A Novel Secure Message Transmission using Elliptic Curve Diffie Hellman Key Exchange Protocol

Shaik Hedayath Basha, Jaison B

Abstract: The main objective of the proposed work is to develop a new simple method to secure the text messages in the transmission systems. ELLIPTIC CURVE DIFFIE HELMAN (ECDH) key exchange protocol is adopted which is one of the highly secure cryptography technique compared with other cryptographic techniques. In the proposed work prime elliptic curve is used to encrypt the input message signal. In the first step, a new convolution wheel is developed to convert the text message into modified ASCII value. Using these values and the elliptic prime curves the message is encrypted at the transmitter section, the channel is considered as a lossless noisy channel and the basic attacks like cipher text attack, cipher text only attack and chosen key attack were analyzed. It is found that the cipher text is very robust to various attacks and the probability that the attacker decrypt is very less. The cipher text is decrypted with the private key at the receiver end.

Index Terms: Attacks, Convolution Wheel, Decryption, ECDH, Encryption, Modified ASCII, Secure.

1 INTRODUCTION

in the elliptic crypto system there are three schemes to solve the crypto problems they are integer factorization, discrete logarithm and elliptic curve discrete logarithm problem. In the public cryptography system a key pair is selected so that the problem of deriving the sender's private key from the corresponding public key is equivalent to solving a computational problem that is believed to be intractable. The elliptic curve cryptography problem can be done in the four different methods they are EC over real numbers, EC over complex numbers, EC over prime curves (Zp) and EC over Galois field or finite fields (F_{2^m}).

1.1 General Elliptic Curve over a real number field 'F':

Over a real number field, let a_1, a_2, a_3, a_4 and a_6 are the variables defined in the elliptic curve (E) it is defined as

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

Δ is the discriminant of E, it is defined as the following and $\Delta \neq 0$.

$$\Delta = -d_2^2d_8 - 8d_3^4 - 27d_6^2 + 9d_2d_4d_6 \quad (2)$$
$$d_2 = a_1^2 + 4a_2 \quad (3)$$
$$d_4 = 2a_4 + a_1a_3 \quad (4)$$
$$d_6 = a_3^2 + 4a_6 \quad (5)$$
$$d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \quad (6)$$

If L is rational point on E, then

$$E(L) = \{(x, y) \in L\ X\ L: y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\} \quad (7)$$

where ∞ is point at infinity.

- *Shaik Hedayath Basha is currently working as Assistant Professor in the Department of Electronics and Communication Engineering at RMK College of Engineering and Technology and pursuing Doctor in Philosophy degree in Information and Communication Engineering at Anna University, Chennai, India, PH-09104467900679. E-mail: shaikhedayathbasha@rmkcet.ac.in*
- *Dr. Jaison B is currently working as Associate Professor in the Department of Computer Science and Engineering at RMK Engineering College affiliated to Anna University, Chennai, India, PH-09104467906790. E-mail: bjn.cse@rmkec.ac.in*

1.2 Elliptic curve over real numbers(R) is simplified as

$$E/R = y^2 = x^3 + ax + b; a, b \in \boldsymbol{R} \quad (8)$$
$$\text{Where } \Delta = 4a^3 + 27b^2 \neq 0 \quad (9)$$

If there are two points $P = (x_1, y_1), Q = (x_2, y_2)$ and if $P \neq Q$ then, the third point is obtained by point addition $P + Q = R; R = (x_3, y_3)$

if $P = Q$ then the third point is obtained by point doubling i.e. $P + Q = P + P = 2P$

$$x_3 = \lambda^2 - x_1 - x_2 \quad (10)$$
$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (11)$$

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}; if\ P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1};\ if\ P = Q \end{cases} \quad (12)$$

1.3 Elliptic curve over Prime field (Zp) is defined as

$$E/\boldsymbol{Z_p} = y^2 mod\ p = x^3 + ax + b\ mod\ p \quad (13)$$

If there are two points $P = (x_1, y_1), Q = (x_2, y_2) \in \mathbf{Z_p}$ and if $P \neq Q$ then the third point is obtained by point addition $P + Q = R; R = (x_3, y_3)$

If $P = Q$ then the third point is obtained by point doubling i.e. $P + Q = P + P = 2P$

$$x_3 = \lambda^2 - x_1 - x_2\ mod\ p \quad (14)$$
$$y_3 = \lambda(x_1 - x_3) - y_1 mod\ p \quad (15)$$
$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}; if\ P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1};\ if\ P = Q \end{cases} \quad (16)$$

1.4 Elliptic curve over Galois field or finite fields $(\mathbf{F_{2^m}})$ is defined as

$$E/\boldsymbol{F}_{2^m} = y^2 + cy = x^3 + ax + b \quad (17)$$

If there are two points $P = (x_1, y_1), Q = (x_2, y_2) \in \boldsymbol{F}_{2^m}$ and if $P \neq Q$ then the third point is obtained by point addition $P + Q = R; R = (x_3, y_3)$

$$x_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2 \quad (18)$$
$$y_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + y_1 + c \quad (19)$$

If $P = Q$ then the third point is obtained by point doubling i.e. $P + Q = P + P = 2P = (x_3, y_3)$

$$x_3 = \left(\frac{x_1^2 + a}{c}\right)^2 \quad (20)$$

$$y_3 = \left(\frac{x_1^2 + a}{c}\right)(x_1 + x_3) + y_1 + c \quad (21)$$

1.5 Problem is defined such that to find the points on an Elliptic Curve (EC) 'E':

In the search of elements on the curve 'E' assume a primitive element or generator element 'P' and the target element 'T'. To find 'T' from 'P', we need to point doubling or scalar multiplication with point 'P' to get 'T', i.e. $\mathbf{P + P + \cdots + P = dP = T}$. Finding the value of 'd' is discrete logarithm problem. Where $\mathbf{1 \leq d \leq E}$. In the crypto system 'd' is the private key which is an integer and the 'T' is the public key with coordinates $(\mathbf{x_T, y_T})$.

By the definition of Hasse's theorem the number of points on the EC is given by the equation

$$P + 1 - 2\sqrt{P} \leq \#E \leq P + 1 + 2\sqrt{P} \quad (22)$$

#E is called the order of 'E' or group cardinality of 'E'. The above equation is called as Hasse's bound with the upper and lower limits. Hasse's bound states that the number of points on the EC is approximately in the range of prime 'p'.

The organization of this paper starts with the literature survey which was a backbone for this paper, where authors learn various aspects involved in the ECC. Next the new methodology of convolution wheel is proposed which is used to modify the ASCII values of the text message with the help of private key. In the IV module the complete Diffie-Hellman Key exchange protocol is discussed with an example. V and VI modules are proposed with the combination of convolution wheel operation and DH-EC Encryption and Decryption methodologies with the flow chart, VII modules shows the simulation results, VIII module shows the comparison of the results with the existing methods, In the IX module attacks were discussed and at last X module is the conclusion of the paper.

2 REQUIRED LITERATURE WORK

The motivation of the present approach is from Laiphrakpam D Singh et. al.,[2] where the cryptosystem was analyzed with 192 bit key length with NIST standard EC with the help Mathematica Ver. - 10 software. In [2] six different languages are tested for the encryption process. Various attacks were also analysed like key space, cipher text attack, cipher text only attack, Time complexity. It was shown that using the 192 bit key length, if the attacker attacks using Pollards Rho method and Pollard Lambda method the time taken will be approximately 23 days. Victor S. Miller first proposed the Elliptic Curve Diffie – Hellman Cryptography at that time it was faster by around 20%. [3]. The method of converting text message to ASCII values in ECC was introduced in the paper [4] where these ASCII values are mapped with the points of EC with the use of base value. In [4] to map ASCII values they used mapping table to fix on the EC points in the encryption process and complementary mapping is done in the decryption process, it was implemented in C++ on multimedia text and image. The basic concepts of ECC and DH-EC was learned from [5, 6 and 7] which gives the best information about the cryptography procedures. In U.S. federal government recommends Federal information Processing Standard (FIPS) 186-2 standard, 15 elliptic curves of varying security levels [1]. The three curves are random elliptic curves over a prime field $\mathrm{F_p}$, over a binary field $\mathrm{F_{2^m}}$ and Koblitz elliptic curve over $\mathrm{F_{2^m}}$. With the literature survey authors came to a conclusion that the work done in this paper is very basic with an added security aspect using convolution wheel. In real world the use of ECC in Digital Rights Management System is very awesome where it uses the bit key sizes of 256 bits, 512 bits and even more, which is very hard to crack.

3 PROPOSED CONVOLUTION WHEEL OPERATION

In the proposed method the message is first converted in ASCII code then it is modified according to the convolution wheel. In this convolution wheel there are two wheels the inner wheel and outer wheel shown in the below Fig. 1.

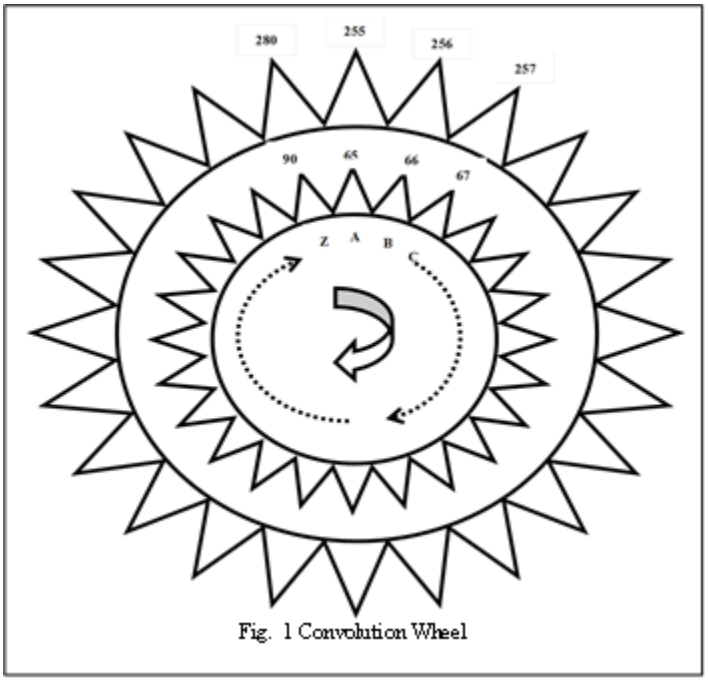

Fig. 1 Convolution Wheel

The inner wheel is not fixed wheel it can be rotatable in clock wise direction, the inner wheel have fixed alphabets and its ASCII values. The outer wheel is fixed which is not rotatable the wheel has some fixed values on the top with a logic. The logic is at the initial condition, the inner wheel ASCII is added with the random number. The random number is another security known only to the sender and receiver. Now we can take an example of its operation, the input message is first converted into ASCII values i.e. if the message is "HEDAYATH" then the ASCII value is "7269686589658472" we use the private key of sender 'A' to rotate the inner wheel the corresponding fixed wheel values is taken as the modified ASCII value of the text message. Consider the private key of sender 'A' is 21 and then rotate the conventional wheel '2' times in clockwise and '1' time counter clockwise.

3 ELLIPTIC CURVE DIFFIE-HELLMAN ENCRYPTION AND DECRYPTION PROCESS

The domain parameters are {p, a, b, G, n, h} where p: field prime number (modulo p), 'a' and 'b' are the elliptic curve parameters chosen to satisfy Eq. 4, G is the generator point or base point, 'n' order of G, 'h' is the cofactor, ideally '1'. In the EC-DH encryption process we consider two entities Sender

('S') and Receiver ('R') and an unknown entity as attacker ('A'). In the process of secure data transmission few parameters are public known to the entities and even attacker they are EC in the field i.e. $E: y^2 = x^3 + ax + b$, a, b, p, G, n and h it is shown in the below TABLE 1.

TABLE 1. *ECDH PROTOCOL*

Sender 'S'	Attacker 'A'	Receiver 'R'
Private Key = KSP	$E: y^2 = x^3 + ax + b$	Private Key = KRP
$\mathbf{1} \leq \boldsymbol{K_{SP}} \leq \boldsymbol{n-1}$	a, b, p, G, n and h.	$1 \leq K_{RP} \leq n-1$
$\boldsymbol{S = K_{SP} * G}$	S	S
R	R	$R = K_{RP} * G$
$\boldsymbol{C = R * K_{SP}}$		$C = S * K_{RP}$

To calculate cipher text from the text message we consider the following example for simplicity, let the elliptic curve is defined as $E: y^2 = x^3 + 4x + 20$, the domain parameters a = 4, b = 20, and the prime field be F29 , p = 29, the value of Eq. 4 is $4(4)^2 + 27(20)^2 = 10864 \neq 0$. Therefore the above curve is Elliptic it is obtained using MATLAB 2018a and it is shown in the Fig. 2

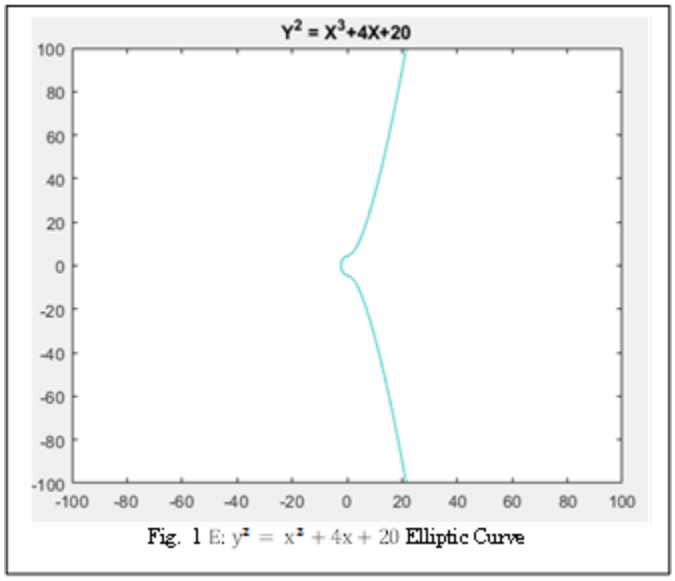

Fig. 1 $E: y^2 = x^3 + 4x + 20$ Elliptic Curve

Let the generator point be G (1, 5). To solve the problem we need to calculate the points on the curve using the G point by the point doubling operation. The solution is as follows:

$G = (1,5) = (x_1, y_1)$ = P

$2G = (1,5) + (1,5) = (x_3, y_3) = 2P$

To solve 2G we use the "(14)", "(15)" and "(19)"

First we solve for x3

$x_3 = \lambda^2 - x_1 - x_2 \bmod p$

where $\lambda = (3x_1^2 + a)(2y_1)^{-1}$

$\lambda \equiv (3 * (1)^2 + 4) * (2 * 5)^{-1} \bmod 29$

$\lambda \equiv 7 \bmod 29 * (10)^{-1} \bmod 29$

$\lambda \equiv 7 * 3 = 21 \bmod 29 = 21$

$x_3 = \lambda^2 - x_1 - x_2 \bmod 29 \equiv (21^2 - 2) \bmod 29$

$x_3 = 439 \bmod 29 = 4$

$y_3 = \lambda(x_1 - x_3) - y_1 \bmod 29$

$y_3 = (21(1-4) - 5) \bmod 29$

$y_3 = 19$

$(x_3, y_3) = (4, 19)$

Similarly Using "(14)", "(15)" and "(19)" we can find

$3G = 3P = 2P + P = (x_4, y_4) = (20, 3)$

$(x_4, y_4) = (20, 3)$

If the sender entity 'S' secret key or Private Key = KSP = 11, then 'S' will send 11G = 11P to 'R'. Similarly if 'R' Private Key = KRP = 19 then 'R' will send 19G or 19P to 'S'. The attacker knows both the messages (10, 25) and (2, 6) but finding Private Key of 'S' and 'R' is very hard which is considered as intractable problem it shown in below TABLE 2.

TABLE 2. *SHARING OF SECRET KEYS*

Sender 'S'	Attacker 'A'	Receiver 'R'
Private Key = KSP	$E: y^2 = x^3 + ax + b$	Private Key = KRP
KSP = 11	a, b, p, G, n and h.	KRP = 19
11G = (10, 25)	(10,25)	(10,25)
(2, 6)	(2, 6)	19G = (2, 6)
$\boldsymbol{C = 19G * 11}$	Finding KSP or KRP is very hard problem for the attacker.	$C = 11G * 19$
Message Transmitted Securely with EC-DH Protocol		

4 PROPOSED ENCRYPTION

4.1 Encryption Process

The encryption is carried out in the following steps and it is described in the below flow chart in Fig. 3

STEP 1. Get the Input text message.

STEP 2. Convert the input text into the corresponding Modified ASCII values using the 'S' Secret Key K_{SP}.

STEP 3. Choose the Base value or Generator Value between [3 to 36].

STEP 4. Use Public key 'G' point and convert to decimal to base.

STEP 5. Calculate group size (grp) using the Equation

$$grp = \text{length}(\text{dec2base}) - 1 \quad (22)$$

here grp =3.

STEP 6. Divide ASCII value in the group size and it is Pm.

STEP 7. Select private key $K_{SP.}$

STEP 8. Compute Cipher Text

$$P_c = (GK_{SP,} P_m + C) \quad (23)$$

STEP 9. Send the Cipher text to 'R' Entity

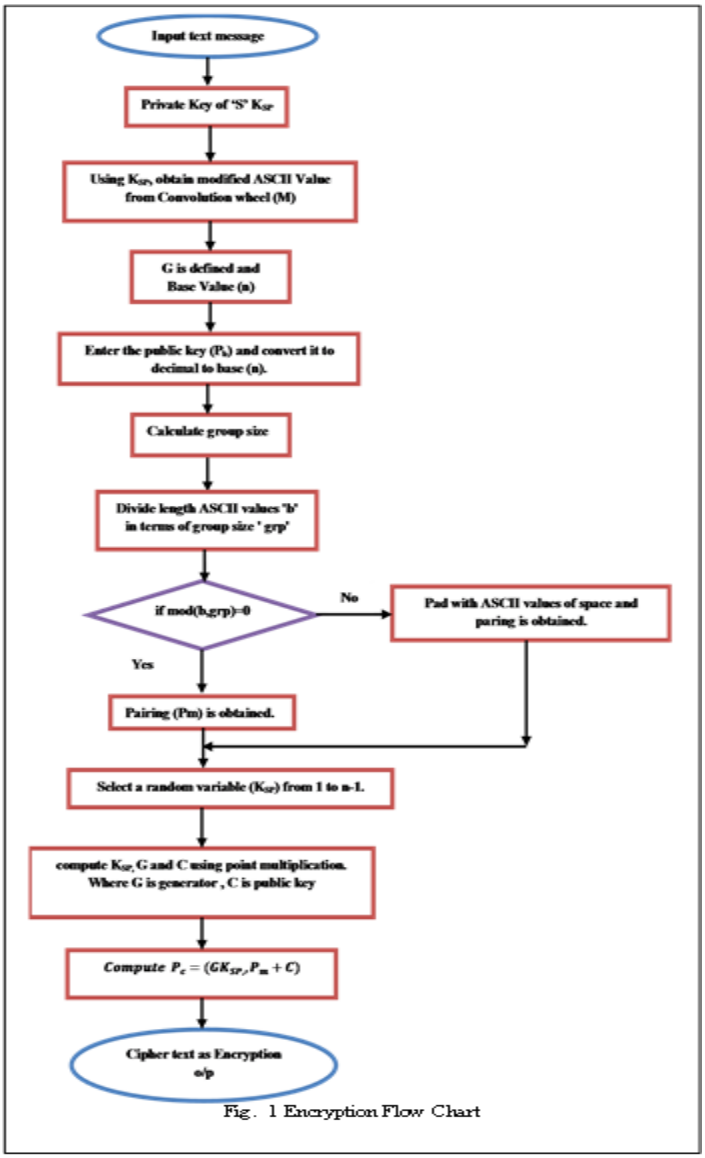

Fig. 1 Encryption Flow Chart

4.2 DECRYPTION PROCESS

The Decryption steps are as follows:

STEP 1. Obtain the Cipher Text from the entity 'S'.

STEP 2. Calculate the Pm from the equation,

$$P_m = (P_m + C) - C \quad (24)$$

STEP 3. Convert the Pm to corresponding ASCII values from the Convolution whell 'R' entity.

STEP 4. Required text is obtained.

The entire process is shown in below flow chart Fig. 4

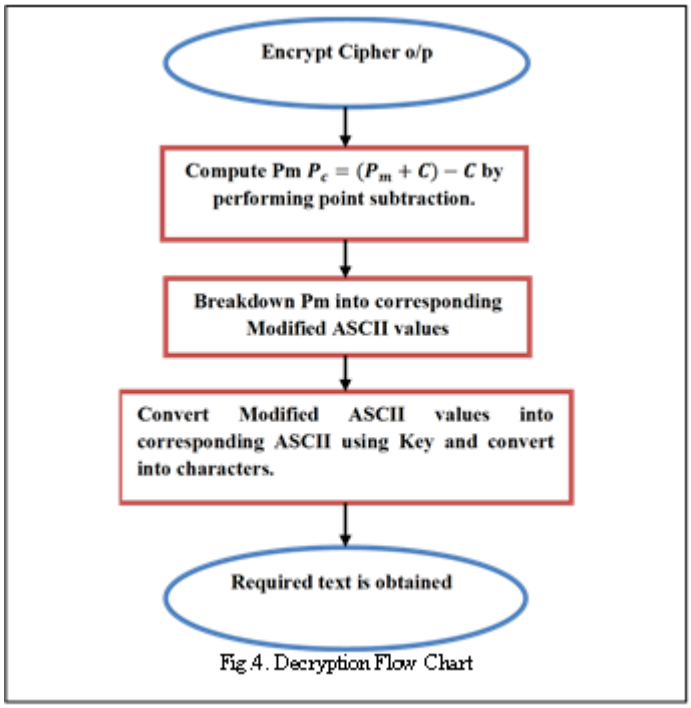

Fig.4. Decryption Flow Chart

5 STIMULATION RESULTS

The entire encryption and decryption was done in MATLAB R2018a software. The results of the entire work are shown below.

Input message:

Enter the String:
R.M.K. COLLEGE OF ENGINEERING AND TECHNOLOGY
ASCII Values of the Text Message:
L1 = Length of the message = 44
ASCII_C =
Columns 1 through 21
82 46 77 46 75 46 32 67 79 76 76 69
71 69 32 79 70 32 69 78 71
Columns 22 through 42
73 78 69 69 82 73 78 71 32 65 78 68
32 84 69 67 72 78 79 76 79
Columns 43 through 44
71 89
Modified ASCII Values using convolution wheel:
Private Key of Sender K_{SP} = 11
MOD_ASCII_INNER_VALUES =
Columns 1 through 21
83 45 78 45 76 45 33 66 80 75 77 68
72 68 33 78 71 31 70 77 72
Columns 22 through 42
72 79 68 70 81 74 77 72 31 66 77 69
31 85 68 68 71 79 78 77 78
Columns 43 through 44
72 88
First_Cipher_Text =
'S-N-L-!BPKMDHD!NGFMHHODFQJMHBMEUDDGONMNHX'
MOD_ASCII_OUTER_VALUES =
Columns 1 through 21
63 235 63 235 63 235 223 63 63 63 63 63
63 63 223 63 63 221 63 63 63

Columns 22 through 42
63 63 63 63 63 63 63 221 63 63 251 221 63 63 63 63 63 63 63 63 63
Columns 43 through 44
63 63
Elapsed time is 0.05007 seconds.
Cipher_Text =
'ËëČëČëßĂĎĉċĂĆĂßČąÝĄċĆąĂĄďĈăĆÝĂăûÝëĂĂąćăċČĆĖ'
Decrypted_Message =
'R.M.K. COLLEGE OF ENGINEERING AND TECHNOLOGY'
Elapsed time is 0.1007 seconds

TABLE 3. *COMPARISONS OF RESULTS*

Method	*Words Count*	*Encryption Time (Sec)*	*Decryption Time (Sec)*	*Cipher data size*
S. Meria et. al. [3]	*409*	*1.95*	*0.83*	*459.118 KB*
Megha Kolhekar et. al. [4]	*1*	*0.2*	*0.30*	*1.146 KB*
Laipharkpam et.al. [2]	*409*	*0.093*	*0.14*	*21.017 KB*
Proposed method	*14*	*0.05007*	*0.107*	*352 Bytes*

6. ATTACKS

6.1 Cipher text attack

The attacker gets the entity parameters to decrypt the cipher text using all the EC-DH algorithms but it is very hard to get the private keys of 'S' and 'R'. If he gets the 'S' and 'R' by default he need to get the logic to crack the convolution wheel code which is the user desire it can be very random number and it can shared frequently by the two entities to improve the complexity of attacker.

6.2 Cipher text only attack

The cipher text only attack gets vulnerable due to advancement in many new algorithms. In the proposed method the strength of vulnerability is increased for Brute force attack many random attack.

6.3 Chosen key attack

In this attack the attacker chose various keys to decrypt the cipher message in the random way. So there are chances that the attacker gets the keys in any one chance, but in order to increase the strength of the cipher text the convolution wheel can be changed frequently and also the private key changes with a certain time period to increase the robustness of cryptosystem.

7. CONCLUSION

In this proposed method new simple concept of convolution wheel is used to improve the robustness of the cipher text and confuse the attacker with the rotation of the wheel which can be done secretly between the two entities 'S' and 'R'. The concept of converting the text message to ASCII is old which is used in many applications so the authors added few complications with the convolution wheel which is considered as pubic but the rotations are based on the private key of the 'S' and 'R' entities. The concept of Diffie – Hellman is explained from the scratch so that the readers can understand and promote a new standard to the cryptography systems. The encryption time, decryption time, the word length and attacks were analyzed in TABLE 3 and it is better than the available cryptosystems. This method is less vulnerable to the attackers compared with the other methods. The work is done in MATLAB 2018a because to extend the work for image encryption and decryption in future.

8 REFERENCES

[1] Darrel Hankerson, Alfred Menezes and Scott Vanstone, Guide to Elliptic Curve Cryptography with 38 illustrations, Springer (2004).

[2] Laiphrakpam D Singh and Khumanthem M Singh "Implementation of Text encryption using Elliptic Curve Cryptography", 11th IMCIP, ELSEVIER Procedia Computer Science, pp. 73 – 82- 2015.

[3] Victor S. Miller, 'use of Elliptic Curve in Cryptography', Advances in Cryptology-CRYPTO' 85 proceedings, Springer, Vol. 218, pp 417 – 426, December - 2000.

[4] S. Maria C Vigila and K. Muneeswaran, "Implementation of Text based Cryptosystem using ECC", ICAC, IEEE, PP. 82-85, December – 2009.

[5] Megha Kolhekar and Anita Jadhav, "Implementation of Elliptic Curve Cryptography on Text and Image", IJECBS, Vol. 1, issue-2, July – 2011.

[6] Elliptic Curve Cryptography NPTEL Videos - https://youtu.be/2RVLBUncHJk.,

[7] Diffie – Hellaman Elliptic Curve Cryptography NPTEL Videos - https://youtu.be/1plMO7ChXMU?list=PLJ5C_6qdAvBFAuGoLC2wFGruY_E2gYtev.

[8] Video Lecture by Chrisof Paar - https://youtu.be/1plMO7ChXMU?list=PLJ5C_6qdAvBFAuGoLC2wFGruY_E2gYtev.