Elliptic Curve Cryptography System Based On Indexing Dictionary Techniques

Hsu Myat Nandar
"University of Computer Studies, Yangon, Myanmar"
phwethayalphi@gmail.com,

Abstract

Cryptography is one of the most important sciences in the current area. Elliptic Curve Cryptography (ECC) has attracted the attention of researchers and product developers due to its robust mathematical structure and highest security compared to other existing algorithms. ECC provides greater security more efficient performance than the first generation public key techniques. In this paper, application for elliptic curve cryptosystem work as symmetric cryptographic system by investigates from indexing dictionary techniques. This system is implemented to transfer secret messages between the sender and receiver using indexing dictionary techniques for English text. In this system, linear feedback shift register (LFSR) is used to generate the secret key that used in the encryption and decryption process. Secret permutation and inverse permutation key is used to increase randomized for points sequence of data. This system test it by execute encryption and decryption process with more flexible and efficient.

1. INTRODUCTION

The ability to compute security functions with limited computing resources has become increasingly precious. In mobile devices such as smart card, personal digital assistants (PDA) and multimedia cell phones, the processing resources, memory and power are all very limited but this need for secure transmission of information may increase due to the vulnerability to attackers of the publicly accessible wireless transmission channel [1]. Smaller and faster security algorithms provide part of the solution. Elliptic curve cryptography (ECC) provides a faster alternative for public key cryptography. Elliptic curve cryptography(ECC) provides the require security for all these low processor devices in much smaller key lengths as compared to the other public key or symmetric key. The term elliptic curve cipher and elliptic curve cryptography refers to an existing generic cryptosystem which use numbers generated from an elliptic curve. Such cryptosystems that utilize number derived from elliptic curve can be more secure [2]. In the last couple of years, the first commercial implementations are appearing as toolkits but also in real-world applications, email security, web security, smart cards, etc. These papers to produce application for ECC work as symmetric key system that make the secret messages transfer faster and more efficient.

The remainder of the paper is formed as follows: Section 2 describes some related work. Section 3 discuss about the elliptic curve cryptography (ECC), linear feedback shift register (LFSR) and permutation and inverse permutation, architecture of the system is presented in section 4. In section 5, we present testing results and experimental results. Finally, section 6 presents conclusion and future work.

2. RELATED WORK

Introduces a novel hardware architecture for ECC over GF(p) C J. Mclvor , et al, the work presented by Gang Chen presents a high performance EC cryptography process for general curves over GF(p) [3]. A simple tutorial of ECC concept is very well documented and illustrated in the text authored by Williams Stallings, et al. Kamlesh Gupta, et al[4]. Some cryptographic algorithms have gained popularity due to properties that make them suitable for use in constrained environment like mobile information appliances where computing resources and power availability are limited. One of these cryptosystems is Elliptic curve which requires less computational power, memory and communication bandwidth compared to other cryptosystem. The use of elliptic curves in public key cryptography was independently proposed by Koblitz and Miller in 1985 [5] and since then, a lot of work has been done on elliptic curve cryptography. Various techniques have been proposed in the literature, many authors have tried to exploit the features of ECC field to deploy for security applications.[6] Has been proposed Performance Analysis for Image Encryption using ECC.[7]technique was based upon a prime curve over Z_P, use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through p-1 and in which calculations are performed modulo p.

3. CRYPTOGRAPHY

Cryptography is one of the technological means to provide security to data being on information and communications system. Cryptography is the art or science of keeping messages secure. It provides an important tool for protecting information and is used in many aspects of computer security. Cryptography involves encryption and decryption of messages. Encryption is the process of converting a plaintext into cipher text by using an algorithm and decryption is the process of getting back the encryption messages. In addition to, provide data confidentiality, Integrity, Authentication, and Non-repudiation.

3.1 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz as an alternative mechanism for implementing public key cryptography [8].

The mathematics used for ECC is deeper and more difficult than mathematics used for conventional cryptography. Elliptic curve combine number theory and algebraic geometry. These curves can be defined over any field of numbers (i.e., real, integer, complex).An elliptic curve consists of the set of real numbers(x, y) that satisfies the equation: $\mathbf{y^2 \bmod p = x^3+ax+b \bmod p}$, where **x , y ,a** and **b** are real numbers. Two points $\mathbf{P(x_1, y_1)}$ and **Q(x2, y2)** in the elliptic curve and then **P+Q** given by $\mathbf{R(x_3, y_3)}$**.** An elliptic curve group consists of the points on the curve and a special point O.

The set of all of the solutions to the equation forms the elliptic curve. Changing a and b changes the shape of the curve. The parameters a and b must satisfy the following condition**:** $\mathbf{(4a^3+27b^2) \bmod p}$ **is not p.** Small changes in a and b parameters can result in major changes in the set (x, y) solutions. Referred as $E_p(a, b)$.Figure1:Show the addition of two points on an elliptic curve. Elliptic Curves have the interesting property that adding two points on the elliptic curve yields a third point on the curve.

Point addition can be described graphically: point R, with R represented by R=P+Q where P and Q are both points on the elliptic curve can be found by drawing the secant line between P and Q. The point where the line interests the elliptic curve is taken and reflected across the curve's horizontal line of symmetry which much of the time is the x-axis. The resultant point is the sum of P and Q. The operation is demonstrated below:

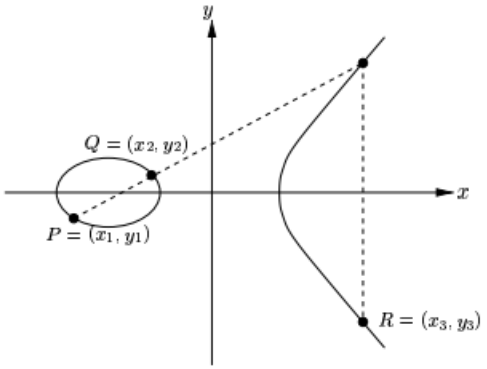

Figure 1: Elliptic curve addition

If two points having the same x-coordinate are added, the sum of the points will be infinity or the identity point O. Adding can also be defined by the following equations:

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \; for\_ x_1 \neq x_2 \\ \dfrac{3x_1^{\,2} + a}{2y_1} \; for\_ x_1 = x_2 \end{cases}$$

$$\boxed{\begin{aligned} x_3 &= \lambda - x_1 - x_2 \\ y_3 &= \lambda(x_3 - x_1) + y_1 \end{aligned}}$$

3.1.1 Elliptic Curves over Zp

Elliptic Curve Cryptography (ECC) makes use of elliptic curves in which the variables and coefficients are all to elements of a finite field. Two families of elliptic curves are used in cryptographic applications: prime curves over Zp and binary curves over GF (2m). For prime curve over Zp, we use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through p-1 and in which calculations are performed modulo p. For binary curve defined over GF (2m), the variables and coefficients all take on values in GF (2n) and in calculations are performed over GF (2n).Points out that prime curves are best for software applications because the extended bit-fiddling operations needed by binary curves are not required and that binary curves are best for hardware applications.

3.2 Linear Feedback Shift Register (LFSR)

Linear Feedback Shift Register (LFSR) is known as pseudo-random generator. The random number repeats itself after 2n-1 clock cycles.

Linear Feedback Shift Register (LFSR) is a shift register that input bit is a linear function of its previous state. The most commonly used linear function of single bits is XOR. The initial value of the LFSR is called the seed and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current or previous state [8].

Shift register is a sequence of m cells, b0 to bm-1, where each cell holds a single bit. Cell is initialized to an m-bit word, called initial valued or seed. Whenever an output bit is needed, every bit is shifted one cell to the right, the right most cell bo, give its value as output (Ki).

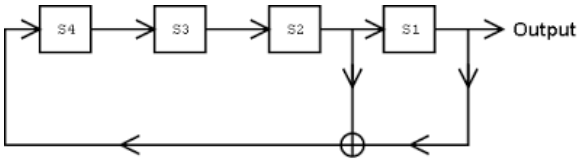

Figure 2: Linear Feedback Shift Register (LFSR)

3.3 Permutation and Inverse Permutation

A permutation of a set of distinct objects is an arrangement of the objects in a specific order without repetitions. Secret permutation or inverse permutation key is used to increase randomized for points sequence of data. [8]

3.4 Indexing Dictionary Techniques

Compression schemes like the popular and patented Lempel-Ziv algorithm are called dictionary schemes because they build a big list of common words in the file [9]. The dictionary is just a list of words. Secure sentences stored in dictionary in this system are fixed length [10]. Fixed lengths are easier to handle.ECC points are used as indexes of dictionary in this system. List is created with English sentences which is agreed between sender and receiver and associated index (points) used as pointer in this system. Indexes of ECC points are encoded into binary format and then encrypted and decrypted.

Table3: Simple design for $E_5(1,1)$ indexing dictionary

No.	$E_5(1,1)$	Secure messages
1	(0,1)	" the meeting at 9 o' clock "
2	(0,4)	"Call back! Please! "
3	(2,1)	"Sorry, I have a meeting now."
4	(2,4)	"Don't worry! I am fine."
5	(3,1)	"Good luck"
6	(3,4)	"this day is sunny day"
7	(4,2)	"work hard this day "
8	(4,3)	"take another home"

4. PROPOSED SYSTEM

In this paper, indexing dictionary techniques based elliptic curve cryptography (ECC) which works as symmetric cryptosystem. This proposed system work to interested for the ability that satisfy in elliptic curve addition over Zp that each addition two points represent third point in curve i.e R(x, y)=P(x, y)+Q(x, y) this feature work well in this proposed system ,in other word the point R(x, y) over Ep(a, b) have many choices for addition different points for P(x, y) and Q(x, y) gives unique point R(x, y), the redundancy for P,Q points help to send the same messages using different points for P,Q, this feature make the system more flexible. This system work according the following steps:

1.Generate dictionary for secure sentences: Dictionary that contained short secure sentences instead of word.

2.Generate table for Elliptic curve points over Ep(a,b): The sender and receiver agreed between them about for the secret key information that represent the following:the Elliptic curve group that used Ep(a,b),the sender and receiver agreed number that used prime number and the parameters.And then permutation key PK and inverse permutation key PK^{-1}: the sender and receiver agreed about the permutation and inverse permutation in oder increased the randomizes for points sequence.

3.Encode the plaintext secure messages : Encode the messages as the x-y coordinate for point are not easy process because not all such coordinate are in Ep(a,b) ,for this reason ,this system for encoding the messages by combine between the dictionary sentences that generated in step1 with the points table that generate in step2 as a way for encoding the message where each sentences in the dictionary linked with unique points R(x,y) according the rules for Elliptic Curve addition.

4. Encryption Process:

- The sender select the secret messages that want to send from the dictionary that generated according steps(1 and 2).
- Convert the points R(x,y) in another form using table of points over Zp,i.e R(x,y)=P(x,y) + Q(x,y) , by this way each point represent by two different points.
- Convert the data points into binary form.
- Used LFSR key stream generator in order generate the secret key that used in encryption process:M xor Ki=C.

5. Decryption Process :

The decryption process work as the same steps using PK^{-1},with reverse order,i.e, C xor Ki=M.And getting as plaintext or points P and Q with related to R(x,y) points.Those points are indexing to dictionary and then display text.The system overview as shown in figure 3.

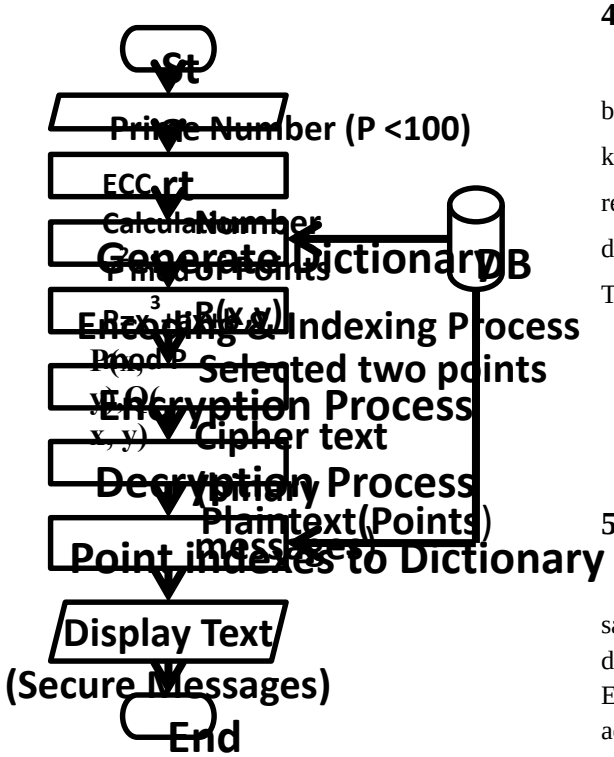

Figure 3: System flow diagram

4.1 System Design for Encryption

In encryption, selected two points are used to secret permutation key to increase randomized for points sequence of data and those permutation points are changed to binary messages. These messages are encrypted with LSFR binary key stream and then generate to cipher text. The system encryption is shown in Figure 4.

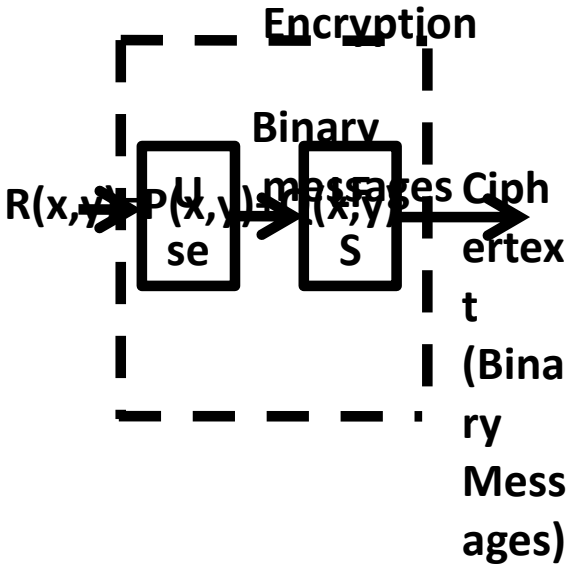

Figure 4: System Design for Encryption

4.2 System Design for Decryption

In decryption, cipher text is decrypted with LFSR binary key stream and also used to inverse permutation key and then getting as plaintext or points P and Q with related to R(x, y) points. Those points are indexing to dictionary and then display text or secure messages. The system decryption is shown in figure 5.

Figure 5: System Design for Decryption

5. EXPERIMENT AND RESULT

In this section, the sender and receiver used the same dictionary according to the secret messages. The dictionary size depends on Ep(a, b) in this used $E_{19}(1,1)$,therefore the dictionary generate to 20 rows according the number for elliptic curve sets. These secure messages are encoded to ECC points and dictionary indexing. As shown in figure 6.

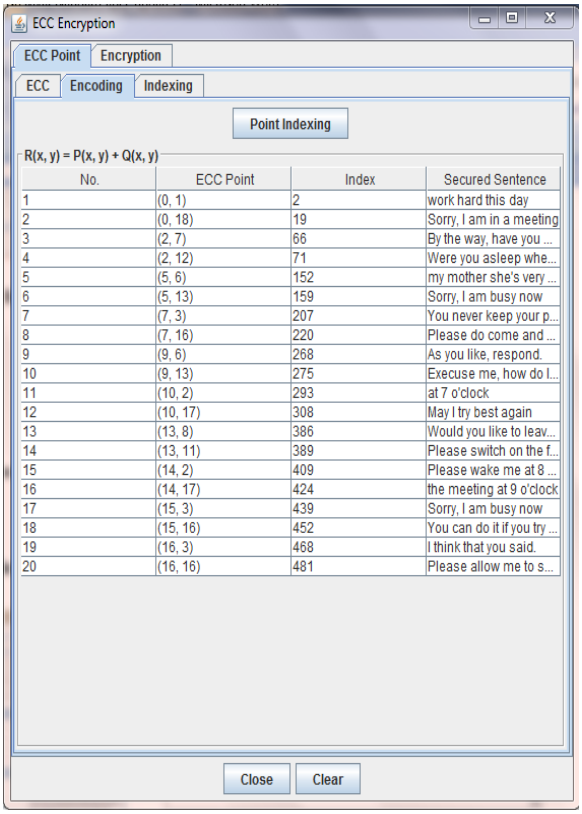

Figure6: Generate Dictionary for Secure Sentences

To encrypt the messages **"As you like,respone.", "the meeting at 9 o' clock"** the encoding process convert this message to points(9,6),(14,17) ,as shown in figure 7and then each point used another form for represent, i.e.(9,6)=(9,13)+(7,3),…There many forms that represent unique(9,6) and this feature to sent the same sentences but with another form. In this used, to select(9,6)=(9,13)+(7,3)and(14,17)=(10,2)+(15,16). As shown in figure 8.

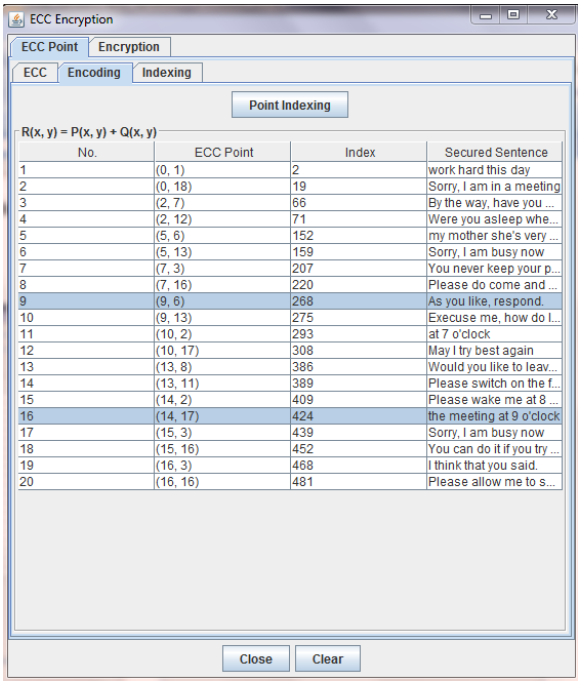

Figure 7: Encoding process

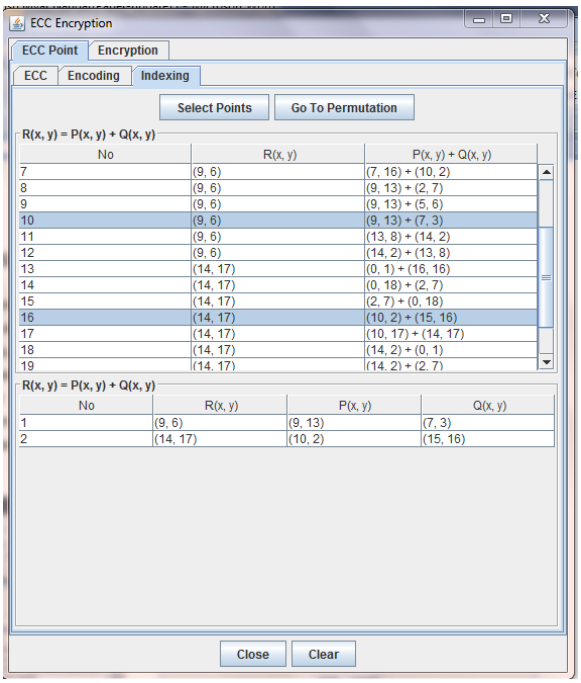

Figure 8: Generate P, Q from R(x, y) and sending points to select

Those sending points P and Q are used secret permutation key PK=3 2 4 1 to increase randomized for points sequence and those points into binary format.Finally, getting as 64 bits binary messages.As shown in figure 9.

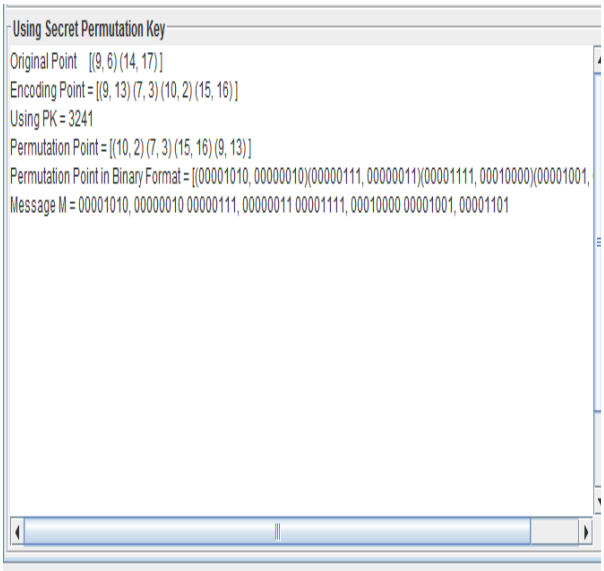

Figure 9: P and Q points used secret permutation key for more secure

In this stage, using key stream generator (LFSR) 64 bits key to encrypt the 64 bits binary messages and then getting as a cipher text C=M xor Ki. As shown in figure 10.

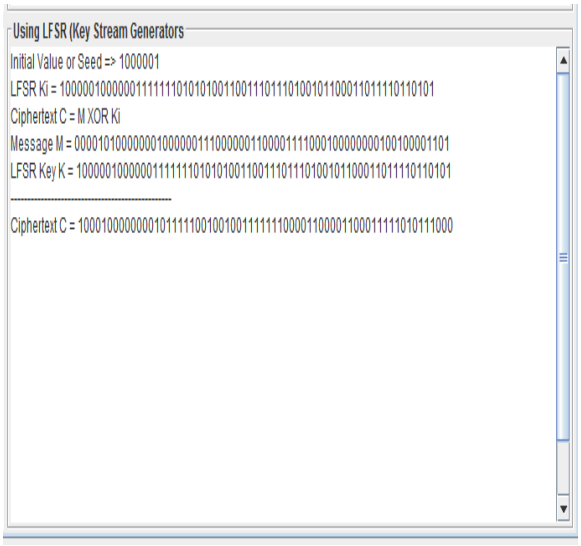

Figure 10: Using key stream generator (LFSR) and Encryption Process

In this decryption process, work as the same steps to decrypt with cipher text and LFSR 64 bits key stream i.e. M=C xor Ki. And using invert permutation key PK^{-1}=4 2 1 3 for points randomized with reverse order and then getting as P and Q with related to R .Those R points are indexing to dictionary with display text or secure messages, as shown in figure 10.

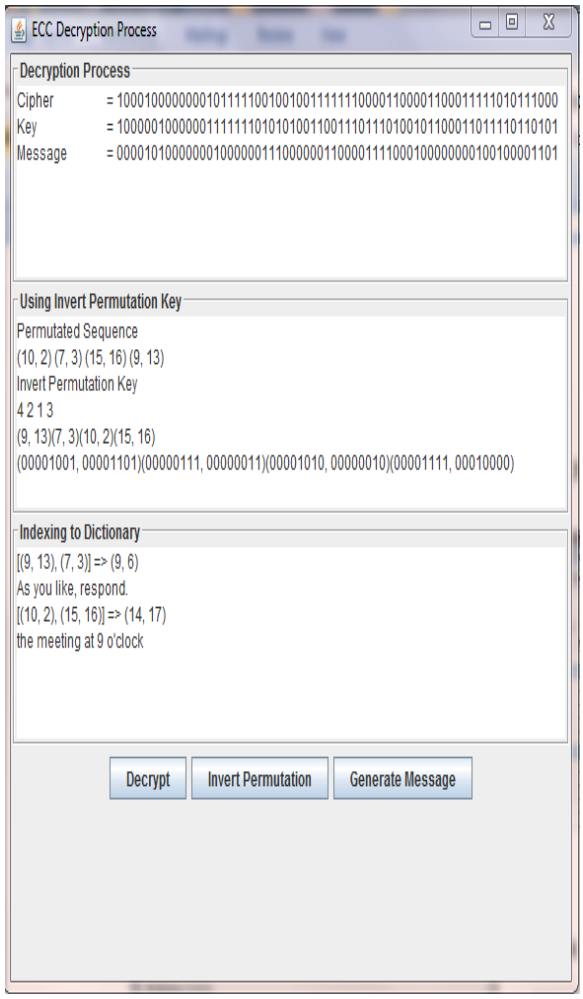

Figure 11: Points indexing to Dictionary and Decryption Process

Proposed system is implemented by using prime number P<100, P =11, 23,53,73,83, a = b=1.Each Ep (a, b) test by depends on points. According to the result, if prime number is greater, the encryption and decryption time is greater. And also if different P and Q points are changed, the encryption and decryption time are changed. This time is depends on prime number and points indexing.Figure12 shows illustrated the graph comparison of encryption time and decryption time different points.

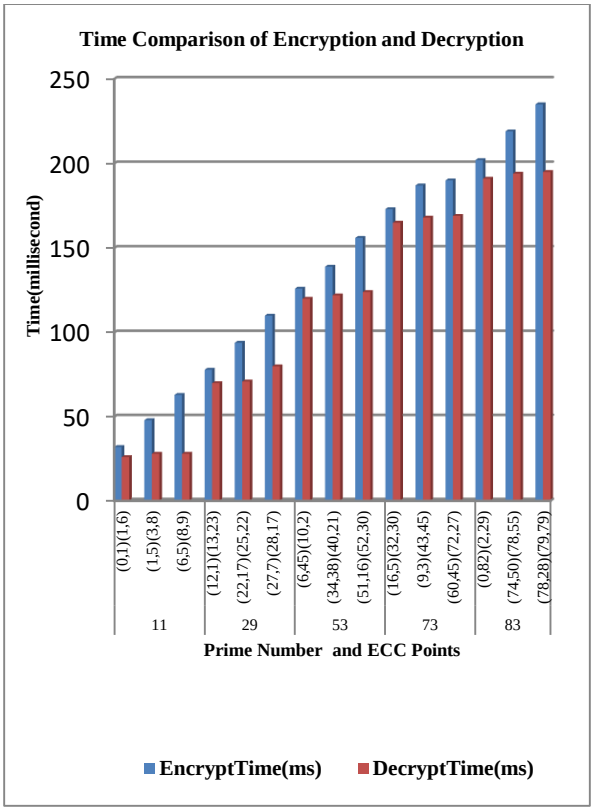

Figure12: Comparison Graph of Encrypt time and Decrypt time between different points.

6. CONCLUSION

In this system presents indexing dictionary techniques using elliptic curve cryptography system has been proposed. Solve the coding secret message and using the same length code for all transfer messages by using the elliptic curve addition and work wall to find for transfer the same message with different coding by useful the many addition choices between P(x, y) and Q(x, y) points that give unique R(x, y) point. Points are generated based on prime number. After selecting the require text and index points of selected text from ECC point table are encrypted instead of encrypting the text. Hence, it reduces the length of code for encryption and enhances the encryption and decryption process and save encrypt and decrypt time. This system can prevent the attacker be useful form the information about the letter frequency for messages and any depended information between the messages itself. In these results, if prime number is greater, the encryption and decryption time is greater. And also if different P and Q points are changed, the encryption and decryption time are changed.This time is depends on prime numbers and points indexing. In this system is tested by prime number P<100 and a and b is 1.This system be more secure when large prime number is used with values a and b parameters over Ep(a, b).

REFERENCES

[1] Kristin Lauter, "The Advantages of Elliptic Curve Cryptography for Wireless Security", Microsoft Corporation ,IEEE Wireless Commucations, February 2004.

[2] Murat Fiskiran, "Workload characterization of elliptic curve cryptography and other network security algorithms for constrained environments" , Proc.IEEE Intl. Workshop on Workload characterization, pp: 127-137, 2002.

[3] C.J Mclvor, M.McLoone, and J. V. McCanny "Hardware elliptic curve cryptography processor over GF(p)," IEEE Trans. Circuits Syst.-I:Red.papers,vol.53,no.9,pp.1946-1957,sep.2006.

[4] William Stallings, "Cryptography and Network Security",2nd edition, Prentice Hall publications.

[5] Kefa Rabah "Elliptic Curve Cryptography over Binary Finite Field GF (2m)". Information Technology Journal 5(1) pp.204-229,ISSN 1812-5638,2006.

[6] Gupta, K., Silakari, S., "Performance Analysis for Image Encryption Using ECC," Computational Intelligence and Communication Networks (CICN), 2010 International Conference on, vol., no., pp.79-82, 26-28 Nov. 2010.

[7] Gupta, K., Silakari, S., Gupta, R.: Khan S.A., "An Ethical Way of Image Encryption Using ECC," Computational Intelligence, Commutation Systems and Networks, 2009. CICSYN ,09. First International Conference on, vol., pp .342-345,23-25 July 2009.

[8] William Stallings , "Cryptography and Network Security", Prentice Hall Publications, 4th edition, 2006.

[9] Peter Wayner, " Disappearing Cryptography: Information Hiding : Steganography & Watermking",3 Edition,2008.

[10]