Elliptic Curve Cryptography with Hill Cipher Generation for Secure Text Cryptosystem

Komal Agrawal
Dept. of Computer Science & Engineering
BSAITM, Faridabad

Anju Gera
Dept. of Computer Science & Engineering
BSAITM, Faridabad

ABSTRACT
Cryptography is an art to protect secret information from attacks. This idea of information security leads to the evolution of cryptography. In this paper, an idea is proposed in which hill cipher is generated with Elliptic Curve Cryptography to provide better security and proper security coverage. Hill Cipher is harder to break due to its linearity and ECC is smaller key size algorithm which provide fast computations as well as memory, speed, bandwidth. ECC provides secure text based cryptography by generating base points on Elliptic curve over the finite field. It starts with plain text conversion by hill cipher then it is converted into its ASCII value to get points on curve and then perform scalar multiplication to encrypt the data and to generate secret and public key. Hill cipher with ECC improves efficiency of cryptography algorithm, provides better security and a level of complexity so that this technique is harder to break.

Keywords
Elliptic Curve Cryptography, Hill Cipher, RSA.

1. INTRODUCTION
Cryptography [4] is the art of information hiding that provide security to important text and keep it secret. It is science of protecting information by transforming it into an unreadable format.. Because value of information decreases with time, good cryptography based security protects information until its value is significantly less than the cost of attempts to obtain the information.

There are two types of cryptography [3]: Symmetric key cryptography and asymmetric key cryptography or public key cryptography.

In symmetric key cryptography, there is only one secret key that is shared by both parties i.e. sender and receiver.

In Asymmetric key cryptography, it involves two keys i.e. private key and public key, both keys are required for encryption and decryption of secret message. Private Key is not shared by anyone, it is kept secret. Public key is public to all users, any user can access public key. Primary advantage of asymmetric key cryptography is to remove the need to exchange the key between sender and receiver. Basic terms used in cryptography [4] are:-

- Plain Text: Original text which is fed into the encryption algorithm as input text.
- Cipher Text: Output message which is encrypted by encryption algorithm into non readable form i.e. cipher text.
- Encryption Algorithm: It is a process of converting plain text into cipher text, Encryption (plain text + key) = cipher text.
- Decryption Algorithm: It is a process of converting cipher text into plain/original text, Decryption (cipher text + key) = cipher text.
- Public and Private Keys: This pair of keys used for both encryption and decryption.

Most widely used public key cryptography are: RSA, ECC. These public key cryptography algorithms provide security requirements for data i.e. authentication (the process of providing sender's identity), non-repudiation (a mechanism that prevents the sender from denying that they sent the message), confidentiality (to ensure that information is accessed by an authorized party), integrity (to ensure that received message is not altered), and access control (to ensure that only authorized parties are able to access the given information).

Victor Miller and Neal Koblitz introduced Elliptic Curve Cryptography [1] in 1984. Elliptic curve cryptography is public key cryptography. Many standards that uses public key cryptography for encryption majorly use RSA, but elliptic curve cryptography is appearing as a competition to RSA. Uses of elliptic curve cryptography arises from the fact that equal security level can be achieved with shorter keys. ECC's 160 bit key is equally secured as RSA's 1024 bit key. Hence ECC provides equal security as compare to RSA with smaller key size. ECC provides ideal environment for pager, PDAs, cellular phones and smart cards.

ECC makes use of elliptic curves over the finite field. Affine points (x, y) are calculated which may be the base points (B) or any close point to base point which satisfy Elliptic curve. Base points are smallest coordinates on elliptic curve. General form of Elliptic curve is:

E: $y^2 \bmod p = x^3+x+1 \bmod p$

Where x, y are base points and a, b are integer modulo p in the finite field Fp such that where $4a^3 + 27b^2 \neq 0 \pmod p$. Where p is prime integer making the EC finite field.

General form of elliptic curve is used to generate points to create elliptic curve. ECC public key is a point on the elliptic curve and private key is random number. Public key (K_b) is generated by multiplication of private key (K_a) and Base point (B). The multiplication of the points are implemented by the repeated addition and doubling strategy of ECC technique. In

ECC algorithm, a message is in form of character initially then it is converted to point on Elliptic curve by multiplying message character with affine points E.g.: $P_{ML} = M * P_M$ where M is message character, P_M is affine points and P_{ML} is a point on elliptic curve determined by applying scalar multiplication on the EC points. Scalar multiplication is implemented by repeated operation of point addition and point doubling. Point addition [2] and point doubling are two operations used in ECC technique to convert the characters, addition, subtraction and multiplication to elliptic curve points.

According to ECC technique P_{ML} is added with NK_b where N is randomly chosen large secret integer and K_b is public key. Encrypted message is made up of two sets (NB, $P_{ML} + NK_b$) where NB is multiplication of large secret integer and Base points.

In ECC [8] characters are implemented in points on Elliptic curve using scalar multiplication. ECC use two operation addition and doubling to perform scalar multiplication. No of doubling and addition operation depends upon the ASCII [10] value of message character.

Next part of this paper is structured as follows. A background study has been point out in section 2. Section 3 holds proposed methodology and operations used in ECC algorithm. Result Analysis has been done in section 4. Conclusion and future scope have been presented in section 6.

2. BACKGROUND STUDY

In cryptography, Ciphers are used to provide security to secret text. There are no. of ciphers: Hill cipher [4][9] is an interesting multi-letter cipher, developed by the mathematician Lester Hill in 1929. Hill cipher which convert secret text into an unreadable form and then convert it again into its original form. Hill cipher was the first polygraphic cipher. Polygraphic cipher in which plaintext is divided into groups of adjacent letters of the same fixed length n and then each group is transformed into a different group of n letters. While using hill cipher it is harder to break security provided by cipher algorithm.

This Hill cipher algorithm [4][9] takes m successive plaintext letter and substitutes for m cipher letters that's why called polygraphic cipher. The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1, c = 2, …….. z = 25).

Linear algebra equation for hill cipher is:

C = KP mod 26

Where c is cipher text, p is plain text mod 26 denotes assigned integer value for alphabets. This equation is used for encryption. For m = 3,

$$\begin{bmatrix} C_1 = (K_{11} P_1 + K_{12} P_2 + K_{13} P_3) \bmod 26, \\ C_2 = (K_{21} P_1 + K_{12} P_2 + K_{23} P_3) \bmod 26, \\ C_3 = (K_{31} P_1 + K_{32} P_2 + K_{33} P_3) \bmod 26. \end{bmatrix}$$

This can be expressed in term of column vectors and metrics:

$$\begin{matrix} C_1 \\ C_2 \\ C_3 \end{matrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \bmod 26$$

C and P are column vectors of length 3, representing the plain text and cipher text, and k is 3 × 3 matrix representing the encryption key. Operations are performed for mod 26.

Hill Cipher Encryption

Consider the message is "CAT" which is plain text or secret text and key is "HIL Cipher".

We have C = 2, A = 0, and T = 19. Now message in form of vector presentation is:

$$\begin{bmatrix} 2 \\ 0 \\ 19 \end{bmatrix}$$

And Key Matrix is:

$$\begin{bmatrix} 7 & 8 & 11 \\ 2 & 8 & 15 \\ 7 & 4 & 17 \end{bmatrix}$$

Encryption is given by C = KP mod 26

$$\begin{bmatrix} 7 & 8 & 11 \\ 2 & 8 & 15 \\ 7 & 4 & 17 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \\ 19 \end{bmatrix} \text{ Mod } 26$$

$$C = \begin{bmatrix} 15 \\ 3 \\ 25 \end{bmatrix}$$ Here C is Cipher text vector

Where P=15, D=3, Z=25.

We have Cipher text = PDZ.

Hill cipher Decryption

General equation for Hill cipher decryption is:

$P = K^{-1} * C \bmod p$

For example, we have cipher text

$$C = \begin{bmatrix} 15 \\ 3 \\ 25 \end{bmatrix}$$ Here C is Cipher text vector where

And Key Matrix is:

$$\begin{bmatrix} 7 & 8 & 11 \\ 2 & 8 & 15 \\ 7 & 4 & 17 \end{bmatrix}$$

Now original text P is calculated by

$$P = \begin{bmatrix} 7 & 8 & 11 \\ 2 & 8 & 15 \\ 7 & 4 & 17 \end{bmatrix}^{-1} \begin{bmatrix} 15 \\ 3 \\ 25 \end{bmatrix} \text{ Mod } 26$$

$$P = \begin{bmatrix} 2 \\ 0 \\ 19 \end{bmatrix}$$

Where 2 = C, 0 = A, 19 = T. hence original text is retrieved by hill cipher decryption.

Elliptic Curve Cryptography [1] [8] is public key cryptography which provide high security to secret text with short size key. Importance of ECC is increasing day by day because of its attractive challenge of shorter key RSA gives security with 1024 bit secret key and ECC provides equal security with 160 bit key. Elliptic curve cryptography works at elliptic curve defined over finite field $F_{P.}$ General Equation of elliptic curve is:

E: $y^2 = x^3 + ax + b$

Defined over the finite field Fp. Where p is prime number, x and y are the elements of E(Fp).

And a, b are integer modulo p in the finite field Fp such that $4a^3 + 27b^2 \neq 0 \pmod p$. In ECC, a character which is a secret message is firstly converted into its ASCII value because scalar multiplication can be performed on numerical values only Then numerical value of character is transformed into an affine point of the elliptic curve. This is public key cryptography in which two keys are implemented at the time of encryption i.e. private key and public key. In ECC, private key (K_a) is randomly chosen number and Public key (K_b) is generated by multiplication of private key (K_a) and Base point (B). The multiplication of the points are implemented by the repeated addition and doubling strategy of ECC [2] technique. Point addition and point doubling are two basic operations performed in scalar multiplication in ECC [6] to implement the points on Elliptic curve.

POINT ADDITION

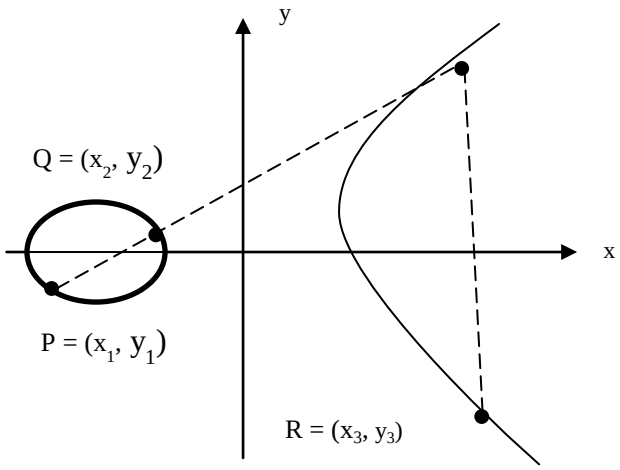

Fig 2.1: Point Doubling

Point addition is addition of two points. Suppose point R represented by R = P + Q where P and Q are points on the elliptic curve can be found by drawing the line between P and Q. The point where the line intersects the elliptic curve is taken and reflected across the curve's horizontal line of symmetry, which much of the time is the x-axis. The resultant Point is the sum of P and Q.

Point addition can also be defined by the following equations:

$\lambda = [(y_2 - y_1) / (x_2 - x_1)] \bmod p$

$x_3 = (\lambda^2 - x_1 - x_2) \bmod p$

$y_3 = [\lambda (x_1 - x_3) - y_1] \bmod p$

POINT DOUBLING

Point doubling deals with single point on curve. If there is a point given on the curve P then R= 2P. It can be found by drawing the tangent line to P, and reflecting the intersection of that line with the curve across the horizontal line of symmetry.

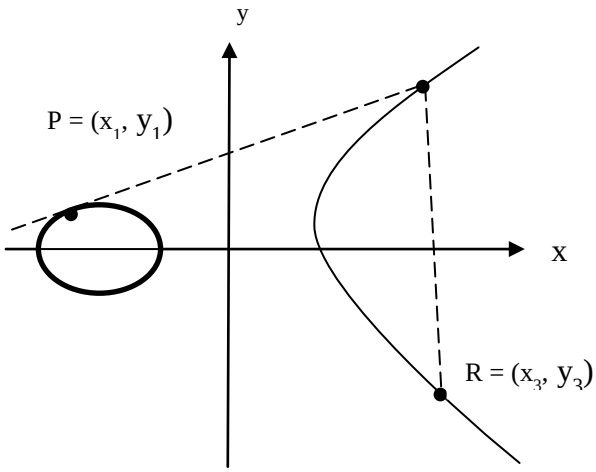

Fig 2.2: Point Doubling

Point addition can also be defined by following equation:

$\lambda = [(3\ x_1^2 + a)/2y_1]$ mod p

2P has affine coordinates (x_3, y_3) given by:

$x_3 = (\lambda^2 - 2\ x_1)$ mod p

$y_3 = [\lambda\ (x_1 - x_3) - y_1]$ mod p

No. of Point addition and doubling operations are depend on a sequence of operations determined for 'N'. Every point calculated by point addition or doubling is an affine point these affine points are on the Elliptic Curve [6].

If there is 13P Where N is 13 then a sequence of repeated addition and doubling operations performed to calculate 13P.

Table 2.1: calculate 13P

P	
2P	**Doubling**
3P	**Addition**
6P	**Doubling**
12P	**Doubling**
13P	**Addition**

According to ECC, encrypted message is combination of two sets (NG, P_{ML} + NK_b)

Where N is randomly chosen large number, G is base point, P_{ML} is point on elliptic curve calculated by message character and affine points. K_b is public key which is a point on elliptic curve and calculated by multiplication of private key (K_a) which a random number and base points (G).

Now to recover secret message from encrypted message, first decryption process of ECC is applied by applying the private key of recipient (Ka). Now evaluate the ASCII value and recover the plain text.

ECC [5] is best public key cryptography technique which provide maximum security to secret message and prevent it from intruders and hackers.

3. PROPOSED METHOD

This paper gives proposed idea to provide an extra level of security to secret message. This proposed idea make secret text more complex for hacker to detect it. The proposed method is elliptic curve cryptography with hill cipher generation for secure text cryptosystem. Hill cipher with ECC provides high level security as compare to RSA with smaller key size. It helps to reduce RSA factorization problem.

Hill cipher is symmetric polygraph cipher which takes groups of adjacent letters of same length. This cipher is harder to break due to its resistance to frequency analysis. It increase the speed of the encryption and decryption.

Elliptic curve cryptography [8] is public key cryptography which provide high level of security with smaller key size. It is harder to break security level provided by ECC by hacker because its scalar multiplication is too complex to implement and to break.

Firstly, Plain text is encrypted using hill cipher generation then encrypted form is converted into its assigned ASCII value. ASCII value is generated to show the numeric value on elliptic curve, message is encrypted using private key and public key. Apply scalar multiplication to calculate points on elliptic curve then original message points converted into encrypted cipher points then these encrypted points are send to other site receiver.

Now original message is retrieved by applying decryption process. In decryption, firstly decrypt cipher points to original points using scalar multiplication by applying user's secret key and then it is converted to ASCII value. Now converted form is not original message it is encrypted form. Now last step is to convert it into original text using hill cipher decryption.

Algorithm Hill Cipher Encryption

Input: (K, P)

Where K is n*n matrix of same row column length

P is given plain text.

1. Separate the plain text P from left to right into j groups of n letters.
2. Replace each letter by its corresponding position (from 0 to m-1) of the alphabet to get j groups of n letters.
3. Now arrange k groups into n row column vector. Multiply K by j column vectors modulo m where m= 0 to 25.
4. Now it have encoded vector column matrix. Now replace each numeric with its corresponding alphabet.
5. Result is text converted with hill cipher i.e. M

This cipher text act as plain text to ECC and it is denoted by M to ECC encryption.

ECC Encryption

A general elliptic curve takes the general form as

E: $y^2 = x^3 + ax + b$ modp.

Where x, y are elements of E(Fp) and a, b are integer modulo p where p is randomly chosen prime number making the EC finite field.

To perform operations with Elliptic curve points in order to encrypt and decrypt firstly, points need to be generated.

Algorithm gen points

Input: a, b, p

Where a, b are integer and p is prime number.

Output: (x, y)

1. Compute if x<p, $y^2 = (x^3 + ax + b)$ mod p
2. If (y^2 is a perfect square in E (Fp)) then return (x, y).

Consider prime number (p) is 37 and a, b are 1 chosen for elliptic curve then typical Elliptic curve is represented by:

PROPOSED ARCHITECTURE

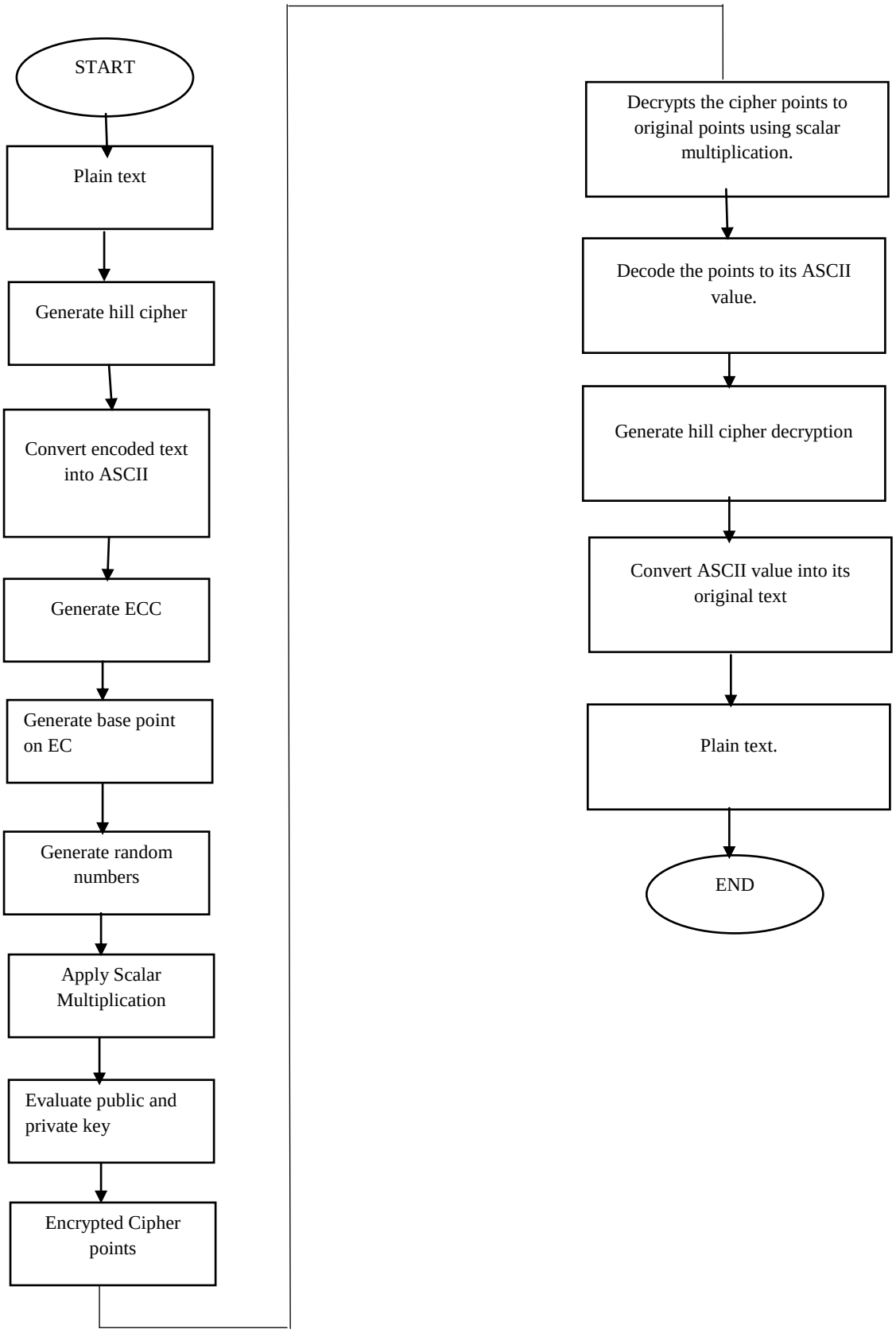

Fig 3.1: Proposed Architecture

y^2 mod 37 = $x^3 + x + 1$ mod 37.

Then points generated on the Elliptic curve as shown in table.

Table 3.1: Generate Point on EC

(0, 1)	(0,36)	(21,25)	(21,12)
(1, 15)	(1,22)	(24,14)	(24,23)
(2, 14)	(2,23)	(25,0)	(25,0)
(6, 36)	(6,1)	(26,18)	(26,19)
(8, 15)	(8,22)	(27,8)	(27,29)
(9, 31)	(9,6)	(28,15)	(28,22)
(10, 7)	(10,30)	(29,31)	(29,6)
(11,14)	(11,23)	(30,24)	(30,13)
(13,18)	(13,19)	(31,36)	(31,1)
(14,24)	(14,13)	(33,9)	(33,28)
(17,11)	(17,26)	(35,18)	(35,19)
(19,16)	(19,21)	(36,6)	(36,31)

Algorithm key pair generation

Input: Elliptic curve parameters (p, E, G, n, Ka)

Where p is prime number, E is Elliptic curve, G is base point on Elliptic curve, Ka is randomly chosen private key and n is public domain parameter.

Output: Public key Kb and Private Key Ka.

1. Select Ka € R [1, n-1].
2. Compute Kb = Ka * G.
3. Return (Kb, Ka).

Algorithm ECC Encryption

Input: Elliptic curve parameters (p, E, G, n, public key Kb and plain text M, P_{ML} is the coordinates of message on Elliptic curve)

Output: Cipher text C_M.

1. Represent plain text M as points P_{ML} in E (Fp).
2. Select N € R [1, n-1].
3. Compute C1 = N*G.
4. Compute C2= P_{ML} + N*Kb.
5. Return (C1, C2).

ECC Decryption

Algorithm ECC Decryption

Input: Elliptic curve parameter (p, E, G, n, Ka, Cipher text C_M,)

Where p is prime number, E is elliptic curve, G is Base point on elliptic curve and Ka is private key.

Output: Plain text M

P_{ML} = C2 – KaC1.

Return (P_{ML}).

4. RESULT ANALYSIS

Proposed work is to introduce a concept of high security by hill cipher generation with elliptic curve cryptography. In result analysis a comparison is done between RSA and ECC.

Table 4.1: Comparison ECC and RSA Key Size

Elliptic Curve Cryptography Key-Size	RSA Key Size	Key Size ration
106 bits	512 bits	1:4
132 bits	768 bits	1:5
160 bits	1024 bits	1:6
224 bits	2048 bits	1:9
256 bits	3072 bits	1:12
384 bits	7680 bits	1:20

Hence proposed method provides high level security with shorter key size as compare to RSA cryptography algorithm.

5. CONCLUSION

In this paper, Elliptic Curve Cryptography with Hill Cipher Generation for Secure Text Based Cryptosystem is presented. This investigates and improves the algorithms for these operations with the goal of increasing the speed and decreasing the required memory. In text based cryptography in which each character converted into an unreadable form using hill cipher and then the message is represented by its ASCII value. Each of these ASCII value is transformed into an affine point on the EC, by using a starting point. Transformation of the plaintext ASCII value by using an affine point is one of the contributions of this work. This proposed work is analyzed on basis of key size. Proposed work provide high security with shorter key size.

The market for Personal Digital Assistants (PDA) is growing sharply and PDAs are becoming increasingly attractive for commercial transactions. One requirement for further growing of E-commerce with mobile devices is the provision of security. We can implement elliptic curves over binary fields on a Palm OS device.

6. REFERENCES

[1] N.Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, volA8, 1987, pp.203-209.

[2] P.K Sahoo, Dr. Gunamani Jena, Dr. R. K Chhotray, Dr. S. Patnaik, "An implementation of Elliptic Curve Cryptography" IJERT ISSN: 2278-0181, vol. 2, Issue 1, Jan 2013.

[3] Ayushi, "A symmetric key cryptographic algorithm" International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15, 2010.

[4] Williams Stallings, Cryptography and Network Security, Prentice Hall, 4th Edition, 2006.

[5] Ruchika Markan, Gurvinder Kaur, "Literature survey on elliptic curve encryption technique" IJARCSSE, vol. 3, issue 9, September 2013.

[6] R.V.Kurja, Kirti Joshi, N.Mohan Kumar, Kapil H Raranape, A.Ramanathan, T.N.Shorey, R.R.Simha, and V.Srinivas, "Elliptic Curves", International Distribution by American Mathematical Society, 2006.

[7] N. Koblitz, Elliptic curve cryptosystems,Mathematics of Computations, 48, 203-209 (1987) of Computation, vol. 77, no. 262, pp. 1075–1104, 2008.

[8] Oswald, E. (2002), "Introduction to Elliptic Curve Cryptography", Institute for Applied Information Processing and Communication, Graz University Technology.

[9] Yuan Xue, " lectur notes on classical cipher".

[10] http://www.asciitable.com/