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
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."
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 perform encryption or decryption of a message with the public key, decrypting it with the private key the cryptosystem should make easy encrypting a message so that when you wish to perform operation the discrete logarithm (ECDLP) is very difficult. ECC arranges itself such that, “Given an elliptic curve E defined over a finite field Fp, a point P ∈ E(Fp) of order n, and a point Q ∈ E(Fp), find the integer k ∈ [0,n −1] such that Q = kP. The integer k is called the discrete logarithm of Q to the base P, denoted k = logpQ”.

Elliptic Curve Over Fp and Fp^m

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

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

Such that y^2 = x^3 + ax + b mod 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 (Fp). Let P(x1, y1) and Q(x2, y2) 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

\[
x_3 = \begin{cases}
\lambda^2 + \lambda + x_1 + x_2 & \text{If } P ≠ ±Q \text{ (Point Addition)} \\
\lambda^2 + \lambda + a & \text{If } P = Q \text{ (Point Doubling)}
\end{cases}
\]

\[
y_3 = \lambda (x_1 + x_2) + x_3 + y_1
\]

and

\[
λ = \begin{cases}
\frac{y_2 + y_1}{x_2 + x_1} & \text{If } P ≠ ±Q \text{ (Point Addition)} \\
\frac{x_1 + x_1}{y_1} & \text{If } P = Q \text{ (Point Doubling)}
\end{cases}
\]

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 Fp, a point P ∈ E(Fp), order n, and a point Q ∈ E(Fp), find the integer k ∈ [0,n −1] such that Q = kP. The integer k is called the discrete logarithm of Q to the base P, denoted k = logpQ”.

\[
R = P + P = \begin{cases}
\frac{y_2 - y_1}{x_2 - x_1} & \text{If } P ≠ ±Q \text{ (Point Addition)} \\
3x_1^2 + a & \text{If } P = Q \text{ (Point Doubling)}
\end{cases}
\]

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

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

Denote the (non-super singular) elliptic curve over Fp^m by E (Fp^m). If a, b ∈ Fp^m such that b ≠ 0 then

\[
E (Fp^m) = \{ p(x, y), x, y \in Fp^m \}
\]

such that y^2 + xy = x^3 + ax^2 + b ∈ Fp^m together with a point Q, called the point at infinity.

The addition of points on E (Fp^m) is given as follows: Let P(x1, y1) and Q(x2, y2) be points on the elliptic curve E(Fp^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

\[
x_3 = \begin{cases}
\lambda^2 + \lambda + x_1 + x_2 + 1 & \text{If } P ≠ ±Q \text{ (Point Addition)} \\
\lambda^2 + \lambda + a & \text{If } P = Q \text{ (Point Doubling)}
\end{cases}
\]

\[
y_3 = \lambda (x_1 + x_2) + x_3 + y_1
\]
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 × 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 × 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 (mod 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) |
Table 2: Mapping points for plaintext "Aa@$59Aa@$" and IV = "24"

<table>
<thead>
<tr>
<th>Plaintext Block</th>
<th>Mapping Point</th>
<th>Encrypted Point</th>
<th>Decrypted Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aa</td>
<td>(503400, 797492)</td>
<td>(1378250, 715061)</td>
<td>(503400, 797492)</td>
</tr>
<tr>
<td>@$</td>
<td>(978908, 708756)</td>
<td>(153590, 704662)</td>
<td>(978908, 708756)</td>
</tr>
<tr>
<td>59</td>
<td>(1085662, 709747)</td>
<td>(756400, 1273838)</td>
<td>(1085662, 709747)</td>
</tr>
<tr>
<td>Aa</td>
<td>(1202808, 1273936)</td>
<td>(1204937, 625801)</td>
<td>(1202808, 1273936)</td>
</tr>
<tr>
<td>@$</td>
<td>(41405, 1007904)</td>
<td>(436269, 1049661)</td>
<td>(41405, 1007904)</td>
</tr>
</tbody>
</table>

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 )'
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
3. Efficient and provably-secure identity-based


