International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 7 482 – 485

An Attempt to Improve Data Security in Text Based Cryptosystem Using Elliptic Curve Cryptography

Saudamini B. Ingale[1], Miheeka G. Chaudhary[2], Anjali R. Patil[3],Aishvarya Akshaya V.[4], Dhanashree Toradmalle[5]

[1,2,3,4]Student, B.E. Information Technology, Shah and Anchor Kutchhi Engineering College, Mumbai-400 088, India.
[5]Assistant Professor, Information Technology, Shah and Anchor Kutchhi Engineering College, Mumbai-400 088, India.
[1]*damini.ingale@gmail.com*, [2]*miheeka.chaudhury@gmail.com*, [3]*anjalipatil289@gmail.com*,
[4]*aakshayav10@gmail.com*, [5]*sakec.dhanashreet@gmail.com*

***Abstract*—**Data can be debilitated by hackers and spies. Cryptography helps us find better approaches to secure information in digital form. Elliptic Curve Cryptography (ECC) is favorable over numerous cryptographic systems because of smaller keys and quick key generation. This paper proposes a system which intends to provide multifold security in text based communication. The system has two main modules: encryption, and decryption. Encoding scheme which works on variable length text block mapping technique has been exhibited, thereby enhancing data security provided by ECC in text based cryptosystems. To leverage the advantages of ECC, it is being used in many applications. This papers attempts to utilize ECC in text based cryptosystems efficiently.

Keywords- *ECC, ASCII, Text based cryptosystem, variable length mapping, encoding.*

*****

I. INTRODUCTION

The security of ECC (Elliptic Curve Crytpography) mainly lays on ECDLP[1] (Elliptic Curve Discrete Logarithmic Problem) on the EC (Elliptic Curve) points. The fundamental fascination of ECC over RSA (Rivest-Shamir-Adleman algorithm) and DSA (Digital Signature Algorithm) is that it takes full exponential time while the latter take sub-exponential time. Although smaller keys are used in ECC as contrasted to other cryptosystems such as RSA, the provided security level is equal. ECC, an emerging attractive public-key cryptosystem, also offers lower power consumption along with memory and bandwidth savings.

The elliptic curve over a finite field $E(F_p)$ forms an abelian group under addition. This cryptosystem features three main operations[2]: Point addition, Point Doubling and Point Multiplication.

Let the two points on the elliptic curve be $P(x_1,y_1)$ and N(x2,y2). Then the addition of above two points will give a third point Q on the same elliptic curve where Q=P+N= $Q(x_3,y_3)$. The *point addition* over finite field is computed using the equations:

$$\lambda = (y_2 - y_1)/(x_2 - x_1)$$
$$x_3 = \lambda^2 - (x_1 + x_2)$$
$$y_3 = \lambda (x_1 - x_3) - y_1$$

Doubling of point P will give point $Q(x_3,y_3)$ such that Q=2P. *Point doubling* over finite field is computed using the equations:

$$\lambda = (3x_1^2 + a)/ 2y_1$$
$$x_3 = \lambda^2 - 2x_1$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

Point Multiplication: Scalar multiplication of a point P by a scalar k as being performed by repeated point addition and point doubling. Many algorithms are available for performing scalar multiplication efficiently[3].

Various protocols have been implemented over Elliptic Curve. One of the public key agreement protocols, which is based on ECC, is Elliptic Curve Diffie-Hellman (ECDH)[4]. It enables the execution of Diffie-Hellman key trading algorithm using a group of points on an elliptic curve.

II. LITERATURE REVIEW

Since ECC can encrypt and decrypt only a point, comparative analysis of some important encoding schemes to map text onto a point on EC can be understood from the paper[5], A Survey of Different Encoding Schemes for Improving the Efficiency of Text Based Cryptosystem using ECC.

JayabhaskarMuthukuru and BachalaSathyanarayana[6] have placed forth mapping techniques for text based messages of fixed and variable lengths. Their paper presents implementation of mapping of a text message into multiple points on elliptic curve with Initial Vector (IV). Here, the text message is initially divided into blocks, and every block is EX-ORed with the IV. Then the resultant block is turned again into ASCII (American Standard Code for Information Interchange) format of base 256 format. At the receiver side, an equivalent whole encryption method is applied in reverse manner to get the corresponding plaintext message block. In

 ISSN: 2321-8169
482 – 485

fixed length block mapping technique, the block size is fixed before beginning the encoding method, whereas in variable length block mapping technique, every word is taken into account as a block and null characters are cushioned to the IV or message block to equate their lengths.

S. Pramela Devi and Sindhuja K.[7] have proposed a algorithm which includes application of genetic functions after getting intermediate cipher. In this paper, a genetic rule based elliptic curve cryptosystem has been proposed. Here the message (plaintext) is encoded as x-y point on elliptic curve. Then the key pair's non-public and public keys are calculated. Then the generated keys are used over the plaintext to encrypt it and supply associate degree intermediate cipher. Then the intermediate cipher is passed to the genetic functions crossover and mutation to supply the ultimate or final cipher.

In his paper[8],Marc Joye has portrayed a basic system to accelerate the arithmetic operations in ECC by utilizing appropriate to-left strategies. In specific settings, this prompts a non-insignificant execution increment contrasted with the left-to-right partners. In Elliptic curve point multiplication — namely, the computation of Q = [k]P given a point P on an elliptic curve and a scalar k —it's productivity relies on upon various elements: the field definition, the elliptic bend show, the interior point portrayal and, obviously, the scalar augmentation technique itself (which likewise incorporates point expansion and point multiplying strategies).Fundamentally, there exist two primary groups of scalar augmentation strategies, contingent upon the bearing scalar k is examined: left-to-right techniques and ideal to-left techniques. Suitable choice of point augmentation calculation is required by the application where ECC is being used..

III. PROPOSED SYSTEM

Fig.1 shows the overall workflow of the proposed system. The EC parameters such as a, b, p and G are agreed between the sender and receiver before the communication begins, where '$y^2 = (x^3 + ax + b) \bmod p$' is the EC equation. The system presented in this paper consists of the following modules:

A. Encryption – Plaintext to Ciphertext

1. Plaintext Encoding

In this phase, the proposed framework[6] involves a mapping method for text messages of variable length utilizing ECC. Refer Fig.2.

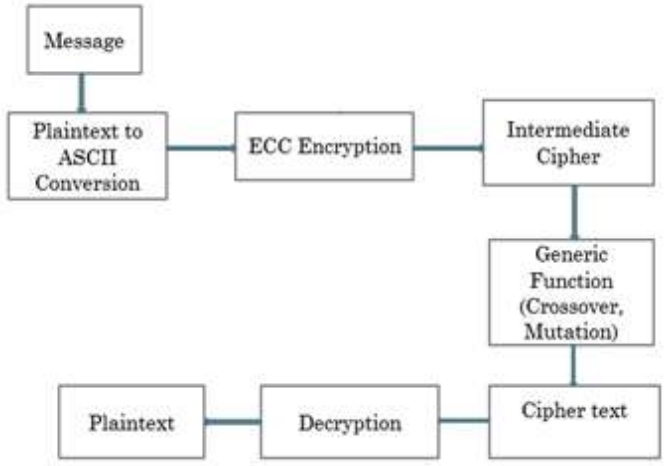

Figure 1. Overall System

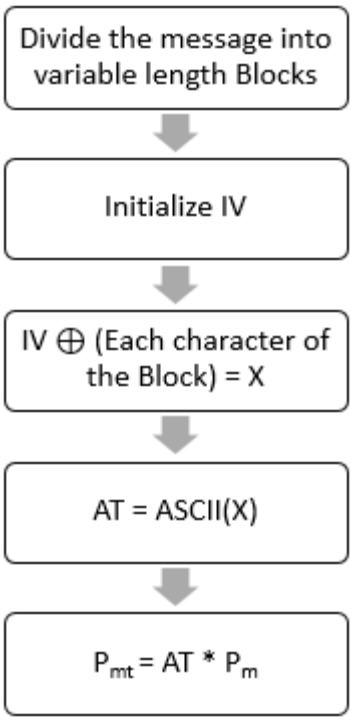

Figure 2. Mapping a message block onto an affine point on elliptic curve

This strategy gives mapping of atext message into multiple points on elliptic curve with an Initial Vector (IV). The text message is initially partitioned into blocks and each character in the block is EX-ORed with the IV. The resultant block obtained is converted into ASCII convention of base 256 format. This value is used as a multiplier to the chosen starting point of the elliptic curve to transform/map the message block into an affine point.

Message: Input text/string

IV: Initialization Vector

G: Base point of the selected EC

X: EXOR resultant

AT: ASCII value of the EX-ORed string

P_m: Base point or the Chosen starting point of EC

P_{mt}: Transformed Point corresponding to a block of message

2. Basic ECC Encryption

The two points using formulae for Cm, as shown in Fig.3, also known as intermediate cipher points are calculated.

3. Obtaining final Ciphertext

The next phase involves performing genetic functions[9] – 2-point crossover and bit flip mutation - on the intermediate cipher points. Refer Fig.3. The crossover points are chosen and agreed upon between the communicating parties.

k: random number

P_B: Public key of receiver

C_m: Intermediate cipher

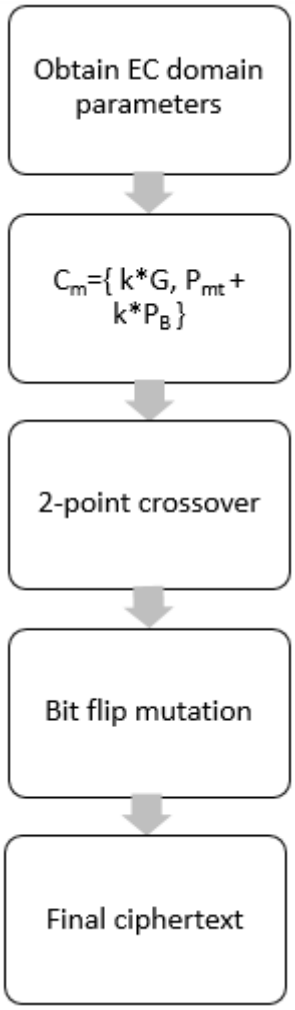

Figure 3. Affine Point to Final Cipher

B. Decryption – Ciphertext to Plaintext

In decryption process using ECC, the key is 'scalar multiplication'. At the receiver side, the same entire encryption process is applied in reverse manner to obtain the corresponding plaintext message block. Each character in the block is obtained sequentially which together form the message block, thereby keeping this sub-process transparent to the user. Scalar multiplication is the way for the utilization of elliptic curve for asymmetric cryptography; the basic operation is itself genuinely straightforward, however its reverse (the elliptic curve discrete logarithm) is exceptionally difficult. Decryption is done with the assistance of private key of the receiver where the operation utilized with it is point multiplication. Refer Fig. 4.

n_B: Private key of the receiver.

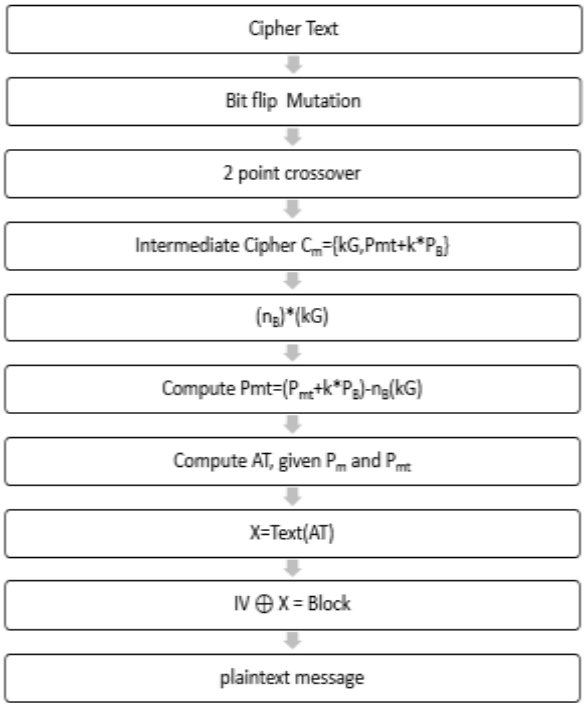

Figure 4. Decryption.

IV. RESULTS

The algorithm takes a string as input and separates it into words, after which each word is processed character-by-character through the algorithm proposed.

Output snippet 1:

Enter the input string:

The quick brown fox jumps over the lazy dog.

Outputsnippet 2: shows the results of algorithm when encryption is implemented on character T from the above input:

Biginteger value of IV:[50]

k:29

AT:102

Pmt: 337 , 33

C1= kG: 596 , 661

kPb : 194 , 123

C2 = Pmt+kPb : 82 , 254

CROSSOVER

Parent 1 -- binary kG:10010101001010010101

Parent 2 -- binary C2:00010100100011111110

crossover point:4

crossover point:12

child1:

10010100100010010101

child2:

00010101001011111110

MUTATION:

mutation child1:01101011011101101010

mutation child2:11101010110100000001

Final Cipher Points :

Point I:429,874

Point II:939,257

Output snippet 3 shows the results of algorithm when decryption is done on the ciphertext obtained from the above snippet:

reverse mutation chld1:10010100100010010101

reverse mutation child2:00010101001011111110

child1:

10010101001010010101

child2:

00010100100011111110

Receiver side C1 : 596 , 661

Receiver side C2 : 82 , 254

nkG : 194 , 123

RPmt : 337 , 33

Value of AT on receiver side:102

returned ASCII:102

binary value of X:1100110

plaintext in ASCII form after xor:84

plaintext:T

Similarly after executing the algorithm over the whole input string, we get the plaintext message back as shown below:

The quick brown fox jumps over the lazy dog.

BUILD SUCCESSFUL (total time: 4 seconds)

The proposed system can also encrypt and decrypt input from plain text files (such as files with .txt and .xml extensions).

V. FUTURE SCOPE

Awareness about Elliptic Curve Cryptography is raising day-by-day among communities working in the field of security. Few standard implementations over ECC such as ECDSA and ECDH can be used to raise level of protection in the current cryptosystems. They can also be incorporated in various proposed systems utilizing ECC such as the above one. Complexity based analysis can be employed to compare these existing systems with the proposed system and discover its areas of application further. Also the difficulty of the proposed system can be raised by affiliating genetic algorithm(GA) with it; GA can be employed to optimize some or all of the elliptic curve domain parameters.

REFERENCES

[1] Darrel Hankerson, Alfred Menezes, and Scott Vanstone, “Guide to Elliptic Curve Cryptography”, Springer: 2014, pp. 153-154.

[2] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, “Implementation of Text Encryption using Elliptic Curve Cryptography”, IMCIP: 2015.

[3] Kaalidoss Rajamani and Dr. A. Arul L.S., “Survey: Elliptic Curve Cryptography using Scalar Multiplication Algorithms”, International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 1: March 2014.

[4] Kaalidoss Rajamani and Dr. A. Arul L.S., “Survey: Elliptic Curve Cryptography using Scalar Multiplication Algorithms”, International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 1: March 2014, pp. 3.

[5] Prof. Dhanashree Toradmalle, Saudamini B. Ingale, Miheeka G. Chaudhary, Aishvarya Akshaya V., and Anjali R. Patil, “A Survey of Different Encoding Schemes for Improving the Efficiency of Text Based Cryptosystem using ECC”, IJCA: November 2016.

[6] Jayabhaskar Muthukuru and Bachala Sathyanarayana, “Fixed and Variable Size Text Based Message Mapping Techniques Using ECC”, Global Journal of Computer Science and Technology, Volume 12, Issue 3, Version 1.0: February 2012.

[7] S. Pramela Devi, Sindhuja K., “A Public Key Cryptosystem using ECC and Genetic Algorithm”, IJERT, 2014.

[8] Marc Joye, “Fast Point Multiplication on Elliptic Curves Without Precomputation”, Vol. 5130 of Lecture Notes in Computer Science, Springer, 2008, pp. 36-44.

[9] http://www.obitko.com/tutorials/genetic-algorithms/crossover-mutation