block diagram of ETE.

of both Encryption and Decryption of ETE algorithm. The key ki is generated by Key Stream Generator. Before proceeding to N number of rounds, plain text pt and key ki is undergone preprocessing (i.e.,) reversed key value is XORed with plain text pt. The output of the preprocessing stage is given as input to the Round 1. N number of rounds is performed. At each round key ki values are shifted right by n bits. The shifted bits are reversed and XORed with the previous round output, to get the output for present round. The reverse procedure of this Encryption gives us Decryption.

4. Pseudocode

4.1 Encryption

BEGIN
INPUT : PT(Plain Text), K(key)

- Choose a key with length equal to plain text.
- Convert both Plain text and key into its ASCII values and then to their equivalent binary values.
- In preprocessing
  $PT_1 = PT_b(XOR)_{(REV)}K_b$ //plain text is XOR-ed with the reversed key value
  PT_b = binary value of plain text,
  K_b = reversed binary value of key.
- Calculate n :
  n = MAX(ASCII in K)/16 // n is calculated by dividing the highest ASCII value by 16
  n = number of bits shifted right.
- Calculate N :
  $N= ((r^b \bmod u)^a \bmod u)$
  (or) $N= ((S)^a \bmod u)$
  N = Number of rounds to be performed.
- Shifted key values are XOR-ed with the result of previous round XOR-ed value
  $PT_2 = PT_1 (XOR)_{(rev)}K_{(nRShift)}$ // at round 1.
  Where n = 1,
- $K_{nRShift}$ = n bits of key value are right shifted.
- At Nth Round, cipher text is obtained
  $CT_b = PT_N (XOR)_{(rev)}K_{(nRShift)}$
  CT_b = binary values of the cipher text,
  $K_{(nRShift)}$= multiples of n bits values are right shifted.
- Convert the binary values of the cipher text to its corresponding decimal values, and then to its respective characters Eg: 0 = A, 1=B….

END

4.2 Decryption

INPUT: K (Key), CT (Cipher text)
BEGIN

- Cipher text is converted to its equivalent integer values, and then to its binary values.
- Calculate N:
  $N= ((r^a \bmod u)^b \bmod u)$
  (or) $N= ((Q)^b \bmod u)$.
- At round 1 in decryption
  $PT_N = CT_b (XOR)_{(rev)}K_{(nRShift).}$
- After Round N,
  $PT_b = PT1 (XOR)_{(rev)}K$.
- Obtained PT_b is converted to its equivalent ASCII values, from which the plain text PT is recovered.

END.

5. Comparision Chart

The analysis of Vernam cipher, Monoalphabetic cipher, and Vignere cipher are abstracted in Figure 2 and also in Table 1. It is clear that ETE algorithm secures data from both Brute Force attack and Cryptanalyst. The advantage of ETE algorithm is the length of the cipher text is greater than the plain text.

6. Conclusion

In this paper we proposed new technique named ETE (End To End cipher), in which Number of rounds N and number of bits n to shifted right are not constant. N is determined by using Diffie Hellman algorithm and n is evaluated based on key value. This algorithm can be

Table 1. Comparison table

	Vignere cipher	Mono alphabetic cipher	Vernam cipher	ETE
Symmetric method				
Brute force attack				X
PT.length!= CT.length	X	X	X	
Absence of relative frequency	X	X		
Key length	X		X	X

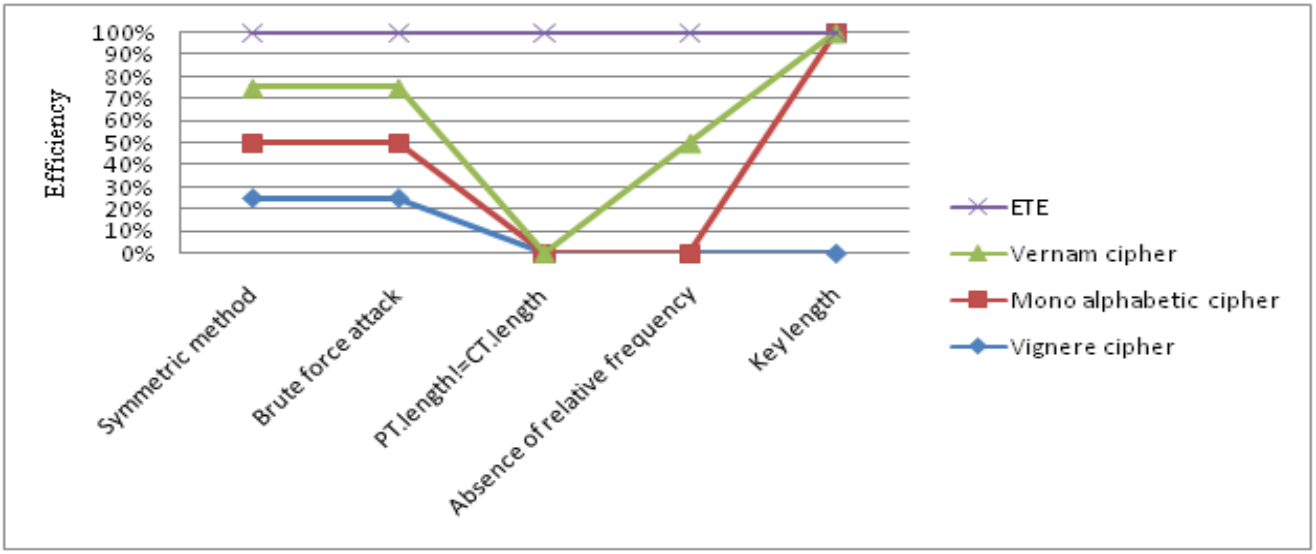

Figure 2. Proposed method comparison chart with existing methods.

further enhanced by reducing length of the key or by compressing the plain text.

7. References

1. Mohan M, Devi MK, Prakash VJ. Security analysis and modification of classical encryption scheme. Indian Journal of Science and Technology. 2015; 8(14):542–8.
2. Vincent PM, Raj D, Amber IS, Karan B, Kamalkant K. Cryptography: Mathematical approach. Indian Journal of Science and Technology. 2013; 6(12):5607–11.
3. Tandon A, Sharma R, Sodhiya S, Vincent PMD. Universal encryption algorithm using logical operations and bits shuffling for Unicode. Indian Journal of Science and Technology. 2015; 8(15):1–5.
4. Nithin N, Vivek V, Vaidyal G. Revisiting the one time pad. IJNS Journal. 2008; 6(1):94–102.
5. Chandrakar S, Shree JB, Shrikant T. An innovative approach for implementation of OTP. IJCA Journal. 2014; 89(13):35–7.
6. Imamoto K, Sakurai K. Design and analysis of Diffie Hellman based key exchange using one time ID by SVO logic. Electronic Notes in Theoretical Computer Science. 2005; 135(1):79–94.
7. Chatterjee T, Das T, Dey S, Nath J, Nath A. Symmetric key cryptography using two way updated-Generalized vernam-cipher method: TTSJA algorithm. International Journal of Computer Applications. 2012; 42(1):34–9.
8. Pandey KK, Rangari V, Siteshkumar SK. An enchanced symmetric key cryptographic algorithm to improve data security. International Journal of Computer Applications. 2013; 74(20):29–33.
9. Aizanini, Bakhtiari MM. An efficient stream cipher algorithm for data encryption. IJCSI Journal. 2011; 8(3):247–53.
10. Dirk R. The complete guide to secure communication one time pad cipher. Cipher Machines and Cryptology. 2014.
11. Borowski M, Grzonkowski M, Lesniewicz M, Wicik R. Generation of random keys for cryptographic systems. Annales UMCS Informatics. 2012; 12(3):75–87.
12. Hsu C, Zeng B, Zhang M. A novel group key transfer for bigdata security. Applied Mathematics and Computation. 2014; 249:436–43.