Global Journal of Computer Science and Technology
Volume 12 Issue 3 Version 1.0 February 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Fixed and Variable Size Text Based Message Mapping Techniques Using ECC

By Jayabhaskar Muthukuru & Bachala Sathyanarayana
Sri Krishnadevaraya University. Ananthapur, A.P. India

Abstract - Elliptic Curve Cryptography recently gained a lot of attention in industry. The principal attraction of ECC compared to RSA is that it offers equal security for a smaller bit size, thereby reducing processing overhead. ECC is ideal for constrained environment such as pager, PDAs, cellular phones and smart cards. ECC Encryption and Decryption methods can only encrypt and decrypt a point on the curve and not messages. This paper presents the implementation of mapping of text message into multiple points on Elliptic Curve with an Initial Vector (IV) using ECC. Further it also includes the transformation of fixed and variable size word in source text on to Elliptic Curve. These proposed methods enhance the security of ECC with multi fold encryption.

Keywords : *Elliptic Curve Cryptography, finite fields,Smart Cards, public key cryptography, discrete logarithm.*

GJCST Classification: *G.2, B.6, E.3, C.3*

Strictly as per the compliance and regulations of:

Fixed and Variable Size Text Based Message Mapping Techniques Using ECC

Jayabhaskar Muthukuru [α] & Prof. Bachala Sathyanarayana [σ]

Abstract - Elliptic Curve Cryptography recently gained a lot of attention in industry. The principal attraction of ECC compared to RSA is that it offers equal security for a smaller bit size, thereby reducing processing overhead. ECC is ideal for constrained environment such as pager, PDAs, cellular phones and smart cards. ECC Encryption and Decryption methods can only encrypt and decrypt a point on the curve and not messages. This paper presents the implementation of mapping of text message into multiple points on Elliptic Curve with an Initial Vector (IV) using ECC. Further it also includes the transformation of fixed and variable size word in source text on to Elliptic Curve. These proposed methods enhance the security of ECC with multi fold encryption.

Keywords : Elliptic Curve Cryptography, finite fields,Smart Cards, public key cryptography, discrete logarithm.

I. Introduction

Elliptic curve cryptography was independently proposed by Koblitz and Miller in 1985[1]. Unlike standard public-key methods that operate over integer fields, the elliptic curve cryptosystems operate over points on an elliptic curve. Similar to other Public Key encryption techniques, the security level of ECC also depends on the sizes of the keys used. The sizes of the cryptographic keys can be decided considering the following points [4].

- The approximate duration for which the information requires to be kept secure.
- The allowable level of impracticability of an attack to be carried out.
- The advancements in the computational resources, which are available to the attackers.
- The progress in the area of cryptanalysis.

Cryptographic algorithms based on discrete logarithm problem can be efficiently implemented using elliptic curves [2].

Elliptic curve cryptography is emerging as an attractive public-key cryptosystem for resource constrained devices like smart cards because compared to traditional cryptosystems like RSA/DH, it offers equivalent security with smaller key sizes, faster computation, lower power consumption, as well as memory and bandwidth savings [3].

II. Elliptic Curve Arithmetic

Elliptic curves are not like an ellipse or curve in shape. They look similar to doughnuts. Geometrically speaking they somehow resemble the shape of torus, which is the product of two circles when projected in three-dimensional coordinates. ECC makes use of elliptic curves in which the variables and coefficients are restricted to elements of a finite field. There are two families of elliptic curves defined for use in cryptography: prime curves defined over odd prime field F_P and binary curves defined over Galois field $GF(2^m)$.

a) Geometrical Definition Of Point Addition And Point Doubling Using Chord-And-Tangent Rule

For any two points $P(x_1, y_1) \neq Q(x_2, y_2)$ on an elliptic curve, EC group law point addition can be defined geometrically (Figure 1) as: "If we draw a line through P and Q, this line will intersect the elliptic curve at a third point (-R). The reflection of this point about x-axis, $R(x_3, y_3)$ is the addition of P and Q".

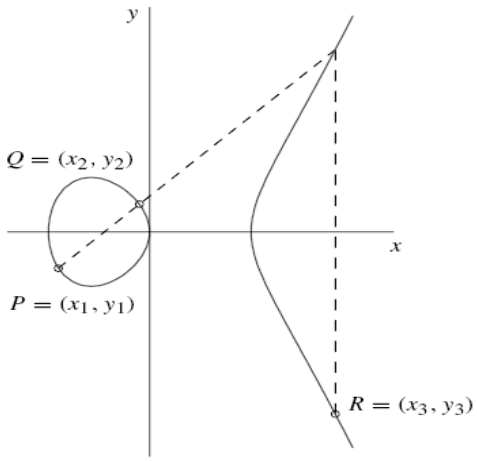

Fig. 1. Addition: R=P+Q

For P=Q, point doubling, geometrically (Figure 2) if we draw a tangent line at point P, this line intersects elliptic curve at a point (-R). Then, R is the reflection of this point about x-axis.

Author α : PhD Scholar, Department of Computer Science & Technology, Sri Krishnadevaraya University.
E -mail : jayabhaskarm@gmail.com
Author σ : Professor, Department of Computer Science & Technology, Sri Krishnadevaraya University. Ananthapur, A.P. India.
E -mail : bachalasatya@yahoo.com

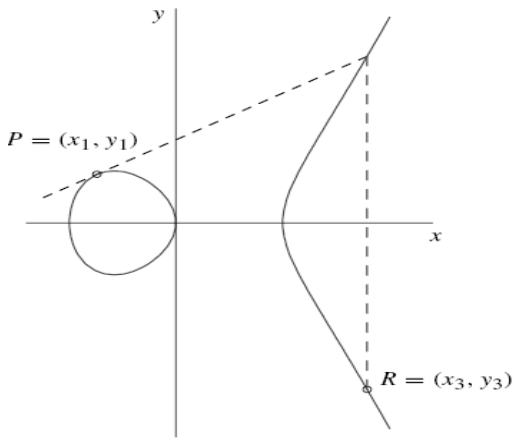

Fig.2. Doubling: R=P+P

b) Point Multiplication

The dominant operation in ECC cryptographic schemes is point multiplication. This is the operation which is the key to the use of elliptic curves for asymmetric cryptography---the critical operation which is itself fairly simple, but whose inverse (the elliptic curve discrete logarithm) is very difficult. ECC arranges itself so that when you wish to performance operation the cryptosystem should make easy encrypting a message with the public key, decrypting it with the private key the operation you are performing is point multiplication. Scalar multiplication of a point P by a scalar k as being performed by repeated point addition and point doubling for example 7P=(2((2P)+P)+P.

c) Elliptic Curve Over F_P And F_2^m

Definition of elliptic curve over F_P as follows [5]. Let p be a prime in F_P and a, b$\in$ F_P such that $4a^3 + 27b^2 \neq 0 \bmod p$ in F_P, then an elliptic curve E (F_P) is defined as

$$E(F_P) := \{ p(x, y), x, y \in F_P \}$$

Such that $y^2 = x^3 + ax + b \bmod p$ together with a point O, called the point at infinity. Below is the definition of addition of points P and Q on the elliptic curve E (F_P). Let $P(x_1, y_1)$ and $Q(x_2, y_2)$ then

$$R = P+Q = \begin{cases} O & \text{If } x_1 = x_2 \text{ and } y_2 = -y_1 \\ Q = Q+P & \text{If } P = O \\ (x_3, y_3) & \text{otherwise} \end{cases}$$

Where

$$x_3 = \begin{cases} \lambda^2 - x_1 - x_2 & \text{If } P \neq \pm Q \text{ (Point Addition)} \\ \lambda^2 - 2x_1 & \text{If } P = Q \text{ (Point Doubling)} \end{cases}$$

$$y_3 = \lambda(x_1 - x_3) - y_1, \text{ and}$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{If } P \neq \pm Q \text{ (Point Addition)} \\ \dfrac{3x_1^2 + a}{2y_1} & \text{If } P = Q \text{ (Point Doubling)} \end{cases}$$

The point p(x, -y) is said to be the negation of p(x, y).

The elliptic curves over F_2^m is defined as follows.

Denote the (non-super singular) elliptic curve over F_2^m by E (F_2^m). If a, b $\in$ F_2^m such that b $\neq$ 0 then

$$E(F_2^m) = \{p(x, y), x, y \in F_2^m\}$$

such that $y^2 + xy = x^3 + ax^2 + b \in F_P^m$ together with a point O, called the point at infinity.

The addition of points on E (F_2^m) is given as follows: Let $P(x_1, y_1)$ and $Q(x_2, y_2)$ be points on the elliptic curve E(F_2^m), then

$$R = P+Q = \begin{cases} O & \text{If } x_1 = x_2 \text{ and } y_2 = -y_1 \\ Q = Q+P & \text{If } P = O \\ (x_3, y_3) & \text{otherwise} \end{cases}$$

Where

$$x_3 = \begin{cases} \lambda^2+\lambda + x_2 + x_1 + a & \text{If } P \neq \pm Q \text{ (Point Addition)} \\ \lambda^2 + \lambda + a & \text{If } P = Q \text{ (Point Doubling)} \end{cases}$$

$$y_3 = \lambda (x_1 + x_3) + x_3 + y_1$$

and

$$\lambda = \begin{cases} \dfrac{y_2 + y_1}{x_2 + x_1} & \text{If } P \neq \pm Q \text{ (Point Addition)} \\ x_1 + \dfrac{x_1}{y_1} & \text{If } P = Q \text{ (Point Doubling)} \end{cases}$$

III. Elliptic Curve Cryptography

Elliptic curve cryptosystems over finite field have some advantages like the key size can be much smaller compared to other cryptosystems like RSA, Diffie-Hellman since only exponential-time attack is known so far if the curve is carefully chosen [5] [1] and Elliptic Curve Cryptography relies on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem ECDLP, which states that, "Given an elliptic curve E defined over a finite field F_P , a point P$\in$E (F_P) of order n, and a point Q$\in$E (F_P) , find the integer k $\in$ [0,n $-$1] such that Q = k P. The integer k is called the discrete logarithm of Q to the base P, denoted $k = \log_P Q$".

a) Elliptic Curve Encryption/Decryption

Consider a message 'Pmt' sent from A to B. 'A' chooses a random positive integer 'k', a private key 'n_A' and generates the public key $P_A = n_A \times G$ and produces the cipher text 'Cm' consisting of pair of points $Cm = \{ kG , Pmt + kP_B \}$ where G is the base point selected on the Elliptic Curve, $P_B = n_B \times G$ is the public key of B with private key 'n_B'.

To decrypt the cipher text, B multiplies the 1st point in the pair by B's secret & subtracts the result from the 2nd point $Pmt + kP_B - n_B(kG) = Pmt + k(n_BG) - n_B(kG) = Pmt$

IV. Proposed Mapping Methods

The proposed method the text message could be represented with all 256 symbols included in the standard ASCII codes.

a) Fixed Length Block Mapping Technique

In ECC the computation basically consists of an affine point Pm(x, y). This point and Base point (G) may represent the same point or both may be different. Base point implies it has the smallest (x, y) co-ordinates, which satisfy the EC. Following are the mapping algorithm for fixed length block message.

Notation : m - Message
IV - Initial Vector
K - Block Size
G - Base point
Pmt - Transformed point
Cm - Cipher text
AT - ASCII Value of the text

Encryption Algorithm :
Step 1: Begin
Step 2: n = m/k
Step 3: XORed_str = IV
Step 4: for i = 1 to n
Step 4.1: XORed_str = XORed_str ⊕ Block[i]
Step 4.2: AT = ASCII(XORed_str) //ASCII value of XORed_str in base 256 format
Step 4.3: Pmt = AT * Pm
Step 4.4: Cm[i] = { kG , Pmt + kP_B } //Pmt encrypted using ECC (Presented in section II)
Step5: End.

Decryption Algorithm:
Step1: Begin
Step 2: XORed_str = IV
Step 3: for i = 1 to n
Step 3.1: Pmt = Pmt + $k(n_BG) - n_B(kG)$ // get Pmt using private key n_B (Presented in section II)
Step 3.2: Get Pm, AT //Calculate these values from Pmt using discrete logarithm
Step 3.3: XORed_str = Text(AT) //generate string using AT which is in base 256 format
Step 3.4: Decrypt_block[i] = XORed_str ⊕ Block[i]
Step 3.5: XORed_str = Block[i]
Step 4: End

b) Variable Length Block Mapping Technique

In this mapping technique we consider each word as a block and null characters are padded to IV or message block if their lengths are not same. The other encoding and decoding techniques are same as fixed length block mapping technique.

V. Implementation of Proposed Method

The typical Elliptic Curve is represented by:
$y^2 = x^3 + 3x - 3 \pmod{1386491}$

The base point G is selected as (1, 1). Base point implies that it has the smallest (x, y) co-ordinates which satisfy the EC.

a) Fixed Length Block Mapping Implementation

Under fixed length block implementation we have implemented for single character block and two characters block and presented the results.

For single character block mapping results shown in table 1 and their graphical representation is shown in Fig.3, Fig.4 and Fig.4 for the plaintext message "A#2AAZ"

For two characters block mapping results shown in table.2 and their graphical representation is shown in Fig.6, Fig.7 and Fig.8 for the plaintext message "Aa@$59Aa@$"

Table 1: Mapping points for plaintext "A#2AAZ" and IV ="2"

Plaintext Block	Mapping Point	Encrypted Point	Decrypted Point
A	(845227, 1303111)	(612399, 1262010)	(845227, 1303111)
#	(824245, 1138831)	(520953, 403024)	(824245, 1138831)
2	(867657, 460591)	(591611, 904819)	(867657, 460591)
A	(603452, 158814)	(725362, 106713)	(603452, 158814)
A	(867657, 460591)	(591611, 904819)	(867657, 460591)
Z	(1255016, 1103602)	(19218, 623927)	(1255016, 1103602)

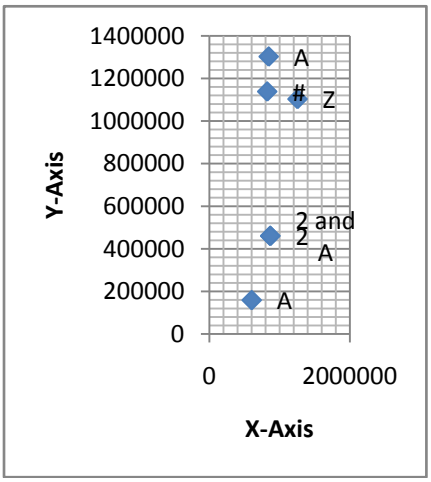

Fig.3. Mapping

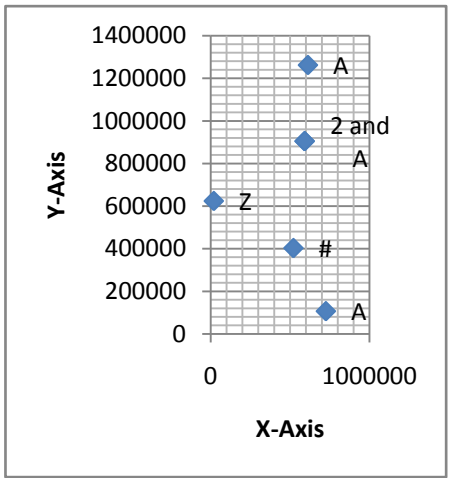

Fig.4. Encrypted

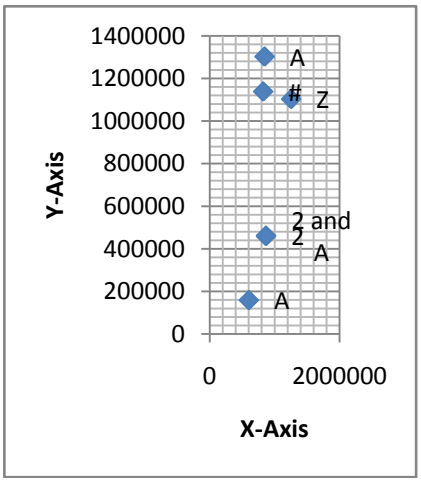

Fig.5. Decrypted

Table 2: Mapping points for plaintext "Aa@$59Aa@$" and IV = "24"

Plaintext Block	Mapping Point	Encrypted Point	Decrypted Point
Aa	(503400, 797492)	(1378250, 715061)	(503400, 797492)
@$	(978908, 708756)	(153590, 704662)	(978908, 708756)
59	(1085662, 709747)	(756400, 1273838)	(1085662, 709747)
Aa	(1202808, 1273936)	(1204937, 625801)	(1202808, 1273936)
@$	(41405, 1007904)	(436269, 1049661)	(41405, 1007904)

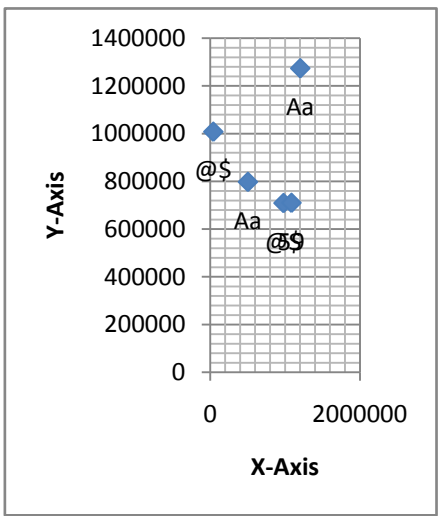

Fig.6. Mapping

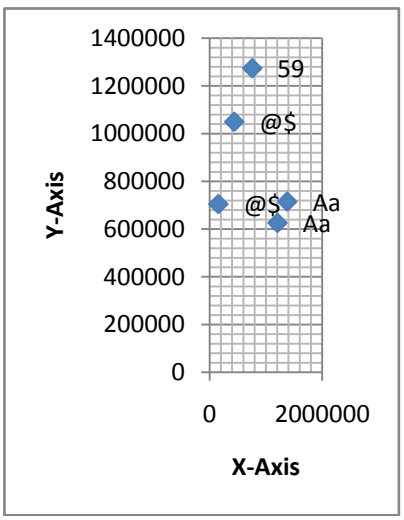

Fig.7. Encrypted

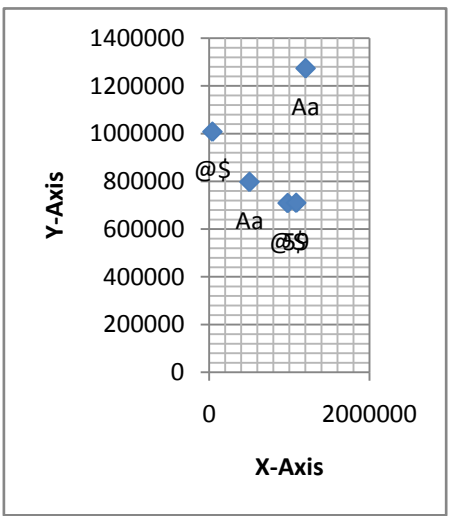

Fig.8. Decrypted

b) *Variable Length Block Mapping Implementation*

Under variable length block implementation we have implemented for one word block presented the results.

Mapping results shown in table 3 and their graphical representation is shown in Fig.9, Fig.10 and Fig.11 for the plaintext message "A to Z 1 to 10 ! to)"

Table 3 : Mapping points for plaintext "A to Z 1 to 10 ! to)" and IV = "69"

Plaintext Block	Mapping Point	Encrypted Point	Decrypted Point
A	(1143751, 1132381)	(1269235, 391778)	(1143751, 1132381)
to	(84586, 283729)	(1353127, 582406)	(84586, 283729)
Z	(321420, 867260)	(699790, 1214960)	(321420, 867260)
1	(988208, 942508)	(453764, 347504)	(988208, 942508)
to	(802250, 650335)	(672017, 694990)	(802250, 650335)
10	(416579, 1085820)	(4704, 95182)	(416579, 1085820)
!	(257086, 28323)	(1279171, 987239)	(257086, 28323)
to	(589667, 1090547)	(1356372, 1172684)	(589667, 1090547)
)	(680970, 712757)	(1345141, 1117444)	(680970, 712757)

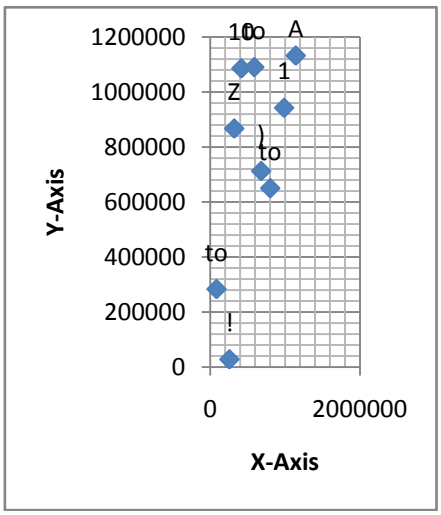

Fig.9. Mapping

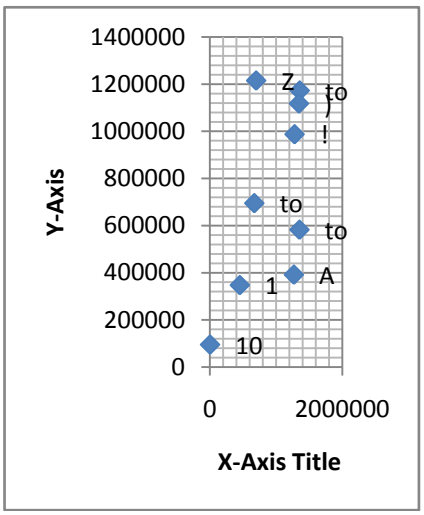

Fig.10. Encrypted

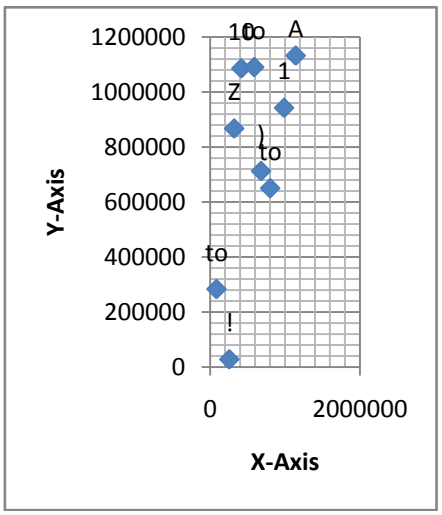

Fig.11. Decrypted

If a block of message using same mapping point from plaintext to cipher text throughout encrypted message[6][8] then It is easy to decipher using substitution ciphers with frequency analysis because the simple mappings preserve letter frequencies of the plaintext message[7]. The main disadvantage of the existing methods [6] [8] is attacker need not require private key of the receiver when attacker uses letter frequency attack to decipher plaintext message. In proposed mapping methods if a block of message is repeated then every time it maps to different points. So it is difficult to decipher using uses letter frequency analysis. It hides letter frequencies of the plaintext message.

VI. Conclusion

This paper presented a method to embed the message blocks in point form before using Elliptic Curve Cryptosystem. The modified scheme is believed to be secure because it involves multi fold encryption. Even security is needed to protect data during their transmission also, as there are many people hiding in the cyber space who have the inclination skills to steal from both individuals and corporations. In the proposed methods if a block of message is repeated then every time it maps to different points. Proposed methods strengthen the cryptosystem, i.e., for an intruder it would be very difficult to guess on which points the message blocks are mapped and it hides letter frequencies of the plaintext message.

References Références Referencias

1. N. Koblitz, "EllipticCurve Cryptosystems", Mathematics of Computation, 48, 1987, pp. 203-209.
2. I. Branovic, R. Giorgi, E. Martinelli, "A Workload Characterization of Elliptic Curve Cryptography Methods in Embedded Environments", ACM, Vol. 32, No. 3, June- 2004.
3. Efficient and provably-secure identity-based

signatures and signcryption from bilinear maps. In Proc. Of ASIACRYPT'05, volume 3778 of LNCS, pages 515–532, 2005.

4. Elliptic Curve Cryptography in Constrained Environments: A review, IEEE, 2011 International Conference on Communication Systems and Network Technologies, pp. 120-124, Sep-2011.
5. Darrel Hankerson, Alfred Menezes and Scott Vanstone,"Guide to Elliptic Curve Cryptography".
6. S. Maria Celestin Vigila , K. Muneeswaran "Implementation of Text based Cryptosystem using Elliptic Curve Cryptography", IEEE Sep-2009, pp. 82-85.
7. David Oranchak "Evolutionary Algorithm for ecryption of Monoalphabetic Homophonic Substitution Ciphers Encoded as Constraint Satisfaction Problems", ACM GECCO'08, July 12–16, 2008, pp.1717-1718.
8. Padma Bh, D.Chandravathi, P.Prapoorna Roja, "Encoding and Decoding of a message in the Implementation of Elliptic Curve Cryptography uing Koblitz Method", IJCSE May-2010, pp. 1904-1907.