IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 6, Dec-Jan, 2015
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Enhancing The Security Of Koblitz's Method Using Transposition Techniques For Elliptic Curve Cryptography

Santoshi Pote

Electronics and Communication Engineering, Asso.Professor, SNDT Women's University, India

Abstract- Security plays a very importantrole in network communication systems and internet. Elliptic curve cryptography (ECC) is a public key cryptosystem like RSA. But differs from RSA in its quicker evolving capacity and by providing attractive and alternative way to researchers of cryptographic algorithm. ECC can only encrypt and decrypt a point on the curve and not message. This paper discusses Koblitz's method and its implementation using system for algebra and geometry experimentation (SAGE) software. It also describes transposition techniques to enhance the security of Koblitz's method for ECC.

Keywords: Encryption, Decryption, Elliptic curve cryptography, Transposition techniques, Encoding, Decoding.

I. INTRODUCTION

Cryptography is the science of information security. Elliptic curve cryptography (ECC) is a relatively new crypto-system, in existence, from the second half of 19th century, independently suggested by Neals Koblitz [1] and Victor Millor [2]. Elliptic Curve Cryptography (ECC) is a public key cryptosystem based on elliptic curve theory. Elliptic curve can be applied to cryptography as it is secure to the best of current knowledge.The benefit of using elliptic curves is that similar level of security can be achieved with smaller key size than other public key cryptography. Elliptic curve cryptography provides the same level of security as RSA. Also it requires less storage and smaller bandwidth. At present ECC has been commercially accepted, and has also been adopted by many standardizing bodies such as ANSI, IEEE [3], ISO and NIST [4]. Since then, it has been the focus of a lot of attention and gained great popularity. Some public key algorithm may require a set of predefined constants to be known by all the devices taking parts in the communication. In ECC we call these predefined constants as 'Domain Parameters. Understanding ECC needs full mathematical background of elliptic curve [1].

The aim of this paper is to explain encoding and decoding a message in ECC using Koblitz's method [5]. Also explaining the enhanced security in ECC by using transposition techniques. This paper is organized as follows. After a brief introduction in section 1, an overview of elliptic curve cryptography is given in section 2. We present in Section 3, the encoding and decoding of message. The transposition techniques are explained in Section 4. The proposed work with the algorithm is given in Section 5. Finally, conclusion is summarized in section 6.

1. Elliptic Curve Cryptography

1.1 Elliptic Curves

An elliptic curve is a cubic equation of the form:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

Where a, b, c, d and e are real numbers.

A special addition operation is defined over elliptic curves, and this with the inclusion of a point O, called *point at infinity*. If three points are on a line intersecting an elliptic curve, then their sum is equal to this point at infinity O (which acts as the identity element for this addition operation).

Figure 1 shows the elliptic curves $y^2 = x^3 + 2x + 5$ and$y^2 = x^3 - 2x + 1$.

1.2 Elliptic Curves over Galois Fields

An elliptic group over the Galois Field $E_P(a, b)$ is obtained by computing $x^3 + ax + b \; mod \; p$ for 0≤x<p. The constants *a* and*b* are non-negative integers smaller than the prime number *p* and must satisfy the condition:

$$4a^3 + 27\,b^2 \, mod\, p \;\neq 0$$

For each value of x, one needs to determine whether or not it is a *quadratic residue*. If it is the case, then there are two values in the elliptic group. If not, then the point is not in the elliptic group $E_P(a,b)$.

Example (construction of an elliptic group):

Let the prime number p = 23 and let the constants let the constants a = 1 and b = 1. We first verify that:

$$4a^3 + 27\, b^2 \, mod \; p = 4 \times 1^3 + 1^2 mod \; 23$$

$$4a^3 + 27\, b^2 \, mod \; p = 4 + 27 mod 23 = 31 mod 23$$

$4a^3 + 27\, b^2 \, mod \; p = 8 \neq 0$

We then determine the quadratic residues **Q**$_{23}$ from the reduced set of residues **Z**$_{23}$ ={1, 2, 3, …, 21,22}:

$x^2 mod\; p$	$(p-x)^2 mod\; p$	=
$1^2 mod\; 23$	$22^2 mod\; 23$	1
$2^2 mod\; 23$	$21^2 mod\; 23$	4
$3^2 mod\; 23$	$20^2 mod\; 23$	9
$4^2 mod\; 23$	$19^2 mod\; 23$	16
$5^2 mod\; 23$	$18^2 mod\; 23$	2
$6^2 mod\; 23$	$17^2 mod\; 23$	13
$7^2 mod\; 23$	$16^2 mod\; 23$	3
$8^2 mod\; 23$	$15^2 mod\; 23$	18
$9^2 mod\; 23$	$14^2 mod\; 23$	12
$10^2 mod\; 23$	$13^2 mod\; 23$	8
$11^2 mod\; 23$	$12^2 mod\; 23$	6

Therefore, the set of $\frac{p-1}{2} = 11$ quadratic residues **Q**$_{23}$ = {1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18}.

Now, for 0≤x<p, compute $y^2 = x^3 + x + 1 \; mod \; 23$ and determine if y^2 is in the set of the quadratic residues **Q**$_{23:}$

x	0	1	2	3	4	5	6	7	8	9	10	11
y^2	1	3	11	8	0	16	16	6	15	3	22	9
$y^2 \in Q_{23}$?	yes	yes	no	yes	no	Yes	yes	yes	no	yes	no	yes
Y_1	1	7		10	0	4	4	11		7		3
Y_2	22	16		13	0	19	19	12		16		20

x	12	13	14	15	16	17	18	19	20	21	22
y^2	1	3	11	8	0	16	16	6	15	3	22
$y^2 \in Q_{23}$?	yes	yes	no	no	no	Yes	yes	yes	no	no	no
Y_1	4	7				3	3	5			
Y_2	19	16				20	20	18			

The elliptic group $E_p(a, b) = E_{23}(1, 1)$ thus include the points:

$$E_{23}(1,1) = \begin{cases} (0,1)(0,22)(1,7)(1,16)(3,10)(3,13)(4,0)(5,4)(5,19) \\ (6,4)(6,19)(7,11)(7,12)(9,7)(9,16)(11,3)(11,20)(12,4) \\ (12,19)(13,7\ )(13,16)(17,3)(17,20)(18,3)(18,20)(19,5)(19,18) \end{cases}$$

Figure 2 shows a scatterplot of the elliptic group E_p *(a, b)* = E_{23} *(1, 1).*

1.3 Addition and Multiplication operations over elliptic groups

Let the points *P = (x_1, y_1)* and *Q = (x_2, y_2)* be in the elliptic group E_p *(a, b),* and O be the point at infinity. The rules for addition over the elliptic group E_p *(a, b)* are:

1. $P + O = O + P = P$
2. If $x_2 = x_1$ and $y_2 = -y_1$, that is *P = (x_1, y_1)* and *Q = (x_2, y_2) = (x_1,-y_1) = -P,* then *P+Q=O.*
3. If *Q ≠ - P* , then their sum *P+Q=(x_3, y_3)*is given by:

$$x_3 = \lambda^2 - x_1 - x_2 mod\ p$$

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

Where

$$\lambda \triangleq \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & if\ P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & if\ P = Q \end{cases}$$

Example (*Multiplication over an elliptic curve group*):

The multiplication over an elliptic curve group E_p *(a, b)* is the equivalent operation of the modular exponentiation in RSA.

Let P = (3, 10) ϵ E_{23} *(1, 1)*. Then $2P = (x_3, y_3)$is equal to:

$$2P = P + P = (x_1, y_1) + (x_1, y_1)$$

Since P = Q and $x_2 = x_1$, the values of λ, x_3 and y_3 are given by:

$$\lambda = \frac{{x_1}^2 + a}{2y_1} mod\ p = \frac{3 \times (3^2) + 1}{2 \times 10} mod\ 23 = \frac{5}{20} mod\ 23 = 4^{-1} mod\ 23$$

$$= 6$$

$$x_3 = \lambda^2 - x_1 - x_2 mod\ p = 6^2 - 3 - 3mod\ 23 = 30mod23 = 7$$

$$y_3 = \lambda(x_1 - x_3) - y_1 mod\ p = 6 \times (3 - 7) - 10mod23 = -34mod23 = 12$$

Therefore $2P = (x_3, y_3)$= (7, 12).

The multiplication kP is obtained by repeating the elliptic curve addition operation k times by the following the same additive rules.

K	λ = $\frac{y_2 - y_1}{x_2 - x_1}$ $if\ P \neq Q$
	or
	λ = $\frac{3x_1^2 + a}{2y_1}$ $if\ P = Q$
		x_3
		$\lambda^2 - x_1 - x_2 mod\ 23$
			y_3
			$\lambda(x_1 - x_3) - y_1 mod\ 23$
				kP
				(x_3, y_3)

1				(3,10)
2	6	7	12	(7,12)
3	12	19	5	(19,5)

4	4	17	3	(17,3)
5	11	9	19	(9,16)
6	1	12	4	(12,4)
7	7	11	3	(11,3)
8	2	13	16	(13,16)
9	19	0	1	(0,1)
10	3	6	4	(6,4)
11	21	18	20	(18,20)
12	16	5	4	(5,4)
13	20	1	7	(1,7)
14	13	4	0	(4,0)
15	13	1	16	(1,16)
16	20	5	19	(5,19)
17	16	18	3	(18,3)
18	21	6	19	(6,19)
19	3	0	22	(0,22)
20	19	13	7	(13,7)
21	2	11	20	(11,20)
22	7	12	19	(12,19)
23	1	9	7	(9,7)
24	11	17	20	(17,20)
25	4	19	18	(19,18)
26	12	7	11	(7,11)
27	6	3	13	(3,13)

II. ELLIPTIC CURVE CRYPTOGRAPHY

A. Basic idea of Elliptic Curve Cryptography

Elliptic Curve Cryptography is a public key cryptographic algorithm. In public key cryptography each user or the device taking part generally has a pair of keys, a public key and a private key, and a set of operations are associated with the keys to do their cryptographic operations. Only a particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithms may require a set of predefined constants to be known by all the devices taking part in the communication. 'Domain parameters' in Elliptic Curve Cryptography are an example of such constants. [6]

An elliptic curve E over a field R of real number is defined by an equation

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

Here a_1, a_2, a_3, a_4, a_6 are real numbers ϵ R, x and y take on values in the real numbers. This equation could either be defined on complex, real, integers or any kind of field element. This equation is called the Weierstrass equation. Hence the elliptic curve E is defined over the field of integers K, because a_1, a_2, a_3,a_4, a_6 are integers. If E is defined over the field of integers K, then E is also defined over any extension field of K. The condition $\square \neq 0$ ensures that the elliptic curve is "smooth", i.e., there are no points at which the curve has two or more distinct tangent lines. The point at ∞ is the only point on the line at infinity that satisfies the projective form of the Weierstrass equation [1,7,8]. For the purpose of the encryption and decryption it is sufficient to consider the equation of the form $y^2= x^3+ ax + b$. For the given values of a and b the plot consists of positive and negative values of y for each value of x. Thus this curve is symmetric about the x-axis.

The fig.1 shows a model of Elliptic Curve Cryptography. Elliptic Curve Cryptography is divided into three kinds of fields. Field over real numbers, over prime numbers, and a binary Galois field. The main operations in Elliptic Curve Cryptography are Point Multiplication, Point Addition and Point Doubling. These operations can be performed over all kinds of fields, however this implementation deals only with the prime field, which is better suited for software implementation purposes.

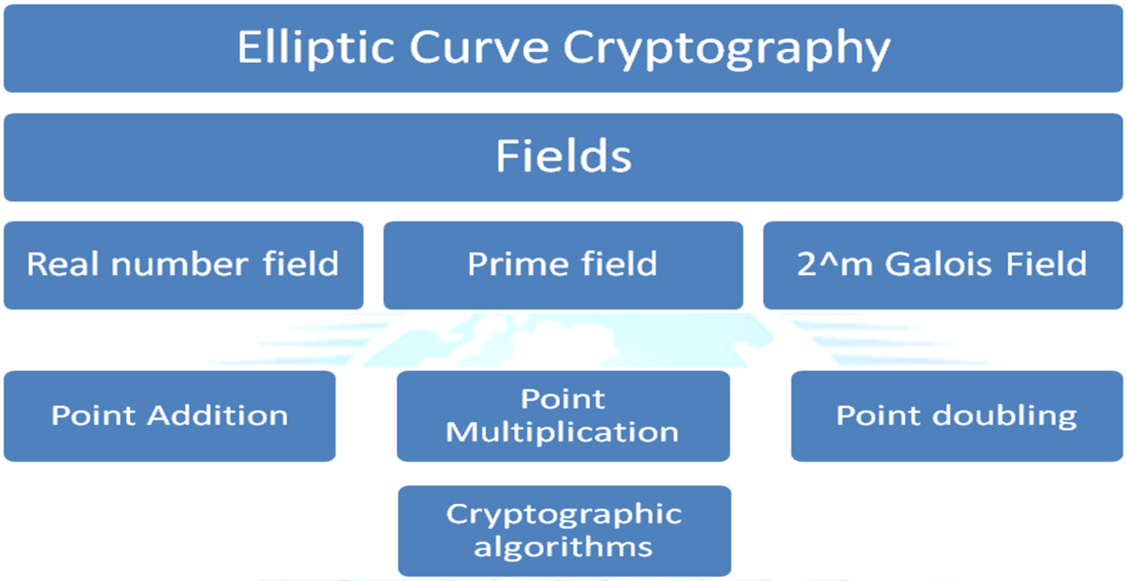

Fig.1 Elliptic Curve Cryptography

B .Basic properties to build Elliptic Curve Cryptography

Firstly, select secure finite field; secondly, the main consideration of selecting this background finite field is to realize modular addition and multiplication faster, because finite field must involve modular operation. For all public key algorithms such as RSA and ECC algorithm, their background finite fields are similar. Cryptography is interested in doing research on two kinds of finite fields: 1) finite field of large prime number [9] 2) finite field of characteristics 2.

When q=p , p is a prime number , then this kind of finite field is usually written by $G(F_p)$, called prime field. Field have p integers in the range of 0, 1, 2…..p-1.

When $Q=2^m$, it is called the finite field of characteristics 2 and usually written:GF (2^m).

For prime field, the mode of prime field is large prime number, and its length is even numbers, for example, 1024bits or 2048 bits. For binary field, mode is not a number but an algebraic expression, for example it may be irreducible polynomial. The distinction decides that it is absolutely different to realize modular addition and modular multiplication in prime field and binary field. I t is difficult to understand the calculation in finite field of characteristics 2, which is not addition, subtraction, multiplication and division in common sense. The difference in two kinds of finite fields is very great [10].

C. Basic Arithmetic operation in Elliptic Curve Cryptography.

The basic arithmetic operation performed in Elliptic Curve Cryptography includes point addition, point doubling, point multiplication. These operations are foundation upon which all Elliptic Curve Algorithms are implemented

1. Point Addition

Point addition is the addition of two points P and Q on an elliptic curve to obtain another point S on the same elliptic curve as shown in fig.2.

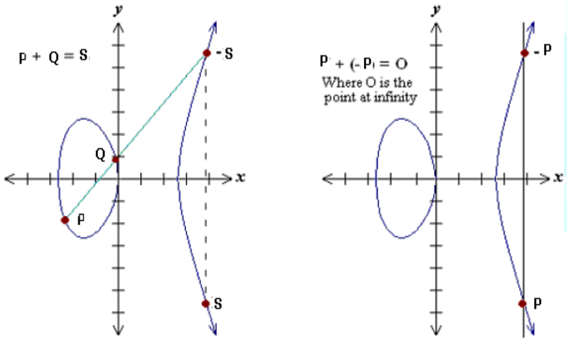

Fig.2 Point Addition

The operation is the addition of two points on the curve to obtain a third point on the curve. Let P(x_1, y1), Q(x_2, y2) € E_K(a, b) where P ≠ Q. Then P + Q = (x_3, y3) where,

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

$$y_3 = \lambda(x_1 - x_3) - y_1 \qquad (3)$$

Whereas λ is the slope of the line joining points P and Q,

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2} \; P \neq Q \qquad (4)$$

Suppose P(x_1, y1) € E_K(a, b) then,

$$P + (-P) = O_{\infty} \qquad (5)$$

Where (–P) = (x_1, -y_1), and this property is called as point at infinity. [1, 5, 6]

2. Point Doubling

Point doubling is the addition of point P on the elliptic curve to itself to obtain another point Q on the same elliptic curve.[1,5,6]

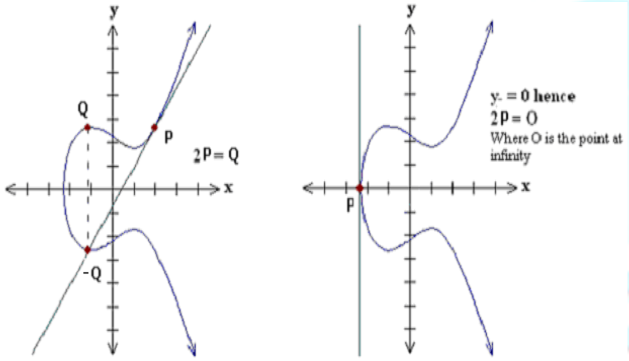

Fig.3 Point Doubling

To double a point P to get Q, i.e. to find P = 2Q, consider a point P on an elliptic curve as shown in Fig. 3. If y coordinate of the point P is not zero then the tangent line at P will intersect the elliptic curve at exactly one more point –Q. The reflection of the point –Q with respect to x-axis gives the point Q, which is the result of doubling the point P.

Thus Q= 2P. If y coordinate of the point P is zero then the tangent at this point intersects at a point at infinity O. Hence 2P = O when y_p = 0. This is shown in Fig. 3.

Let P=(x_1, y_1) € E_K(a, b) where P≠ -P then, 2P= (x_3, y_3) where,

$$x_3 = \lambda^2 - x_1 - x_2 \quad (6)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \qquad (7)$$

And λ is the slope of the line joining points P and (-P),

$$\lambda = \frac{3x_1^2 + a}{2y_1} \qquad (8)$$

3. Scalar Multiplication

In Scalar multiplication, a point P on the elliptic curve is multiplied with a scalar k using elliptic curve equation to obtain another point Q on the same elliptic curve. That is kP=Q. Scalar multiplication is achieved by two basic elliptic curve operations:-

• Point addition, adding two points P and Q to obtain another point S i.e., S = P + Q.

• Point doubling, adding a point P to itself to obtain another point Q i.e. Q = 2P.

Here is a simple example of point multiplication. Let P be a point on an elliptic curve. Let k be a scalar that is multiplied with the point P to obtain another point Q on the curve. i.e. to find Q = kP.

If k = 23 then kP = 2(2(2(2P) + P) + P) + P.

Thus point multiplication uses point addition and point doubling repeatedly to find the result [1, 5, and 6].

III. ENCODING AND DECODING OF MESSAGE IN THE IMPLEMENTATION OF ECC

ECC encryption and decryption methods can only encrypt and decrypt point on the curve not messages. There is no known polynomial time algorithm for finding large number of points on an arbitrary curve. We want a systematic way of finding points on $E_{P(a,\ b)}$ relating somehow to the plaintext message. Therefore we are forced to use probabilistic algorithms to do this, where the chance of failure is acceptably small. Thus encoding and decoding methods are important while encryption and decryption, [11]. Message encoding and decoding can be obtained by mapping all the points on the elliptic curve to an ASCII value. This is easiest method for embedding a message but less efficient in terms of security. The following steps are required for encoding and decoding message.

Step1: Pick an elliptic curve Ep(a,b).

Step 2: Let us say that E has N points on it.

Step 3: Let us say that our alphabet consists of the digits 0,1,2,3,4,5,6,7,8,9 and the letters A, B, C. . . X,Y,Z coded as 10, 11,. . . , 35.

Step 4: This converts our message into a series of numbers between 0 and 35.

Step 5: Now choose an auxiliary base parameter, for example k = 20. (Both parties should agree upon this)

Step 6: For each number mk (say), take x=mk + 1 and try to solve for *y*.

Step 7: If you can't do it, then try x = mk+2 and then x = mk+3 until you can solve for y.

Step 8: In practice, you will find such a y before you hit x = mk+ k - 1. Then take the point(x,y). This now converts the number m into a point on the elliptic curve. In this way, the entire message becomes a sequence of points.

Step 9: For decoding Consider each point (x,y) and set m to be the greatest integer less than $(x-1)/k$. Then the point (x,y) decodes as the symbol m.

The implementation of encoding and decoding message using SAGE (system for Algebra and Geometry Experimentation) software is shown in fig.8.

IV. THE TRANSPOSITION TECHNIQUES

The transposition technique does not replace one alphabet with another like the substitution technique but perform the permutation on the plaintext to convert it into cipher text. The various transposition techniques are used to perform the operation given below [12].

The Rail Fence technique is a simplest transposition technique. It involves writing plain text as a sequence of diagnosis and reading it row by row to produce cipher text. An example is shown below in fig. in this figure the plain text HELLO and the cipher text is HLOEL.

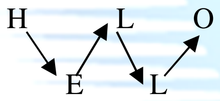

Fig 4. Rail Fence Technique

The simple columnar transposition technique is the variation of the Rail Fence technique. This technique simply arranges the plaintext as a sequence of rows of the rectangle that are read in column randomly. Example of this technique is shown in fig. 5. The plain text is COME HOME TOMORROW and the cipher text is OMOETRHOOMERCOMW if we choose the column order 2, 4,5,3,1. The simple Columnar transposition technique is also used multiple rounds to provide a tight security.Cipher text produced byusing Simple Columnar Transposition Technique with multiple rounds is much more complex to crack as compared to the basic technique.

Column1	Column2	Column3	Column4	Column5
C	O	M	E	H
O	M	E	T	O
M	O	R	R	O
W				

Fig 5. Simple Columnar Transposition Technique

V. THE PROPOSED WORK

If two communicating parties Alice and Bob want to communicate the messages then they agree upon to use an elliptic curve E_p (a,b) where P is prime number. ECC encryption and decryption method can only encrypt and decrypt a point on the curve not messages. The encoding (message to point) and decoding (point to message) methods are important while encryption and decryption. All the points on the elliptic curve can be directly mapped to an ASCII value, select a curve on which we will get minimum of 128 points, so that we have fix each point on the curve to an ASCII value. This is (Koblitz's method) easiest method for embedding a message but less efficient in terms of security [6].

The proposed scheme shown in fig.5 has first to process the Simple Columnar Technique with multiple rounds (SCTTMR). The plaintext message is first converted into the ciphertext by using Simpler Columnar Transposition Technique. The various rounds of SCTTMR may depend upon the security to provide the message. If the more security is needed then add more rounds of the SCTTMR scheme and if the normal security then uses minimum 1 or 2 rounds. The input to the SCTTMR is plaintext message and the output is cipher text message. The cipher text message is converted into points by using Koblitz's method and then applies ECC to obtain encryption of the message as shown in fig.6.
The decryption process is reverse of the encryption process.

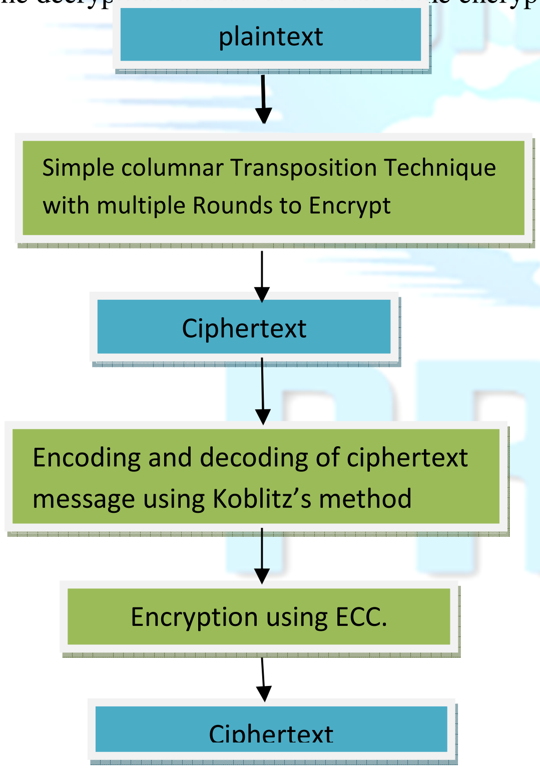
plaintext
Simple columnar Transposition Technique with multiple Rounds to Encrypt
Ciphertext
Encoding and decoding of ciphertext message using Koblitz's method
Encryption using ECC.
Ciphertext

Fig 6.Encryption with Enhanced ECC

VIII. THE RESULT AND DISCUSSION

To test the enhanced ECC algorithm, we have to take the input plaintext "HOW ARE YOU" and then apply the simple Columnar Transposition scheme to encrypt plaintext which is shown in fig. 7.

Column1	Column2	Column3
H	O	W
A	R	E
Y	O	U

Fig.7 simple Columnar Transposition Technique1st round to encrypt.

The random column number is 2, 3, 1, is taken in the 1st round and the output of the first round is ciphertext " OROWEUHAY". Now apply the 2nd round which have been taken the output of 1st round as an input and used the same random number to produce the cipher text which is as "REAOUYOWH". The obtained ciphertext is the input to koblitz's method which will produce the (x,y) points for message. Now we will perform encryption on the above points by using elliptic curve cryptography. The decryption process is the reverse of encryption process We take the output ciphertext from ECC. Then convert the cipher text points into message usingkoblitz method. The output of koblitz'smethod is applied to the transposition decryption technique to obtain plaintext.

IX. Conclusion

In today's time, the security is playing a very important and powerful role in the field of networking, Internet and various communication systems. The Elliptic curve cryptography is less secured by using Koblitz's method. The proposed work improved the security power of ECC using Transposition Techniques.

REFERENCES

[1] N.Koblitz, "Elliptic Curve Cryptosystem," *Mathematics of Computation,* vol.48, pages 203-209, 1987.

[2]V.S. Miller, "Use of Elliptic Curves in cryptography," Advances in Cryptography-CRYPTO '85,LectureNotes in Computer Science, vol.128,Springer-Verlag,pages 417-426,1985, Hugh C. Williams(Ed.)

[3] IEEE P1363, “Standard Specification for public key Cryptography,” 2000.

[4] Digital Signature Standard (DSS),*Federal Information processing Standards Publication*, National Institute of standards and Technology.2000.

[5] JeffreyHoffstein, Jill Pipher, Joseph H. Silverman, “*An Introduction to Mathematical Cryptography,”* Springer.

[6] Lawrence C. Washington, University of Maryland, “*Elliptic Curves Number Theory and Cryptography*”Chapman and Hall /CRC.

[7]Enge A. “Elliptic Curves and their applications to Cryptography”, Norwell,MA: Kulwer Academic publishers 1999

[8]Neil Koblitz, “An Elliptic Curve implementation of the finite field Digital Signature algorithm, “in Advances in Cryptography, (CRYPTO1998) , Springer Lectures Notes in Computer Sciences, 1462,327-337,1998.

[9]BAI Zhong-iian, YANG Hao-miao , ZHANG Wen-ke. Study on Fast Implementation of prime – field ECC. Communicatios Technology, 2011,12,87-89,92 .

[10]“Research on Design Principles of Elliptic Curve Public Key Cryptography and its Implementation” IEEE,Computer Science and Service System pages 1224-1227.

[11] N.Koblitz. A Course in Number Theory and Cryptography, Springer-Verlag second edition 1994.

[12]WilliamStalling, “Cryptography and Network security Principles and practices,” Pentice Hall, November 16, 2005.