Journal of Theoretical and Applied Information Technology
20th February 2016. Vol.84. No.2
© 2005 - 2016 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURE METHOD FOR EMBEDDING PLAINTEXT ON AN ELLIPTIC CURVE USING TDMRC CODE AND KOBLITZ METHOD

[1]CIMI THOMAS M, [2]DR. VARGHESE PAUL

[1]Research Scholar, Department Of Computer Science, Karpagam University, Coimbatore, India

[2] Research Co-ordinator, Department of IT, Cochin University Of Science and Technology, Kochi, India

Email: [1]cimithomas@yahoo.co.in, [2]vp.itcusat@gmail.com

ABSTRACT

The web applications are becoming popular and there is an increase in the amount of sensitive information transmitted over internet. Encryption algorithms play an important role in ensuring the security of data. Elliptic Curve Cryptography (ECC) is a public key encryption method which can be used for message encryption, key exchange and for creating digital signatures. ECC is considered as a good alternative to RSA and other public key encryption algorithms as it offers high level of security with smaller key sizes. ECC is well suited for applications which run on devices with power and memory constraints like smart cards and cell phones. SMS messages can be encrypted using ECC without degrading the performance of mobile devices. In elliptic curve analog of ElGamal system, the plaintext message has to be encoded into an elliptic curve before encryption. In this paper different methods suggested in the literature for encoding characters in the text message to an elliptic curve are examined and a new method for encoding the characters to the curve using TDMRC code is proposed. TDMRC code is a symmetric key encryption algorithm and is polyalphabetic. The polyalphabetic nature of TDMRC code can be utilized to defeat cryptanalysis based on letter frequencies .The proposed encryption scheme will be a reliable scheme and will offer high security as the plaintext is encrypted twice.

Keywords: *Encryption, Decryption, Elliptic Curve Cryptography, Encoding, Decoding*

1. INTRODUCTION

Elliptic curve cryptography was introduced in mid-1980's by Victor Miller[1] and Neil Koblitz [2].Applications using elliptic curve cryptography were not popular initially but now there are many protocols and products which use ECC for encryption, authentication and for producing digital signatures. A number of research papers have been published showing the utilization of ECC for enhancing the security of web applications. The application of ECC in pervasive computing environment is studied in [3].ECC can provide high security with smaller key sizes and so they are best choice for securing applications running on memory and power constraint devices like mobile devices. Financial institutions have started using SMS to communicate with customers and so the security of SMS is of great concern. A survey of existing security schemes for SMS and together with a point *O,* called the point at infinity or the zero point. In the cryptographic schemes, their performance impact on mobile devices were presented in [4] and is concluded that elliptic curve cryptography is suitable for SMS security because of smaller key sizes. Elliptic Curve ElGamal system [2] is widely used for encrypting short messages and is a secure scheme. But the advancement in both computing technology and cryptanalysis demand the enhancement of existing scheme. This research work aims to develop a secure encoding method which can enhance the security of elliptic curve ElGamal system by making the scheme polyalphabetic.

1.1 Overview Of Elliptic Curve Cryptography

Elliptic Curve Cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. An elliptic curve defined over a field F is the curve defined by the equation $y^2=x^3+ax+b$ elliptic curves over two finite fields are mostly used, prime field Fp, where p is a prime and binary field F_2^m, where m is a positive integer. Prime curves are more suitable for software applications and the equation of the elliptic curve over Fp is defined as y^2 mod p =(x^3+ax+b) mod p where ($4a^3+27b^2$) mod p !=0 and x, y, a,b Є [0,p-1].

The fundamental operation in elliptic curve arithmetic is scalar point multiplication which computes Q=kP, a point P on the curve multiplied k times to get another point Q on the curve. Scalar multiplication is performed by a combination of point additions and point doublings. For example, 11P can be expressed as (2*((2*(2*P)) +P)) +P. The operations of point addition and point doubling are explained as follows. If A= (x_A,y_A) and B=(x_B,y_B) are two points on an elliptic curve y^2 mod p =(x^3+ax+b) mod p, then C=A+B= (x_C,y_C) is determined by the rules [5]: x_C= (λ^2-x_A-x_B)mod p, y_C=(λ(x_A-x_C)-y_A)modp where λ= ((y_B-y_A)/ ($x_B x_A$))mod p if A!=B and λ= ((3x_A^2+a)/(2y_A))modp if A=B.

The security of ECC rests on the hardness of discrete logarithm problem over the points on the elliptic curve. Elliptic Curve Discrete Logarithm Problem (ECDLP) states that given a base point P and a point Q=kP lying on the curve, it is hard to determine k.

Elliptic Curve analog of Massey-Omura system and ElGamal system are described in [2]. In Elliptic curve ElGamal system, the plaintext message has to be encoded into an elliptic curve before encryption. Each character in the message is mapped to a point P_m on the curve and then the point P_m is encrypted and transmitted as a pair of points (kG, P_m +kP_B), where k is a random integer chosen by the Sender A,G is the base point and P_B is the public key of receiver B. To read the message, B multiplies the first point with his private key and subtracts the result from the second point in the pair.

When the plaintext is encrypted using Elliptic Curve ElGamal System, the ciphertext obtained is a monoalphabetic cipher. Most common cryptanalysis on monoalphabetic cipher is based on frequency analysis. The frequency of letters in ciphertext can be directly mapped to letter frequency of English language. An efficient method to defeat cryptanalysis based on letter frequency is to hide the letter frequency of plaintext using polyalphabetic ciphers. Elliptic Curve ElGamal System can be made polyalphabetic by incorporating a polyalphabetic cipher at the encoding stage. In this paper different methods suggested in the literature for encoding characters to an elliptic curve is studied and a secure encoding method using TDMRC code is proposed.

1.2 Time Dependent Multiple Random Cipher Code (TDMRC Code)

TDMRC code [6] is an ASCII value based symmetric encryption method. TDMRC code was designed to use in fault tolerant hard real time systems to prevent eaves dropping but it can be used to encrypt any text or multimedia data. Data is treated as a chain of ASCII characters and each ASCII character is substituted with TDMRC virtual character. TDMRC character set is generated by pseudo random number generation technique. Depending upon the random seed, the codes will change.

TDMRC code is Time Dependent and Poly Alphabetic .Master key is derived from real time clock with accuracy to centisecond to form 8 digit number. Poly Alphabetic Coefficient (P) decides the number of codes used corresponding to each plain text character.

1.2.1 Algorithm to generate TDMRC code and encrypt messages

Step: 1 Choose poly alphabetic coefficient P (usually single digit number).
Step: 2 Choose P number of sub keys, each of 4 digits.
Step: 3 Derive Master key by reading the system time with accuracy to centisecond to form 8 digit number.
Step: 4 Each sub key is multiplied by master key, and 8 digits from the extreme right is taken from the product to form P random seeds.
Step: 5 Generate P number of random series using the P number of random seeds derived in the above step. The random series have 256 unique values in the range 0-255.
Step: 6 The data to be encrypted is taken in blocks of P number of characters, the ASCII value of each plain text character is found and is substituted by corresponding value in the random series to obtain cipher text character. The first character is substituted by the element from the first series and the second character from second series and so on.

1.2.2 Algorithm for decryption.

Step: 1 The same keys used for encryption are used to regenerate P random seeds and P number of random series with 256 unique elements.
Step: 2 Take cipher text in blocks of P number of characters. The ASCII value of each character is found and substitute each character with the string character of the serial number value in the random series to obtain plain text character. The first character is substituted by the element from the first series, second character from second series and so on.

2. RELATED WORKS

Different methods are suggested in the literature for encoding message to an elliptic curve. The simplest method is to use the ASCII value of characters in the message to find the points on the curve. A curve with 256 points can be selected and each point can be directly mapped to the ASCII value of character. But this method is inefficient in terms of security. Koblitz has given a probabilistic method for encoding the points to the curve in [2], where the message is first converted to a series of numbers. Each number 'n' is then multiplied by an auxiliary base parameter 'k' and take it as the x coordinate of the point and try to solve for y. If it can't be solved then take x=nk+1, nk+2 …nk+ (k-1) and find y. In this way the number n is encoded to the point(x, y) on the curve. At the receiving end, the point (x,y) is decoded to the number n by taking the greatest integer less than x/k. An implementation of Koblitz method is given in [7]. A method for encrypting messages using elliptic curves over finite field is proposed in [8] where each character in the message is encoded to a point on the curve by using a code table which is agreed upon by communicating parties and each message point is encrypted to a pair of cipher points. These cipher points are decoded back to characters using the same code table before transmission. At the receiving end before decryption the characters are converted back to cipher points on the curve using the same code table. To make the algorithm polyalphabetic a random number is used for encrypting characters in the message and this random number is different for each character. In order to encrypt a message with 10 characters, 10 random numbers are needed. In [9] authors have suggested the use of a nonsingular matrix to map same characters in the message to different points on the curve. In [10], authors have suggested the use of a two dimensional alphabetic table to convert plain text characters to two dimensional co-ordinate representation. These points are then added with elliptic curve points for encryption. To defeat cryptanalysis based on letter frequency attack, in [11] the message is encrypted using hill cipher algorithm [5] and ASCII value of cipher characters are used to find points on the elliptic curve. An implementation of message encryption using ECC is discussed in [12] where an affine point is chosen first and a character is transformed to a point on the curve by multiplying its ASCII value with the chosen affine point. This point is then encrypted by ElGamal elliptic curve encryption method. In this method the same characters in the message are mapped to same point on the elliptic curve and thus encrypted to the same cipher points. In [13] authors have proposed an extension of Koblitz method by using mirrored elliptic curves. If Koblitz method fails to find a point on the curve for a character 'c', and if there exist a point (-c, y) on the curve, then the embedding point can be taken as (-c,-y). The method suggested in [14] applies transposition techniques on the plain text before using Koblitz method to encode message to the curve. In [15] authors have suggested the use of an initial vector and XOR operation is done on plain text character and initial vector before the characters are mapped to the curve. Thus encryption of mapped points will result in a polyalphabetic cipher. The methods used to make the encoding polyalphabetic require extensive calculations, need more computing time for long messages and may not be suitable for memory constraint devices.

3. PROPOSED METHOD DESCRIPTION

The proposed method uses TDMRC code with Koblitz method to encode message characters to an elliptic curve. The aim of the method is to provide an additional level of security in the elliptic curve ElGamal system by making use of the polyalphabetic nature of TDMRC code. The characters in the message are first converted in to TDMRC virtual characters and these virtual characters are then encoded to the curve using Koblitz method. Since TDMRC code is Polyalphabetic, the same characters in the message are converted to different virtual characters and thus mapped to different points on the curve. These points can be converted to cipher points by ElGamal encryption. The letter frequencies in the plain text are not preserved in the cipher text and thus the cryptanalysis based on letter frequency can be defeated. This method is suitable for encrypting short messages.

4. PROPOSED ALGORITHM

4.1 Algorithm For Encoding Plaintext To The curve

Step 1: Choose an elliptic curve Ep (a,b).
Step 2: Generate TDMRC code.
Step 3: Take the first character of the plaintext. Let its ASCII value be 'n_1'.Substitute it with the corresponding value in the first random series and let the new value be 'n_2'.
Step 4: Multiply n_2 with 2P, where P is the polyalphabetic coefficient chosen during the generation of TDMRC code.
Step 5: Take $x=n_2*2P$ and try to solve for y in the equation for elliptic curve.
Step 6: If a solution for y cannot be found for x in the chosen elliptic curve, try to solve y for $x=(n_2*2P)+1$, $x=(n_2*2P)+2$, $x=(n_2*2P)+3$ …. $x=(n_2*2P) + (2P-1)$ until y can be solved.
Step7: This point (x,y) on the elliptic curve corresponds to the first character in the plaintext.
Step 8: The procedure is repeated for all other characters in the plain text.

The point (x,y) can be encrypted to two cipher text points using ECC ElGamal encryption and can be send to the receiver. The receiver will decrypt the cipher text to the point (x,y).The next step is to decode the point (x,y) to the number n_2 and then apply TDMRC decryption algorithm to get plain text character.

4.2 Algorithm For Decoding The Message

Step: 1 Find out x/2P. Return the greatest integer less than or equal to x/2P, which will be the number n2.
Step: 2 Apply TDMRC decryption algorithm and obtain n1.

5. IMPLEMENTATION OF THE PROPOSED ALGORITHM AND RESULTS

The proposed algorithm is implemented in MATLAB for a chosen curve and message. TDMRC codes are generated by taking suitable master key and sub keys. Polyalphabetic coefficient P is taken as 3. The part of the TDMRC code for ASCII values 65-90(A-Z) is shown in the Table 1. Let the plaintext to be encrypted is "SUCCESSFUL". The ASCII value of the characters in the plaintext are 83,85,67,67,69 83,83,70,85,76.Since the poly alphabetic coefficient is 3,there are 3 random series(TDMRC codes) and they are shown in column3 to column10 in Table 1.

Applying TDMRC encryption algorithm the above plain text is converted to virtual characters YtvumRYH0) with ASCII values 89,116,118,117,109,82,89,72,48,41 respectively. These values are mapped to points on the elliptic curve by following Step4 to Step8 in the proposed algorithm.

The elliptic curve chosen has parameters p(787), a(1) and b(125) .The message characters are encoded to the following points on the curve. (535,213),(699,41),(708,258),(703,286),(656,44), (492,265),(535,213),(433,117),(289 ,348),(246,155) and there are nine different points. Figure 1 shows the nine different mapped points.

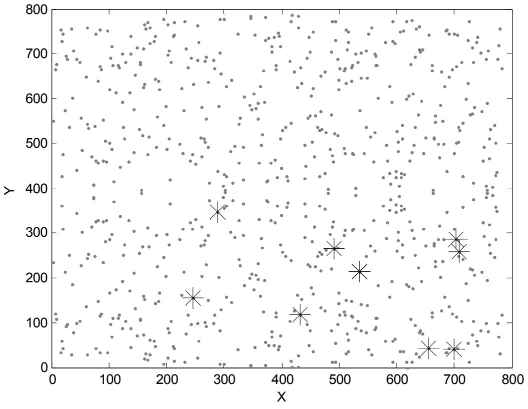

Figure 1:Encoded points using Koblitz Method

To decode the point (x,y),divide x/2P and return the greatest integer less than or equal to x/2P.For example to decode (535,213),divide 535/6 =89.167 and return 89.

The same plaintext SUCCESSFUL was encoded to the curve using only Koblitz method skipping Step2 and Step3 of the proposed algorithm. Here the ASCII value of the characters are taken as the value for 'n_2' in Step4.The plaintext is mapped to the points(498,167),(510 ,308),(406,249),(406,249),(415,240),(498,167),(498 167),(421,127),(510,308),(456,315) and there are only six different mapped points which is shown in Figure 2.

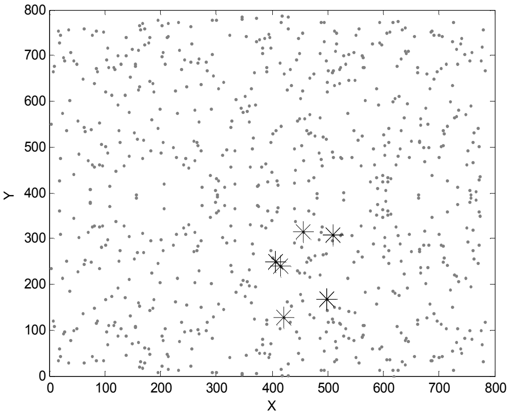

Figure 2:Encoded points without using Koblitz Method

Results of the implementation are summarized in the Table 2 and it is clear that the number of different encoded points are more when TDMRC code is used with Koblitz method increasing the security of encoding.

Table 2: Results of Implementation

Plain text	ASCII Value	Value of TDMRC character	Encoded points using TDMRC with Koblitz method	Encoded points without TDMRC
S	83	89	(535,213)	(498,167)
U	85	116	(699,41)	(510,308)
C	67	118	(708,258)	(406,249)
C	67	117	(703,286)	(406,249)
E	69	109	(656,44)	(415,240)
S	83	82	(492,265)	(498,167)
S	83	89	(535,213)	(498,167)
F	70	72	(433,117)	(421,127)
U	85	48	(289,348)	(510,308)
L	76	41	(246,155)	(456,315)

The same characters in plaintext are mapped to different points. These encoded points can be encrypted using ElGamal encryption. The use of TDMRC code makes the encryption polyalphabetic and cryptanalysis based on letter frequency of plaintext can be defeated. High values of polyalphabetic coefficient increases the efficiency of encoding but requires more computing time. When this algorithm is used to encrypt long messages, TDMRC codes can be generated and stored in advance and hence time delay during TDMRC encryption and decryption can be reduced.

6. CONCLUSION

Elliptic curve cryptography has the ability to provide adequate security with smaller key size and can be used for encrypting text messages. Elliptic Curve ElGamal system is a secure method and is widely used for encrypting text messages. But the advancement in the areas of cryptanalysis demands the enhancement of existing scheme. We have proposed a method to encode plaintext message to an elliptic curve which provides an additional level of security for Elliptic Curve ElGamal Encryption. In the proposed method plaintext is first encrypted using a symmetric key encryption scheme before encoding the points to elliptic curve using Koblitz method. The advantage of the method is that the same characters in the plain text will be mapped to different points on the curve which can then be encrypted to different cipher points using Elliptic Curve ElGamal encryption. The use of TDMRC code makes the encryption polyalphabetic and thus the letter frequency attack can be defeated. The proposed method is a strong and reliable scheme as the plaintext is encrypted twice and is suitable for encrypting messages. The method is implemented by taking polyalphabetic coefficient as 3.Increasing the value of polyalphabetic coefficient increases the security of encryption algorithm. Limitation of the method is that high values of polyalphabetic coefficient increases the TDMRC encryption and decryption time. The method can be improved in future by using Unicode characters instead of ASCII as Unicode represents most of the written languages in the world.

REFERENCES

[1] Victor S. Miller, “Use of elliptic curves in cryptography”, H.C Williams Edition, *Advances in Cryptology CRYPTO’85*, Springer-Verlag,1986 vol.218 of Lecture Notes in Computer Science, pp. 417-426,

[2] Neal Koblitz , “Elliptic Curve Cryptosystems”, *Mathematics Of Computation*, Volume 48,Number 177,January 1987,Pages 203-209.

[3] Vivek Katiyar,Kamlesh Datta,Syona Gupta,” A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment”, *International Journal Of Computer Applications*,Vol1, No:10,December 2010.

[4] Mohammed Wasim Khan," SMS Security in Mobile Devices:A Survey",*Int.J.Advanced Networking and Applications*,Vol05,Issue:02, Pages:1873-1882

[5] William Stallings, Cryptography and Network Security,Principles and Practices,Fourth Edition,Prentice Hall,November 2005

[6] Varghese Paul, "Data Security in Fault Tolerant Hard Real Time System-Use of Time dependent Muitiple Random Cipher Code", Ph.D Dissertation, Cochin University Of Science and Technology, April2003.

[7] Padma Bh, D Chandravathi, P Prapoorna Roja, "Encoding and Decoding of a message in the implementation of elliptic curve cryptography using Koblitz's method",*Internal Journal on Computer Science and Engineering,*Vol 02,No. 05,2010,1904-1907.

[8] D.Sravana Kumar, CH Suneetha, A.Chadrasekhar, "Encryption of data using Elliptic Curve over finite fields",*International Journal of Distributed and Parallel Systems*, Vol 3, No:1, January 2012.

[9] F.Amounas, E.H.EI Kinani, "Fast Mapping Method based on Matrix Approach for Elliptic Curve Cryptography",*International Journal Of Information and Network Security*,Vol-1,No.2,June2012,PP 54-59.

[10] Tarun Narayan Shankar, G.Sahoo," Cryptography with Elliptic Curves",*International Journal Of Computer Science and Applications,* Vol 2,No.1,April/May 2009.

[11] Komal Agarwal,Anju Gera,"Elliptic Curve Cryptography with Hill Cipher Generation for secure Text Cryptosystem",*International Journal Of Computer Applications*, Vol 106-No.1,November 2014.

[12] S.Maria Celestin Vigila,K Muneeswaran, "Implementation of text based cryptosystem using elliptic curve cryptography",*ICAC 2009,IEEE*,PP 82-85.

[13] M.S Srinath, V.Chandrasekaran,"Elliptic Curve Cryptography using Mirrored Elliptic Curves over Prime Fields". *International Conference on Information and Knowledge Engineering*,IKE2010, PP 271-277.

[14] Santhoshi Pote, "Enhancing the Security of Koblitz's Method Using Transposition Techniques for Elliptic Curve Cryptography", *International Journal of Research in Engineering & Advanced Technology"*, Vol2, Issue 6, Dec-Jan 2015.

[15] Jayabhaskar Muthukuru, Bachala Sathyanarayan, "Fixed and Variable Size Text Based Mapping Techniques using ECC",*Global Journal Of Computer Science and Technology*,vol12,Issue 3 ,Version 1,Feb 2012.

Table-1 : TDMRC codes for ASCII values A-Z

		Plaintext									
ASCII Values		S	U	C	C	E	S	S	F	U	L
A	65	47	122	77	47	122	77	47	122	77	47
B	66	62	107	125	62	107	125	62	107	125	62
C	67	117	97	118	117	97	118	117	97	118	117
D	68	64	44	93	64	44	93	64	44	93	64
E	69	39	109	99	39	109	99	39	109	99	39
F	70	61	72	34	61	72	34	61	72	34	61
G	71	86	119	101	86	119	101	86	119	101	86
H	72	75	92	71	75	92	71	75	92	71	75
I	73	35	95	59	35	95	59	35	95	59	35
J	74	37	105	70	37	105	70	37	105	70	37
K	75	96	56	65	96	56	65	96	56	65	96
L	76	41	42	103	41	42	103	41	42	103	41
M	77	66	98	67	66	98	67	66	98	67	66
N	78	50	78	111	50	78	111	50	78	111	50
O	79	69	94	102	69	94	102	69	94	102	69
P	80	55	43	90	55	43	90	55	43	90	55
Q	81	123	85	81	123	85	81	123	85	81	123
R	82	84	74	87	84	74	87	84	74	87	84
S	83	89	112	82	89	112	82	89	112	82	89
T	84	100	114	76	100	114	76	100	114	76	100
U	85	115	116	48	115	116	48	115	116	48	115
V	86	120	49	104	120	49	104	120	49	104	120
W	87	38	52	40	38	52	40	38	52	40	38
X	88	73	63	88	73	63	88	73	63	88	73
Y	89	54	113	92	54	113	92	54	113	92	54
Z	90	83	53	95	83	53	95	83	53	95	83