Volume 3, Issue 11, November-2016, pp. 568-572 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Multiple Encryption using ECC and Its Time Complexity Analysis

Vishal Kumar, Ratnesh Kumar, Mashud A. Barbhuiya and Monjul Saikia
Department of Computer Science and Engineering
North Eastern Regional Institute of Science and Technology
Arunachal Pradesh, INDIA

Abstract- Rapid growth of information technology in present era, secure communication, strong data encryption technique and trusted third party are considered to be major topics of study. Robust encryption algorithm development to secure sensitive data is of great significance among researchers at present. The conventional methods of encryption used as of today may not sufficient and therefore new ideas for the purpose are to be design, analyze and need to be fit into the existing system of security to provide protection of our data from unauthorized access. An effective encryption/ decryption algorithm design to enhance data security is a challenging task while computation, complexity, robustness etc. are concerned. The multiple encryption technique is a process of applying encryption over a single encryption process in a number of iteration. Elliptic Curve Cryptography (ECC) is well known and well accepted cryptographic algorithm and used in many application as of today. In this paper, we discuss multiple encryptions and analyze the computation overhead in the process and study the feasibility of practical application. In the process we use ECC as a multiple-ECC algorithm and try to analyze degree of security, encryption/decryption computation time and complexity of the algorithm. Performance measure of the algorithm is evaluated by analyzing encryption time as well as decryption time in single ECC as well as multiple-ECC are compared with the help of various examples.

Index Terms- ECC, Koblitz Method, Multiple Encryption, Message Encoding, Decryption etc

1. INTRODUCTION

CRYPTOGRAPHY deals with hiding information in such a way that allows information to be sent in a secure form so that only person able to retrieve hided information is the intended recipient. In present times, cryptography is considered as a branch of both mathematics and computer science, and is affiliated closely with information theory, information security and engineering technology. Use of cryptography is growing in various applications where information security is mainly concerned. Examples include the ATM transaction security, computer passwords security, and electronic commerce security, which all depend on robust cryptographic algorithms.

- *Vishal Kumar, Ratnesh Kumar and Mashud A. Barbhuiya are BTech Students in Computer science and Engineering Department NERIST, Arunachal Pradesh.*
- *Mr. Monjul Saikia is currently Assistant Professor in Computer science and Engineering Department NERIST, Arunachal Pradesh. E-mail: monjuls@gmail.com*

The basic architecture of Cryptographic system can be defined as: a message being sent is known as plaintext, the message is then coded using a cryptographic algorithm (called encryption) and an encrypted message is known as ciphertext, is turned back into plaintext at destination by use of the same cryptographic algorithm (called decryption). The method for decryption is the same as that for encryption but in reverse direction. A simple graphical representation of the architecture of cryptographic system is as shown in figure 1.

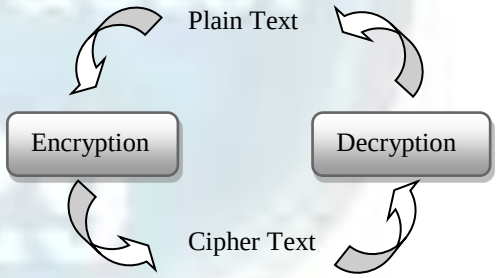

Fig.1. Encryption-decryption process

Multiple encryptions are a process of performing encryption over an already encrypted message several times, either using the same or a different encryption algorithm. Similar terms such as cascade encryption, cascade ciphering, multiple encryption, multiple ciphering etc. been used in the literature for the same meaning. Under the same key length and for the same size of the processed data different cryptographic algorithm requires different computation time. Well known RSA [3] algorithm is seemed to several times slower than AES algorithm; triple-DES is about three times slower than AES. Design of an efficient robust cryptographic algorithm is a challenging task. In cryptography, as the complexity increases in the encryption

 DOI:10.22362/ijcert/2016/v3/i11/XXXX

algorithm, execution time may be increased but it enhances the data security enormously.

2. Proposed Multiple Encryption Technique

The technique of multiple encryption in the proposed scheme is based on well-established data encryption algorithm called Elliptic Curve Cryptography (ECC).Performing the process of encryption several times enhance the security by minimizing key size by splitting it in every phase. It enhances security because of performing the same operation multiple times with different encryption key at every step. Due to repetitive application of encryption algorithm increases time complexity but at the same time splitting the main key into part key reduces time complexity to some extent. An example of multiple encryption technique is given below.

Example of Multiple Encryption Technique:

In cryptography, we would expected that by encrypting a plaintext twice with some block cipher, either with the same key or by using two different keys, the resultant encryption to be stronger in almost all circumstances. By using this process we would expect to achieve more security. For example, a plaintext "CRYPTOGRAPHY" is passes through Caesar cipher encryption, *N=3* times at which multiple encryption gives substantial improvements in security.

Let original data/ plaintext be CRYPTOGRAPHY

Algorithm: C = ((P + 3) + 3) + 3 ……. + 3) (N Times)

C	R	Y	P	T	O	G	R	A	P	H	Y	Plain Text
F	U	B	S	X	R	J	U	D	S	K	B	Cipher Cycle#1
I	Y	E	V	A	U	M	Y	G	V	N	E	Cipher Cycle#2
L	B	H	Z	D	Y	P	B	J	Z	Q	H	Cipher Cycle#3

This process of multiple encryptions can be performed with different encryption keys at each phase and process can be repeated number of times as desired.

3. Key exchange Between User Alice and Bob

Elliptic curve cryptographic key exchange can be done in the following way. First a large integer *q is* chosen randomly, which is either a prime number *p* or an integer of the form $2^m$and elliptic curve parameters *a* and *b* for the elliptic curve equation. This defines the elliptic group of points$E_p(a,b)$. Next, pick a *base point* $G = (x_1, y_1)$ in $E_p(a,b)$whose order is very large order value *n*. The order *n* of a point *G* on an elliptic curve is the smallest positive integer *n* such that $nG=O$. $E_p(a,b)$ and *G* are parameters of the cryptosystem known to all parties.

A key exchange between the intended users can be accomplished as shown in the figure 2.

1. Alice selects an integer n_A less than *n*. This is Alice's private key. A then generates a public key$P_A = n_A \times G$; where the public key is a point in$E_p(a,b)$.
2. Bob similarly selects a private key$n_B$and computes a public keyP_B.
3. Alice generates the secret key $k = n_A \times P_B$ .Bob generates the secret key $k = n_B \times P_A$.

These two calculations in step 3 produce the same result because

$$n_A \times P_B = n_A \times (n_B \times G) = n_B \times (n_A \times G) = n_B \times P_A$$

To break this scheme, an attacker would need to be able to compute *K* for given *G* and *kG*, which is assumed hard.

Message Encryption:

Message *m* is considered as a point P_m with coordinates *(x, y)* in the elliptic curve P_m. The point P_m is encrypted as a ciphertext C_m and subsequently decrypted.

To encrypt and send a message P_m to Bob, Alice chooses a random positive integer *k* and produces the ciphertext C_m consisting of the pair of points:

$$C_m = \{kG, P_m + kP_B\}$$

Note: Alice has used Bob's public keyP_B.

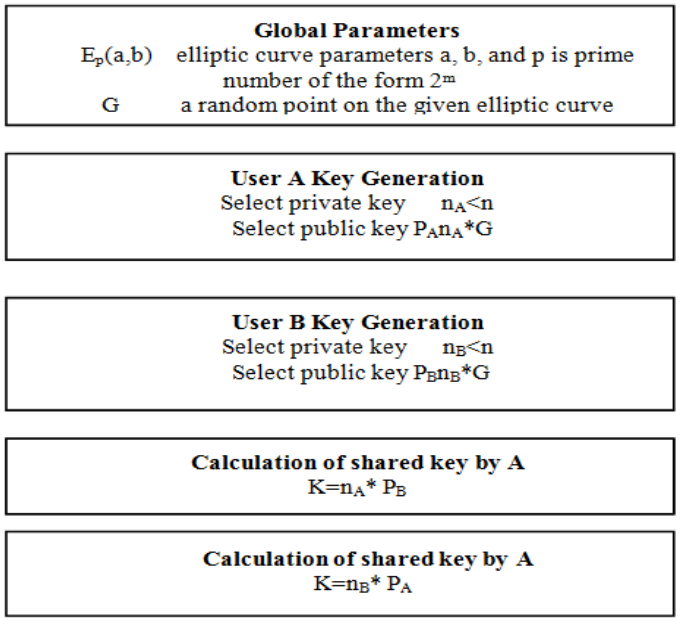

Fig 2: Diffie - Hellman ECC key exchange algorithm.

Message Decryption:

Bob decrypts the ciphertext $C_m$by multiplying the first point in the pair by Bob's secret key and subtracts the result from the second point:

$$P_m + kP_B - n_B(kG)$$
$$= P_m + k(n_B G) - n_B(kG)$$
$$= P_m$$

 DOI:**10.22362/ijcert/2016/v3/i11/XXXX**

Alice has masked the message P_m by adding kP_B to it.

4. KOBLITZ'S METHOD FOR MESSAGE ENCODING AND DECODING

Let us assume that a text file containing printable characters has to be encrypted, a user can perform encryption on the ASCII code of each character. The sequence of steps to be followed when a message to be encrypted and decrypted using elliptic Curve Cryptography is shown in Figure 3.All the points on the elliptic curve can be directly mapped to an ASCII value, select a curve on which we will get a minimum of 128 points, so that we fix each point on the curve to an ASCII value. For example, ASCII characters of the message 'ENCRYPT' can be written as sequence 69, 78, 67, 82, 89, 80,and 84.The easiest possible method for embedding a message is to map these values to fixed points on the elliptic curve. In flowchart 2 we show the steps to be followed during encoding and decoding.

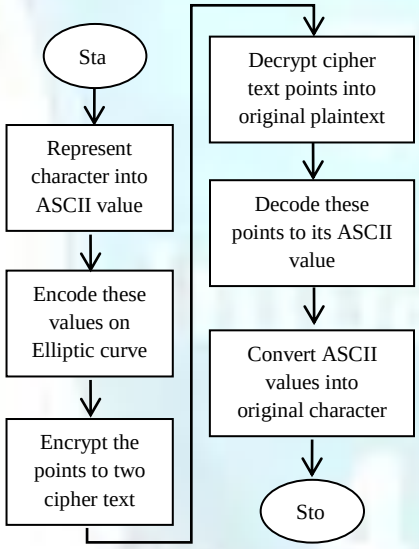

Fig 3: Flow Chart for Message Encoding and Decoding using Koblitz'z method

For getting the ASCII values and characters we have used a look up table as shown below:

Table 1: Look up Table used for Encoding and Decoding

Char	Taken Value	ASCII Value	Char	Taken Value	ASCII Value
0	0	48	.	75	46
to	to	to	/	76	47
9	9	57	:	76	58
A	10	65	;	78	59
to	to	to	<	79	60
Z	35	90	=	80	61
a	36	97	>	81	62
to	to	to	?	82	63
z	61	122	@	83	64
!	62	33	[	84	91
"	63	34	\	85	92
#	64	35	]	86	93
$	65	36	^	87	94
%	66	37	_	88	95
&	67	38	{	89	123
'	68	39	|	90	124
(	69	40	}	91	125
)	70	41	~	92	126
*	71	42	space	93	32
+	72	43	BS	94	10
,	73	44	TAB	95	11
-	74	45	newline	96	12

5. SINGLE ECC ENCRYPTION AND MULTIPLE ECC TIME COMPLEXITY ANALYSES

Plot of time taken against number of characters in a file in encryption process and decryption process in case of single ECC is as shown in figure 4(a). The solid line in the graph represents encryption time and dashed line represents decryption time.

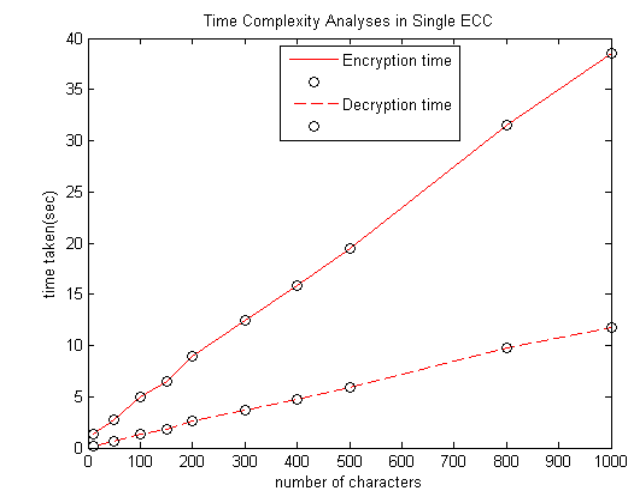

Fig 4(a): Time Taken in Single ECC.

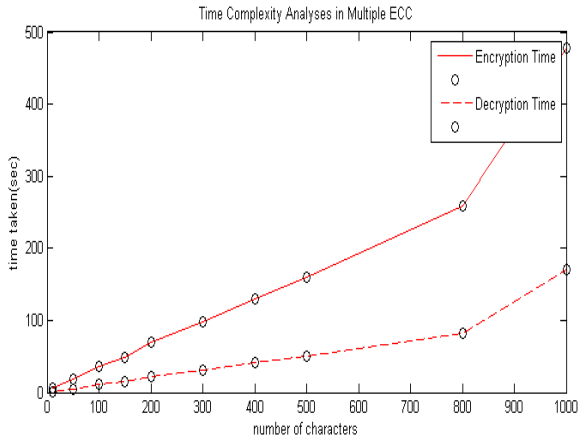

Fig 4 (b): Time complexity graph in Single ECC.

 DOI:**10.22362/ijcert/2016/v3/i11/XXXX**

Plot of time taken against number of characters in a file in encryption process and decryption process in case of multiple ECC is as shown in figure 4(b).

Table 2(a): Time Taken in single ECC.

S.N.	No of Char	Enc. Time	Dec. Time
1	10	1.3728	0.2119
2	50	2.7465	0.6248
3	100	4.9452	1.3264
4	150	6.4428	1.7546
5	200	8.9701	2.6052
6	300	12.4489	3.6054
7	400	15.8965	4.7824
8	500	19.4845	5.8656
9	800	31.5746	9.7813
10	1000	38.5010	11.7001
Single Enc. K=20, p=751, A=-1, B=188			

Table 2(b): Time Complexity in Multiple ECC.

S.N.	No of Char	Enc. Time	Dec. Time
1	10	6.2401	1.7316
2	50	18.2521	5.1948
3	100	35.6462	10.9669
4	150	48.3964	15.0385
5	200	69.6765	21.6977
6	300	98.3742	31.2158
7	400	129.0596	40.8099
8	500	159.1678	49.7331
9	800	258.1817	81.7601
10	1000	478.2198	170.1742
Single Enc. K=20, p=751, A=-1, B=188			
Multiple enc. k=20, p=2011, A=-1, B=188			
platform: Intel core i3 2.4 GHz, 2GB RAM			

As we can see in the graphs obtained, the time taken in Multiple ECC is larger for the same number of characters input as compared to single encryption. This shows that the time complexity increases by encrypting ciphertext multiple times in the encryption technique which in turn enhances the security of the data.

6. Flow Chart For Single ECC And Multiple ECC Encryption Technique

As we can see in figure 5, in Multiple ECC the plaintext is encrypted to get two ciphertext points and again these two points are encrypted to get four ciphertext points and the process is repeated in reverse to get the original plaintext message. Hence encrypting the plaintext again and again with same or different key multiple times makes an encryption technique a multiple encryption technique. This increases the security as well as complexity and makes it more and more difficult for an attacker to break the ciphertext.

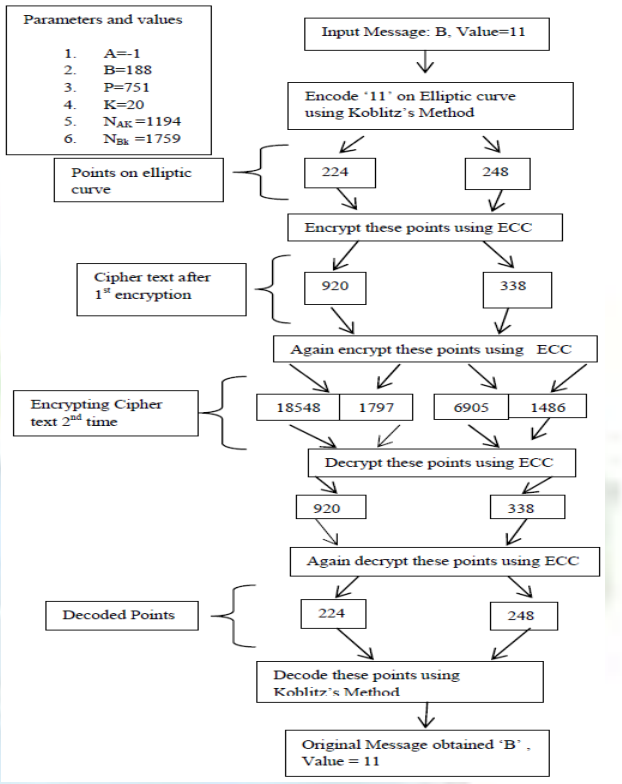

Fig 5: Multiple ECC on a single character

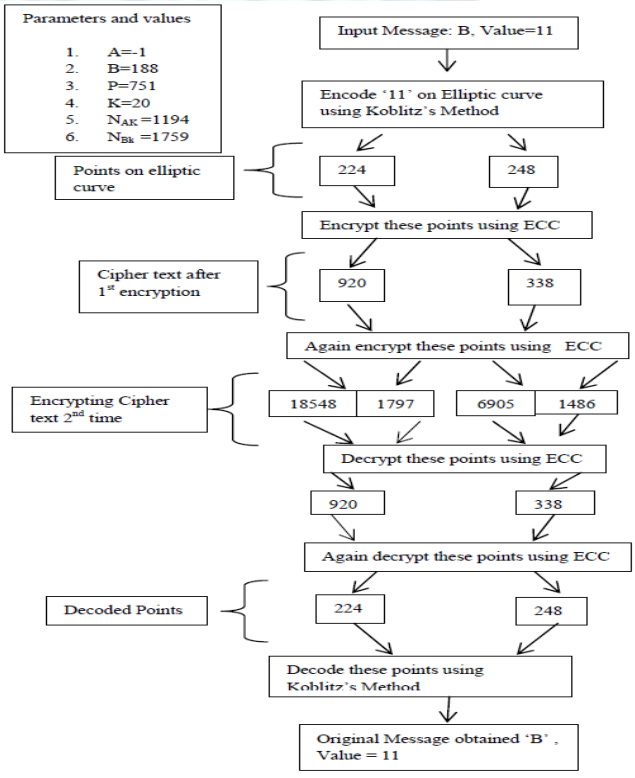

Fig 6: Decryption process

 DOI:**10.22362/ijcert/2016/v3/i11/XXXX**

7. CONCLUSION

In this paper, our work includes implementation of ECC and the encrypting the cipher text multiple times. It was observed that in multiple ECC time complexity increases as the cipher text is encrypted multiple times with the same or different keys in the process of encryption. The process of multiple encryption increases security and the scheme is preferable when high security requirements are needed excluding the time constraints. The said method can be further enhanced with help of multiphase encryption where we have number of phases where in each phase multiple encryptions can be performed.

ACKNOWLEDGMENT

The authors wish to thank faculty members of Computer Science and Engineering department of NERIST for valuable suggestions and comments in preparing this paper.

REFERENCES

[1] Anoop MS "Elliptic Curve Cryptography-An Implementation Guide" anoopms@tataelxsi.co.in.

[2] Himanshu Gupta and Vinod Kumar Sharma "Multiphase Encryption: A New Concept in Modern Cryptography" IJCTE 2013 Vol.5(4): 638-640 ISSN: 1793-8201 DOI: 10.7763/IJCTE.2013.V5.765 is referred.

[3] William Stalling "Cryptography and Network Security" book (fourth edition).

[4] N. Koblitz. "A Course in Number Theory and Cryptography", Springer-Verlag, second edition, 1994.

[5] W. Diffie and M. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard", June 1977, pp. 74-84.

[6] NIST Special Publication 800-78-2, "Cryptographic Algorithms and Key Sizes for Personal Identity Verification", February 2010.

[7] Darrel Hankerson, Julio Lopez Hernandez, Alfred Menezes, "Software Implementation of Elliptic Curve Cryptography over Binary Fields", 2000

[8] M. Brown, D. Hankerson, J. Lopez, A. Menezes, "Software Implementation of the NIST Elliptic Curves Over Prime Fields", 2001

[9] Certicom, "Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography", Version 1.0, September 2000

[10] Certicom, "Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters", Version 1.0, September 2000,

[11] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996

[12] Data Security for e-Transaction. Retrieved on April 12th 2008, from Weblink: http://www.comp.nus.edu.sg/~jervis /cs3235/set.html

[13] Ralph C. Merkle, Martin E. Hellman, "On the Security of Multiple Encryption, A technical note on Programming Technique & Data Structure" published in ACM, 1981, Volume 24, Number 7.

[14] M. Saikia, S.J. Bora, Md. A. Hussain "A Review on Applications of Multimedia Encryption" in ISBN: 987-81-8487-088-6 in national conference on Network Security- issues 2010, Tezpur University

[15] Vandana Thakur, Monjul Saikia "Comprehensive Survey of Multimedia Encryption Techniques" 26th National Conv. of Comp. Eng. held at the IEI (India), Assam February 4, 2012

[16] Boruah, Debabrat; Saikia, Monjul, "Implementation of ElGamal Elliptic Curve Cryptography over prime field using C," International Conference on Information Communication and Embedded Systems (ICICES), 2014, vol., no., pp.1,7, 27-28 Feb. 2014

[17] Kapoor, Vivek, Vivek Sonny Abraham, and Ramesh Singh. "Elliptic curve cryptography." Ubiquity 2008.May (2008): 7.

[18] Merkle, Ralph C., and Martin E. Hellman. "On the security of multiple encryption." Communications of the ACM 24.7 (1981): 465-467.

[19] Dahl, Ulf. "Data security system for a database having multiple encryption levels applicable on a data element value level." U.S. Patent No. 6,321,201. 20 Nov. 2001.

[20] Zhang, Linhua. "Cryptanalysis of the public key encryption based on multiple chaotic systems." Chaos, Solitons & Fractals 37.3 (2008): 669-674.

[21] Raju, G. V. S., and Rehan Akbani. "Elliptic curve cryptosystem and its applications." Systems, Man and Cybernetics, 2003. IEEE International Conference on. Vol. 2. IEEE, 2003.

[22] Önen, Melek, and Refik Molva. "Secure data aggregation with multiple encryption." European Conference on Wireless Sensor Networks. Springer Berlin Heidelberg, 2007.

[23] Bhati, Sunita, Anita Bhati, and S. K. Sharma. "A New Approach towards Encryption Schemes: Byte–Rotation Encryption Algorithm." Proceedings of the World Congress on Engineering and Computer Science. Vol. 2. 2012.

