Volume 3, Issue 5, May-2016, pp. 222-225 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Data Security Using Elliptic Curve Cryptography

Karishma Bhirud, Dipashree Kulkarni, Renuka Pawar, Prachi Patil.

Abstract:- Cryptography technique is used to provide data security. In existing cryptography technique the key generation takes place randomly. Key generation require shared key. If shared key is access by unauthorized user then security becomes disoriented. Hence existing problems are alleviated to give more security to data. In proposed system a algorithm called as Elliptic Curve Cryptography is used. The ECC generates the key by using the point on the curve. The ECC is used for generating the key by using point on the curve and encryption and decryption operation takes place through curve. In the proposed system the encryption and key generation process takes place rapidly.

Keywords – Curve Cryptography, shared key, encryption, decryption.

—————————— ◆ ——————————

1. INTRODUCTION

The Cryptography is a technique which provides security to data. In cryptography all the data is presented in the encrypted form and only authorized user can decrypt information.The main goals of cryptography are to maintain data confidentiality, integrity, availability, centralized data collection to provide data authenticity in the digital world that provide high security to database. Plaintext is a term used in cryptography that refers to a message before encryption or after decryption. That is, it is a dispatch in a form that is easily readable by humans. Cipher text is also known as encrypted or encoded data because it contains a form of the unique plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. A cryptographic key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.

In cryptography Elliptic Curve Cryptography (ECC) is one of the effective cryptography algorithm which was discovered in 1985 by Neil Koblitz and Victor Miller. Elliptic Curve Cryptographic (ECC) are Public-key mechanisms that provide the same functionality as Rivest-Shamir-Adlemon algorithm. Most of the standards that use public-key cryptography for encryption based on RSA algorithm. Their security is based on the hardness of a different problems. The competing algorithm to RSA [1] is elliptic curve cryptography over finite fields.

2. RELATED WORK

In last twenty years, elliptic curve cryptography has been thoroughly researched. The actual application of elliptic curve cryptography and the practical execution of cryptosystem primitives in the real world constitute interdisciplinary research in computer science as well as in electrical engineering. Elliptic curve cryptography has moved to a cutting edge technology adopted by an increasing number of organizations. There are two reasons for this new development. One is that ECC has survived a generation of attacks. Second, in the growing industries, its advantages over RSA have made it an attractive security alternative. Elliptic curve cryptography is not only emerged as an attractive public key cryptosystem for mobile or wireless environments but also provides bandwidth savings. ECC has a high level of security which can be achieved with high considerably shorter keys than other conventional public key cryptography. ECC has a advantage that it helps to establish equivalent security with lower calculating power and battery resource usage for mobile applications. The strength of encryption depends on its key and the alphabetical table. As much as the key size is affecting the execution time, it should be preserved to be as short as possible for an acceptable security requirement. There will be no impact on strength and runtime performance. ECC provides an excellent solution of data and secure transfer of keys between two communicating parties [2]. An elliptic curve cryptography based communication system, where the various characters can be symbolized as the co-ordinates of the elliptic curves, can also be generated [3]. ECC structure is a group structure based on non-singular curve having finite number of integer points with each of this point having a finite order. A novel idea of ECC encryption and decryption based on Knapsack also shows on how the elliptic curves technology can be used for encryption and decryption [4].

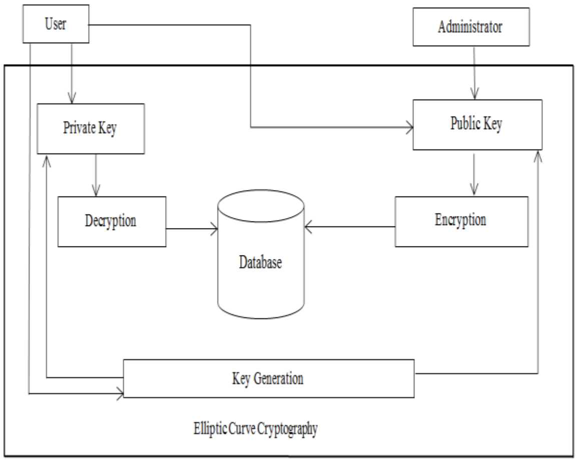

Fig.6 System architecture

3. PROPOSED SYSTEM

A general Elliptic Curve equation takes the general form:

$y^2 = x^3 + ax + b$…………………… (1)

(x, y) = co-ordinates on the Elliptic curve

a, b = coefficients.

Though ,for fixed fields a improved equation is used [5]:

$y^2 \bmod q = (x^3 + ax + b) \bmod q$……….. (2)

Where q = prime number for which the Elliptic curve be defined a, b satisfy the equation [2]

$(4a^3 + 27b^3) \bmod q \neq 0 \bmod q$……….. (3)

An elliptic curve E over GF (q) consist of the answers (x, y) distinct by (1) and (2), along with an supplementary element called 0, which is the point of EC at perpetuity. The set of points (x, y) are said to be affine synchronize point demonstration. The basic actions on elliptic curves are calculation and replication. A scalar reproduction with a point can be denoted as a combination of calculation operations.

Say, given a point P (x, y) is to be multiplied k times,

say k = 37.

Thus we have to compute 37P.

In terms of addition it can be represented as
37P = P + P + P +… + P (37 times)

For addition of two points P(x1, y1) & Q(x2, y2) where P≠Q.

3.1. SYSTEM ARCHITECTURE

Fig 1 shows the architecture of the system. System architecture describes the various modules present in paper which are interrelated to each other. The previously implemented some algorithm like RSA, Diffie Hellman has drawbacks which could slow down the key generation and encryption process. So elliptic curve cryptography algorithm is effective to increase the speed of key generation and encryption process. Encryption is done by the administrator by using public key of user. Then decryption takes place by user by using private key. As each user has its separate private key so no other user can access the information. If Administrator and user want to encrypt and decrypt the messages then they agree upon to use an elliptic curve Ep (a,b) where p is a prime number and a random point C on the elliptic curve. User selects a random number and a point A on the elliptic curve. User computes A1 = a (C +A) and A2 = a A. User keeps the random number a and the point A as her private keys and distributes A1 and A 2 as her general public keys.

Following keys are required for ECC:

Step 1.

User’s private key 1 = a, a random number less than the order of the generator.

Step 2.

User's private key 2 = a point A on the elliptic curve Ep (a,b).

Step 3.

User's general public key 1 = a point A1 on the elliptic curve Ep (a,b).

Step 4.

User's general public key 2 = a point A2 on the elliptic curve Ep (a,b).

Step 5.

User's specific public key for administrator = a point AB on the elliptic curve Ep(a,b).

If administrator wants to encrypt the message M then all the characters of the dispatch are coded to the points on the elliptic curve using the code table which is agreed upon by the administrator and student. Then each message point is encrypted to a pair of cipher points E1,E2 .[6]

Administrator uses a random number r.

$E1 = r C$

$E2 = M + (b + r) A 1 – r A 2 + AB$

After encrypting all the characters of the message administrator converts the pair of points of each message point into the text characters using the code table. Then administrator encrypts the plain text.

After encrypting the cipher text, User converts the cipher text into the points on the elliptic curve and identifies the points E1 and E2 of each character. Then decrypts the message as follows.

$M = E2 – (a E1 + a B 1 + B A)$

Hence, User can view this decrypted data as he wants.

3.2. ALGORITHM OF ECC:

```
1. Start
2: user perform the registration
3. User enter private key1 and private key2(x,y).
4. User calculate the public key,
   Calculates s
   s=(3(x)^2+a)/2y x2=s^2-2x y2=s(x-x2)-y
5. User broadcast public key (X2,Y2)
6. Admin performs encryption
      6.1. Calculate 1G to 5G for each character
      6.2. Retrieve matched G from generated table
      6.3. Calculate G of that character which admin wants to encrypt and store cipher text.
7. User performs decryption
      7.1. Calculate 1G to 5G of each character.
      7.2. Retrieve matched G from generated table and stores the plain text.
8. Stop.
```

4. RESULT:

RSA key generation is expressively slower than ECC key generation for RSA key of sizes 1024 bits which is greater than key size of ECC. RSA has more computational overheads than ECC because in RSA algorithm, users have to choose particular prime number for calculation of key generation. As the key size of ECC is smaller than the key size of RSA so, encryption of Elliptic curve cryptography is much faster than RSA. ECC is more efficient for small devices. If ECC algorithm is used for communication purpose then it offers good bandwidth than RSA.

Table 1. Comparison of ECC and RSA

Parameters	ECC	RSA
Computational overheads	Roughly 10 times than that of RSA can be Saved.	More than ECC.
Key sizes	System parameters and key pairs are shorter for the ECC	System parameters and key pairs are longer for the RSA
Key generation	Faster	Slower
Encryption	Much faster Than RSA.	Have good speed but slower than ECC.
Small devices efficiency	Much more Efficient.	Less efficient Than ECC.

5. CONCLUSION

In this paper, Data security is important issue in day to day life. The elliptic curve cryptography is one of the useful techniques to hide the data or information so that data must be access by authorized user. In this technique all the calculations are takes place by considering the points on the elliptic curve. The encryption and key generation process is faster. Wireless devices are speedily becoming more reliant on safety features such as the ability to do secure email, confident Web browsing, and cybernetic private networking to commercial networks and ECC allows more efficient implementation of all of these features. ECC make available better security and more efficient performance than the first generation public key techniques.

REFERENCES

[1]. J.Edge, An introduction to elliptic curve cryptography, http://lwn.net/Articles/174127/, 2006.

[2]. Ch. Suneetha, D. Sravana Kumar and A. Chandrasekhar, "*Secure key transport in symmetric cryptographic protocols using elliptic curves over finite fields*", International Journal of Computer.

[3]. R. Rajaram Ramasamy, M. Amutha Prabakar, M. Indra Devi and M.Suguna, ―Knapsack based ECC encryption and decryption‖, *International Journal of Network Security*, Vol. 9, No. 3, PP. 218-226,Nov. 2009.

[4]. D.Sravana Kumar, CH. Suneetha and A. Chandrasekhar, Encryption of data using Elliptic Curve over Finite Field‖, IJDPS, Vol. 3, No. 1, 2012.

[5]. Nautiyal et al., *International Journal of Advanced Research in Computer Science and Software Engineering* 4(1), January - 2014, pp. 620-625

[6]. Alfred J. Menezes and Scott A. Vanstone, "Elliptic Curve Cryptosystems and their implementations", *Journal of Cryptology, 1993*, Volume-6, Number-4, pages 209-224.

[7]. Krithika K Annapoorna Shetty, Shravya Shetty K. A review on asymmetric cryptography RSA and elgamal algorithm. International Journal of Innovative Research in Computer and Communication Engineering, 2014.

[8]. Richard Helm Erich Gamma. Design patterns: *Elements of reusable object oriented software*. communication Engineering, 2015.

[9]. James Rumbaugh Grady Booch, Ivar Jacobson. Eleptic curve cryptography,2nd edition. Computer Engineering, 2004.

[10]. Kistin Lauter. The advantage of eleptic curve cryptography for wireless security. IEEE wireless Communication, 2004