A Public Key Cryptosystem using ECC and Genetic Algorithm

S. Pramela Devi
Department of Computer Science & Engineering
M.V.J College of Engineering
Bangalore, India

Sindhuja K
Department of Computer Science & Engineering
M.V.J College of Engineering
Bangalore, India

***Abstract*— Elliptic Curve Cryptography is a public key cryptographic technique based on elliptic curve theory. In this paper we propose a genetic algorithm based elliptic curve cryptography. Here the message (plaintext) is encoded as x-y point using elliptic curve. Then the key pair's private and public keys are calculated. Then using the above generated keys the plaintext point is encrypted to produce an intermediate cipher. Then the intermediate cipher is passed to the genetic functions crossover and mutation to produce the final cipher. The proposed algorithm provides a greater security using elliptic curve cryptography and genetic algorithm.**

Keywords— Plaintext, ciphertext, ECC

I. Introduction

Information security is the process of defending information from unauthorized access. Cryptographic techniques are used to encrypt and decrypt the information and provide confidentiality, integrity and authentication of the data. There are two types of cryptographic techniques symmetric key and asymmetric key cryptography [2]. Symmetric key cryptography uses same key to encrypt and decrypt the message where as the other uses two keys (private, public) for encryption and decryption.

Elliptic Curve Cryptography (ECC) is a public key cryptographic technique based on algebraic structure of elliptic curve over finite fields. In public key cryptosystem the public key is shared between the participants. The elliptic curve has a property that any two points in the elliptic curve is used to produce a new point on the curve [9]. The elliptic curve cryptography uses smaller key size and reduces the processing overhead. ECC is the second generation public key systems based on RSA algorithm and Diffie – Hellman key exchange algorithms.

ECC uses elliptic curve which consists of points satisfying the equation $y^2= x^3 + ax +b$ defined over the finite field E_p and a, b are real numbers belongs to E_p and x and y take on values in the real numbers. The security of ECC depends on difficult of discrete logarithmic problem. Given some point on the curve it is difficult to find the value of key k. The main operation involved in ECC is a point multiplication (i.e) multiplication of scalar k with any point p in the curve to obtain the point q in the curve [3]. Points in curve are defined as in terms of x, y coordinates. Elliptic curves are used in Bitcoin, Secure shell, and providing security in Transport layer.

Genetic algorithm is a heuristic search algorithm based on natural genetics and natural selection. Genetic algorithm is based on evolutionary programming which uses stochastic optimization techniques. There are many basic operations used in the genetic algorithm such as crossover, mutation, inheritance and selection [8]. Genetic algorithm provides convenient representation of genetics and their parts are easily aligned due to their fixed size which easily aligned due to their fixed size, which helps for crossover operations. Once the genetic representation and the fitness function are defined, a GA proceeds to initialize a population of solutions and then to improve it through repetitive application of the reproduction, crossover, mutation and inversion operations.

Reproduction or selection operation produces new better strings in the new population. In crossover operation child string is produced by combining two parent strings. There are many types of crossover techniques used namely single point crossover, two point crossovers, multipoint crossover [5]. Mutation operation is used to maintain the generic diversity from parent string to next generation child string. There are many types of mutation such as bit string, flip bit, boundary, non uniform, uniform and Gaussian. In this paper we use two point crossover and flip bit mutation techniques for encryption and decryption.

II. The Proposed Method

The proposed algorithm uses the following steps to perform encryption and decryption

1. Plaintext encoding and Key generation
2. Encryption
3. Crossover and Mutation

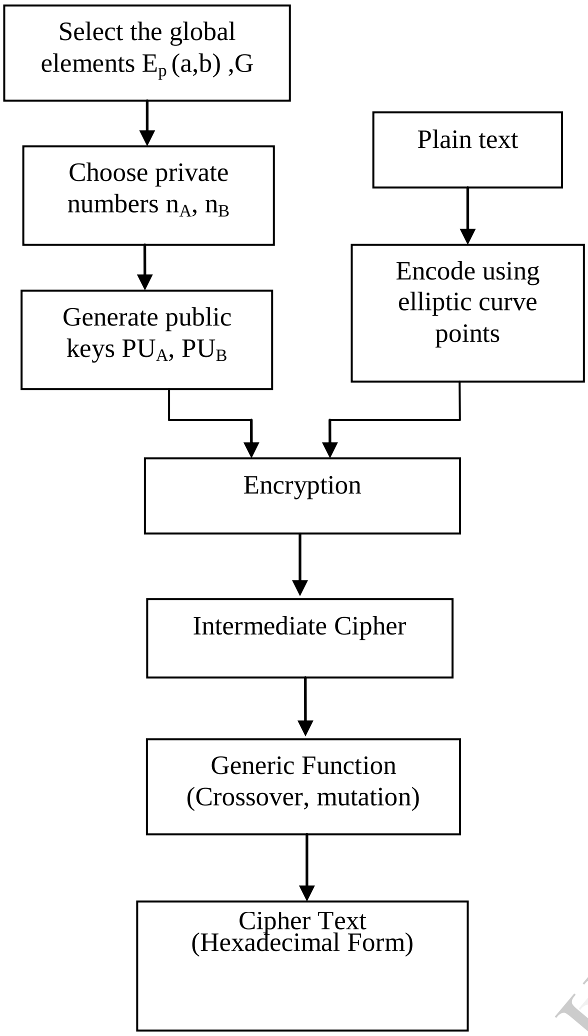
Select the global elements E_p (a,b) ,G
Choose private numbers n_A, n_B
Generate public keys PU_A, PU_B
Plain text
Encode using elliptic curve points
Encryption
Intermediate Cipher
Generic Function (Crossover, mutation)
Cipher Text (Hexadecimal Form)

Fig1. Flow diagram for encryption

A. *Plain text encoding & Key Generation:*

- Encode the message M using x-y point in elliptic curve to get P_m.
- Select two public global elements E_p (a,b) and G where a, b are elliptic curve parameters and p is a prime number , G is a point in an elliptic curve.
- Select two private numbers n_A and n_B for A and B
- Calculate public keys PU_A and PU_B by multiplying private numbers n_A and n_B by G respectively
- Generate key in A , k=n_A X PU_B, and in B k = n_B X PU_A

B. *Encryption Algorithm*

- Select the generated key k
- Produce an intermediate cipher

  IC_m= [kG, P_m+kPU_B]
- A genetic functions 2 point crossover and mutation are applied to IC_m to produce the cipher text.
- The cipher text and crossover points are sent to the receiver to retrieve the original plaintext.
- Public keys PU_A , PU_B , G and Ep(a,b) are globally shared between A and B.

C. *Decryption Algorithm:*

The step for decryption algorithm is reverse of an encryption algorithm. First reverse mutation and crossover functions are used to get the intermediate cipher. Then B calculates the plaintext by using the following formula

$$P_m = kPU_B - n_B(kG)$$

D. *Example*

- Select a integer p=751, and elliptic curve parameter is E_p(-1,188) and point on elliptic curve G=(0,376) Sender A select a plaintext and encode as a plaintext point P_m using elliptic curve.
- B select a private key PR_B= 85 and calculate the public key PU_B= 85(0,376) = (671,558) and send to A
- A select a random number k = 113, and use PU_B to encrypt the message.
- After encoding the plaintext P_m= (443,253) calculate intermediate cipher

  IC_m = (kG,P_m+KPU_B)

  IC_m=((113(0,376)),((443,253)+ (671,558))

  IC_m= ((34,633),(217,606))

1) *Crossover and Mutation*

- Convert the above intermediate cipher into equivalent binary.

  00100010 00000010 01111001

  11011001 00000010 01011110
- Divide the above binary streams into two parts.

  001000100000001001111001

  110110010000001001011110
- Apply 2 point crossover to the above binary stream

  001000100000001001011001

  110110010000001001111110
- Apply mutation to the above stream

  110111011111110110100110

  001001101111110110000001
- Divide the binary stream into 8 bits

  11011101 11111101 10100110

  00100110 11111101 10000001
- Convert the stream into hexadecimal we get

  DD FD A6 26 FD 81

The cipher text ((DD, FDA6), (26, FD81)), 921 is send to the receiver. Here ((DD, FDA6), (26, FD81)) is a cipher text and 9, 21 are crossover points.

III. Analysis

The proposed algorithm uses discrete logarithm concept to produce an intermediate cipher and crossover, mutation function to produce the cipher text. So it is expected when the encryption and decryption is done by proposed the algorithm the order growth will be O (√n).

IV. Conclusion

The proposed method provides good level of security. It is difficult for the intruder to hack the message because of the properties of the elliptic curves. The key used to generate the intermediate cipher is less in length when compared to the keys used in RSA algorithm, so it takes less CPU consumption and less memory to store and process the data. Here public key elliptic curve cryptography is used along with the genetic algorithm to ensure greater security and confidentiality of data.

In the future we are planning to use different types of encoding methods to create a plaintext point. The algorithm can be analysed by using different plaintext and key pairs. Also different elliptic curves can be used to achieve a better level of security.

References

[1] A.Tragha , F.Omary, A.Mouloudi ,” ICIGA: Improved Cryptography Inspired by Genetic Algorithms” , International Conference on Hybrid Information Technology ,IEEE, 335-341,2006.

[2] Behrouz A. Forouzan, “Cryptography & Network security “, Tata McGraw – Hill , 2007.

[3] Douglas, R.Stinson, “Cryptography – Theory and Practice “, CRC Press, 1995.

[4] Holland J. “Adaptation in Natural and Artificial Systems” University of Michigan Press, Ann Arbor, Michigan, 1975.

[5] P. Stepaj, G. Marin, “Comparison of a crossover operator in binary coded genetic algorithms,” Wseas Trans. on Computers, 9 , 1064–1073, 2010.

[6] Subhranil Som, Niladri Shekhar Chatergee, J.K Mandal, “Key Based Bit Level Cryptographic Technique (KBGCT)”, 7th International Conference on Information Assurance and Security, 2011

[7] M. Mitchell, “An Introduction to Genetic Algorithms,” The MIT Press, Cambridge, USA, 1999.

[8] S. N. Sivanandan S. N. Deepa, “Introduction to Genetic Algorithm”,Springer Verlag Berlin Heidelberg, 2008.

[9] William Stallings, “Cryptography and Network Security”, 3rd Edition.