International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Implementation of Double Fold Text Encryption Based on Elliptic Curve Cryptography (ECC) with Digital Signature

CH. Suneetha, T. Surendra, CH. Neelima

Abstract:As the internet provides access to millions of communications in every second around the world, security implications are tremendously increasing. Transfer of important files like banking transactions, tenders, and e commerce require special security and authenticated mechanism in its journey from the sender to the receiver. Recent attention of cryptography is mainly focused on use of elliptic curves in public key cryptosystems. The present paper explains an innovative public key cryptographic scheme for protecting sensitive of critical information using elliptic curve over finite field. This mechanism besides providing the robustness of the cipher contributes the authentication of the message with digital signature.

Key Words: Encryption, Decryption, Elliptic curve over finite field, Digital Signature Algorithm.

I. INTRODUCTION

Use of elliptic curves in public key cryptography was first designed and launched by Koblitz and Miller. The principal reason for wide attraction of the researchers towards ECC is it provides the same security level as conventional public key systems with comparatively shorter key length, due to the hardness of Elliptic Curve Discrete logarithmic Problem (ECDLP). Public key cryptography is computationally very expensive for small devices unless it is accelerated by cryptographic hardware. The security of the ECC relies on the complexity of the hidden mathematical problem. A comparison of ECC with conventional systems reports that ECC is more suitable in mobile computing applications and wireless sensor networks with limited resources. The present paper describes a new encryption scheme using ECC and logical XOR operation. A digital signature is designed using elliptic curve domain parameters and one way cryptographic hash function and attached to the cipher.

Manuscript published on January 30, 2020.
* Correspondence Author
CH. Suneetha*, Associate Professor, Dept. of Applied Mathematics GITAM University, Visakhapatnam, India gurukripachs@gmail.com
T. Surendra, Assistant Professor, Dept. of Applied Mathematics GITAM University, Visakhapatnam, India surendrat.bw@gmail.com
CH. Neelima, Faculty of Mathematics, Sankethika Engineering college Visakhapatnam, India neeluchallarapu@gmail.com

Digital signature is identical to handwritten signature which is the hash value of the secret key combined with the cipher computed by the sender and appended by the sender to the cipher. The receiver verifies the digital signature before decrypting the cipher. At this verification end the signer's secret key will not be broken. Due to this the present algorithm not only conceals but also provides the integrity, authentication and non repudiation of the information that is being transmitted.

II. PRELIMINARIES

For cryptographic purpose elliptic curve is defined by the equation $y^2 = x^3 + ax + b$, $4a^3+27b^2 \neq 0$ over the finite field F_q of a prime number q.

Group laws of elliptic curve:- On an elliptic curve E defined over the finite field of integers, addition of two points uses chord-and-tangent rule to get the third point [1,2]. The set of all points on the elliptic curve over the finite field with addition as binary operation forms an abelian group with ∞, the point at infinity as identity element.

Basic Elliptic curve operations:-

1. **Addition Operation**: For given two points $P(x_1,y_1)$ and $Q(x_2,y_2)$ on the elliptic curve, sum of P and Q is $R(x_3,y_3)$ which is the reflection of the point of intersection of the line through the points P & Q and the elliptic curve about x axis. The same rule applies to two points P and – P, with the same x-coordinate, where points are joined by a vertical line considered as the intersecting point on the curve at the point infinity. $P + (-P) = \infty$, the identity element which is the point at infinity.
   For $P \neq Q$, $P + Q = R(x_3,y_3)$ [1,2] where

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \text{ and}$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

2. **Doubling the point on the elliptic curve:-** Given the point P (x_1,y_1) on the elliptic curve 2 P is the reflection of the point of intersection of the tangent line at P and the elliptic curve about x axis [1,2].
   For $P \neq -P$, 2P is given by

(x_3, y_3) where $x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$ and $y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$ E xample of addition of two points and doubling of a point are shown in the following figures 1 and figure 2 for the elliptic curve $\mathbf{y^2 = x^3 - x}$.

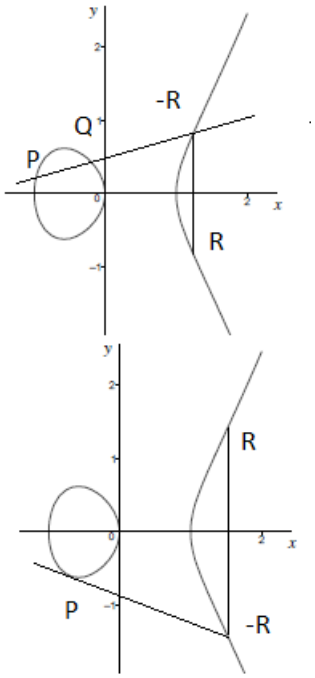


Figure 1: Geometric addition
Figure 2: Geometric doubling

Identity:- $\mathrm{P} + \infty = \infty + \mathrm{P} = \mathrm{P}$ for all E where ∞ is the point at infinity [1,2].

Negatives: - If P(x,y) is a point on the elliptic curve then (x,y) + (x,-y) = ∞, where $(x, -y)$ is the negative of P denoted by – P [1,2].

Point Multiplication:- Let P be any point on the elliptic curve over finite field of integers. Then the operation multiplication of P is defined as repeated addition [5,6].

kP = P + P +……..k times.

Elliptic Curve Discrete logarithmic Problem (ECDLP):- The strength of Elliptic Curve Cryptography depends on the hard problem known as Elliptic Curve Discrete Logarithmic Problem [3,4,5]. For two points P & Q on the elliptic curve over the finite field and Q = xP it is relatively easy to calculate Q for given x and P but hard to determine x.

Related Work: Several authors explored and came up with many encryption techniques in the history of ECC. Several authors explored and came up with many text based encryption techniques in the history of ECC. J. Muthukuru, B. Sathyanarayana [6] designed fixed and variable size text encryptions using ECC with some initial vectors. Keerthi K.B. Surendiran [7] proposed elliptic curve cryptography for secured text encryption. In that chapter the authors mapped the message to equivalent ASCII Hex values and the hex values are grouped together to form x and y coordinates. Ansah Jeelani Zargar et.al. [8] suggested encryption/decryption technique using ECC . Kamlesh Gupta Et.al. [9] used ECC for images encryption where each pixel of the original image is transformed to affine point on elliptic curve and converted to cipher image pixels. Zhongjian Zhao1 and Xiaoqiang Zhang [10] developed and demonstrated ECC-based image encryption using code computing. Omar Reyad [11] designed text message encoding based on elliptic curve cryptography and a mapping methodology. SM Celestin and K. Muneeswaran [12] suggested the text encryption using ECC. In that paper they designed a new technique of encryption by mapping the corresponding ASCII values of the message to affine points on the elliptic curve and adding each message point to ASCII value times the generator. Balamurugan Et.al. [9] proposed a fast mapping technique by mapping the message characters to affine points on elliptic curve and encrypting each character using ElGamal encryption with extra parameter a non-singular matrix.

III. PROPOSED METHOD:

Suppose two legitimate users want to converse with each other they select an elliptic curve the users agree upon to use an elliptic curve E_q (a,b) having large order say n. In selecting the elliptic curve they take precautionary measures to protect the cipher from all types of frequent physical attacks on ECC like side channel attacks and fault analysis. To escape from the physical attacks ECC friendly curves are chosen basing on the desired features.

(i). To resist against Pollig-Hellman attack the order of the selected curve # E_q(a,b) should not be factorized into small primes
(ii). The chosen elliptic curve should be non super singular
(iii). Should be non-anomalous. i.e., the
order # E_q(a,b) $\neq$ q.

In addition the users select the curve having prime order because if the order is prime, set of all points on the selected curve forms a cyclic group and every point is generator of the cyclic group. They also select a point C which acts as the generator of the cyclic group. A common look up code table is constructed by them assigning all the 256 ASCII characters to affine points on the curve randomly called ASCII coded Elliptic Curve table (ASCII coded EC table). They publish the selected elliptic curve E_q(a,b) , the generator C and ASCII coded EC table. Plain text is encrypted at two different stages: first stage is using ECC and the second stage is applying the logical XOR operation on each character of the first stage outcome.

I. Stage Encryption using elliptic curve over finite field :
If Alice and Bob want to communicate with each other Alice chooses a big random number α less than the order of the curve and calculates

A1 = α (C+A) and A2 = αA
She keeps α as the secret key with her and publishes A_1,A_2.
In the same way Bob selects a big random number β and calculates
B1= β(C+B) and B2= βB.

He keeps β as the secret key with him and publishes B1, B2. Again Alice calculates $A_B = \alpha B1$ and communicates to Bob as specific public key to Bob.
Bob calculates $B_A = \beta A1$ and communicates to Alice as her specific public key.

Encryption : If Bob wants to transmit the message 'M' with characters M1,M2,M3…..Mk to Alice then all the characters are coded to affine points P1,P2,P3……Pkusing common look up table. Each point Pi is encrypted to two affine points Ei1, Ei2 where i takes the values 1 through k. For encrypting the first point P_1 Bob selects a big random number $\Upsilon 1 < n$ and encrypts P1 to

$E11 = \beta\Upsilon 1A1$ and $E12 = P1 + \Upsilon 1B_A$

For encrypting the second point Bob selects a $\Upsilon 2$ and encrypts as

$E21 = \beta\ \Upsilon 2\ A1$ and $E22 = P2 + \Upsilon 2B_A$. Ingeneral we define

$Ei1 = \beta\ \Upsilon i\ A1$ and $Ei2 = Pi + \Upsilon iB_A$i takes the values 1 to k.

II. Stage encryption using logical XOR operation :

Step 1:

The co-ordinates of all the elliptic curve affine points E11 E12; E21E22 ……; Ei1 Ei2, i = 1 to k which are decimal numbers obtained at the first stage encryption are arranged successively as the elements of square matrices of order ω less thank. The order of the matrix ω is confidential between the users. If the decimal numbers are less than ω^2 then the remaining elements are filled randomly to complete the matrix. All the elements are reduced to mod 256 and converted to ASCII equivalent 8 bit binary numbers.

Step 2 :

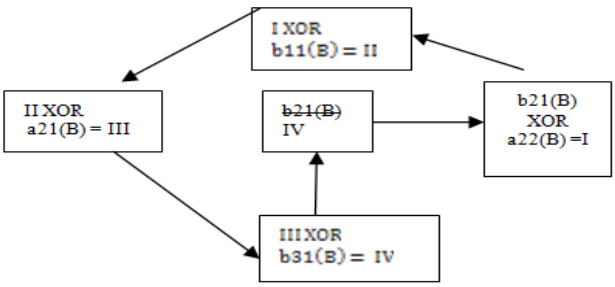
Logical XOR operation is applied on each 8 bit binary number starting from the first element with all the four surrounding elements consecutively in the anticlockwise direction and the resulting number is entered in its original position.

For instance if the first stage affine points are E11E12; E21E22; E31E32 ; E41 E42with coordinates (x11,y11) (x12,y12) ; (x21,y21) (x22,y22) ; (x31,y31) (x32,y32) ; (x41,y41) (x42,y42) the numbers are successively written as elements of 4x4 matrix and reduced to mod 256. The matrix when reduced to mod 256 divides into two parts the integer part I and residue part R. For instance if the decimal number 1,116 is reduced to mod 256 then the integer part is and residue part is 92.

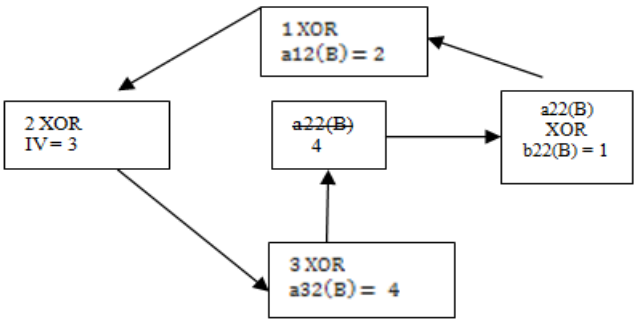
$$I = \begin{bmatrix} Ia11 & Ib11 & Ia12 & Ib12 \\ Ia21 & Ib21 & Ia22 & Ib22 \\ Ia31 & Ib31 & Ia32 & Ib32 \\ Ia41 & Ib41 & Ia42 & Ib42 \end{bmatrix}$$

$$R = \begin{bmatrix} a11 & b11 & a12 & b12 \\ a21 & b21 & a22 & b22 \\ a31 & b31 & a32 & b32 \\ a41 & b41 & a42 & b42 \end{bmatrix}$$

The elements of the matrix R are written as ASCII equivalent binary 8 bit binary numbers. Logical XOR operation is applied on each element starting from the first element. Consider the element y21(B), it is XORed as b21(B) XOR a22(B) XOR b11(B) XOR a21(B) XOR b31(B) and the result is placed in b21(B) position.



a22(B) is XORed and the result is placed in a22(B) position as



The resulting binary numbers are coded to equivalent ASCII characters is the cipher text C and the integer matrix I are transmitted to the receiver. Bob signs the cipher before transmitting to the receiver. The digital signature is computed using his secret key and one way cryptographic hash function.

Elliptic Curve Digital Signature Algorithm (ECDSA):

For computing the digital signature Alice and Bob agree upon to use elliptic curve domain parameters and a random function f(x,y) of coordinates of the elliptic curve affine points. The signature scheme involves the following steps.

1. Alice computes the function fG = f(xG,yG) = δ where G (xG,yG) is the generator of the cyclic group agreed upon by the users
2. A = (xA,yA) is Alice's secret which is a point on the elliptic curve. She computes fA = f(xA,yA) = ϵ
3. Alice calculates K1 = δ^{ϵ} mod q and sends to Bob
4. B = (xB,yB) is Bob's secret, a point on the elliptic curve. He computes fB = f(xB,yB) = ρ
5. Bob calculates K2 = $K1^{\rho}$modq and sends to Alice
6. Both calculate K =$K2^{\epsilon}$=$K1^{\rho}$ = $\delta^{\epsilon\rho}$
7. Bob combines the cipher text to be transmitted with the above calculated K value and finds the hash value using available one-way cryptographic functions. The hash value is communicated to the receiver along with the cipher text.

Decryption:-

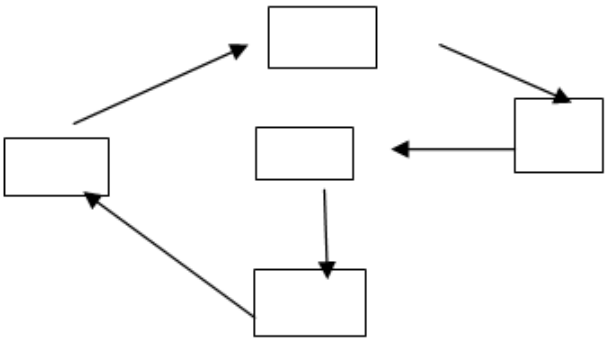
Digital Signature verification:

Alice after receiving the cipher text protected with the digital signature first verifies the signature by computing the hash value of the cipher combined with the key K and confirms the Bob's message. Then she starts decrypting the message as follows

I Stage decryption using logical XOR operation:

Step 1

Alice writes ASCII equivalent 8 bit binary numbers for the received cipher text and arranges as square matrices of order ω. Logical XOR operation is applied on each element of the matrix with all the surrounding elements in clock wise direction starting from the last element and the resulting element is placed in its original position.



Step 2 : All the 8 bit binary numbers are written as ASCII equivalent decimal numbers to obtain the matrix R. Then the coordinates of elliptic curve affine points are obtained by multiplying the integer matrix I with 256 and adding the corresponding elements of the matrix R.

x11= Ia11 * 256 + a11

The resulting decimal numbers are successively written as (x11,y11) (x12,y12) ; (x21,y21) (x22,y22) ; (x31,y31) (x32,y32) ; (x41,y41) (x42,y42)……(xi1,yi1) (xi2,yi2) to get the points E11 E12 ; E21E22 ……;Ei1 Ei2, i = 1 to k.

II. Stage Decryption :

Each point Pi, i = 1 to k is decrypted as

Pi = Ei2 – Ei1.

Decryption works out properly

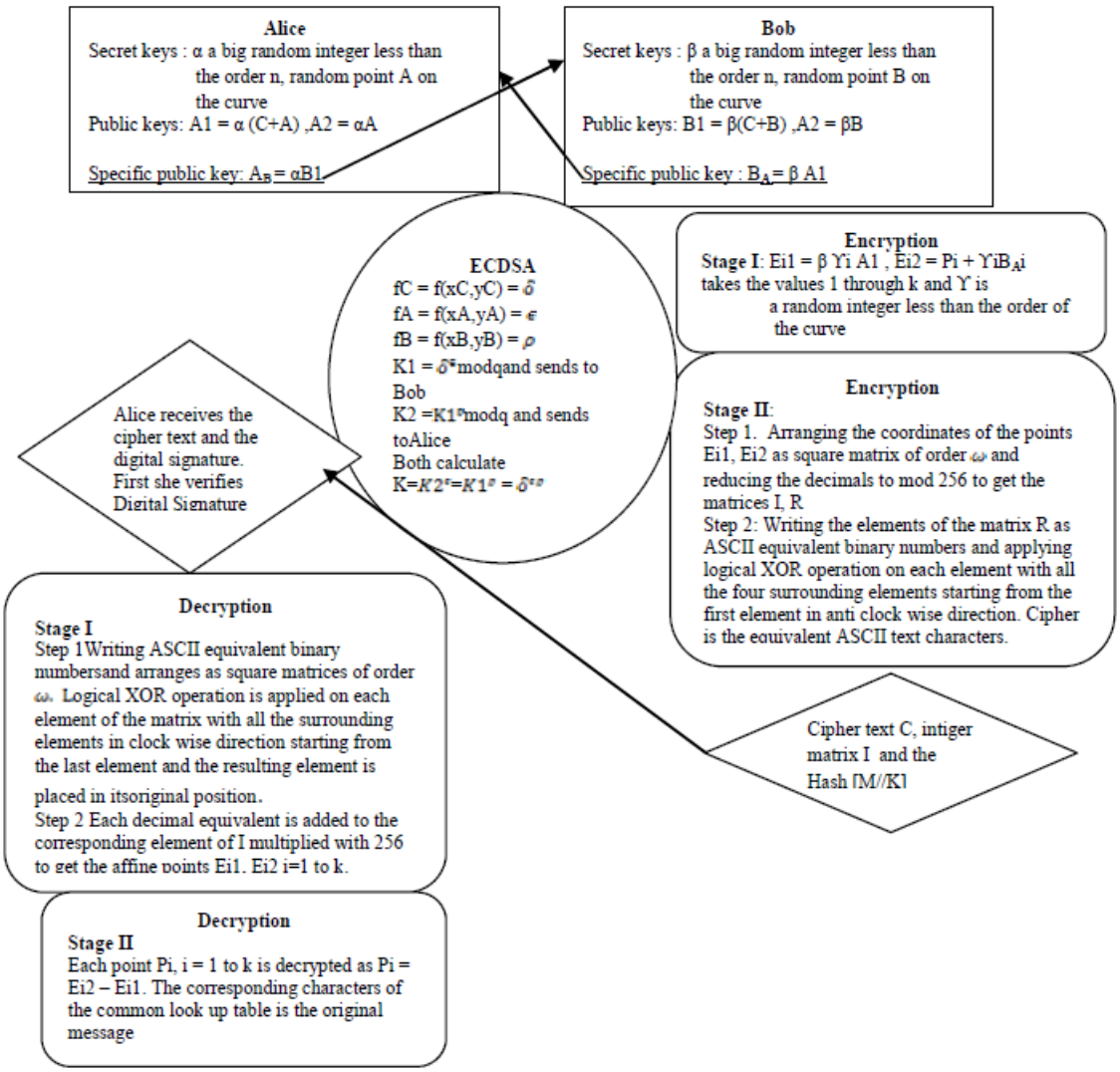
Pi = Ei2 -Ei1 = Pi + ϒiB_A - Ei1

= Pi + ϒi (β A1) - β ϒi A1

= Pi

Corresponding text characters M1, M2,……Mi i = 1 to k from the common look up table is the original message.

Working Procedure:



IV. IMPLEMENTATION:

An elliptic curve $y^2 = x^3 + 3x + 27 \ (mod\ 331)$ with all the desired properties with order n = 317 points is public. If two legitimate users Alice and Bob want to transmit message they agree upon a generator G (301,108), a function f (x,y) = $x^2y^2 + xy + x + y$ to generate the digital signature and a common look up ASCII coded EC table by assigning any 256 points to ASCII characters randomly.

Alice select α=257<n & A=(273,299) from the Elliptic curve points and finds the points as

A1=α(C+A)=(61,159) , A2=αA=(79,171) and

Alice keeps α, A as her secret keys and publishes A1, A2.

Similarly Bob selects select β=163<n and B=(17,41) and finds

B1=β (C+B)=(257,52) , B2=307,73). He keeps β ,B as his secret keys and publishes B1,B2.

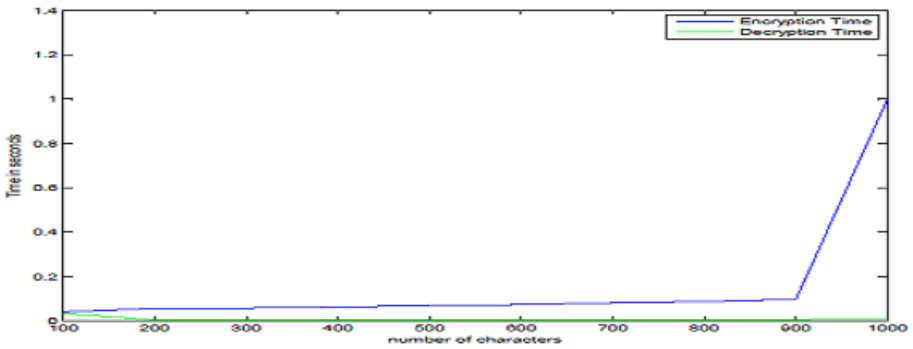
Again Alice finds A_B=αB_1= (266,54) and communicates to Bob as specific public key for Bob only. Bob finds B_A=βA_1= (53,171) and sends to Alice as the specific public key for Alice only.

If Bob wants to transmits the message “GOOD” he encrypts the message at two stages as described above to get the cipher C = “PUSOH†ÊâGP**VT**b**é**DPš1¿”. Bob finds the digital signature by padding the cipher with the generated key K as 505d9155926fbb1e43ab58c2eaee92e0 (Hash MD 5). Bob transmits the cipher text, integer matrix I and the digital signature to Alice via public channel. Alice first verifies the signature and decrypts the message “GOOD” as the above mentioned procedure

Implementation Results and Discussion: The encryption and decryption times for different size messages are recorded on a machine with 1GB RAM and 1.6 GHz processor speed on Win XP platform using MATLAB7

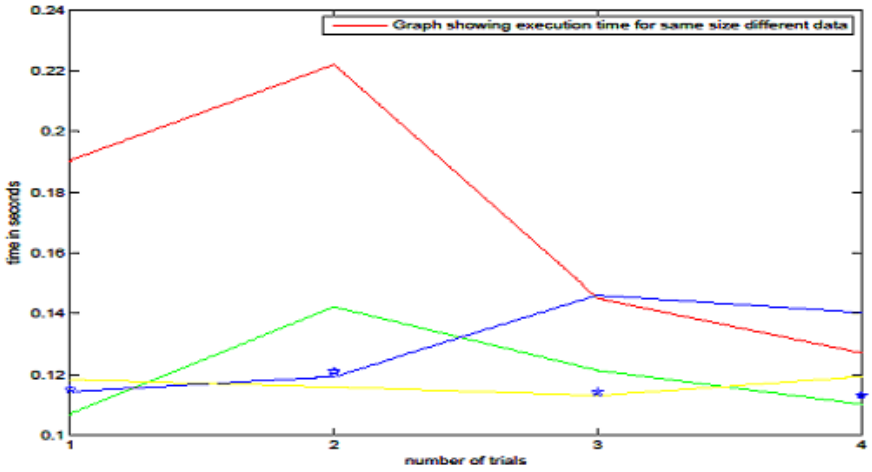
No. of Characters	Encryption Time(Seconds)	Decryption Time(Seconds)
100	0.0409	0.0343
200	0.0554	0.00349
300	0.0572	0.00367
400	0.0623	0.00382
500	0.0692	0.0041
600	0.0735	0.00421
700	0.0812	0.00478
800	0.0869	0.00511
900	0.0967	0.00565
1000	1.0013	0.00621

Graphs showing encryption, decryption times are



In cryptography timing attack is a side channel attack where the adversary breaks the cipher by observing the response time for various messages. Here the execution time for various different messages with same size is calculated for many trials. It is found that the execution time is different for different same size messages. The following table and graph show different execution time for different same size messages. This assures that the side channel attacks are impossible to implement for this algorithm.

No. of trials	Execution time for 100 'A' characters	Execution time for 100 'B' characters	Execution time for 100 'C' characters	Execution time for 100 'D' characters	Execution time for 100 'E' characters
Trial 1	0.1904	0.1069	0.1143	0.1182	0.115
Trial 2	0.2219	0.1421	0.1192	0.1158	0.1209
Trial3	0.145	0.1212	0.146	0.113	0.1142
Trial 4	0.1271	0.1101	0.1403	0.1192	0.1131



V. CONCLUSIONS:

In this paper the authors proposed a creative cascade encryption scheme using ECC at the first stage and XOR encryption at the second stage. One of the attractive features of ECC is it reduces the processing overhead with higher speed and lower power consumption which is based on the hardness of Elliptic Curve Discrete Logarithm Problem (ECDLP). One of the general attacks on ECC to break discrete logarithmic problem is Pollard Rho attack. But Pollard Rho attack is hard to implement here in this algorithm since γ value is variable for encrypting each character. Though an

adversary succeeds to implement the Pollard Rho attack and derives some information, the message is double fold encrypted at the second stage by XOR. XOR encryption is a simple method but difficult to break by brute force method. The XOR encryption in the proposed manner supports the security of the cipher by providing a remarkable avalanche affect. Here each element is undergone XOR encryption 4 times by concatenating the present and preceding 8 bit binary element. In addition the main issue of authenticity, as well as integrity is done by a digital signature technique. The parameters δ, ϵ and ρ used to generate the digital signature are the function values of the generator point G, A and B where the function is confidential between the users. The present text based algorithm using ECC and logical operation is suitable for transmitting both short and long messages securely.

REFERENCES:

1. Koblitz N., "Elliptic curve cryptosystems, mathematics of computation", Vol. 48, No.177, pp. 203-209, January 1987.
2. Miller V., "Uses of elliptic curves in cryptography". In advances in Cryptography (CRYPTO 1985), Springer LNCS, 1985, vol. 218, pp 417-4, 26.
3. Maurer U., A. Menzes and E. Teske, "Analysis of GHS weil decent attack on the ECDLP over characteristic two fields of composite degree". LMS journal of computation and Mathematics, 5:127-174, 2002.
4. Arron Blumenfeld, "Discrete logarithms on Elliptic curves", 2011.
5. Menzes A., and Vanstone S. "Hand book of applied cryptography", The CRC-Pressseries of Discrete Mathematics and its Applications CRC-Press,1997.
6. J. Muthukuru, B. Sathyanarayana, "Fixed and Variable Size Text Based Message Mapping Techniques using ECC", Global journal of computer science and technology, Volume 12 Issue 3 Version 1.0 February 2012 vol. 12, no. 3, 2012.
7. K. Keerthi, Surendiran B Elliptic curve cryptography for secured text encryption https://www.researchgate.net/publication/320662889.
8. Ansah JeelaniZargar, Mehreen Manzoor, Taha Mukhtar, ENCRYPTION/DECRYPTION USING ELLIPTICAL CURVE CRYPTOGRAPHY, Volume 8, No. 7, July – August 2017 International Journal of Advanced Research in Computer Science.
9. Kamlesh Gupta1 , Sanjay Silakari2 , Ranu Gupta3 , Suhel A. Khan4, An Ethical way for Image Encryption using ECC, 978-0-7695-3743-6/09 $25.00 © 2009 IEEE DOI 10.1109/CICSYN.2009.33.
10. Zhongjian Zhao1 and Xiaoqiang Zhang2, ECC-Based Image Encryption Using Code Computing Proceedings of the 2012 International Conference on Communication, Electronics and Automation Engineering pp 859-865.
11. Omar Reyad, Text Message Encoding Based on Elliptic Curve Cryptography and a Mapping Methodology, Information Sciences Letters An International Journal http://dx.doi.org/10.12785/isl/070102.
12. S. Maria Celestin Vigila & K. Muneeswaran, "Implementation of text based cryptosystem using elliptic curve cryptography", International conference on advanced computing, IEEE pp 82-85 December 2009.

AUTHORS PROFILE

Dr. Ch. Suneetha, is Associate Professor in Department of Mathematics, GIS, GITAM Deemed to be University, Visakhapatnam, India. She got 20 years of teaching and 13 years of research experience. She has been working in the area of Cryptography for the last 12 years and published 25 research papers in different reputed journals including Scopus and IEEE index. One scholar was awarded Ph.D. degree and one scholar is pursuing her Ph.D. under her guidance. Her research area of interest includes Number theory and Applied Cryptography.

Dr. T. Surendra, M.Sc., M.Phil., Ph.D. has been into teaching profession for the past 17 years. He is presently working for GITAM Deemed to be University as Assistant Professor in the Department of Mathematics. He obtained M.Sc. and M.Phil. from Andhra University. He did Ph.D. in the area Number Theory and Cryptography from Andhra University.He has published various research papers including Scopus. He qualified SET (State Eligibility Test). He is recipient of best library user award for the year 2018 in GITAM. He is vice president for CRPF (Child Right Protection Forum-State level) Visakhapatnam urban Committee.

Ch.Neelima, M.Sc. has been into teaching profession for the past 15years in engineering colleges. She is presently working for Sanketika Vidya parishad as Assistant professor in the department of Basic science. She is pursuing her Ph.D. under the guidance of Dr. Ch. Suneethe in GITAM Deemed to be University, Visakhapatnam.