

## ENCODING OF TEXT TO POINT IN ELLIPTIC CURVE CRYPTOGRAPHY USING CHINESE REMAINDER THEOREM

<sup>1</sup>Josepha Menandas J , <sup>2</sup>Mary Subaja Christo

1. Research Scholar, School of Computing, SRM Institute of Science and Technology, Kattangulathur, Chennai, India.
2. Associate Professor, School of Computing, SRM Institute of Science and Technology, Kattangulathur, Chennai, India, [marysubaja@gmail.com](mailto:marysubaja@gmail.com)

\*Corresponding Author: Mary Subaja Christo<sup>2</sup>

### 1. Abstract

One of the most crucial requirements in this digital age is data security. The number of data usage increased drastically now a days, but how far the data is secured is the very big problem, though we have enough cryptographic algorithms for securing real time applications, but the level of the security against modern attacks is not determined. Elliptic Curve based Cryptography (ECC) is the most important cryptographic algorithm for confidentiality and authentication, providing high security level with small length keys when compared to other asymmetric algorithms like RSA, Diffie-Hellman, etc. The real time system usage of ECC is very less due to computational complexity. So, to increase the real time system usage we propose the novel method of combining the ECC with the Chinese Remainder Theorem (CRT), to reduce the larger values to the smaller one, so that the complexity of constructing ECC points can be reduced nearly 40% when compared to the existing ECC based algorithms. Also, its proved that the level of security getting increased and can be used as the fundamental component in real time communication system.

**Keywords:** Elliptic Curve Cryptography, Chinese Remainder Theorem, Confidentiality, high Security, Prime Field, Encryption, Decryption

### 2. Introduction

Elliptic curve cryptography (ECC) is a type of public-key cryptography that is based on the mathematics of elliptic curves over finite fields. It provides a secure method for key exchange, digital signatures, and encryption.

In ECC, each user has a pair of cryptographic keys: a private key and a public key. The private key is kept secret and used for generating digital signatures or decrypting messages, while the public key is shared with others and used for verifying signatures or encrypting messages.

The security of ECC is based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). The ECDLP states that given a point P on an elliptic curve and another point Q, it is computationally infeasible to find an integer k such that  $Q = kP$ , where k is the private key and Q is the public key.

ECC offers several advantages over other public-key cryptosystems, such as RSA:

1. Security: ECC provides the same level of security as other public-key cryptosystems but with shorter key lengths. This results in faster computation and lower resource requirements.

2. Efficiency: ECC operations, such as key generation, encryption, and decryption, can be performed with fewer computational resources compared to other algorithms, making it suitable for resource-constrained environments like mobile devices and embedded systems.
3. Bandwidth and storage efficiency: ECC produces shorter key sizes, which results in smaller digital signatures, ciphertexts, and certificates. This makes ECC more efficient in terms of bandwidth usage and storage requirements.
4. Future-proofing: ECC is considered more resistant to attacks from quantum computers compared to traditional public-key algorithms like RSA and DSA. This makes ECC a potential choice for long-term security.

ECC is widely used in various applications, including secure communication protocols like Transport Layer Security (TLS), digital signatures, key exchange protocols like Diffie-Hellman key exchange, and more in [5]-[11].

It's important to note that while ECC offers strong security, its implementation must be done carefully to avoid vulnerabilities. Keeping software and hardware up to date, using well-vetted elliptic curve parameters, and following best practices are crucial for maintaining the security of ECC systems. The importance of Elliptic Curve Cryptography lies in its ability to provide strong security, efficiency, scalability, and standardization for various cryptographic operations, including key exchange and digital signatures. Its small key sizes and computational efficiency make it particularly valuable in resource-constrained environments, while its wide adoption ensures interoperability and compatibility in modern cryptographic systems.

### 3. Related Work

#### 3.1 Literature Review of Text to Point Mapping Process

Several attempts have been made to take advantage of the ECC's strength in a variety of public-key encryption activities, including confidentiality, authentication, integrity and nonrepudiation. Koblitz [12] presents an encoding a message to a point on an elliptic curve using a probabilistic approach that involves first turning the message into a string of numbers. The auxiliary base parameter 'k' is then multiplied by each number 'n', taken as the x-coordinate value and find possible y value which solves the elliptic curve equation. According to [17], the authors propose a matrix with non-singular property to transfer the identical alphabets in the input text to several positions along the curve. In [10], the ASCII cypher characters are utilised to locate the elliptic curve points while the Hill cypher method is employed to encrypt the message. [14] discusses a method for implementing message encryption using the ECC algorithm in which a character is transformed into a point on the curve by multiplying its ASCII value by the original affine point. The ElGamal elliptic curve encryption method is then used to encrypt this point. In [12], authors suggested employing mirrored elliptic curves to extend the Koblitz approach. [13] suggested the same Koblitz method with transposition technique. Before characters are mapped to the curve, [18]'s authors propose the usage vector and XOR function on plaintext characters. This means that a polyalphabetic cypher will be produced by encrypting the mapped locations. The Koblitz method and the Time Dependent Multiple Random Cypher (TDMRC) code were suggested in [19] as a secure way to put plaintext on an elliptic curve. A quick mapping method utilising a non-singular matrix was suggested in [17].

In [18] provided a succinct overview of key exchange, encryption, and decryption using ECC. The authors used a mapping table to translate the ASCII value into an elliptic curve coordinate.

### 3.2 Elliptic Curve Cryptography

In ECC, the process of converting text to points on an elliptic curve involves a mathematical operation known as scalar multiplication of an elliptic curve. According to [12],[15] Here's a high-level overview of the steps involved:

**Choose an Elliptic Curve:** Select an appropriate finite field elliptic curve. The equation of the elliptic curve is  $y^2 = x^3 + ax + b$ , where a and b are constants specific to the curve.

**Define a Base Point:** Select a point P on the curve called the base point or generator. This point should have a large prime order, meaning that when you repeatedly add it to itself, you eventually get the identity element (point at infinity).

**Convert Text to a Numeric Representation:** Encode the text you want to encrypt into a numeric representation. This step can involve various encoding schemes, such as ASCII or Unicode, depending on the specific implementation or requirements.

**Generate a Private Key:** Choose a random integer k as your private key and the key value should be in the range between 1 and the order of the high base point.

**Perform Scalar Multiplication:** Multiply the base point P by the private key k. Scalar multiplication involves adding the base point to itself k times. This operation results in a new point on the elliptic curve, which is your public key.

The output of the resulting point is the public key corresponding to the private key. It can be represented as coordinates (x, y) on the curve.

It's important to note that the conversion of text to points is only a part of the ECC encryption process. With the help of elliptic curve mathematical properties, provide secure key exchange, digital signatures, and encryption. The encryption process typically involves additional steps, such as generating a shared secret using the recipient's public key and performing symmetric encryption with that shared secret.

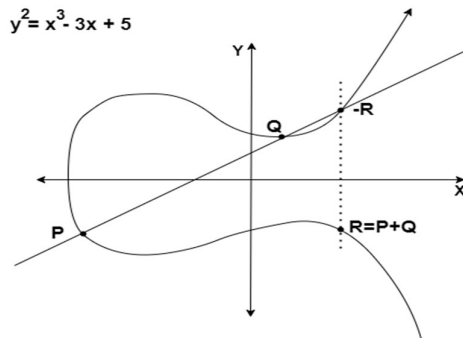


Fig 1: - Elliptic Curve Points Addition. ( $R=P+Q$ )

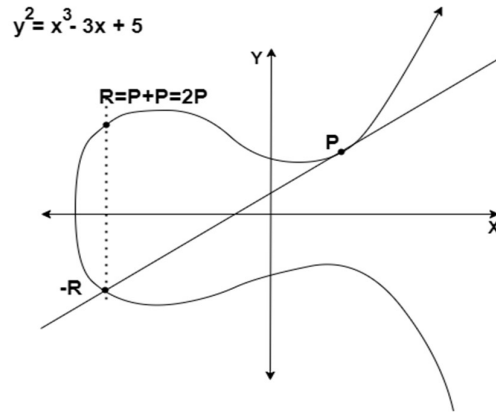


Fig 2: - Elliptic Curve Points Doubling( $R=P+P=2P$ )

### 3.3 Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) is a fundamental theory in modular arithmetic and the most important number theory. It gives a deterministic steps to solve a problem of congruences or modular equations with pairwise coprime moduli.

Let's say we have a system of congruences:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

...

$$x \equiv a_n \pmod{m_n}$$

where  $a_1, a_2, \dots, a_n$  are given remainders, and  $m_1, m_2, \dots, m_n$  are pairwise coprime moduli (i.e., the greatest common divisor of any two moduli is 1).

The CRT states that there exists a unique solution for  $x$  modulo  $M$ , where  $M$  is the product of all the moduli:

$$M = m_1 \times m_2 \times \dots \times m_n$$

The theorem provides a constructive method to find this solution, known as the Chinese Remainder Theorem algorithm. Here's a simplified version of the algorithm:

Compute  $m_1, m_2, \dots, m_n$  where  $M = m_1 \times m_2 \times \dots \times m_n$  with no common multiplicative factors of  $m_i$ .

For each congruence  $x \equiv a_i \pmod{m_i}$ , compute the value  $b_i$  such that

$$b_i \equiv \left(\frac{M}{m_i}\right) \pmod{m_i}.$$

This can be done using the extended Euclidean algorithm or by using modular inverses.

Calculate the solution  $x$  by taking the sum of the products of  $a_i$  and  $b_i$  modulo  $M$ :

$$X = (a_1 \times b_1 \times \frac{M}{m_1} + a_2 \times b_2 \times \frac{M}{m_2} + \dots + a_n \times b_n \times \frac{M}{m_n}) \pmod{M}$$

The value of  $x$  obtained in step 3 is the unique solution to the system of congruences.

The Chinese Remainder Theorem has various applications in number theory, cryptography, and computer science[20]. It is particularly useful for solving modular equations in cryptographic protocols, optimizing computations in certain algorithms, and finding solutions in modular arithmetic systems[21].

#### 4. Proposed Methodology

##### 4.1 Architectural Framework of proposed method

The Fig X shows the overall architectural frame work of the proposed methodology, which consists of four primitive functionalities. They are

- i. Text to Elliptic Curve Point Mapping
- ii. ECC-CRT Encryption
- iii. ECC-CRT Decryption
- iv. Reverse Mapping of Elliptic Curve Point to Text

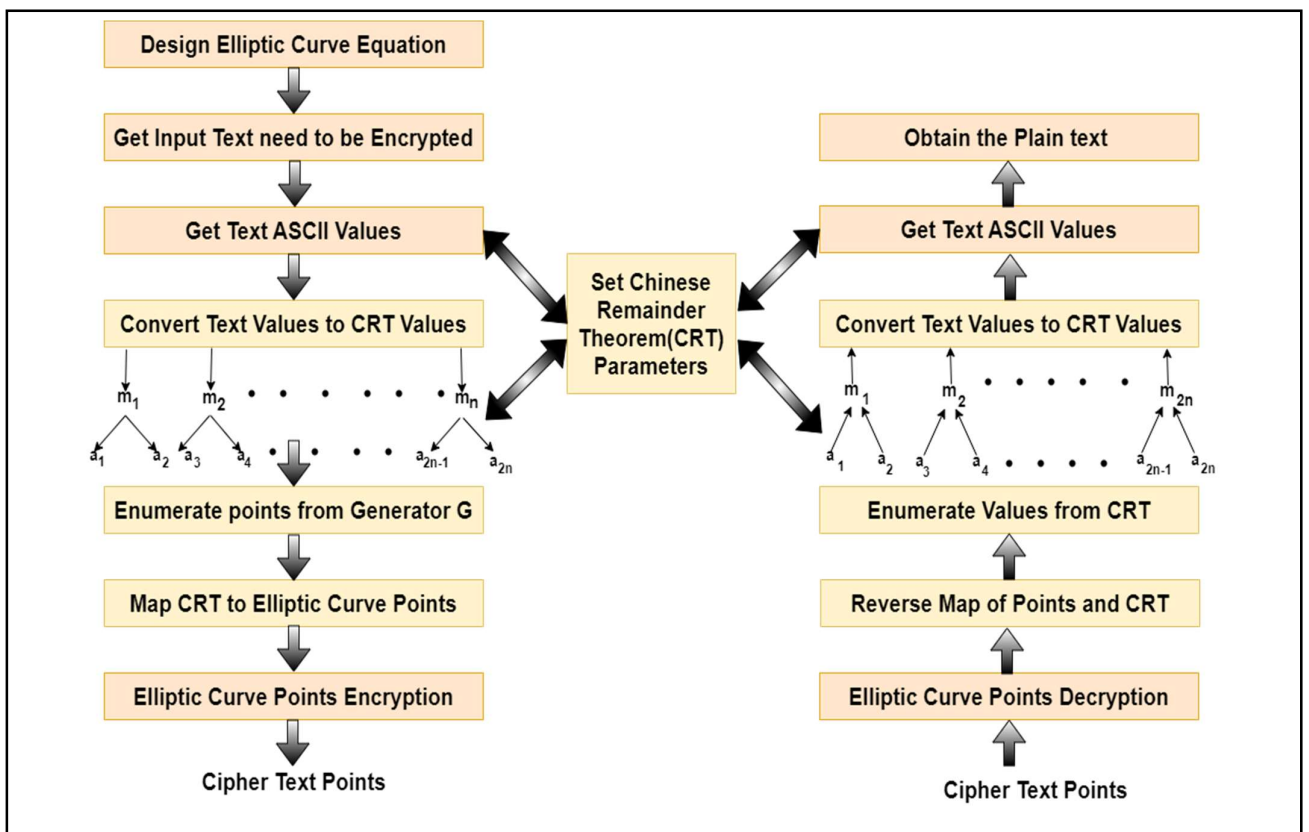


Fig 3: Architectural framework of Proposed ECC-CRT algorithm

##### 4.2 Setting of Prime Modules of Chinese Remainder Theorem

The ASCII value of every character is obtained then, every ASCII values are converted to pair of values based on the multiplicative prime moduli ( $m_1, m_2$ ) of  $M$  of the Chinese Remainder Theorem. Further, every CRT values are converted to Elliptic Curve Points, based on the Elliptic Curve Generator function[22]. The following algorithm shows the conversion of text to ECC points using CRT.

### 4.3 Text to Elliptic Point Conversion Algorithm

Global parameters:  $E_p(a, b), G, N, M, m_1, m_2, T$  where,

$P$  – prime number

$a, b$  are integers satisfies the equation(#)

$G$  – Generator points  $\in E_p(a, b)$

$N$  – Order of the Elliptic Curve Points

$m_1, m_2$  are multiplicative prime moduli of  $M$ , and  $GCD(m_1, m_2) = 1$

$T$  – Text Message

**Input:** Readable message, can be given any language provided the ASCII value of the alphabet should be defined.

**Output:** Produce set of Elliptic Curve Points(X,Y).

**Method:**

Convert\_Text\_To\_ECC\_Points(T)

```
{
    A[] = ASCII(T)           // Get Ascii values of T
    Set CRT Parameters  $M, m_1, m_2$ 
    Let  $\alpha [ ] = \text{empty}$ 
    For each A do
         $\alpha [j] = A_i \text{ mod } m_1, \alpha [j + 1] = A_i \text{ mod } m_2$ 
    X = Find_Max( $\alpha_i$ ) // find the largest value of  $\alpha_i$ 
    For each  $\alpha$  values should be mapped with finding  $P [ ] = \alpha_i \cdot G$ 
    Create Mappable[Point,CRT_Value] = ( $P [ ], \alpha_i$ )
}
```

### 4.4 ECC-CRT Encryption & Decryption Process

Encryption using Elliptic curve cryptography.

**Input:** Set of points(X,Y) on the elliptic curve  $E_p(a, b)$

**Output:** Set of points (X,Y)  $\in E_p(a, b)$

**Method:**

ECC-CRT-Encryption(Points( $P_{m_1}, P_{m_2}, \dots, P_{m_n}$ ))

```
{
    public keys of sender and receiver,
     $PUB_a = n_a \times G$ 
     $PUB_b = n_b \times G$  where  $n_a, n_b$  chosen private keys.  $0 < n_a, n_b < N - 1$ 
    let  $k$  be the chosen random variable, such that  $0 < k < N - 1$ .
    Calculate  $C_1 = k \times G$ 
```

For each pair  $(P_{m_i}, P_{m_{i+1}})$  do  
 $C_i, C_{i+1} = \{P_{m_i} + k \times PUB_b, P_{m_{i+1}} + k \times PUB_b\}$   
 $C_m = C_1, C_i, C_{i+1}, i = 1, 2, \dots, n$   
 Output  $C_m$   
 }

---

Decryption using Elliptic curve Cryptography.

**Input:** Set of points  $(X, Y)$  on the elliptic curve  $E_p(a, b)$

---

**Output:** Set of points  $(X, Y) \in E_p(a, b)$

---

**Method:**

ECC-CRT-Decryption(Points( $C_1, C_2, \dots, C_n$ ))

{

Extract key from  $C_1$

$K = n_b \times C_1$  (where  $n_b$  is the private key of the receiver).

For every  $C_i, i = 2, 3, \dots, n$

from  $C_2$  to obtain  $P_{m_1}$ ,

$$P_{m_1} = P_{m_1} + k \times PUB_b - n_b \times k \times G$$

$$= P_{m_1} + k \times n_b \times G - n_b \times k \times G$$

$$= P_{m_1} + n_b \times k \times G - n_b \times k \times G = P_{m_1}$$

from  $C_3$  to obtain  $P_{m_2}$ .

$$P_{m_2} = P_{m_2} + k \times PUB_b - n_b \times k \times G$$

$$= P_{m_2} + k \times n_b \times G - n_b \times k \times G$$

$$= P_{m_2} + n_b \times k \times G - n_b \times k \times G = P_{m_2}$$

}

---

#### 4.5 Reverse Mapping of Elliptic Curve Points to Text

Reverse of points to Tamil text using Chinese Remainder Theorem.

Now calculate M from  $m_1$  and  $m_2$

$M = (m_1 \times n_1 \times \text{inverse}(n_1) + m_2 \times n_2 \times \text{inverse}(n_2)) \bmod N$ , described in the following algorithm.

---

**Input:** Set of Elliptic Curve Points  $(X, Y)$

**Output:** Readable input message.

---

**Method:**

Reverse\_Mapping\_ECC\_Points\_To\_Text( $W$ )

{

Find inverse of  $m_1 \bmod m_2$  and  $m_2 \bmod m_1$ ;

For each point  $W(x, y)$  using Mappable find

$$\alpha_i = W(x, y) \text{ where } W(x, y) \text{ equal to } P(x, y)$$

```

For a pair of  $\alpha$  values ( $\alpha_i, \alpha_{i+1}$ ) do
    Temp1 =  $\alpha_i \times m_1 \times m_1^{-1}$ 
    Temp2 =  $\alpha_{i+1} \times m_2 \times m_2^{-1}$ 
    A[i] = (Temp1 + Temp2) mod M
    Get A[i] th ASCII character  $T_i$ 
Combine every  $T_i$  to get the Text Message T
}

```

## 5. Message encryption and decryption implementation using ECC-CRT

The implementation was done using Subline Text version-3 on Lenovo ThinkBook laptop model with the system configuration of intel CORE i5 processor with 2.20 GHz and 16 GB Ram with 192-bit keysize of NIST (National Institute of Standards and Technology) recommended for the implementation of Elliptic curve parameter[23]. They are,

```

a = 11;
b = 2455155546008943817740293915197451784769108058161191238065;
p = 6277101735386680763835789423207666416083908700390324961279;
nB = 28186466892849679686038856807396267537577176687436853369;
G={60204628237568865675821348058752611191669876636884684818,
174050332293622031404857552280219410364023488927386650641};
Pb={2803000786541617331377384897435095499124748881890727495642,
4269718021105944287201929298168253040958383009157463900739};
Text = "SRM Institute of Science and Technology"

```

### 5.1 Text to Elliptic point conversion Process

- Input Text = "SRM Institute of Science and Technology"
- ASCII values of the input = [83, 82, 77, 32, 73, 110, 115, 116, 105, 116, 117, 116, 101, 32, 111, 102, 32, 83, 99, 105, 101, 110, 99, 101, 32, 97, 110, 100, 32, 84, 101, 99, 104, 110, 111, 108, 111, 103, 121]
- Get Maximum(ASCII input values), that is 121, then set M is greater than 121 and  $M = m_1, m_2$  such that,  $\text{GCD}(m_1, m_2) = 1$ . Here  $M = 143$
- Group ASCII Values according to M.
- [5, 6, 4, 5, 12, 0, 6, 10, 8, 7, 6, 0, 11, 5, 12, 6, 1, 6, 12, 6, 0, 7, 12, 6, 10, 2, 6, 10, 7, 1, 11, 3, 6, 10, 5, 6, 8, 0, 1, 6, 10, 2, 6, 0, 8, 0, 10, 2, 6, 10, 6, 9, 6, 0, 9, 1, 6, 10, 6, 7, 10, 2, 8, 0, 0, 5, 6, 0, 7, 1, 4, 9, 7, 1, 12, 4, 4, 0]
- With the generator G, constructed points on elliptic curve are,
- Pm= [3443036292837963759546685842252818034438575132436169939548, 568215723800040768087579915035785248418187453186037543584], [4181600039257606811702445814091795515382674993670451363594, 4145864787418078582741371957294208579442183461049606472962], [5816974679166206479449678315796610621695041936087021819827, 5990665915885689608438704467746222618933646319921982157727],



[3786948970427612552829445802542365824897011513834778634630,  
4298963390352331878364098142582004096663285750649430704591] and so on...

### 5.2 Encryption Process

- Each point consider as  $P_m$ , and encrypted as,  $C = kG, P_m + kP_{pub}$ , where  
 $kG = (2553986348910663776233311747947521386085452801244003930239,$   
 $6054206530771321844149094895450517595579248348317492258426),$   
 and  $P_m + kP_{pub} =$   
 $(4650517478818334322569896490468044831719046727403924728252,$   
 $4799912126540324155491715700097021953177600481154529961843),$   
 $(5103177365715759592064308134138930589690629186607826991365,$   
 $1961307840107939418010565929966263512444030943913685583437),$   
 $(6193199055113969152687712056392098586164011469546956708719,$   
 $3968060648383654175232669533869346046476775347528732426056),$   
 $(4650517478818334322569896490468044831719046727403924728252,$   
 $4799912126540324155491715700097021953177600481154529961843),$   
 $(1579701179631292406088991148392154677185778402116125967385,$   
 $2805267123498414860490239994873784424572054494203738930942),$   
 $(2355477037527639396321212673447711444596965044207895531821,$   
 $1943714316891614729861689740853781228872124693286185146405)$  and so on...

The obtained values are with respect to the selected Generator value, if the generator value is different and for the same input text, then accordingly, we get the different ciphertext value. Also, the same for selecting different  $k$  values. This ciphertext will be sent to the receiver.

### 5.3 Decryption Process

- In decryption, from  $kG$ , key is extracted, and using the extracted key  $P_m$  is obtained by,
- $(45157833212313172622820565487488628232320607903046191557,$   
 $3416643315589709844888130285908365692064465573445880563824),$   
 $(3511977767041722340803634309370047399223581713793412001154,$   
 $22635282023438897720799494022530414118255720611850115995),$   
 $(5008627072379688015859085641769200051967712136055683167836,$   
 $171988491142659365744790108100019648217239346159555842925),$   
 $(45157833212313172622820565487488628232320607903046191557,$   
 $3416643315589709844888130285908365692064465573445880563824),$   
 $(1267287162293117354266037246381199791649550490142650107179,$   
 $319149749247514537745477719083287431841068322622128640297),$   
 $(60204628237568865675821348058752611191669876636884684818,$   
 $174050332293622031404857552280219410364023488927386650641),$  and so on...

### 5.4 Elliptic point to Text conversion Process

- From the above points, are then mapped with the values [5, 6, 4, 5, 12, 0,.....]
- The values are converted to the original ASCII values by [83, 82, 77, 32,.....]
- the corresponding ASCII character conversion, we obtain the Plain text Message as, "SRM Institute of Science and Technology"

## 6. Performance evaluation

Elliptic curve cryptography algorithm is best algorithm for providing strong security even with small length keys when compared to all other asymmetric cryptographic algorithms. Now the overall complexity of the proposed algorithm is analysed and given in table.

Process Module	Input size (points/text)	Time for execution (ms)	Size of the Output(points/text)
Input Text to Elliptic Curve Points	3	0.3	6
Encryption	3	1.2	7
Decryption	7	1.6	6
Elliptic Curve Points to Text Message	6	0.6	3

Table 1: Overall Complexity analysis of the Proposed Algorithm

There are several methods exists for converting text message to elliptic curve points, used in the implementation of elliptic curve cryptography[24]. The following table shows the comparative performance of proposed algorithm with the existing algorithms.

Algorithm References	Input size (word)	Encryption Time(ms)	Decryption Time(ms)	Look-up Table (Y/N)
Reference[21]	1	20	30	Y
Reference[14]	2	10.5	9.35	Y
Reference[2]	2	10	11.7	Y
Reference [20]	3	4.8	7.2	N
Proposed (ECC-CRT)	3	1.5	2.1	N

Table 2: Comparative Performance with existing algorithms

The following diagram shows the graphical representation of the performance of the proposed algorithm with the existing algorithms[25].

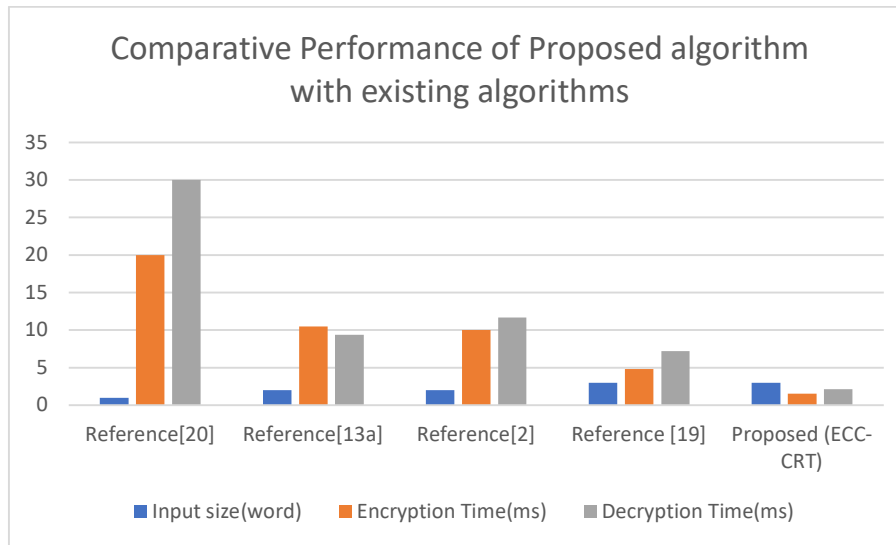


Fig 4: Comparative Performance of Proposed algorithm with existing algorithms

The proposed ECC-CRT algorithm can be implemented in any languages whose alphabets are defined by the ASCII values, so that, the security level will be increased, also tested that, the vulnerability is very low for any cryptanalysis.

## 7. Conclusion

The proposed algorithm using Chinese Remainder Theorem, construct points from the text message with a smaller number of iterations from the generator point by reducing the larger values to smaller one, proved that, which reduce the time complexity of overall elliptic curve cryptographic algorithm by 40%, also proved that the strength of the security getting increased by introducing the intermediate values between the curve points and the messages.

## 8. References

- [1]. TAPAS KUMAR GHOSH, "A CONVERSION ALGORITHM OF TEXT MESSAGES INTO ELLIPTIC CURVE POINTS", *Advances and Applications in Mathematical Sciences* Volume 21, Issue 9, July 2022, Pages 5445-5456 © 2022 Mili Publications, India.
- [2]. prasenjit Das, Chandan Giri, "An Efficient Method for text Encryption using Elliptic Curve Cryptography", 8th International Advance Computing Conference (IACC), 978-1-5386-6678-4/18/\$31.00 c 2018 IEEE.
- [3]. Omar Reyad, "Text Message Encoding Based on Elliptic Curve Cryptography and a Mapping Methodology", *Information Sciences Letters An International Journal*, Inf. Sci. Lett. 7, No. 1, 7-11 (2018) <http://dx.doi.org/10.12785/isl/070102>
- [4]. ROLLA SUBRAHMANYAM , N. RUKMA REKHA, AND Y. V. SUBBA RAO, "Authenticated Distributed Group Key Agreement Protocol Using Elliptic Curve Secret Sharing Scheme", *IEEE Access*, Digital Object Identifier 10.1109/ACCESS.2023.3274468.
- [5]. Bore Gowda S B, "Implementation of Elliptic Curve Cryptography over a Server-Client network", 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), 978-1-7281-6368-0/20/\$31.00 ©2020 IEEE
- [6]. Josepha Menandas J, Mary Subaja Christo, "The Revelation of Tamil Cryptographic Lexicon – Connecting Tamil Characteristics and Cubic Curve", *International Conference on*

- Networking and Communications,(ICNWC), 979-8-3503-3600-9/23/\$31.00 ©2023 IEEE  
DOI: 10.1109/ICNWC57852.2023.10127454
- [7]. Mary Subaja Christo, V.Elizabeth Jesi, Uma Priyadarsini, V. Anbarasu, Hridya Venugopal, and Marimuthu Karuppiah, “Ensuring Improved Security in Medical Data Using ECC and Blockchain Technology with Edge Devices”, Hindawi Security and Communication Networks Volume 2021, Article ID 6966206, <https://doi.org/10.1155/2021/696620>
- [8]. Premanand, R.P., Rajaram, A. Enhanced data accuracy based PATH discovery using backing route selection algorithm in MANET. Peer-to-Peer Netw. Appl. 13, 2089–2098(2020).
- [9]. B Rasina Begum and P Chitra, “ECC-CRT: An Elliptical Curve Cryptographic Encryption and Chinese Remainder Theorem based Deduplication in Cloud”, Wireless Personal Communications (2021) 116:1683–1702 <https://doi.org/10.1007/s11277-020-07756-7>].
- [10]. Freeda J, Josepha Menandas J, “IoT Based Innovation Schemes in Smart Irrigation System with Pest Control”, Lecture Notes on Data Engineering and Communications Technologies Volume 35, Pages 657 – 669 in 2020
- [11]. A. Sengupta and U. K. Ray “Message mapping and reverse mapping in elliptic curve cryptosystem” Secure Communication Network, 9(18), 5363–5375 (2016), doi:101002/sec.1702.
- [12]. Josepha Menandas J, Priyanka k, “Building an Web Based Cloud Framework for Rustic School Improvement”, Lecture Notes on Data Engineering and Communications Technologies Volume 35, Pages 838 – 845 in 2020
- [13]. Kumar, K. V., & Rajaram, A. (2019). Energy efficient and node mobility based data replication algorithm for MANET. International Journal of Computer Science, 2019.
- [14]. Neal Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation 48 (1987), 203- 209.
- [15]. M. Celestin Vigila and K. Muneeswaran, Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications, International Journal of Network Security, Vol.14, No.4, PP.236-242, July 2012.
- [16]. M.C. Vigila and K. Muneeswaran, Implementation of text based cryptosystem using elliptic curve cryptography, ICAC IEEE 10, 82–85 (2009)
- [17]. Anand, R. P., & Rajaram, A. (2020, December). Effective timer count scheduling with spectator routing using stifle restriction algorithm in manet. In IOP Conference series: materials science and engineering (Vol. 994, No. 1, p. 012031). IOP Publishing.
- [18]. Victor Miller, Uses of Elliptic Curve in Cryptography, Advances in cryptology-CRYPTO Springer Heidelberg 85(218) (1986), 417-426.
- [19]. Brian King, Mapping an Arbitrary Message to an Elliptic Curve when Defined over  $GF(2^n)$ , International Journal of Network Security, Vol.8, No.2, PP.169-176, Mar. 2009.
- [20]. F. Amounas and E.H. El Kinani, Fast Mapping Method based on Matrix Approach for Elliptic Curve Cryptography, Int J of Information and Network Security 1, 54–59 (2012)
- [21]. Rajaram.A., Dr.S.Palaniswami . Malicious Node Detection System for Mobile Ad hoc Networks. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010, 77-85

- [22]. J. Muthukuru and B. Sathyanarayan, Fixed and Variable Size Text Based Mapping Techniques using ECC, *Global Journal of Computer Science and Technology* 12, 13–18 (2012).
- [23]. M.C. THOMAS and V. PAUL, Secure method for embedding plaintext on an elliptic curve using TDMRC code and Koblitz method, *Journal of Theoretical and Applied Information Technology* Vol-84, pp 298–304 (2016)
- [24]. Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, “Implementation of Text Encryption using Elliptic Curve Cryptography”, Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015), [www.sciencedirect.com](http://www.sciencedirect.com) 1877-0509 © 2015 The Authors. Published by Elsevier doi: 10.1016/j.procs.2015.06.009
- [25]. Megha Kolhekar and 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)