Design Engineering

ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5570 - 5581

Elliptic Curve Cryptography with Reduced Cipher Bandwidth-A New Approach to Conventional ECC

1.D. Sravana Kumar, 2. CH. Neelima, 3. CH. Suneetha

4.K. Uma Karuna Devi,5.G. Lalitha Devi

1.Professor, Department of Physics, Dr. VSK Government Degree College, Visakhapatnam, India
skdharanikota@gmail.com
2. Assistant Professor in Mathematics, BITS Engineering College, Visakhapatnam, India
neeluchapparapu@gmail.com
3. Associate Professor, Dept. of Mathematics GITAM University, Visakhapatnam, India
schivuku@gitam.edu
4. Assistant Professor in Mathematics, Sir CR Reddy Engineering College, Eluru, India
umasai.kakarla@gmail.com
5.Assistant Professor in Mathematics, PRISM Degree & PG College, Visakhapatnam, India
lalithasana07@gmail.com

Abstract:

Public key Cryptosystem (PKC) is ever expanding in the history of cryptography. Traditional Public Key Infrastructure (PKI) certificates assure the authenticity in the form of digital signature. Elliptic curve cryptography is an incredible and complex public key cryptosystem having wide range of practical applications in wireless environments like smartcards, tokens, and mobile phones. The attractive feature of ECC is it offers equivalent level of security as RSA/DSA with much smaller keys. This is the reason that ECC has several applications in wireless constrained environments especially in Secure Sockets Layer (SSL) handshakes to establish SSL connection. For implementing the text encryption in ECC one plaintext point on the elliptic curve is encrypted as two cipher text points. So, the main drawbacks of ECC is that it increases the size of the cipher significantly more than RSA encryption. This paper aims at presenting innovative elliptic curve cryptosystem that reduces the cipher size equivalent to that of the plaintext which reduces the communication risk, storage space and power consumption.

Keywords *Elliptic Curve Cryptography, Encryption, Decryption*

ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5570 - 5581

I. INTRODUCTION

Diffie Hellman Key Exchange Algorithm is an attractive protocol for beginning an encrypted conversation between two unfamiliar parties that relies on exponentiation of large groups. It greatly enhances the security of the internet and is proposed as internet standard. But the algorithm is suffered with security implication as man-in-middle attack. Later, several authors published modifications to Diffie Hellman Key Exchange algorithm. On the other hand RSA is a public key cryptosystem which obtains its security from the difficulty of factorizing large integers into their prime. Though the public key operations are faster in RSA the strength of the algorithm will not be increased even if the key size is doubled. An alternative of RSA algorithm to achieve the same security certificate with considerably shorter key length is elliptic curve cryptography came to light in 1985 by Victor and Miller. Elliptic curve cryptography depends of the hardness of Elliptic Curve Discrete Logarithm Problem (ECDLP). Since there are no exponential operations in ECDLP limited processing power, finite storage space with little band width is required for ECC. The hardness of ECDLP makes ECC less vulnerable compared with other classical cryptographic algorithms So, ECC is especially viable for limited applications such as smart cards, cellular phones, and wireless communication devices. Same elliptic curve may be used by many people with distinct key pairs. Despite these advantages ECC algorithm encrypts a point on the elliptic curve to a pair of cipher points. There is a small disadvantage that the encrypted message is twice than that of the unencrypted message. This leads to network congestion and communication risk. The present paper aims at reduction of the size of the cipher besides providing the security.

II. LITERATURE SURVEY

Several researchers in literature studied the benefits of ECC over conventional cryptosystems and deployed elliptic curves over finite fields for security applications. Many authors proposed text-based encryption algorithms using ECC. Benjamin Sebastina, UgarAlpayCenar (7) studied and compared significant advantages of ECC over RSA in SSL and TLS certificates. L. Dolendro and K Manglem(8) implemented text encryption using elliptic curve cryptography . In this chapter authors proposed a classical technique of mapping the characters to affine points in the curve by pairing the ASCII values of the plain text characters. Renee Brady et.al. (9) proposed encryption scheme with elliptic curve cryptography. In that paper they discussed the limitations of communicating text messages through the sites like twitter and used Unicode to encode the text message as a number, Koblitz method to encode the text as a point on elliptic curve. A. Shamir (10) was the first to propose Identity-based cryptosystem to overcome the authenticity issues in a different way to traditional public key infrastructure. Aziz and Diffie [11] also proposed an authentication protocol with requirement of pre-communication. S. Thiraviya and S. Britto (12) proposed enhanced elliptic curve cryptography for online social network users. In that paper they implemented encryption, decryption time analysis, plain text, cipher text size

ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5570 - 5581

analysis. KolhekarM, Jadhav A (13) proposed encryption and decryption using elliptic curves. F. Amounas and E.H. EI Kinani [14] suggested the use of a nonsingular matrix to map same characters in the message to different points on the curve. T.N. Shankar and G. Sahoo (15) showed the use of a two-dimensional alphabetic table to convert plaintext characters to two-dimensional coordinate representation. These points are then added with elliptic curve points for encryption. K. Agrawal and A. Gera [16] designed message encryption using Hill cipher algorithm where the ASCII value of cipher characters are used to find points on the elliptic curve. All these algorithms explain only the encryption methods, but they have not encountered the variation issue of the cipher size. The present text-based encryption algorithm protects the cipher from all types of attacks as well as considers the fixation of the cipher size to that of the original text.

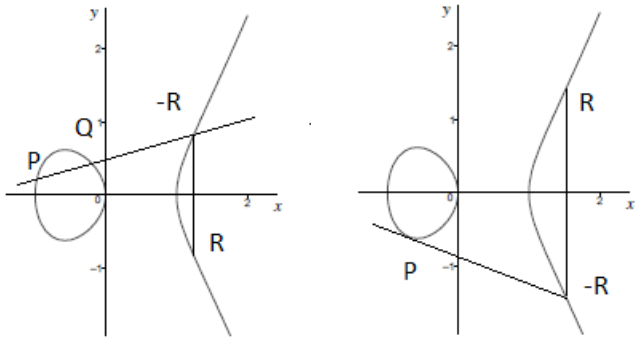
III. ELLIPTIC CURVE ARITHMETIC

An affine equation E: $y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6$ over the set of real numbers is said to be Weierstrass equation, where b_1, b_2, b_3 ,b_4, b_6 and x, y are real numbers. An elliptic curve for cryptographic purpose is defined by the equation $y^2 = x^3 + ax + b$,
$4a^3+27b^2 \neq 0$over the finite field F_q.

Group laws of elliptic curve: - For the elliptic curve ε defined over the finite field of integers F. Addition of two points uses chord-and-tangent rule to get the third point [1,2,3]. 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.

Geometric rules of Addition: - Let $P(\dot{x}_1,\dot{y}_1)$ and $Q(\dot{x}_2,\dot{y}_2)$ be two points on the elliptic curve E. The sum of the two points P and Q is $R(\dot{x}_3,\dot{y}_3)$ 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 geometric interpretation also applies to two points P and – P, with the same x-coordinate. Here the points are joined by a vertical line, which is considered as the intersecting point on the curve at the point infinity. $P + (-P) = \infty$, the identity element which is the point at infinity [1,2,3].

Doubling the point on the elliptic curve: -If $P(\dot{x}_1,\dot{y}_1)$ is point on the elliptic curve then 2P is the reflection of the point of intersection of the tangent line at P and the elliptic curve about x axis [1,2,3].Example of addition of two points and doubling of a point are shown in the following figures 1 and figure 2 for the elliptic curve $\mathbf{y^2 = x^3-x}$.



Design Engineering

ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5570 - 5581

Figure 1. Geometric addition **Figure 2. Geometric doubling**

Identity: - $P + \infty = \infty + P = P$ for all E where ∞ is the point at infinity [1,2,3].

Negatives: - If $P(\dot{x}_1,\dot{y}_1)$ is a point on the elliptic curve then$(\dot{x},y) + (\dot{x},-y) = \infty$. Where $(\dot{x},-\dot{y})$is the negative of P denoted by $-P$ [1,2,3].

Point addition: - If $P(\dot{x}_1,\dot{y}_1)$, $Q(\dot{x}_2,\dot{y}_2)$ are two points where $P \neq Q$. Then $P + Q = (\dot{x}_3, \dot{y}_3)$ [1,2]where $\dot{x}_3 = [(\dot{y}_2 - \dot{y}_1)/(\dot{x}_2 - \dot{x}_1)]^2 - \dot{x}_1 - \dot{x}_2$ and $\dot{y}_3 = [(\dot{y}_2 - \dot{y}_1)/(\dot{x}_2 - \dot{x}_1)](\dot{x}_1 - \dot{x}_3) - \dot{y}_1$

Point Doubling: - Let $P(\dot{x}_1,\dot{y}_1) \in E(F_q)$ where $P \neq -P$ then

$2P = (x_3, y_3)$ [1,2]where $x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$ and $y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$

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 [1,2,3].

kP = P+P+…….ktimes.

Elliptic Curve Discrete Logarithmic Problem (ECDLP): - The strength of Elliptic Curve Cryptography depends on the hard problem known as Elliptic Curve Discrete Logarithmic Problem [4,5,6]. Consider an equation Q = xP where Q, $P \in E_q$ (a,b)the elliptic curve over the finite field and $x \in [1,2,\ldots\ldots q-1]$. It is relatively easy to calculate Q for given x and P. But it is relatively hard to determine $x = \log_P Q$ given.

IV. PROPOSED METHOD

In the present paper the authors designed a new technique to encrypt the message and to reduce the size of the cipher text to that of the plain text so that the computational strain, communication risk, storage space, processing power consumption can be considerably reduced. Suppose two legitimate users want to converse with each other they select a secure elliptic curve $E_q(a,b)$ over finite field with as many points as possible on it and publish. A secure elliptic curve is a curve that protects main physical attacks like side channel analysis and fault analysis. Some of the good features of an elliptic curve for encryption purpose to avoid the risk of attacks are

1. The order of the curve # $E_q(a,b)$ should not be factorizes into small primes to defend against Pollig-Hellman attack
2. The curve should be non-super singular curve
3. It should be non-anomalous curve. i.e., the order # $E_q(a,b) \neq q$.

They also publish an EC coded ASCII table by mapping the ASCII characters to random affine points on the curve and a random function f(x,y)

Alice selects a random point A, a big random number α less than the order n of the curve and calculates

$$A1 = \left[\frac{A}{\alpha} + \alpha^2 A\right] mod q \quad A2 = [\alpha A] mod q$$

Design Engineering

ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5570 - 5581

She keeps α, A as her secret keys and publishes A1, A2 as her general public keys.

In the same way Bob selects a large random number β, a point B on the elliptic curve and computes $B1 = \left[\frac{B}{\beta} + \beta^2 B\right] modq$, $B2 = [\beta B] modq$. He publishes B1, B2as his general public keys and keeps β,B as his secret keys.

Again Alice computes $AB = [\alpha B2] modq$ and publishes as a specific public key for Bob to converse with him. Similarly Bob computes $BA = [\beta A2] modq$ and publishes as a specific public key for Alice to converse with her.

Encryption: If Bob wants to transmit the message M consisting of characters

M1,M2,M3……Mn

1. First he converts the characters to affine elliptic curve points from the common look up EC coded ASCII table. P1,P2,P3…….Pn.
2. He selects a random point P0 with coordinates (x0,y0) on the curve and generates an integer r = $[f(x0,y0)]_{modq}$using the published random function f(x,y).
3. He encrypts the point P0 as $C0 = [P0 + \beta A1] modq$
4. Each point P1,P2….. Pn is encrypted as $Ci = r^i [Pi + \beta A1] modq$ i= 1,2,3……..n
5. He writes the corresponding text characters and communicates the cipher text C to Alice in a public channel

Decryption: Alice first decrypts Co as $P0 = \left\{C0 - \left[\frac{1}{\alpha^2} + \alpha\right] BA\right\} modq$

Then Alice decrypts the cipher text as

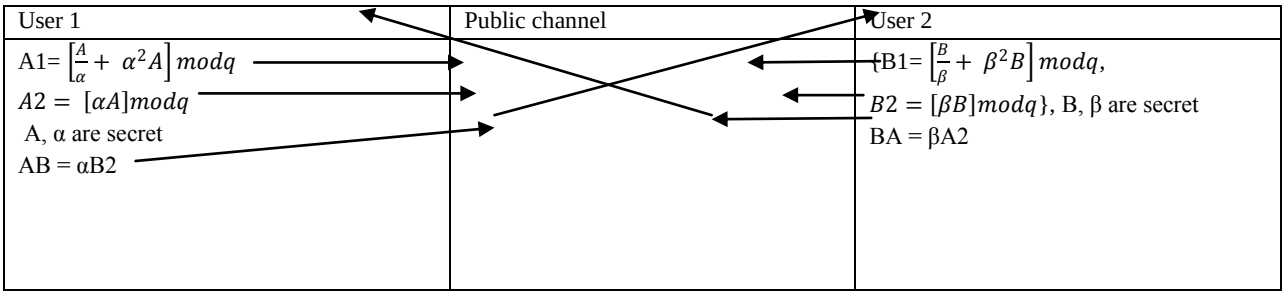
$Pi = \left\{\frac{Ci}{r^i} - \left[\frac{1}{\alpha^2} + \alpha\right] BA\right\} modq$ i=1,2…..n

Decryption works out properly:

$$Pi = \frac{Ci}{r^i} - \left[\frac{1}{\alpha^2} + \alpha\right] BA = Ci = \frac{r^i}{r^i}[Pi + \beta A1] - \left[\frac{1}{\alpha^2} + \alpha\right] BA$$

$$= \left[Pi + \beta\left\{\frac{A}{\alpha} + \alpha^2 A\right\}\right] - \left[\frac{1}{\alpha^2} + \alpha\right] \beta\alpha A$$

$$= Pi + \frac{\beta}{\alpha} A + \beta\alpha^2 A - \frac{\beta}{\alpha} A - \beta\alpha^2 A = Pi$$



ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5570 - 5581

Encryption Algorithm

Input: Plain text with all types of characters

Output: Cipher text

Step1: Begin

Step2: i: Consider the message M1,M2,M3,…Mn

ii: Convert all the characters to affine points P1,P2,P3,…Pn on the curve using common look up table

Step3: Consider a random point P0(x0,y0) and calculate r = $[f(x0,y0)]_{modq}$

Step4: encrypt P0 as $C0 = [P0 + \beta A1]$

Step5: Each point P1,P2… is encrypted as $Ci = \{r^i[Pi + \beta A1]\}modq$ i= 1,2,3….n

Step6: convert the points to the characters from table

Step7: End

Reverse mapping Decryption Algorithm

Input: Cipher text with all types of characters

Output: Plain text

Step1: Begin

Step2: i: Consider the cipher characters C1,C2,C3,…

ii: Convert all the characters to affine points P1,P2,P3,… on the curve using common look up table

Step3: C0 is decrypted as $P0 = \left\{C0 - \left[\frac{1}{\alpha^2} + \alpha\right] BA\right\}modq$

Step4: Compute r = $[f(x0,y0)]_{modq}$ using the first point P0(x0,y0)

Step4: Each point P1,P2… is decrypted as $Pi = \left\{\frac{Ci}{r^i} - \left[\frac{1}{\alpha^2} + \alpha\right] BA\right\}modq$ i=1,2…..n

Step5: convert the points to the characters from table

Step6: End

V. IMPLEMENTATION OF ALGORITHM

Two users Alice and Bob select an elliptic curve $y^2 = x^3 + 3x + 27$ mod 331 with prime order is 317 possessing all the above-mentioned desired features. The curve, an EC coded ASCII table by mapping the 256 ASCII characters to first 256 affine points on the curve and a random function $f(x,y) = [x^2y^2 + xy + x + y]mod\ 331$ are public.

Alice	Bob
$\alpha = 17$, A = (296,210)	$\beta = 19$,B = (231,3)
A1 = (8,296) A2 = (61,159)	B1 = (43,47) B2 = (88,123)
AB = (127,35)	BA = (9,320)

If Bob wants to send the message "SSSS" to Alice, the EC affine point corresponding to the character 'S' from the look up table is (39,144). He selects a random point P0 = (36,38) and generates 'r' value as 68.

He encrypts the plain text as cipher points C1,C2,C3,C4

ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5570 - 5581

Message	Cipher
(39,144), (39,144), (39,144), (39,144)	(320,283)(248,60),(184,330)(257,52),(212,306)

VI. IMPLEMENTATION RESULTS AND PERFORMANCE ANALYSIS

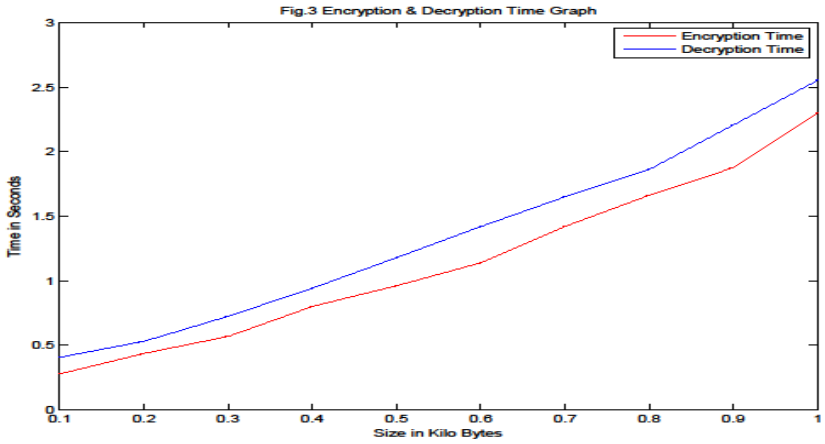
The encryption and decryption times for different size messages are recorded on a machine with 1GB RAM and 1.6 GHz processor speed on Win XP platform using MATLAB14. The following table gives encryption and decryption times in seconds for different size data. The time required for encryption and decryption for different size data are calculated and tabulated as follows

Table 1

Size of the message (in kilo ytes)	Encryption time (in seconds)	Decryption time (in seconds)
0.1	0.2774	0.4064
0.2	0.4372	0.5313
0.3	0.5695	0.7256
0.4	0.8023	0.9439
0.5	0.9617	1.1807
0.6	1.1400	1.4205
0.7	1.4218	1.6523
0.8	1.6627	1.8646
0.9	1.8768	2.2093
1.0	2.2986	2.555

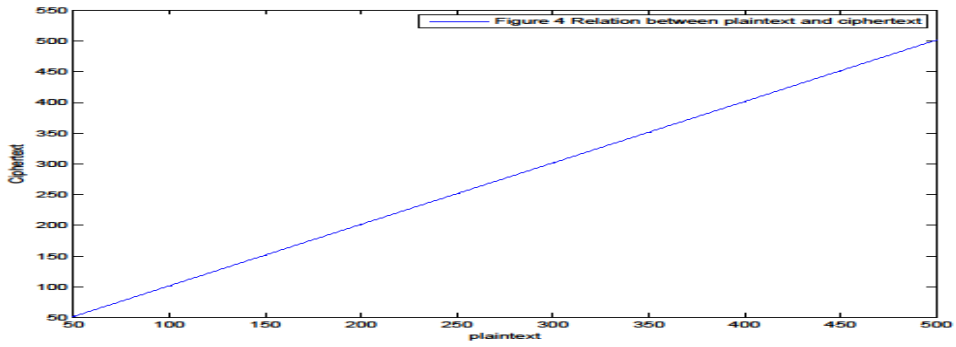
These values are plotted in the graph. The encryption and decryption time plots in figure 3 show that the execution time is very less when compared to other conventional cryptosystems. The time recorded for both encryption and decryption is below 3 seconds. So, the computational and communication risk will be considerably reduced to the required levels.

ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5570 - 5581



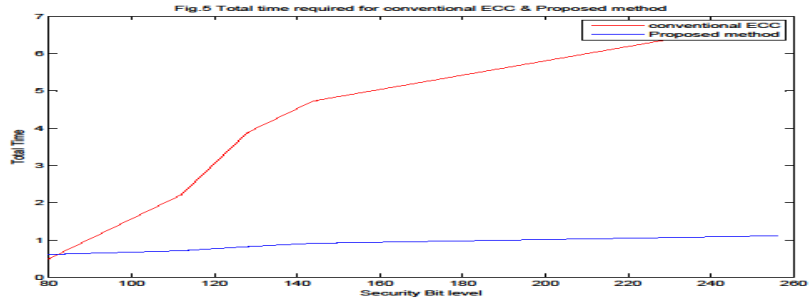
Since the cipher text size is fixed except one-point P0 or one-character C0 appended at the beginning of the cipher there is no network congestion in communication. The graph in figure 4 represents the relationship between plaintext and cipher text size. The graph is linear with negligible variation. So, the present technique is suitable for not only small, medium size messages but also for big data.

ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5570 - 5581



VII. COMPARITIVE STUDY OF CONVENTIONAL ECC AND PROPOSED METHOD

A comparative study on total execution time is implemented between conventional ECC and the present method. The graph in fig. 5 shows that the present algorithm is faster than the conventional algorithm.



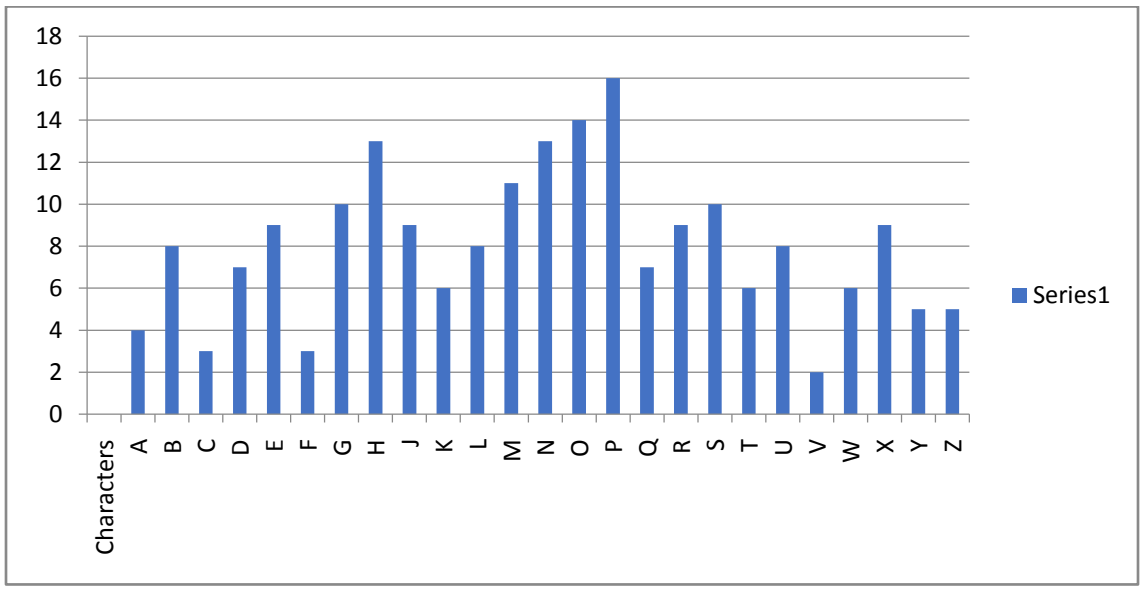
Design Engineering

ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5570 - 5581

VIII. SECURITY ANALYSIS

General attacks like chosen plain text attack and chosen cipher text attack are effective if there is a one-to-one correspondence between plain text and cipher text which leads to the frequency analysis. In the present algorithm each plain text character is encrypted using the value 'r' raised to the power of its position r^i , i = 1,2,3…. So, there is no chance of repetition of the cipher characters for small and medium size messages. In the example shown above all the same 'S' characters of the message are mapped to different points on the curve. To estimate the frequency of the characters a big message of size 1 kilobyte is encrypted using the present technique. Repetition of English alphabets is shown by the bar diagrams in figure 6. It is clear from the graph that the most frequently repeated English alphabets like A,E,S,T are negligible in number and all the other characters are numerals, special ASCII characters. So, the frequency analysis is impossible to execute here even for big data also.

Fig.6



The hardness of ECC depends on the strength of Elliptic Curve Discrete Logarithmic Problem (ECDLP). A well-known attack to solve ECDLP is pollard Rho attack. The process of applying the Pollard Rho attack to solve ECDLP does not arise here since each character is encrypted different r^i.

IX. ADVANTAGES OF PRESENT SCHEME OVER CONVENTIONAL ECC

In ECC a l bit key yields pair of points consisting of 4*l bits due to the two coordinates x and y. Each cipher character has bandwidth 4*l. Thus, the plain text coded to N points on the curve is encrypted as 2*N points with 4*l*N bit bandwidth which is significantly large. This results the transmission expensive and leads to network congestion. But in the present method the plain text

ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5570 - 5581

with N characters is encrypted as (N+1) affine points with bandwidth 2*l*(N+1) almost equal to the size of the plain text. Each character is encrypted to a random character as long as q<n. If n = q+1 and if P0 = P(q+1) they are coded to the same cipher point, since r is a number in the finite field less than q which is the generator of the cyclic group. In ECC generally q is very large so that large volumes of data can be transmitted by communicating parties. The case of n>q occurs rarely. In such a case it is recommended to change either the secret key or the function f(x,y) to calculate r value after communicating q characters.

X. CONCLUSIONS

The encryption technique proposed here offers same level of security as the conventional ECC protocol as it is highly difficult to calculate the secret keys of both the legitimate entities; α, A of Alice and β, B of Bob from the public keys A_1, A_2 and B_1, B_2, if the order of the elliptic curve is very large. Also, it reduces the size of the cipher text to that of the plain text. So, the ECC algorithm designed here is faster than previously proposed schemes. Another special feature of this algorithm is there is no pre sharing of the data before transmission. The curve, EC coded ASCII table and function are public. The keys A1, A2, AB;B1,B2,BA are communicated via public channel only. So, the present cipher is very useful for long messages because the cipher length is same as that of the plain text.

REFERENCES

[1] Koblitz N., "Elliptic curve cryptosystems, mathematics of computation", Vol. 48, No. 177, pp. 203-209, January 1987.v

[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. "Handbook of applied cryptography", The CRC-Pressseries of Discrete Mathematics and its Applications CRC-Press,1997.

[6] Miyaji , Nakabayashi and Takano "Elliptic curves with low embedding degree", Journal of Cryptology, 2006, Volume 19, Number 4, Pages 553-562.

[7] Benjamin Clement Sebastin , UgarAlpayCenar "Advantage of using elliptic curve Cryptography in SSL/TLA, https://koclab.cs.ucsb.edu/teaching/ecc/project/2015Projects/Cenar+Sebastian

[8] LaiphrakpamDolendro Singh and KhumanthemManglem Singh "Implementation of Text Encryption using Elliptic Curve Cryptography", Procedia Computer Science 54 (2015) 73-82, www. Sciencedirect.com.

ISSN: 0011-9342 | Year 2021
Issue: 6 | Pages: 5570 - 5581

[9] Rene'e Brady ,Naleceia David and Anna Tracy, "Encrypting with Elliptic Curve Cryptography, www.math.purdue.edu//Encrypting
[10] A. Shamir, "Identity- based cryptosystems and signature schemes", In Proc. CRYPTO 1984, LNCS Vol. 196, pp. 47-53, Springer 1984.
[11] A.Aziz& W. Diffie, "A secure communications protocol to prevent unauthorized access: privacy and authentication for wireless local area networks, IEEE personal communications, pages 25-31, first quarter 1994.
[12] S. Thiraviya Regina Rajam and S. Britto Ramesh Kumar, "Enhanced Elliptic curve Cryptography", Indian Journal of science and technology, Vol. 8 (26), Oct 2015.
[13] MeghaKohelekar, Anita Jadhav, "Implementation Of Elliptic Curve Cryptography On Text And Image", International Journal of Enterprise Computing and Business Systems , Vol. 1 Issue 2 July 2011
[14] F. Amounas and E.H. EI Kinani, Fast Mapping Method based on Matrix Approach for Elliptic Curve Cryptography, Int J of Information and Network Security 1, 54–59 (2012).
[15] T.N. Shankar and G. Sahoo, Cryptography with Elliptic Curves, Int J of Computer Science and Applications 2, 38– 42 (2009).
[16] K. Agrawal and A. Gera, Elliptic Curve Cryptography with Hill Cipher Generation for secure Text Cryptosystem. Int J of Computer Applications 106, 18–24 (2014).