RCES REVIEW OF COMPUTER ENGINEERING STUDIES

ISSN: 2369-0755 (Print), 2369-0763 (Online)
Vol. 4, No. 2, June 2017, pp. 67-69
DOI: 10.18280/rces.040205
Licensed under CC BY-NC 4.0

A publication of IIETA

IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

http://www.iieta.org/Journals/RCES

Elliptic curve cryptosystem (ECC)

Jyotsna K. Mandal[1*], Arindam Sarkar[2], Avijit Bose[3], Sharmistha Halder[3]

[1] Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia Pin 741235, India
[2] Department of Computer Science and Electronics, Ramakrishna Mission Vidyamandira, Belur Math, Howrah Pin 711202, India
[3] Department of Computer Science and Engineering, MCKV Institute of Engineering, Liluah, Howrah Pin 711204, India

Email: Jkm.cse@gmail.com

ABSTRACT

Security is very essential for all over the world. In every minute researchers are engaged in finding out the best possible way to make the security stronger. Many techniques are used to implement the security by the researchers. The ECC (Elliptic Curve Cryptosystem) is one of the simplest method to enhance the security in the field of cryptography. The aim of this paper is to generate light weight encryption technique based on the ECC method. Here, the session key is generated to secure the original message. SHA2-512 and SHA2-224 bits hash algorithms are applied for session key generation. First of all, plaintext character is taken by the user, the character is converted into ASCII value and then implement ECC technique on it.

Keywords: ECC Method, Addition Operation, SHA2 Hash Algorithm, Elliptic Curve Over GF(p), Session Key Based Encryption.

1. INTRODUCTION

In older days, Symmetric key Cryptography concept is used. But there are such problems like to secure the transmission channel through which the message is transmitted or to keep the key securely, as there is only one key is used. To overcome this problem asymmetric concept is used in the field of cryptography. ECC is an asymmetric key cryptography concept, where two keys are used for encryption and decryption purpose of the message. The elliptic curves are used to make ECC [2, 3, 4, 5] where variables and coefficients are limited by the domains of the finite fields [6]. Mainly work has been done by using two fields of elliptic curves in ECC such as GF(p) [7, 8] and GF(2^m). In this proposed cryptosystem, prime curve over GF(p) is applied using addition operation. The variables and coefficients are taken by the set of integer values (range between 0 to p-1) in the prime field over GF(p). The original message which the sender wants to send the receiver is called Plaintext. The method in which the plaintext is hidden its actual text is called encryption. Encrypted Plaintext message which is hard to make out called cipher-text [1]. The conversion of unreadable data to readable data (the actual message) is called decryption [13].

2. PROBLEM STATEMWNT

Though ECC has provided a higher amount of data to be passed with equal security as compared to other techniques, ECC has less randomness and robustness technique. ECC has many attacks on the system which causes the weaken immunity power.

3. RELATED WORK

The excellent solution is specified by the ECC for encrypting any data and the key is exchanged securely between sender and receiver [9], and the session key establishment protocol is authenticated [10, 11, 12]. The different characters are represented by the coordinates of the elliptic curve in the ECC based system, which can be generated [15]. The cryptographic process has been evaluated by using Koblitz method [16].

Singh and Gillhorta [14] is explained how to encrypt the passage of the document to a mathematical notation in between zero and one. After converting this mathematical noation to binary number, the binary number is encrypted by using one time key. Here, each character is represented by a picture element (3 pixel values are Red, Green and Blue which is represented by integer).

Sobti and Geeta [17] is explained the requirement of hash functions, its different formation, the recent improvement of hash functions and different attacks on the hash functions.

4. MATHEMATICAL BACKGROUND

ECC (Elliptic Curve Cryptosystem) is based on mathematical structure of elliptic curves. Elliptic curves are also called as elliptic integral. The basic equations which are used in the ECC technique are -

$$y^2 = x^3 + ax + b$$

$$\boxed{\lambda = (y_2 - y_1)/(x_2 - x_1)}$$

$$\boxed{\begin{aligned} x_3 &= \lambda - x_1 - x_2 \\ y_3 &= \lambda(x_3 - x_1) + y_1 \end{aligned}}$$

$\lambda = (3x_1^2 + a) / (2y_1)$

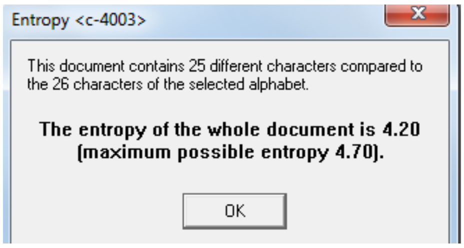
5. PROPOSED WORK

5.1 Session key generation algorithm

- **Step-1:** SHA2-512 bits algorithm is applied for generation of 64 bytes/512 bits digest of the secret key.
- **Step-2:** 4 byte plaintext and 1 byte CRC are concatenate to 5 bytes, SHA2-224 bits is used on this. After that first 96 bits of 224 bits is truncated.
- **Step-3:** These truncated bits are divided into 6 bit group for selecting 16 bytes from the 64 bytes digest, getting 6 bit values equals to 1 byte of 64 bytes digest, the session key1 is formed.
- **Step-4:** Using AES algorithm, the key is applied on the plain-text for forming the cipher-text.

In Elliptic Curve Cryptosystem, if the session key is generated using the above algorithm, then it will be performed better than another cryptosystem. The session key size may be generated by 10cycles of repetition for 128 bit key size or 12cycles of repetition for 192 bit key size. The session key is changed frequently throughout each session and it will enhance the good security. The session key generation will be integrated into the ECC based system to increase the randomness and robustness of the security.

6. RESULT OF ANALYSIS

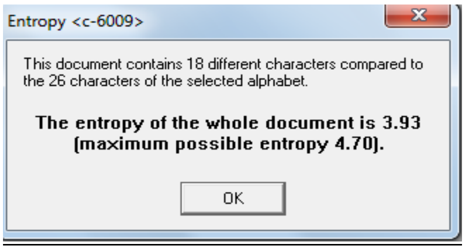


Entropy <c-4003>

This document contains 25 different characters compared to the 26 characters of the selected alphabet.

The entropy of the whole document is 4.20 (maximum possible entropy 4.70).

Figure 6.1 Analysis of entropy of proposed ECC technique



Entropy <c-6009>

This document contains 18 different characters compared to the 26 characters of the selected alphabet.

The entropy of the whole document is 3.93 (maximum possible entropy 4.70).

Figure 6.2 Analysis of entropy of RSA technique

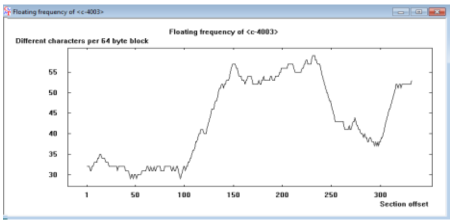


Figure 6.3 Analysis of floating frequency of proposed ECC technique

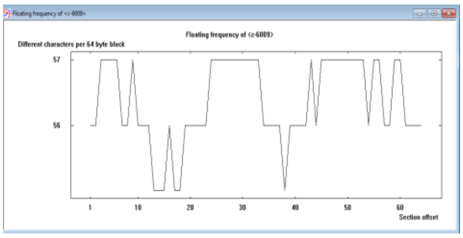


Figure 6.4 Analysis of floating frequency of RSA technique

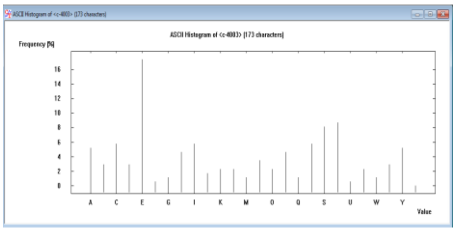


Figure 6.5 Analysis of histogram of proposed ECC technique

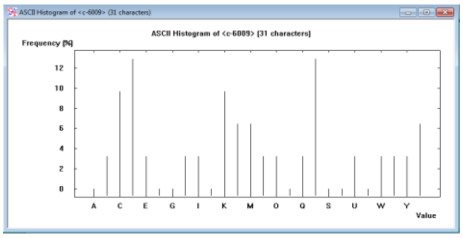


Figure 6.6 Analysis of Histogram of RSA technique

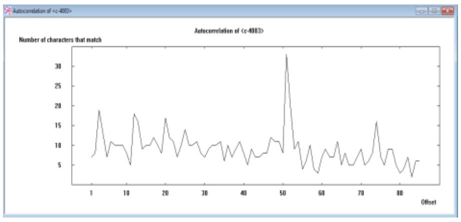


Figure 6.7 Analysis of autocorrelation of proposed ECC technique

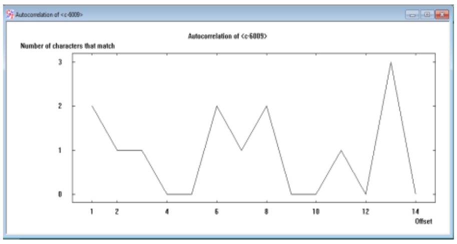
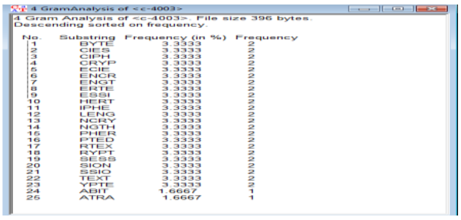


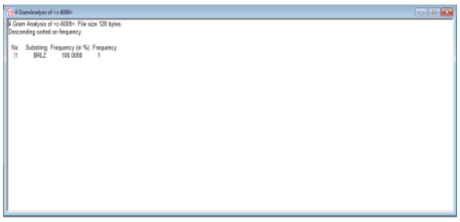
Figure 6.8 Analysis of autocorrelation of RSA technique



```
4 Gram Analysis of <c-4003>. File size 396 bytes.
Descending sorted on frequency.

 No.    Substring  Frequency (in %)  Frequency
  1       BYTE          3.3333           2
  2       CIES          3.3333           2
  3       CIPH          3.3333           2
  4       CRYP          3.3333           2
  5       ECIE          3.3333           2
  6       ENCR          3.3333           2
  7       ENGT          3.3333           2
  8       ERTE          3.3333           2
  9       ESSI          3.3333           2
 10       HERT          3.3333           2
 11       IPHE          3.3333           2
 12       LENG          3.3333           2
 13       NCRY          3.3333           2
 14       NGTH          3.3333           2
 15       PHER          3.3333           2
 16       PTED          3.3333           2
 17       RTEX          3.3333           2
 18       RYPT          3.3333           2
 19       SESS          3.3333           2
 20       SION          3.3333           2
 21       SSIO          3.3333           2
 22       TEXT          3.3333           2
 23       YPTE          3.3333           2
 24       ABIT          1.6667           1
 25       ATRA          1.6667           1
```

Figure 6.9 Analysis of N-gram of proposed ECC technique



```
4 Gram Analysis of <c-6009>. File size 128 bytes.
Descending sorted on frequency.

 No.  Substring  Frequency (in %)  Frequency
 1      BRLZ        100.0000          1
```

Figure 6.10 Analysis of N-gram of RSA technique

The implementation results show that, the proposed cryptosystem has acquired somehow or apart better results from any existing cryptosystem, the proposed cryptosystem destroys any existing patterns in the input and also it, maximizes entropy. The n-grams, autocorrelation, histograms and floating frequency shows that the proposed cryptosystem is secure against RSA method of the cipher text.

7. CONCLUSION & FUTURE SCOPE

Although the ECC is not evaluated completely, the Proposed technique is very simple and easy to implement. The test results also show that the performance and security provided by the Proposed technique is somehow or apart good and comparable to standard technique. The security provided by the Proposed technique is comparable with other techniques.

The future scope of this proposed technique may be done using Choas technique. In future, some other ECC based approach can be used to generate the session key.

ACKNOWLEDGMENT

The authors are gratefully acknowledged to the ICAST 2017 (International Conference on Advances in Science & Technology) and MCKV Institute of Engineering on Computer Science & Engineering department to give the opportunity of publishing the paper work.

REFERENCES

[1] Khate A. Cryptography and network security, Tata MC Graw.

[2] Anna M.J., Peter S.G. (2002). Authentication key exchange provably secure against the man-in-middle attack, *Journal of Cryptology*, Vol. 2002, No. 2, pp. 139-148.

[3] Antoines J. (2004). Aone round protocol for tripartite Diffie-Hellman, *Journal of Cryptology*, Vol. 17, No. 4, pp. 263-276.

[4] Srjen A., Lenstra K., Verheul E.R. (2001). Selecting cryptographic key size, *Journal of Cryptology*, Vol. 14, No. 4, pp. 255-293.

[5] Chandrasekhar A., et.al. (2007). Some algebraic curves in public key cryptosystems, *International Journal of Ultra Scientists and Physical Sciences*.

[6] Gura N., Shantz S., Eberle H., et al. (2002). An end-to-end systems approach to elliptic curve cryptography, Sun Microsystems Laboratories, from http:// research.sun.com / projects/crypto accessed on 10 May.

[7] Darrel H., Alfred M., Scott V. (2004). A guide to elliptic curve cryptography, Springer.

[8] Rosing M. (1999). Implementation ECC Greenwich, CT: Manning Publications.

[9] Suneetha C., Sravana K.D., Chandrasekhar A. (2011). Secure key transport in symmetric cryptographic protocols using Elliptic curves over finite fields, *International Journal of Computer Applications*, Vol. 36, No. 1.

[10] Chandrasekhar P.K.R., Sebastian M.P. (2010). Elliptic curve based authenticated session key establishment protocol for high security applications in constrained network environment international, *Journal of Network Security & Its Application (IJNSA)*, Vol. 2, No. 3.

[11] Kin C.Y., Amol D.A. (2010). Light-weight mutual authentication and key-exchange protocol based of Elliptic Curve cryptography for energy-constrained devices, *International Journal of Network Security & its Applications*, Vol. 2, No. 2.

[12] Mohsen M., et.al. (2010). Coupled FPGA/ASIC implementation of elliptic curve crypto-processor, *International Journal of Network Security & Its Applications*, Vol. 2, No. 2.

[13] http://ijctonline.com/ojs/index.php/ijct/article/view/426.pdf

[14] Singh A., Gilhorta R. (2011). Data security using private key encryption system based on arithmetic coding, *International Journal of Network Security and Its a (IJNSA)*, Vol. 3, No. 3.

[15] Sravana K.D., Suneetha C.H., Chandrasekhar A. (2012). Encryption of data using elliptic curve over finite field, *IJDSP*, Vol. 3, No. 1.

[16] Padma B.H., Chandravathi D., Prapoorna R.P. (2010). Encoding and decoding of a message int the implementation of elliptic curve cryptography using Koblitz's method, *IJCSE*, Vol. 2, No. 5.

[17] Rajeev S., Geetha G. (2012). Cryptographic hash functions: a review international, *Journal of Computer Science Issues*, Vol. 9, No. 2.