Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cryptography Exploitation Elliptic Curve with Matrix Scrambling

[1]Naresh S. Badve, [2]Shyam P. Dubey, [3]Amit Warbhe
[1]Department of Computer Science and Engineering, Nuva College of Engineering and Technology, Nagpur, India
[2]Asst. Prof. & HOD, Nuva College of Engineering and Technology, Nagpur, India
[3]Asst. Prof. Manoharbhai Patel Inst. of Engineering, & Tech, Gondia, India

Abstract: Elliptic curve cryptography is additional powerful than different methodology that gains countless attention within the industry and plays vital role within the world of CRYPTOGRAPHY. This paper explains the strategy of elliptic curve cryptography victimization matrix scrambling method. during this methodology of cryptography we have a tendency to initial rework the plain text to elliptic curve so victimization matrix scrambling methodology we have a tendency to encrypt/decrypt the message. This method keeps information safe from unwanted attack to our information.

Keywords— Matrix scrambling, Elliptic Curve Cryptography, Encryption, Decryption, constant range, Random range generator, Circular shift technique, Prime Number.

I. INTRODUCTION

In the world of communication network and gift era it is additional vital to secure line through that we will send and receive the info or we will communicate firmly over channel and keep information securely. Currently cryptography may be a methodology that protects information while we have a tendency to be transferring information from one network to another network. to stay safe information or avoid the disclosed data ancient and fashionable cryptography are used. There are some standard public-key secret writing algorithms that contain some advanced calculation, for instance ,RSA, ElGamal. Due to properties, options and characteristic of elliptic curve cryptography increased attention of the many skilled and scientists as a result of it have opened wealth potentialities in terms of security. Proposed a matrix scrambling algorithmic rule supported 2 way circular queues. Underneath this case, we have a tendency to introduce a new secret writing methodology on elliptic curve supported matrix Scrambling technique. above all, this paper shows a new technique of encrypting information that permits smart diffusion and has a singular technique of decrypting it back to the plaintext and is straightforward to implement victimization matrix scrambling methodology that is predicated on random function and shifting. The selection of operation performed on rows or columns is predicated on Binary worth of prime no.

Therefore, the paper presents in details its implementation based on an elliptic curve given by the subsequent equation:

$y^2 = x^3 + x + 13$

II. CONCEPT OF ELLIPTIC CURVE

The study of elliptic curves by algebraists, algebraic geometers and range theorists dates back to the center of the nineteenth century. Elliptic Curve Cryptography (ECC) was discovered in 1985 by Neil Koblitz and Victor Miller. Elliptic Curve Cryptography may be a public key Cryptography. ECC is right for environments like cellular phones and sensible cards. Moreover, due to the apparent hardness of the underlying elliptic curve separate logarithm downside (ECDLP), ECC systems also are well suited for applications that require long-run security requirements. Elliptic Curve Cryptography (ECC) may be a public key technology that gives performance blessings at higher security levels. Understanding ECC desires full mathematical background on elliptic curves. Elliptic curves aren't ellipses. the overall cubical equation of elliptic curves is $y^2+axy+by=x^3+cx^2+dx+e$. except for our purpose it's sufficient to limit the equation to the shape $y^2=x^3+ax+b$. Say EP(a,b) consisting of all the points (x,y) that satisfy the on top of equation in conjunction with part at infinity O.

For ECC, we have a tendency to ar involved with a restricted kind of elliptic curve that's outlined over a finite field. Of particular interest for cryptography is what's remarked as the elliptic cluster mod p, wherever p may be a prime. This is outlined as follows. Opt for 2 plus integers, a and b, but p that satisfy: $4a^3+27b^2(\text{mod } p) \neq 0$, Then Ep(a, b) denotes the elliptic group mod p whose elements (x, y) are pairs of nonnegative integers less than p satisfying: $y^2\text{mod } p = (x^3+ ax + b)\text{mod } p$

III. PROPOSE METHOD

In this section we offer the new methodology of secret writing of a message (plain text) and decrypting back once more to the original message (plain text)

A). THE PLANNED METHODOLOGY DESCRIPTION:

1) ENCRYPTION: The plaintext is remodeled on points of elliptic curve and therefore the corresponding code is organized into a circular queue system. within the matrix M of n*m. The parameter p (Prime) represents the count of operations, say, the time of transformation we have a tendency to Created to matrix. The ECC methodology needs that we have a tendency to choose a random integer a, that has to be unbroken secret. Then base on the binary worth of prime circular shift is performed

Let b=bit (rj), wherever j is bit position, the worth of b is considered and supported it circular left shift or circular right shift are performed on rows. Equally as rows, circular upward shift or circular downward shift are performed on columns. The process of secret writing is completed as following:

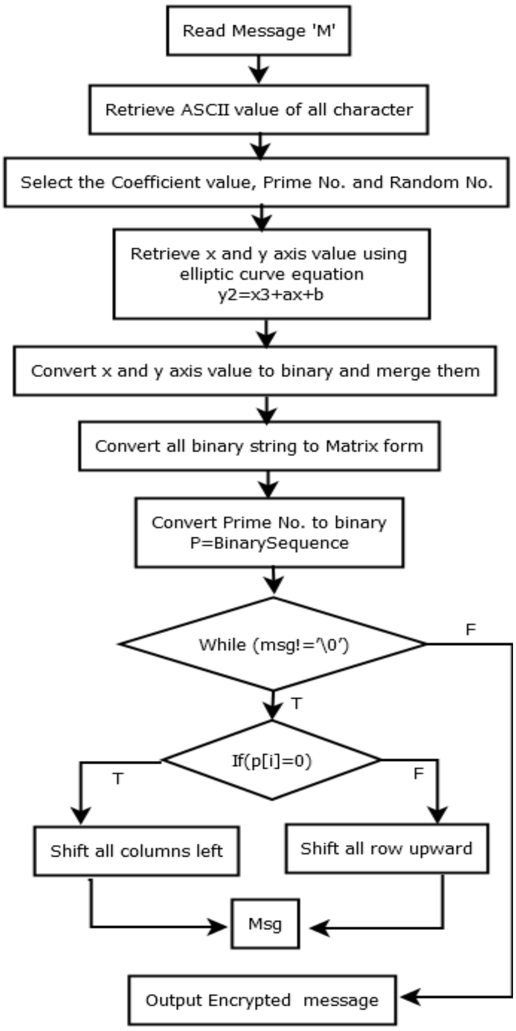

Read Message 'M'
Retrieve ASCII value of all character
Select the Coefficient value, Prime No. and Random No.
Retrieve x and y axis value using elliptic curve equation y2=x3+ax+b
Convert x and y axis value to binary and merge them
Convert all binary string to Matrix form
Convert Prime No. to binary P=BinarySequence
While (msg!='\0')
F
T
If(p[i]=0)
T
F
Shift all columns left
Shift all row upward
Msg
Output Encrypted message

Fig 1. Encryption Process flowchart

STEP1. The plaintext is mapped into points of elliptic curve. Then the code of points is ranged into bi-directional circular queue information sequence, within the matrix of n*m

$$M = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,m} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,m} \\ & \vdots & \vdots & \\ b_{n,1} & b_{n,2} & \cdots & b_{n,m} \end{pmatrix}$$

STEP2. a=Random (), with ‘aP’ may be a random purpose that Decides that transformation is applied on matrix (Row, columns). Once this we have a tendency to choose the code of ‘aP’ and keep in r. the selection of operation performed on rows and columns is predicated on the little bit of the sequence r.

STEP3. Let b=bit (rj), wherever j is bit position (LSB→MSB), that decides that transformation has got to be performed on rows and columns.

STEP4. The worth of bits verified:

If the present bit position is one then shift row upward circularly and if current bit position is zero then shift column circular shift right. Merge the matrix information during a single string to form it additional strong.

2) DECRYPTION:

The process is done by reversing the Operations done in the encryption process. The cipher text is arranged into a matrix of n*m noted M. The algorithm of decryption is given as follows:

STEP 1. Convert merged data into matrix n*m.

$$M = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,m} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,m} \\ & \vdots & \vdots & \\ b_{n,1} & b_{n,2} & \cdots & b_{n,m} \end{pmatrix}$$

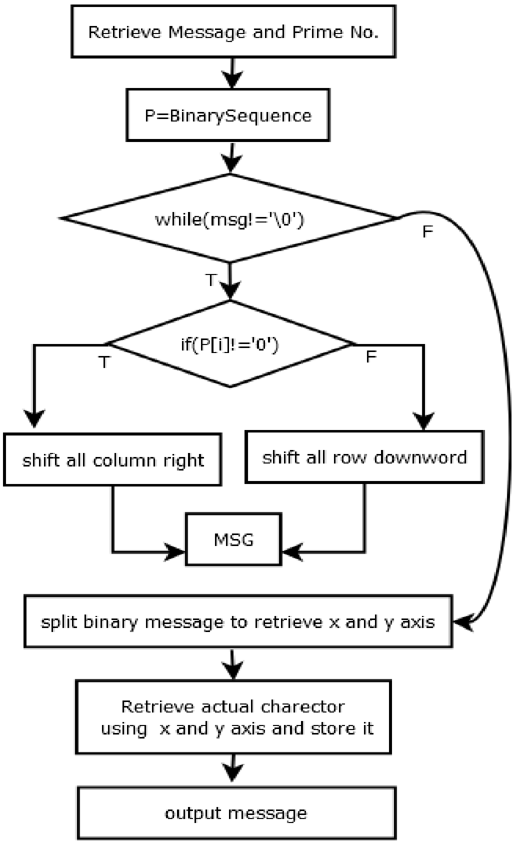

Retrieve Message and Prime No.
P=BinarySequence
while(msg!='\0')
F
T
if(P[i]!='0')
T
F
shift all column right
shift all row downword
MSG
split binary message to retrieve x and y axis
Retrieve actual charector using x and y axis and store it
output message

Fig 2. Decryption Process flowchart

STEP 2. Browse p (prime no.).Reverse the binary sequence of primary such that: r=Reverse (p)
STEP 3. for every worth b=bit (rj), wherever j is bit position such that operation is decoded that is given as :
InverseTrans (M).
In the case: j: LSB _m/2, the InverseTrans (M) is depending on the worth of b transpositions are performed.
If b=0 then upward shift columns else left shift operation is performed on rows. Within the case: j: m/2+1→MSB, the InverseTrans (M) depending on the worth of b transpositions are performed.
If b=0 then right shift rows else downward shift operation is performed on columns. After decipherment the received message M and reverse the imbedding, we have a tendency to get the plaintext.

B. IMPLEMENTATION DETAILS OF THE PLANNED ALGORITHMIC RULE

In this section, we have a tendency to take into account the elliptic curve given by the Weierstrass equation $y^2 = x^3 + x +$ 13Detailed method of our secret writing algorithmic rule by an example. In our case, we have a tendency to shall take a=58, then r=1010011101.
In vector r, solely 10bits is taken into account. This provides the information concerning operation on Rows and columns (Rowtrans and Coltrans).

Here in our case Alice needs to send a message "save" to Bob. First, she imbeds the message "save" into the elliptic curve E.
Next, she represents the plain text "save" as a series of bits recorded in matrix 4*10 as following:
Binary sequence of r is explained within the figure No. 3:

0	0	1	0	1	1	0	1	1	0
0	1	0	0	1	0	1	0	1	0
1	1	1	0	0	1	0	0	1	0
1	1	0	0	1	1	0	0	0	0

Plaintext

The technique of scrambling the matrix bits based on binary sequence of r is explained in the figure No. 3:

0	0	1	0	1	1	0	1	1	0
0	1	0	0	1	0	1	0	1	0
1	1	1	0	0	1	0	0	1	0
1	1	0	0	1	1	0	0	0	0

Plaintext

1	1	0	0	1	1	0	0	0	0
0	0	1	0	1	1	0	1	1	0
0	1	0	0	1	0	1	0	1	0
1	1	1	0	0	1	0	0	1	0

(1) Downward

1	0	0	1	1	0	0	0	0	1
0	1	0	1	1	0	1	1	0	0
1	0	0	1	0	1	0	1	0	0
1	1	0	0	1	0	0	1	0	1

(2) Left

1	1	0	0	1	0	0	1	0	1
1	0	0	1	1	0	0	0	0	1
0	1	0	1	1	0	1	1	0	0
1	0	0	1	0	1	0	1	0	0

(3) Downward

1	0	0	1	0	0	1	0	1	1
0	0	1	1	0	0	0	0	1	1
1	0	1	1	0	1	1	0	0	0
0	0	1	0	1	0	1	0	0	1

(4) Left

0	0	1	0	0	1	0	1	1	1
0	1	1	0	0	0	0	1	1	0
0	1	1	0	1	1	0	0	0	1
0	1	0	1	0	1	0	0	1	0

(5) Left

1	0	0	1	0	0	1	0	1	1
0	0	1	1	0	0	0	0	1	1
1	0	1	1	0	1	1	0	0	0
0	0	1	0	1	0	1	0	0	1

(6) Right

1	1	0	0	1	0	0	1	0	1
1	0	0	1	1	0	0	0	0	1
0	1	0	1	1	0	1	1	0	0
1	0	0	1	0	1	0	1	0	0

(7) Right

1	1	1	0	0	1	0	0	1	0
1	1	0	0	1	1	0	0	0	0
0	0	1	0	1	1	0	1	1	0
0	1	0	0	1	0	1	0	1	0

(8) Right

1	1	0	0	1	1	0	0	0	0
0	0	1	0	1	1	0	1	1	0
0	1	0	0	1	0	1	0	1	0
1	1	1	0	0	1	0	0	1	0

(9) Upward

0	1	1	0	0	1	1	0	0	0
0	0	0	1	0	1	1	0	1	1
0	0	1	0	0	1	0	1	0	1
0	1	1	1	0	0	1	0	0	1

(10) Right

Fig 3. Encryption process.

The cipher text obtained is given as:
0110011000000010110110010010101011100100110100111101

The secret writing process: In this section, we have a tendency to show the elaborated method of our decryption algorithmic rule with AN example.

Consider the cipher text obtained once secret writing as:
0110011000000010110110010010101011100100110100111101

The cipher text once inserting in matrix M of order n and m is given .The secret writing is completed by reading the last sequence of bits noted d in reverse order and reverse operation each Rowtrans and Coltrans. d=1010011101and r=Reverse d=1011100101

Then, the method of secret writing is given below:

0	1	1	0	0	1	1	0	0	0
0	0	0	1	0	1	1	0	1	1
0	0	1	0	0	1	0	1	0	1
0	1	1	1	0	0	1	0	0	1

Cipher text

1	1	0	0	1	1	0	0	0	0
0	0	1	0	1	1	0	1	1	0
0	1	0	0	1	0	1	0	1	0
1	1	1	0	0	1	0	0	1	0

(1) Left

1	1	1	0	0	1	0	0	1	0
1	1	0	0	1	1	0	0	0	0
0	0	1	0	1	1	0	1	1	0
0	1	0	0	1	0	1	0	1	0

(2) Downward

1	1	0	0	1	0	0	1	0	1
1	0	0	1	1	0	0	0	0	1
0	1	0	1	1	0	1	1	0	0
1	0	0	1	0	1	0	1	0	0

(3) Left

1	0	0	1	0	0	1	0	1	1
0	0	1	1	0	0	0	0	1	1
1	0	1	1	0	1	1	0	0	0
0	0	1	0	1	0	1	0	0	1

(4) Left

0	0	1	0	0	1	0	1	1	1
0	1	1	0	0	0	0	1	1	0
0	1	1	0	1	1	0	0	0	1
0	1	0	1	0	1	0	0	1	0

(5) Left

1	0	0	1	0	0	1	0	1	1
0	0	1	1	0	0	0	0	1	1
1	0	1	1	0	1	1	0	0	0
0	0	1	0	1	0	1	0	0	1

(6) Right

1	1	0	0	1	0	0	1	0	1
1	0	0	1	1	0	0	0	0	1
0	1	0	1	1	0	1	1	0	0
1	0	0	1	0	1	0	1	0	0

(7) Right

1	0	0	1	1	0	0	0	0	1
0	1	0	1	1	0	1	1	0	0
1	0	0	1	0	1	0	1	0	0
1	1	0	0	1	0	0	1	0	1

(8) Upward

1	1	0	0	1	1	0	0	0	0
0	0	1	0	1	1	0	1	1	0
0	1	0	0	1	0	1	0	1	0
1	1	1	0	0	1	0	0	1	0

(9) Right

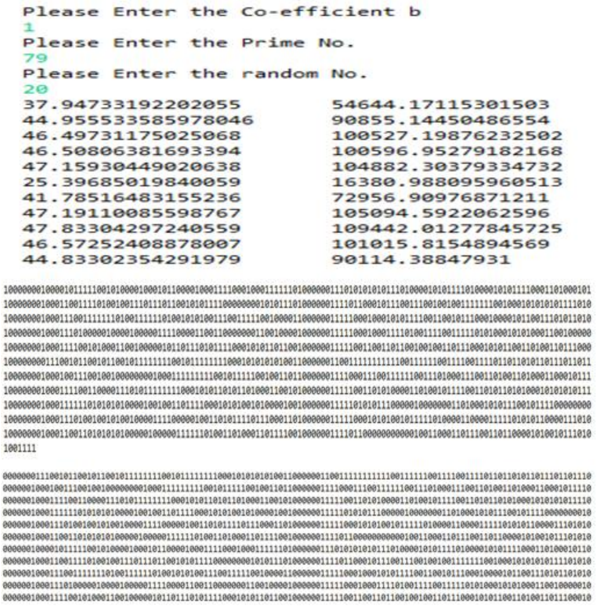
0	0	1	0	1	1	0	1	1	0
0	1	0	0	1	0	1	0	1	0
1	1	1	0	0	1	0	0	1	0
1	1	0	0	1	1	0	0	0	0

(10) Upward

Fig 3. Decryption process.

When a similar plaintext is taken and once the secret writing is performed once more, then the resultant disorganized matrix is different. For an trespasser it'd be terribly troublesome to guess on that purpose the secret writing method is performed and therefore improves the problem of decrypting. Our algorithm is predicated on magic parallelogram ,and therefore it's easy to grasp straightforward and straightforward and simple} to implement the planned algorithm, that additionally uses solely two styles of linear array operations, circular horizontal shifting(left, right) and circular vertical shifting(up, down). therefore it works with efficiency with very little system resources. The parameter ’m’ additionally plays a crucial role in strengthening the intensity of secret writing beside the parameter ’a’. looking on elliptic curve, the worth of parameter ’m’ plays a crucial role au fait the intensity of the secret writing. ’m’ mustn't be too tiny or too large. The experimental results show that the new scheme features a in no time secret writing speed and therefore the x-y coordinate is distended and it will resist all types of cryptanalytic. Thus, we have a tendency to conclude that the planned Fig 3. Secret writing method scheme will strengthens the elliptic curve cryptosystem against most of the present assaultive.

IV. SAMPLE OUTPUT



```
Please Enter the Co-efficient b
1
Please Enter the Prime No.
79
Please Enter the random No.
20
37.94733192202055         54644.17115301503
44.955533585978046        90855.14450486554
46.49731175025068         100527.19876232502
46.50806381693394         100596.95279182168
47.15930449020638         104882.30379334732
25.39685019840059         16380.988095960513
41.78516483155236         72956.90976871211
47.19110085598767         105094.5922062596
47.83304297240559         109442.01277845725
46.57252408878007         101015.8154894569
44.83302354291979         90114.38847931
```

```
10000000100001011111100101000010001011000010001111000100011111101000000111010101010111010000101011110100001010111100011010000101
10000000100011001111010010011101110110010101111000000001010111010000001111011000101110011100100100111111100100010101010101111010
10000000100011100111111101001111110100101010011100111110010000110000001111100010001010111100110010111000100001011001110101101010
10000000100011101000000100001000000111100001100110000000011001000010000001111100010001111010011110011111010100010101000110010000
10000000100011110010100011001000000101101110101111000101011011001000000011111001100110110010010011011100010101100110100110111000
10000000011100101100101100101111111110010111111111000101010101001100000001100111111111110011111100111100111101101101010110111011011
10000000100010011100100100000000010001111111110010111110010011011000000011110001110011111100111010001110011010011010001100010111
10000000100011110011000011101011111111000101011010110100011001010000000111110011010100001101001011110011010110101000101010100111
10000000100011111101010101000010010011011110001010100101000010010000000111110101011100000010000000110100010101110010111100000000
10000000100011101001001010010000111100000010011010111101110001101000000111110001010100101111101000011000011111010101100001111010
10000000100011001101010101000000100000111111010011010001101111001000000111101100000000000010011000110111001101100001010010111010
1001111

00000001110010110010110010111111111001011111111100010101010100110000000110011111111111001111110011110011110110110101011011101011110
000000100010011100100100000000010001111111110010111110010011011000000011110001110011111100111010001110011010011010001100010111110
000000100011110011000011101011111111000101011010110100011001010000000111110011010100001101001011110011010110101000101010101111110
000000100011111101010101000010010011011110001010100101000010010000000111110101011100000010000000110100010101110010111100000000010
000000100011101001001010010000111100000010011010111101110001101000000111110001010100101111101000011000011111010101100001111010101
000000100011001101010101000000100000111111010011010001101111001000000111101100000000000010011000110111001101100001010010111010101
000000100001011111100101000010001011000010001111000100011111101000000111010101010111010000101011110100001010111100011010000101110
000000100011001111010010011101110110010101111000000001010111010000001111011000101110011100100100111111100100010101010101111101010
000000100011100111111101001111110100101010011100111110010000110000001111100010001010111100110010111000100001011001110101101101010
000000100011101000000100001000000111100001100110000000011001000010000001111100010001111010011110011111010100010101000110010000010
000000100011110010100011001000000101101110101111000101011011001000000011111001100110110010010011011100010101100110100110111000010
```

V. CONCLUSION

In this paper, we've developed AN algorithmic rule secret writing and secret writing on elliptic curve victimization matrix scrambling technique. So, the usage of random purpose on elliptic curve firstly and second for choosing the operations for scrambling, avoids the regularity within the resultant cipher text that is remodeled from plaintext matrix, and hence improves the problem for decrypting. Finally, we like to suggests that the great selection of elliptic curve and an whole number worth ’a’ provides higher binary sequence, that is employed to scramble the matrix in each directions with efficiency. At the end, there's many scope to flirt with the choice of the ’aP’ purpose. Looking on the amount of memory demand, one will analyze the use of this algorithmic rule in tiny memory devices like sensible cards and mobile devices. This algorithmic rule is additionally applied to text secret writing, image secret writing, and transmission secret writing and then on. ECC may be a field wherever there's giant scope for higher research.

ACKNOWLEDGMENT

The authors would love to convey the collogues and senior faculty for his or her helpful suggestions and steerage

REFERENCES

[1] J. J. Amador and R.W. Green, Symmetric-Key BlockCipher

[2] Image and Text Cryptography, International Journal of Imaging and Technology, Vol. 15, No. 3, pp. 178-188, 2005.

[3] N. Demytko, a replacement Elliptic Curve based mostly Analogue of RSA, in T.Helleseth, editor, Advances in Cryptology-Eurocrypt93, Springer-Verlag, New York, pp. 4049, 1994.

[4] N. Koblitz, Elliptic Curve Cryptosystems, ed. Mathematics of Computation, Vol. 48, No. 177, pp. 203-209, 1987.

[5] Elliptic curve cryptography victimisation matrix scrambling methodology, IEEE normal 2012

[6] V. S. Miller., Use of Elliptic Curves in Cryptography, Advances in cryptanalysis CRYPTO85, pp. 417-426, 1986.

[7] Suli Wu, Yang Zhang, and Xu Jing, A Novel Encryption AlgorithmBased on Shifting and Exchanging Rule of Bi-column Bi-row Circular Queue, CSSE (3)’2008. pp.841-844, 2008.

[8] Suli Shanghai dialect and Xiaofei Loloish, Text secret writing Algorithm based mostly Cyclic Shift,The Smart Internet’2010. pp.3483-3486, 2010.

[9] Normal Specifications for Public Key Cryptography, IEEE normal p1363, 2000.

[10] W. W. Yan Weimin, system, Tsinghua University Press, Beijing, 1992.