Safe Light Weight Cipher using Ethernet and Pentatop Number

J. Harikrishna, Ch. Rupa, P. Raveendra Babu

Abstract. Current essential factor in this world to send a sensitive information over the unsecured network like the internet is security. Protection of sensitive data is becoming a major raising problem due to rising technologies. A recent attack on Electronic Mail of CBI shows that attacker's efficiency rate. Standard cryptographic algorithms can be exploited by the attackers frequently and unable to apply for standard devices because of their energy consumption due to high computation with slow processing. Lightweight cryptography based algorithms can reduce these problems. This paper deals with symmetric key cryptography technique to encrypt the data where the sender and receiver share a common key which can also be called a secret key cryptography. To encrypt and decrypt the data, randomly generated Pentatope Number has used as a key. Next level of security will be provided using EHA (Ethernet Hardware Address or MAC Address) which is globally unique, to provide secure data transmission. The increasing of attacks on related key attacks motivates this. In particular, we investigate the efficiency impact comparatively other standard algorithms and observed that applications do not always use cryptographic algorithms without their intended use.

Keywords: Light Weight Cryptography, Pentatope Number, EHA, Secret key, Authentication

I. INTRODUCTION

With the help of internet we are communicating with millions of people and it is used as a tool for commerce and hackers are also becoming more powerful nowadays. Security becomes more tremendous. There are many applications and aspects, which range from private communications, secure commerce and payments and password protection. One essential aspect among them for security is cryptography for secured data transmission. Cryptography is the science of information security and it is the study of techniques for communication between the authorized users in the presence of adversaries (third parties). Communication has done in a secure way. Cryptography, closely related to cryptology and cryptanalysis. It has used to protect the e-mail messages, corporate data, credit card information etc. Cryptography mainly deals with encryption and decryption. Encryption is the conversion of information/data from a readable form to unreadable format. At present, cryptography based on mathematical approaches and computer science practice. This involves all legitimate users of information having the keys require accessing that information. The sender who sends the encrypted message (cipher text) shares the decoding technique needed to convert the plain text (original message) only with intended recipients, thereby avoiding un-authorized persons to do the same.

Revised Manuscript Received on 30 July 2019.
* Correspondence Author

J. Harikrishna, Ch. Rupa*, Dept of Computer Science and Engineering V R Siddhartha Engineering College (A), Vijayawada
P. Raveendra Babu Dept of Computer Science and Engineering V R Siddhartha Engineering College (A), Vijayawada

Cryptography is discipline or techniques employed on the electronic messages by converting them into unreadable format by using secret keys. Depending on the key used, encryption techniques divided into different types.

In the traditional symmetric Key Cryptography (SKC), use only single key which is kept secret for both encryption and decryption. This can uses in most common algorithms such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard). It extends to Asymmetric Key Cryptography (AKC) which uses two keys, one for encryption and another for decryption. E.g.: RSA (Rivest, Shamir, Adleman) algorithm [14]. Any one from these approaches chosen to protect the data (Confidentiality) as well as for authentication hash Functions have to be used by the users. In this hash technique we use mathematical transformations irreversibly "encrypt" information. E.g.: MD (Message Digest) algorithm is an example. The main objectives of the proposed algorithm is

- To improve confusion and diffusion rate by using variable length key.
- To provide authentication with the simple and secure method instead of traditional Hash functions like MD5, SHA.
- To emphasize importance of light weight cryptography.
- To provide Confidentiality and Authentication services with a single algorithm.

In this paper, a stream cipher based light weight encryption method has proposed, where integrity and privacy security services can be satisfied in a single pass without additional computational burden. Certainly, it is not similar to any traditional cryptographic approaches. The reminder of this paper as in section 2, we presented some preliminary concepts. Section 3 consists of methodology of proposed stream cipher. In section 4, we discussed about the results analysis with applicability of the proposed scheme. Finally, concluding with future contribution.

II. PRELIMINARIES

Block-cipher operates on blocks, which are as units of bits. The length of the block should vary such as 8, 16, 64,etc. That is depending on the developers. Let us consider the length of the block as 'n' [11,12].

Definition 2.1 : [Block Cipher]. A n-bit block cipher defines as $E: k \times M \rightarrow R$, such that $k \in$ keys, $m \in M$. Where permutations performs from $M = \{0,1\}^n$ which relates to the original text to $R = \{0,1\}^n$ which relates to the encrypted text (cipher text).

The encryption function can performs by the chosen key randomly from the set of keys, keys = $\{0,1\}^k$, such that $E_k(m) = C\ \forall C \in R$. The decryption function is shown as D: k x R → M. $D_k(C) = m$.

Definition 2.2 : [Random Function]. A random function G(n, r) holds that the functions related to f: M → R where M = $\{0,1\}^n$ and R = $\{0,1\}^n$ and a key is the entire function f.

III. PROPOSED EHA BASED AUTHENTICATED ENCRYPTION (EPA)

In the existing techniques, keys involving prime numbers, Armstrong numbers [3] are used. As a step further, we consider a technique (EPA) which involves randomly generated Pentatope value as a key. Here the key size is variable and for more security we append Ethernet Hardware Address (EHA or MAC Address) and row number of the generated Pentatope value to the cipher text using delimiter semi-colon (;) and send it to the receiver. EHA based Pentatope Algorithm process has shown as shown in Fig 1.

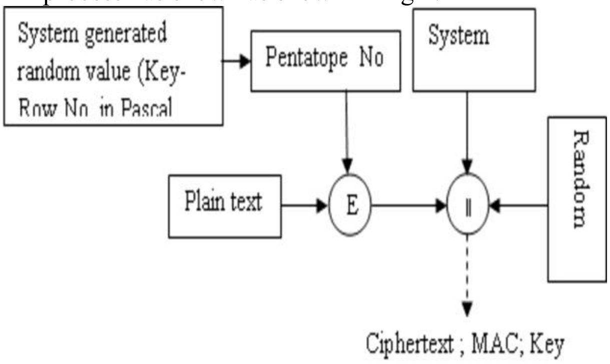

Fig 1. Proposed System State Chart

In the 5th column of a Pascal's triangle [15] as shown in figure 2 can be founded a Pentatope number. These numbers can represent as regular and discrete geometric patterns. The nth Pentatopic number has derived from Eq (1)

$$P_4(n) = \binom{n+3}{4} = \frac{n(n+1)(n+2)(n}{24}$$

(1)

In the fig 2 marked numbers are the pentatope value of the specified row. In this way, can generates any number of rows randomly. To provide more security, we consider the pentatope value from the row > 8 onwards in the proposed system.

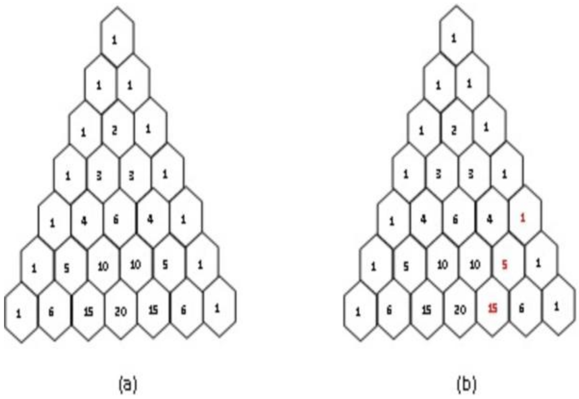

Fig 2. (a) Pascal Triangle (b) Pentatopical Numbers (1,5,15,….n)

Table 1 shows that randomly generated number (Pascal Triangle row number) that has considering as an external key while transmitting along the ciphertext to the receiver and·its corresponding Pentatopical value.

Table 1 Randomly Generated External Key

Random Key (Row Number-External Key)	Pentatopic Value (Inside Key)
20	3876
40	82251
15	1001
25	10626
30	23751
35	46376
45	135751
10	126
12	330

In the proposed system, plaintext (P_t) t bits are XORed with n bits of the Pentatope number (P_n) which has generated by a random key. Thereafter, n bits of the result ($P_t \veebar P_n$) have complemented, that is, $(P_t \veebar P_n)^1$ and then apply 2's complement on $C_t \longleftarrow (P_t \veebar P_n)$ and then fed in as input to the next round. This cycle has repeated up to completion of 8 –rounds in the encryption process as shown in fig 3. Later appends the randomly generated number as an external key and EAH value of the receiver. The resultant (C_b) sends to receiver in order to this every receiver extract the plain text and verifies EAH value

$$C_t \longleftarrow \overline{(P_t \veebar P_n)^1} + 1$$

(2)

$$C_b \longleftarrow C_t \parallel Random\ Key \parallel E$$

(3)

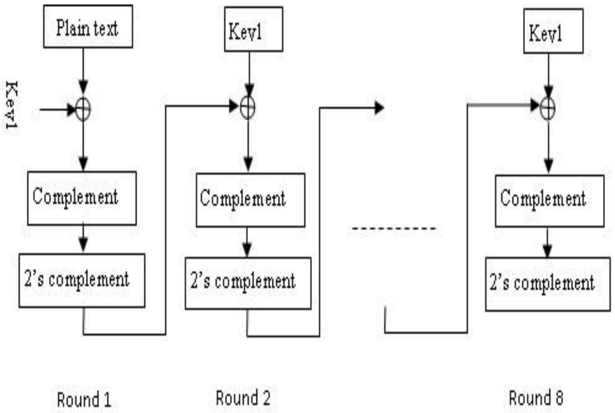

Fig 3. 8-Rounds Logic

When the receiver receives the data that has been sent by the sender, observes it and splits the data such that the key should be generated at the receiver side based on the row no and MAC Address (Ethernet Hardware Address) has to be compared. If the receiver entered MAC Address and the MAC Address which has been sent by the sender does not match, message cannot be decrypted and hence the person is recognized as an un-

Retrieval Number: B2105078219/19©BEIESP
DOI: 10.35940/ijrte.B2105.078219
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

authorized one otherwise the person is recognized as legitimate user and the cipher text is decrypted using the randomly generated key and decryption algorithm which produces the plain text (original message).

Step1 - Sender will enter the data (plain text) which he wants to send it to the receiver.

Step2 - Generate the random number (row no), based on that the pentatope value (Variable Key) is computed from Pascal's Triangle.

Step3 - Perform 8 rounds operations using twos-complement addition, complement, and Exclusive OR operations on the plain text using pentatop number that can generates from random key. This process will do during encryption process.

Step4 - After the encryption process, the resultant cipher text will produced.

Step5 - Using delimiter (;) the resultant cipher text appended with MAC Address and row no (cipher text + MAC Address + row no = data, let's consider) is sent to the receiver.

At receiver side, in-order to decrypt the message, the following process will done.

Step1- On receiving the data (i-e., cipher text + MAC Address row no) the receiver observes it and splits the data using the delimiter (;)

Step2- Receiver has to know the senders MAC Address, and then he has to compare the MAC Address sent by the sender with the MAC address which he knows, and check whether it comes from the authorized user (sender) or any one modifies it.

Step3- If receiver detects that the data has come from authorized user, he will generate the key using row no (which has sent by the sender).

Step4- After the key has generated, receiver will decrypt the cipher text using the key and the inverse encryption process (decryption) has done here.

The above algorithm uses a different approach in generating the key and this provides secure communication between the authorized users. Intruder will not able to generate the key even though he analyses the traffic flow in the network.

3.1 Resistance to KPA and Brute Force Attack

The main advantages of the proposed method are reduce the attacks like Known plain text (KPA) and Brute force by the following way can be achieved the objectives also [9, 10]. The EPA method uses the variable length key which has generated from system generated random number >8, therefore the attacker has less chances for doing attacks on the key with the length *length*(M) < n > 8 where 'M' is message.

Whenever EHA validation success then only can do extraction process by any receiver with the help of External Key (Ext_key : Pascal Row Number). It has works like a Zero-Knolwedge Authentication protocol. Only authorized legitimate persons who have known about the sender's and receivers EHA addresses can able to involve in the process. Authentication has provided by using Ethernet Hardware Address (EHA) by comparing the EHA of sender at receiver side during decryption.

```
If (sender (EHA) = = Reciever (EHA))
  then extract (Ext_Key)
      generates (pent(Ext_Key))
```

As the key generate randomly, the attacker will not able to analyze the key that has to be generate at next phase which can also be reduces the brute force attack. Tracing process also become difficult because this method will not involve the sharing of the key between sender and receiver. Data Secrecy has accomplished by performing the number of rounds during encryption and decryption process. Therefore, in-order to this the key length can be increased if needed, with increase in the character length. The main applications of this work where can be used for generating the passwords at sensitive environment like bank sectors, military code generations and for generating the session keys, etc.

IV. RESULTS AND ANALYSIS

Table 2 shows the comparative analysis of different encryption algorithms such as FISH (Fibonacci Shrinking) [8], RC4 [7], Achterbahn [6], CryptMT [4], AES (Advanced Encryption Standard) [9], Cheating Text [2], Quantum Cryptographic approach [3] along with their attacks information. Here, considered 20,527 bytes of information as the average for reporting comparative analysis.

Table 2. Comparative Analysis of Ciphers

Attributes	**Stream/ Block**	**Symmetric/ Asymmetric**	**Key Length**	**Speed (Cycles Per bytes)**	**Best Known Attack**
FISH (1993) [8]	Stream	Symmetric	Variable	N/A	Known Plain Text Attack (2^{11})
RC4 (1987) [7]	Stream	Symmetric	8 – 20148 (Generally 40 -256)	7 (W_{P5})	KPA-Known Plain Text Attack (2^{13}), Fluhrer, Mantin and Shamir attack
Achterbahn 128/80 (2006) [6]	Stream	Symmetric	80/128	1 (H/W)	Brute Force Attack (>2^{48})
CryptMT (2005) [4]	Stream	Symmetric	Variable	N/A	Brute Force Attack (>2^{50})
AES [9]	Block	Symmetric	128/192/256	4	Related Key Attacks

Cheating Text (2009) [2]	Stream	Symmetric	Variable	N/A	Brute Force Attack (>2^{26})
Quantum (2014) [3]	Stream	Symmetric	Variable	N/A	Brute Force Attack
Proposed Method (EPA)	Stream	Symmetric	Variable	3.12 (W_{64})	N/A

Fig 4 shows that experiment for comparing the performance of various encryption algorithms The results showed that EPA (proposed light Weight Cipher) has a good performance compared to other algorithms.

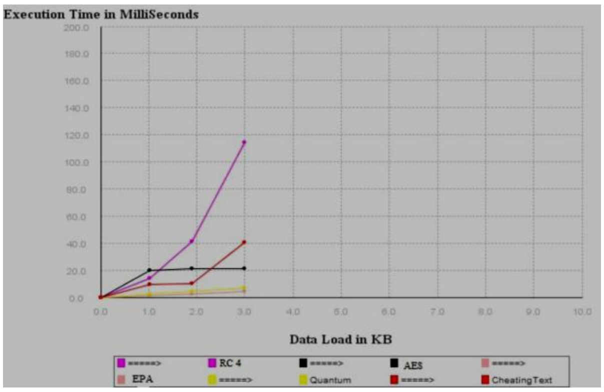

Fig. 4. Comparison Speed of various Ciphers

V. CONCLUSION

EHA and Pentatopical Number based technique can apply mainly in the premises where sensitive data has been handling. It can reduce the cyber attacks on the data like recent attack on Electroinic mail (E-Mail) of CBI (Central Bureau of Investigation). The usage of MAC address ensures that only the authorized persons access the data. The usage of randomly generated pentatope value ensures that the hacker cannot know the key value. It has privacy and protection feature in a single pass by doing concatenation of EHA (Ethernet Hardware Address) with the Cipher value by Pentatope numbers. This approach has mainly developed to say that without using prime numbers also greater security can provided. Further, we would be tested this cipher applicability on various applications of IoT (Internet of Things).

REFERENCES

1. Tzonelih Hwang, "Robust stream-cipher mode of authenticated encryption for secure communication in wireless sensor network", Security and communication Network, Wiley, vol. 9, (2016), 667-679.
2. Ch. Rupa, P.S. Avadhani, "Message Encryption Scheme Using Cheating Text", IEEE Int. Conf on Information Technology, New Generations, Lasvegas, USA, (2009), 470-474.
3. ValerioScarani, ChristianKurtsiefer, "The black paper of quantum cryptography: Real implementation problems", Journal of Theoretical Computer Science, Vol. 560, (2014), 27-32.
4. Khazaei Far, Shahram & Shakour, Elham, " Distinguishing Attack on CryptMT", (2008)..
5. Haina Zhang, Xiaoyun Wang, "On the Security of Stream Cipher CryptMT v3", (2009),eprint.iacr.org/2009/110.pdf.
6. Naya-Plasencia M, "Cryptanalysis of Achterbahn-128/80". In: Biryukov A. (eds) Fast Software Encryption. FSE 2007. Lecture Notes in Computer Science, vol 4593, (2007), 73-86, Springer, Berlin, Heidelberg
7. T. D. B. Weerasinghe, "An effective RC4 stream cipher", International Conference on Industrial and Information Systems, Vol. 8, (2013), IEEE, Srilanka.
8. Blöcher U., Dichtl M, " Fish: A fast software stream cipher". In: Anderson R. (eds) Fast Software Encryption. FSE 1993. Lecture Notes in Computer Science, vol 809, (1994) , 41-44, Springer, Berlin, Heidelberg
9. Dobbertin H., Knudsen L., Robshaw , " The Cryptanalysis of the AES – A Brief Survey", In: Dobbertin H., Rijmen V., Sowa A. (eds) Advanced Encryption Standard – AES. AES 2004. Lecture Notes in Computer Science, vol 3373, (2005), 1-10, Springer, Berlin, Heidelberg.
10. 10.Dmitry Khovratovich, "Attacks on Advanced Encryption Standard: Results and Perspectives",Microsoft Research, RSA Conferences, (2012),.
11. 11.Tezcan, Cihangir,et al., "Differential Attacks on Lightweight Block Ciphers PRESENT, PRIDE, and RECTANGLE Revisited" Lightweight Cryptography for Security and Privacy, (2016), 18-32, Springer.
12. 12.Yibin Dai, Shaozhen Chen, "Cryptanalysis of full PRIDE block cipher", Science China Information Sciences, 2017
13. 13.Delfs H., Knebl H, "Symmetric-Key Cryptography", In: Introduction to Cryptography. Information Security and Cryptography, (2015) , 11-48, Springer, Berlin, Heidelberg.
14. 14.McLoone M., Robshaw M.J.B, "Public Key Cryptography and RFID Tags". In: CT-RSA 2007. CT-RSA 2007. Lecture Notes in Computer Science, vol 4377, (2006), 372-384, Springer, Berlin, Heidelberg.
15. 15.John F. Putz, "Pacal Polytopes: An Extension to N Dimensions of Pascal's Triangle." College Mathematics Journal. Vol. 17. No. 2. (1986), 144-155