Enhancing Security of Elliptic Curve ElGamal Encryption Using a Polyalphabetic Symmetric Cipher

Cimi Thomas M[1], S .Sheeja[2]

ABSTRACT

In today's digital world, we are dependent on internet for a variety of things and in many situations we have to disclose our personal information. Preventing an unauthorized person from viewing and using our personal information is a great challenge. Most of the websites where online transactions take place are secured by security protocols. These security protocols use various symmetric key and asymmetric key encryption algorithms. Elliptic curve cryptography is an asymmetric key encryption algorithm which is suitable for encrypting short messages. In this paper we present a method to enhance the security of Elliptic Curve ElGamal System. The security of El Gamal system is improved by using a polyalphabetic cipher at the time of mapping plaintext message to an elliptic curve.

Keywords : Encryption, Decryption, Elliptic Curve Cryptography, Polyalphabetic Cipher, TDMRC code

I. INTRODUCTION

In today's digital world, many financial transactions take place over internet. Online shopping has become popular so is net banking. Though these websites are secured with strong security protocols, there are reports of sites being hacked and customers losing their money. Security protocols use encryption algorithms for providing confidentiality, authorization and for key exchange. The commonly used asymmetric key encryption in security protocol is RSA. But in last few years the key size of RSA is increased to withstand attacks and large keys have created burden on web servers. Elliptic curve cryptography is an asymmetric key encryption scheme which can be used for creating digital signatures, key exchange and also for message encryption. The advantage of using ECC is high security with smaller keys.

A. Overview of Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) was introduced by Victor Miller [1] and Neil Koblitz [2]. Though ECC was introduced in mid-80, it was not a popular encryption technique until last decade. But now ECC is an active research area and there are many protocols, products and standards which use ECC for asymmetric key encryption. ECC is suitable for securing applications running in power constraint devices like mobile phones.

Elliptic Curve Cryptography uses elliptic curves over a finite field F and elliptic curves are defined by the equation $y^2=x^3+ax+b$,together with a point O, called

[1]Research Scholar, Department Of Computer Science, Karpagam University, Coimbatore, India
cimithomas@yahoo.co.in,
[2] Associate Professor, Department of Computer Applications, Karpagam University, Coimbatore, India
sheejaajize@gmail.com

as the point at infinity. Elliptic curves over prime field F_p are more suitable for software implementation where p is a large prime number. The equation of the elliptic curve over F_p is defined as $y^2 \bmod p = (x^3+ax+b) \bmod p$ where $(4a^3+27b^2) \bmod p!=0$ and x, y, a,b ^{a} [0,p-1]. The security of ECC relies on hardness of discrete logarithm problem defined over the points on the elliptic curve. Elliptic Curve Discrete Logarithm Problem (ECDLP) is explained as for a base point P and a point Q=kP lying on the curve, it is hard to determine k.

Elliptic Curve analogue of ElGamal system is described in [2]. For message encryption using Elliptic curve ElGamal system, the characters in the plaintext message has to be mapped to an elliptic curve before encryption. Each character is mapped to a point P on the curve and the point P is then encrypted and transmitted as a pair of points (kG, $P+kP_B$), 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. The cipher text obtained is a mono alphabetic cipher. Since the same characters in the plaintext are mapped to same characters in the cipher text, letter frequency based cryptanalysis is possible. One method to defeat frequency based cryptanalysis is to make the encryption scheme polyalphabetic. In this research work TDMRC code [3] , which is a symmetric key encryption algorithm is used before mapping the points to the curve and the application of TDMRC code makes the encryption scheme polyalphabetic.

B. Time Dependent Multiple Random Cipher Code (TDMRC) Code

TDMRC code is an ASCII value based symmetric encryption method. Data in any form can be encrypted by treating it as a chain of ASCII characters. Each ASCII character is then substituted with TDMRC virtual character. The features of TDMRC code are (i) Time dependent as master key is calculated from real time clock (ii) Polyalphabetic and Poly Alphabetic Coefficient (P) decides the number of codes used in the algorithm. (iii) Pseudorandom number generation technique is used to generate TDMRC character set. The algorithm for TDMRC encryption and decryption are explained in [3].

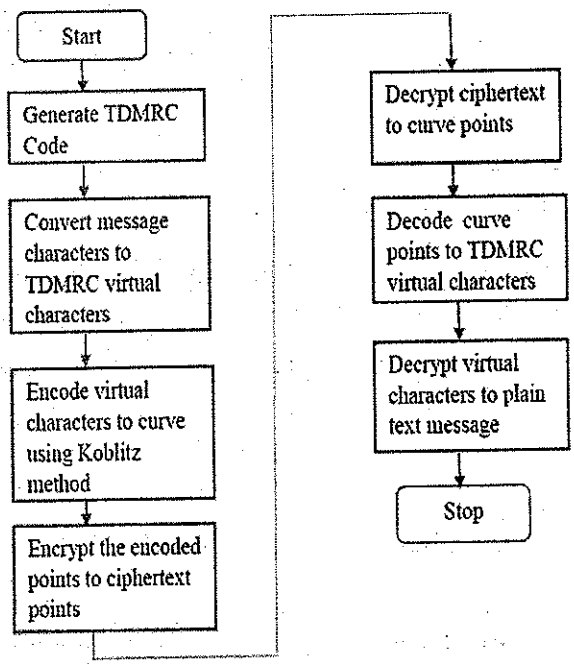
II. Related Works

Many algorithms are available in the literature for mapping points to the elliptic curve and to make ElGamal encryption polyalphabetic. In [4] characters in the plaintext are mapped to an elliptic curve with the help of a code table agreed upon by both communicating parties. They make use f random numbers while encrypting characters to make the algorithm polyalphabetic. In [5] authors have used a non-singular matrix to map same characters in the message to different points on the curve. To make the algorithm polyalphabetic, in [6] the message is encrypted using hill cipher algorithm before mapping the points to the elliptic curve. In [7] authors have applied transposition techniques on the plain text before using Koblitz method to encode message to the curve. The authors of [8] have done an XOR

operation on plain text character and initial vector before the characters are mapped to the curve and thus encryption of mapped points result in a polyalphabetic cipher.

III. Methodology

The proposed method provides an additional layer of security in the elliptic curve ElGamal system. This is done by encrypting plain text using TDMRC encryption before mapping the points to elliptic curve. The flowchart of the proposed method is shown in Fig.1 below.



To generate TDMRC code, a Polyalphabetic coefficient P is chosen, where P is a single digit number . P subkeys of four digits have to be chosen. Master key has to be derived by reading the system time with accuracy to centisecond to form 8 digit number. P random seeds have to be generated by multiplying master key with sub keys and taking 8 characters from the right. P number of random series have to be generated using the random seeds. The random series have 256 unique values in the range 0-255.

TDMRC code is a block cipher and block size is same as the value of P. To convert message characters to TDMRC virtual characters, ASCII value of each plain text character has to be found and has to be substituted by corresponding value in the random series to obtain cipher text character. The first character has to be substituted by the element from the first series and the second character from second series and so on.

An elliptic curve Ep (a, b) has to be selected and the virtual characters have to be mapped to the curve using Koblitz method[2]. Let 'n' be the ASCII value of the first virtual character. 'n' is multiplied by an auxiliary base parameter 'k' .In this method k is taken as 2P, polyalphabetic coefficient. The product of 'n' and 'k' is taken as the x coordinate of the point and y is found out by substituting x in elliptic curve equation.to solve for y. If y can't be solved then try by taking x=nk+1, nk+2 ...nk+ (k-1) and find y. (x, y) will be the encoded point. The procedure is repeated for all other characters in the plain text.

After encoding, the point (x,y) can be encrypted to two cipher text points using ECC ElGamal encryption. Since TDMRC code is used before encoding, same characters in the message are mapped to different points on the curve and they are encrypted to different cipher points and thus the encryption becomes polyalphabetic.

ElGamal decryption is used to decrypt the cipher text back to the point (x,y).Then the point (x,y) is decoded to the value 'n'. This is done by dividing x/2P. The greatest integer less than or equal to x/2P, will be the number n TDMRC decryption algorithm is applied to convert virtual characters to plain text character.

I. Results

Proposed method is implemented in Matlab by choosing proper curve parameters. TDMRC code is generated by taking polyalphabetic coefficient P as 3. The elliptic curve chosen has parameters p(809), a(1) and b(135). Let the plaintext to be encrypted is "IMPLEMENT". This text is first mapped to the curve without applying TDMRC code and we got only 7 different curve points as the letters 'M' and 'E' are repeated. But when the text is mapped according to the proposed method after applying TDMRC code, we get 9 different points as same characters are not mapped to same points. These mapped points are then converted to cipher points using ElGamal encryption. The result of encoding is shown in Table1.

TABLE 1
RESULTS OF IMPLEMENTATION

Plain text	Encoded points using TDMRC with Koblitz method	Encoded points without TDMRC
I	(210,340)	(438,265)
M	(593,117)	(462,87)
P	(543,134)	(480,395)
L	(248,54)	(456,227)
E	(656,150)	(415,196)
M	(402,384)	(462,87)
E	(236,209)	(415,196)
N	(468,104)	(468,104)
T	(456,227)	(504,260)

V. Discussion

The implementation results show that the use of TDMRC code gives more cipher points. By incorporating a polyalphabetic symmetric key encryption at the encoding stage ElGamal encryption scheme is made polyalphabetic. Thus cryptanalysis based on letter frequency can be defeated. Monoalphabetic ciphers are not safe as frequency of letters in the ciphertext can be directly mapped to frequency of letters in the English alphabet. The execution time of the proposed method is almost same as the time for normal encoding. The number of TDMRC codes generated depends on Polyalphabetic coefficient P .When more codes are used, algorithm will be more secure but more codes increases execution time which is undesirable. In power constraint devices, TDMRC encryption and decryption can be done using previously generated codes to avoid time delays.

VI. Conclusion

Reliable and strong encryption schemes are available to secure data transmitted over network. But increased computing power and advancement in cryptanalysis requires new encryption schemes or enhancement of existing schemes. Elliptic curve cryptography can provide adequate security with smaller key size without creating burden on processors. Elliptic Curve ElGamal system is widely used for encrypting text messages. The proposed method makes Elliptic Curve ElGamal Encryption more secure by using a symmetric polyalphabetic cipher. Plain text characters are first converted to

TDMRC virtual characters and these virtual characters are mapped to curve points and same characters will be mapped to different points. When these points are encrypted using ElGamal encryption, the resulting cipher points are also polyalphabetic. Thus the ElGamal encryption will be resistant to letter frequency attacks. Since plain text is encrypted twice the proposed method is strong and reliable.

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] P.Varghese, *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, April 2003.

[4] 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.

[5] 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.

[6] 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.

[7] Santhoshi Pote, *Enhancing the Security of Koblitz's Method Using Transposition Techniques for Elliptic Curve Cryptography*, International Journal of Research in Engineering & Advanced Technology", Vol 2, Issue 6, Dec-Jan 2015.

[8] 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.

AUTHOR PROFILES

Ms. Cimi Thomas. M received master's degree in Computer Applications from Cochin University of Science And Technology in 2002. She is a research scholar of Karpagam University, Coimbatore and Assistant Professor at Waljat College Of Applied Sciences, Oman. She has 10 years of teaching experience and has published paper in International journal. Her research interests are in Cryptography and Distributed Computing.

Dr. S. Sheeja, is currently working as Associate Professor and Head of the Department of Computer Applications at Karpagam University, Coimbatore. She had completed Ph.D in Computer Science at Bharathiar University in 2015. She has more than 13 years of teaching experience to her credit. Her primary research interests are related to Computer Networks, Mobile Adhoc Networks, Mobile Computing, Image Processing and Data mining. She has achieved best paper award in IEEE International Conference in the year 2014. She has published more than 10 papers in International Journals and conferences. At present she is guiding 8 Ph.D and 1 M.Phil scholars. She is also an editor for Journal of Computer Science.