International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 12 | Dec -2016 www.irjet.net p-ISSN: 2395-0072

OUTLINE OF MODIFIED MENEZES VANSTONE ELLIPTIC CURVE CRYPTOGRAPHY ALGORITHM

Kavyashree B[1], Girijamba D L[2], Kavya A P[3]

[1]*Assistant Professor, Dept. of ECE, VVCE, Mysuru, Karnataka, India*
[2]*Assistant Professor, Dept. of ECE, VVCE, Mysuru, Karnataka, India*
[3]*Assistant Professor, Dept. of ECE, VVCE, Mysuru, Karnataka, India*

Abstract - *Elliptic Curve Cryptosystems (ECC) have recently received significant attention by researchers due to their performance. This paper proposes a new approach to encrypt data (message) with new modified version of Menezes Vanstone cryptosystem based on elliptic curve. This new version basically utilizes the original Menezes Vanstone cryptosystem, but it added additional features to cryptosystem's encryption method that uses character's hexadecimal values that can encrypt data. Thus knowledge of each character's point does not have to be sent to recipient. The implementation of this algorithm is done using MATLAB.*

Key Words*: *Menezes Vanstone Elliptic Curve Cryptosystem, Elliptic Curve Cryptography, Cryptology, Encryption, Decryption, Elliptic Curves, Security

1. INTRODUCTION

Cryptography is the study of information hiding and verification. It contains the protocols, algorithms and approaches to securely and consistently prevent or delay unauthorized access to sensitive information and allow verifiability of every component in a communication.

It aims to secure communication between sender and recipient in the insecure communication medium like internet. When information is transformed from a useful form of understanding to an opaque form of understanding, this is called encryption. At the point when the data is returned into an appropriate frame, it is called unscrambling or decryption. Expected beneficiaries or approved utilization of the data is controlled by whether the client has a specific bit of mystery information. Just clients with the mystery learning can change the hazy data once more into its helpful shape. The mystery information is regularly called the key, however the mystery learning may incorporate the whole procedure or calculation that is utilized as a part of the encryption/decoding. The data in its helpful frame is called plaintext (or cleartext); in its encoded shape it is called ciphertext. The calculation utilized for encryption and unscrambling is known as a figure.

In the mid-1980s Miller [1] and Kibitz [2] introduced elliptic curves into cryptography. After Olestra [3] showed how to use elliptic curves to factor integers, elliptic curves played an increasingly important role in many cryptographic situations are required security and privacy.

Elliptic curve cryptography is a public key cryptography based on the properties and functions of elliptic curves. Elliptic curve cryptography (ECC) is one of high potential applicants for WSN's (wireless sensor networks), which requires less computational power, communication bandwidth, and memory in comparison with other Cryptosystems. It has gained considerable attention in the recent and has attracted many researchers because of the higher security levels it has been able to achieve.

ECC is based on something called the elliptic curve discrete log problem, and it's a much harder problem than factoring integers. Another reason of using elliptic curves in cryptography is that they seem to offer a level security needs comparable to classical cryptosystems that use much larger key sizes. Using of smaller key sizes is important in the environments where resources like processing power, storage bandwidth and power consumption are limited. Elliptic curve cryptography (ECC) algorithm is an encryption algorithm. We use its mechanism which is Menezes Vanstone cryptosystem [4] in our study.

To provide an efficient alternative to other cryptosystems, a new method is implemented in this paper that show how to encrypt characters with their hexadecimal values that provides secured communication media without the necessity of code table which is agreed by communication parties with modified version of Menezes Vanstone cryptosystem based on elliptic curve.

2. REVIEW ON THE ECC ALGORITHM

An elliptic curve E takes the general form as:
E: $y^2 = x^3 + ax + b$ [p]
Where a, b are in the appropriate set (rational numbers, real numbers, integers mod p, etc.) and x, y are elements of the finite field GF (p) satisfying $4(17)^3 + 27(33)^2 \neq 0 \pmod p$

and p is known as modular prime integer making the elliptic curve finite field.

There are two basic group operations on elliptic curve which are point addition and point doubling.

A. Point Addition

Addition means that given two points on E and their coordinates, P = (x_1, y_1) and Q = (x_2, y_2), E (GF (p)), we have to compute the coordinates of a third point R such that:

P +Q = R

(x_1, y_1) +(x_2, y_2) = (x_3, y_3)

This is the case where we compute R = P + Q and P≠Q. Point R's coordinates (x_3, y_3) also E (GF (p)).

$s= (y_p- y_q) / (x_p – x_q)$

$x_r = [s^2 – x_p- x_q] \mod p$

$y_r = [- y_p + s(x_p – x_r)] \mod p$

B. Point Doubling

Point doubling is the addition of a point P on E to itself to obtain another point R. This is the case where we compute P +Q but P = Q. Hence we can write R = P + P = 2P.

$s = (3x_p{}^2 + a) / (2y_p)$

$x_r = s^2 – 2x_p \mod p$

$y_L = [-y_p + s(x_p – x_r)] \mod p$

3. MENEZES VANSTONE CRYPTOSYSTEM

Menezes Vanstone Elliptic Curve Cryptosystem is a solution to the problem of encoding a message in a point. It uses a point on an elliptic curve to mask a point in the plane.

Menezes Vanstone Elliptic Curve Cryptosystem that is a variant of EIGamal's [5]encryption system. These systems basically use elliptic curves. However, there is one main difference between these two cryptosystem.

The difference is that, in Menezes Vanstone cryptosystem, the message to be encrypted is masked instead of embed over E elliptic curve. This situation indicates that the message must be expressed as a point on E elliptic curve when EIGamal's [5] cryptosystem is used but this is a limiting factor. The message is independent from the points on elliptic curve which is important in terms of security because person who is trying to obtain secret message can guess this situation. Menezes Vanstone cryptosystem is fast and simple. Therefore we choose to use Menezes Vanstone cryptosystem.

Encryption and decryption methods are for Menezes Vanstone elliptic curve cryptosystem as:

E is an elliptic curve defined on Zp, P > 3, p is a prime number or for n > 1 is defined on finite field GF (p^n). E also contains a cyclic group in which the discrete log problem is impossible.

The process of encryption and decryption has two entities, sender (A) and recipient (B). Both the entities agree upon a, b, p, G, n which are called domain parameters.

A. Key Generation

Recipient B selects a random number n_B and it is private key, G is the generator point and n is the order of G, computes P_B public key as follows:

$$P_B = n_B * G$$

B. Encryption

Sender A gets B's public key P_B, selects a random number k[1, n-l], selects the message (plaintext) x = (x1, x2) that wants to encrypt it then computes:

Yo = k· G

(C1,C2) = k .P_B

Yl = Cl . Xl mod p

Y2= C2. Xl mod p

After calculating these equations, sends plaintext as a point (Yo, Yl, Y2) called ciphertext.

C. Decryption

Recipient B uses whose secret key nB for calculating:

(C1, C2) = nB . Yo

x = (Y1.$C1^{-1}$ mod p, Y2. $C2^{-1}$ mod p)

The point (Yl .$C1^{-1}$ mod p, Y2 . $C2^{-1}$ mod p) represents the plaintext x.

4. THE MODIFIED CRYPTOSYSTEM

The altered cryptosystem can scramble point as well as message as per demand of sender. As per our encryption technique, firstly the message is isolated into hinders that contain just a single character, and after that every character is changed over to hexadecimal configuration. Hexadecimal estimations of every character have two digits. These two digits permit us to express the message as a point. Hence information of every character's indicate does not have be sent to beneficiary.

If sender wants to encrypt the message, the plaintext dimension d is calculated then divided into blocks as the size of plaintext and each block is encrypted by an identical key set K' = {(E', a', a', P'): P' = a' .a'} that has exactly the same characteristic of the original Menezes Vanstone ECC cryptosystem. Every block has only one character. After that this character's equivalent of hexadecimal (base-16) number system is calculated. Every character's equivalent of hexadecimal value is given in Table. l.

Table -1: Hexadecimal Values of Each Character

00 nul	01 soh	02 stx	03 etx	04 eot	05 enq	06 ack	07 bel
08 bs	09 ht	0A nl	0B vt	0C np	0D cr	0E so	0F si
10 dle	11 dc1	12 dc2	13 dc3	14 dc4	15 nak	16 syn	17 etb
18 can	19 em	1A sub	1B esc	1C fs	1D gs	1E rs	1F us
20 sp	21 !	22 "	23 #	24 $	25 %	26 &	27 '
28 (	29)	2A *	2B +	2C ,	2D -	2E .	2F /
30 0	31 1	32 2	33 3	34 4	35 5	36 6	37 7
38 8	39 9	3A :	3B ;	3C <	3D =	3E >	3F ?
40 @	41 A	42 B	43 C	44 D	45 E	46 F	47 G
48 H	49 I	4A J	4B K	4C L	4D M	4E N	4F O
50 P	51 Q	52 R	53 S	54 T	55 U	56 V	57 W
58 X	59 Y	5A Z	5B [	5C \	5D]	5E ^	5F _
60 `	61 a	62 b	63 c	64 d	65 e	66 f	67 g
68 h	69 i	6A j	6B k	6C l	6D m	6E n	6F o
70 p	71 q	72 r	73 s	74 t	75 u	76 v	77 w
78 x	79 y	7A z	7B {	7C |	7D }	7E ~	7F del

According to Table. 1, that can be easily shown, each character's hexadecimal value, is located to the left of character's in the table, has two digits whose units digit indicatesX2i and tens digit indicates Xli for that reason the character represented as a point (Xli, x2D, subscript I symbolizes block number, it is an integer and I <:: I <:: d. However X2i can be one of these letters A, B, C, D, E, and F, in this case hexadecimal value is converted to decimal. These are A ---> 10, B---> 11, C--->12, D--->13, E--->14, and F--->15.As mentioned before, the key structure is the same with Menezes Vanstone ECC.

A. Key Generation

Recipient B selects a random number nB' and it is private key, G' is the generator point and n' is the order of G',computes P_B' public key as follows:

P_B' = nB'· G'

B. Encryption

Sender A gets B's public key P_B' selects a random number k'[1, n'-I], selects the plaintext x'. Then x' sent to the Convert toPoint function.

The function converts to plaintext's value as x' = (xli, x2i) than computes:

Encryption of a plaintext (x1, x2) Z^*_p x Z^*_p

$y'_o = k' \cdot G'$

$(c'_1, c'_2) = k' \cdot P_B'$

$y'_{li} = c'_1 \cdot x_{li} \bmod p$

$y'_{2i} = c'_2 \cdot x_{2i} \bmod p$

After calculating these equations, every character of the plaintext as a point (y'_o, y'_1' y'_2) is sent n' times.

C. Decryption

Recipient B uses whose secret key nB' calculating:

$(c'_1, c'_2) = nB' \cdot y'_o$

$xi = (y'_{li} \cdot c_1^{-1} \bmod p, y'_{2i} \cdot c_2^{-1} \bmod p)$

Using this equation ($x_i = x_{li} \cdot 16 + x_{2i}$) that represents plaintext x' = {($x_1 x_2 \ldots, x_n$): i = 1, 2, 3. ....n}

The steps to be followed during encryption and decryption are given in the following flowchart in fig. 1

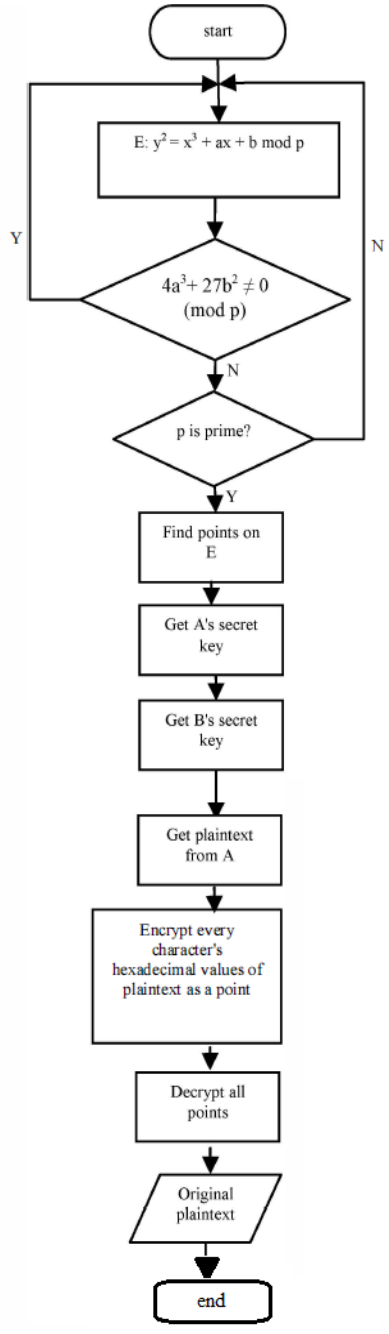

Fig -1: Proposed Flowchart of Encryption and Decryption.

5. IMPLEMENTED RESULT

For example sender A wants to sent the plaintext "Menezes Vanstone Elliptic Curve Cryptosystem" to recipient B. Every character of plaintext "Menezes" is represented by a point. These values can be shown Fig-1.
M:4D---> (4, 13), e:65---> (6, 5), n:6E---> (6, 14), e:65---> (6, 5), z:7 A---> (7, 10), e:65---> (6,5), s:73---> (7, 3).
E: $y^2 = x^3 + 17x + 33 \bmod 107$,
As $4(17)^3 + 27(33)^2 \neq 0 \bmod 107$, E is an elliptic curve.
nB = 27, G = (5, 55), pB= nB .G = 27· (5, 55) = (45, 63), k=19, d = 7
As mentioned before, G is generator point on E, we use it while finding P_B . It is clear that P_B must be on E elliptic curve.

Encryption

The cipher text obtained after encryption is a pair of the points (Y0, Y1, and Y2)

i = {l, 2, 3 ... , 7},

Yo = k . G = 19 . (5, 55) = (73, 13), where Yo is the 1st pair of the cipher text which is common to all the points.

(c1, c2) = k· P_B = 19· (45, 63) = (60, 48),

The plaintext is divided into seven blocks and every block is sent to B. First character "M" is encrypted and the others are found the same method.
The value of Yo does not change therefore we use it only first character. The plaintext is converted to ciphertext as Character "M" is encrypted as: (73, 13, 26, 89)

Y11= C1. Xl mod p = 60· 4 mod 107= 26,

Y21 = C2. X2 mod p = 48 . 13 mod 107= 89,

And ciphertext as shown in fig.2 for the word Menezes, all the characters follows the similar method.

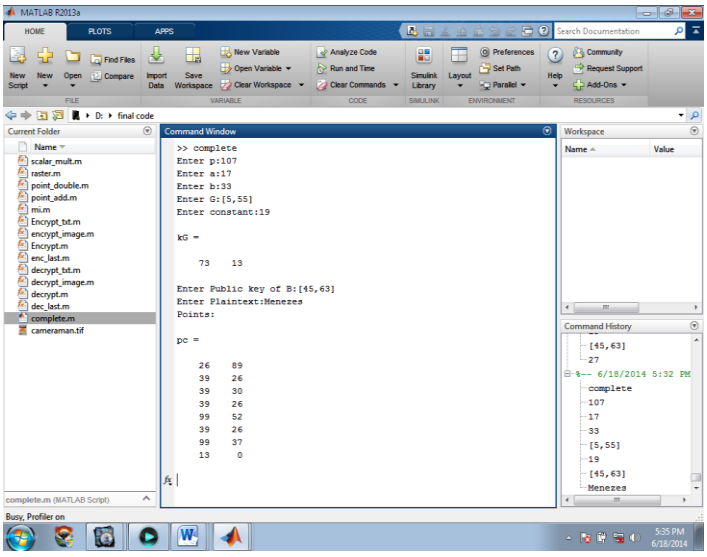

Fig-2: Encrypted output of text

Decryption

Receiver B uses its secret key n_B to perform decryption.

Where n_B=27.

(c1, c2)= n_B.Yo

The secret key is multiplied with the first pair of the cipher text and the obtained value is just inversed and multiplied to the next pair of the cipher text with their respective co-ordinates to obtain the original plain text.

(c1, c2) = 27· (73, 13) = (60, 48),

For i =1--->(y_{li},y_{2i} = (y_{l1},y_{21}) = (26, 89),

xi = (y'_{li} . c_1^{-1}mod p, y'_{2i} . c_2^{-1} mod p = (26 . 60^{-1}mod 107,89 .48^{-1}mod 107) = (4, 13) ---> (4, D) which corresponds to the character "M".

The cipher text is decrypted with this method. At the end of these operations, plaintext is obtained successfully with our implementation as shown in fig-3.

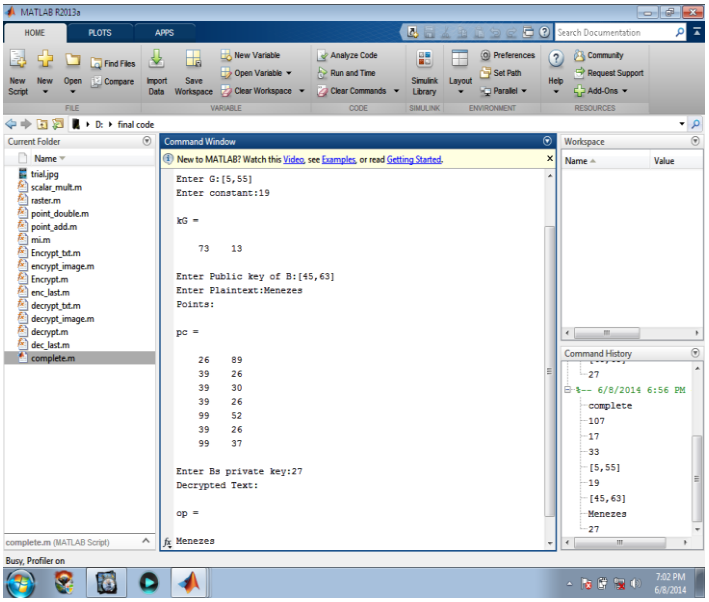

Fig- 3: Decrypted output of text

The ciphertext is decrypted with this method. At the end of these operations plaintext is obtained successfully with our implementation.

The CPU times are also calculated for encryption and decryption,the encoding and decoding time varies processor to processor.

6. CONCLUSIONS

The reason for the review is left unfulfilled if the outcomes are not appropriately investigated. Elliptic curve cryptosystem provides an efficient alternative to other cryptosystems. In this study we explain how to encrypt characters with their hexadecimal values that provides secured communication media without the necessity of code table which is agreed by communication parties with modified version of Menezes Vanstone cryptosystem based on elliptic curve.

In future, encryption of images using the same modified algorithm will be made.

REFERENCES

[1] V. S. Miller, "Use of elliptic curves in cryptography", Advanced in Cryptology, Proceedings of Crypto85, Lecture note in Computer Science. 218, Springer Vela, pp. 417-426, 1986.
[2] N. Kibitz, "Elliptic curve cryptosystem"', Mathematics of Computation,48: pp. 203-209,1987
[3] H. W. Olestra, "Factoring integers with elliptic curves"', Annals of Mathematics 126, pp. 649-673,1987
[4] A. Meekness, S. Vanstone, "Elliptic curve cryptosystem and their implementation"', Journal of Cryptography 6 (4), pp. 209-224, 1993.
[5] T. EI Gama, "A public key cryptosystem and a signature scheme based on discrete logarithms"', Advanced in Cryptology, Proceedings ofCrypto84, Springer Vela, pp. 10-18, 1988.

BIOGRAPHIES

Kavyashree B is working as Assistant professor in VVCE, Mysuru. She pursued her M.Tech from KVGCE, Sullia-DK in Digital Electronics and Communication. Her areas of interest are Image Processing, Cryptography, Communication and Networking.

Girijamba D L is working as Assistant professor in VVCE, Mysuru. She pursued her M.Tech from MCE, Hassan in Digital Electronics and Communication Systems. Her areas of interest are Photonics, Communication and Networking.

Kavya A P is working as Assistant professor in VVCE, Mysuru. She pursued her M.Tech from VTURC, Mysuru in Digital Electronics and Communication Systems. Her areas of interest are Wireless Sensor Networks and Communication.