International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-7)

Research Article | **July 2017**

A Novel Hybrid Encryption Method for Multimedia Encryption Using Elliptic Curve Cryptography and TDMRC

Sreekala M
Research Scholar, Department of Computer Applications,
Cochin University of Science and Technology,
Kerala, India

Dr. Varghese Paul
Professor, Department of Information Technology,
Rajagiri School of Engineering and Technology,
Kerala, India

Abstract—

We are in the era of digital revolution and the benefits are remarkable. People are much dependent on digital technology and can't survive without it. With the advancement of Internet and its applications, we share a wide range of data including texts, images, audios and videos in a more extensive space and time scope that we never had before. This increases the need for security day by day. Cryptography is an art of Science that uses complex logic in order to design powerful encryption techniques. Both symmetric and asymmetric key encryptions have their own advantages. Time Dependant Multiple Random Cipher(TDMRC) code is one of the best symmetric encryption schemes. Elliptic curve cryptography(ECC) is widely used because of its less key size and faster key generation. This paper proposes a new method of hybrid encryption method using ECC and TDMRC.

Keywords— ECC, TDMRC, Text Encryption, Image Encryption, Audio Encryption, Video Encryption

I. INTRODUCTION

In today's society, multimedia plays an important role in human life. It has explosive growth in the area of entertainment, politics, military, business, and industries. Also, threats to multimedia data increased with the considerable growth of the Internet. Data can be easily hacked by unauthorized persons. Secure transmission of multimedia involves provision for confidentiality, integrity, and ownership. Encryption is the most important part of security. It helps us to be safe in our online transactions, cell phone conversations etc. This paper discusses how encryption can be done in multimedia data using ECC. Multimedia covers textual data, images, audios, and videos. Recent advancements in technology demand the protection of multimedia data nowadays. In the year 1985, Victor Miller and Neal Koblitz independently developed a new public key cryptosystem called Elliptic curve cryptography which is smaller in key size and faster than RSA. The recent advances in the computer industry and communications create a market for digital multimedia distribution through open networks. In open networks, confidentiality is one of the primary concerns for commercial uses of multimedia contents [1].

Hybrid encryption combines the features of both symmetric and asymmetric key encryptions. Encryption is done using receiver's public key and generates a new symmetric key for data encapsulation. Both the plain text and key are encrypted using receiver's public key under the data and key encapsulation scheme and are send to receiver. Decryption is done by using receiver's private key. This paper proposes a new technique to implement multimedia encryption using ECC and TDMRC.

This paper is organized as follows: Working of ECC is described in section 2. In section 3, encryption of textual data using ECC is described. The theory of image encryption and decryption is described in section 4. Sections 5 and 6 describe the encryption and decryption of audio and video data. Section 7 describes the encryption of multimedia data using ECC and TDMRC. Conclusions are given in the last section.

II. WORKING OF ECC

Elliptic Curve Cryptography is one of the public key encryption schemes. It is based on the discrete logarithmic problem. Efficient key management and computation are the peculiarities of ECC. The equation of elliptic curve is given as,

$y^2=x^3 + ax + b$ ..... (1)

Let E represents an Elliptic curve, P be a point on the curve and n be a prime number which represents the maximum limit.

Then key generation is as follows:

1. Select a number 'd' within the range of 'n'
2. Generate public key using Q = d * P, where d is the random number within the range of 1 to n-1
3. Q is the public key and d is the private key.

Encryption is performed as follows:

1. Let 'm' be the message
2. Represent the message on the elliptic curve
3. Let 'm' has the point 'M' on the elliptic curve 'E'
4. Select 'k' randomly from 1 to n-1

5. Generate two cipher texts C1 = k * P, C2 = M + k * Q
6. Sent C1, C2

Decryption is done as follows:

1. M = C2 – d * C1
2. C2 – d * C1 = (M + k * Q) – d * (k * P) = M + k * d * P – d * k *P = M, which is the original message

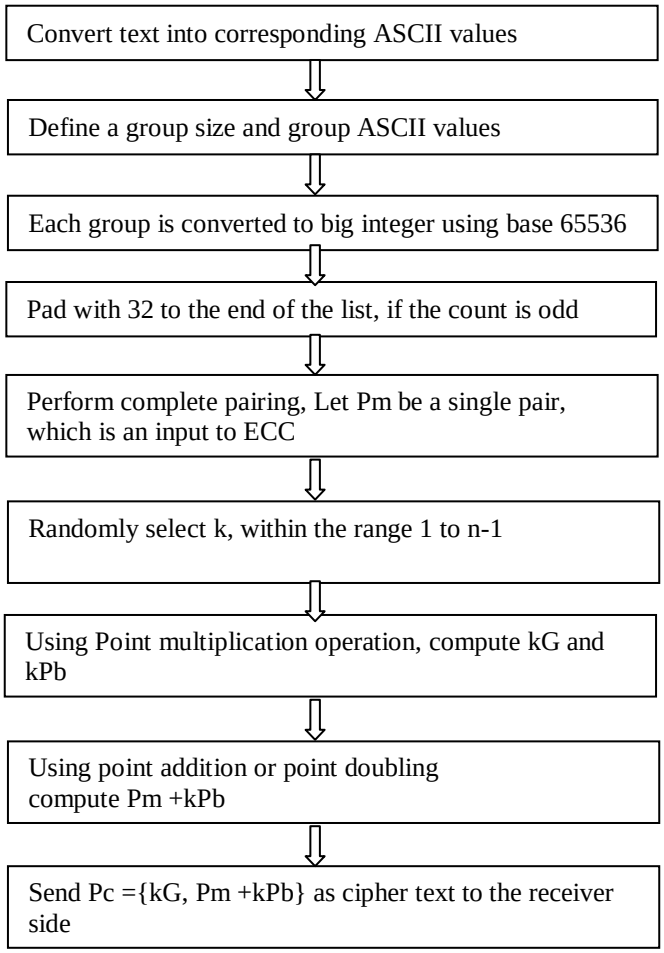
III. ENCRYPTION OF TEXTUAL DATA

There are many methods to perform the encryption of textual data. In this paper two methods are described to perform text encryption. The first one uses ASCII code [2] and the second one uses TDMRC code.

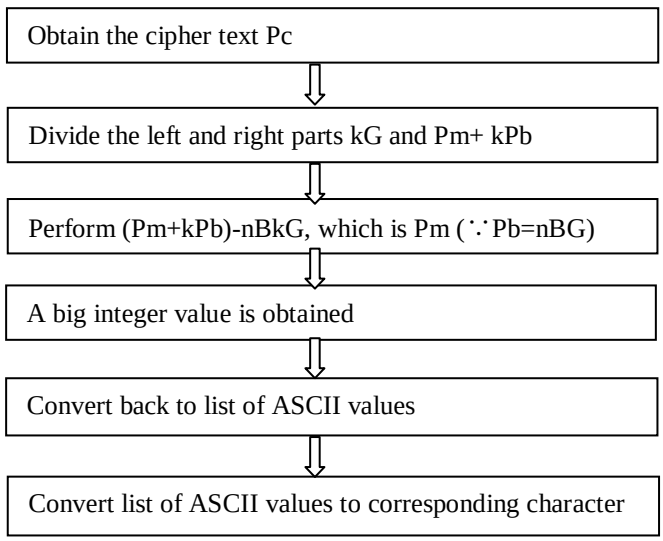
A. Using ASCII code

The encryption and decryption are described below:

Encryption process:

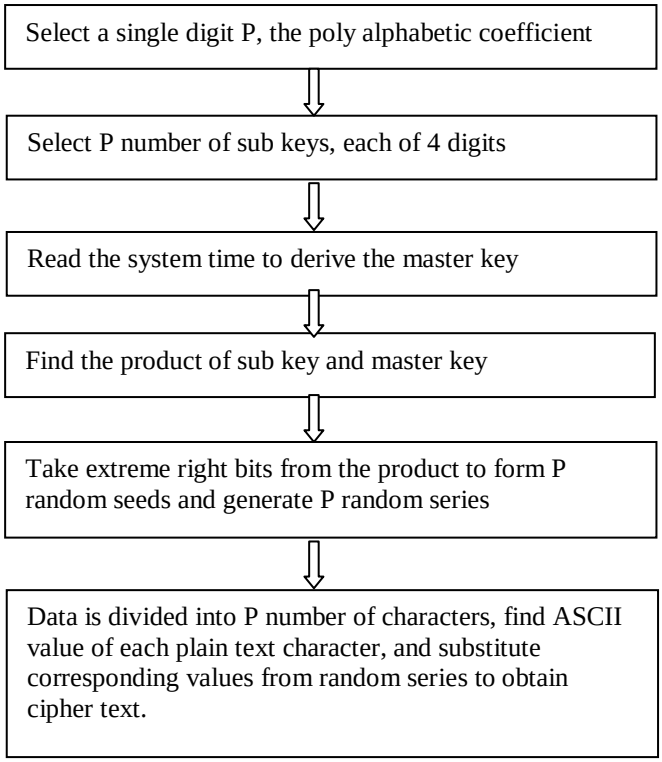


Decryption process

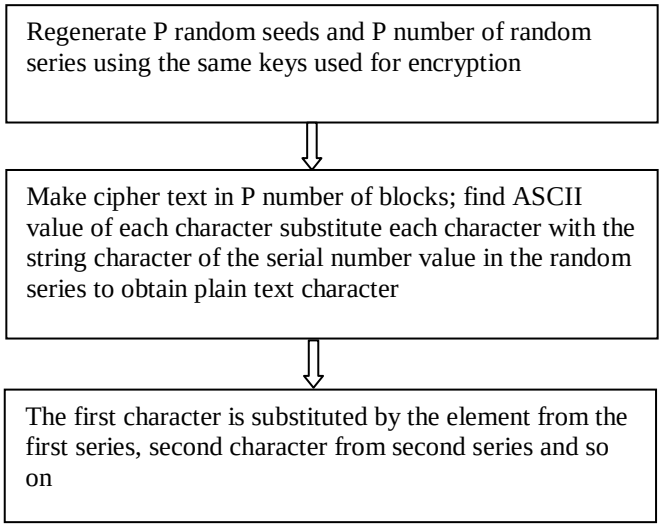


B. Using TDMRC code

TDMRC code 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 [3]. The method to generate TDMRC code and encrypt text is as follows:



The method of decryption is as follows:



IV. IMAGE ENCRYPTION

In this method, every pixel of the original image is transformed into the elliptic curve point (Xm,Ym), these elliptic curve point convert into cipher image pixel. The resulting system gives comparatively small block size, high speed and high security [4]. The encryption and decryption algorithm is described below:

Step1: Let X be the input, an MxN binary image

Step2: Each pixel value 'm' of the image X is converted into the coordinates (X_m, Y_m) on the elliptic curve

Step3: Select K, a random positive integer

Step 4: Select a prime number 'P' such that (X_m, Y_m) is a square modulo P and P>K.m

Step5: To encrypt and send message from A to B, cipher text is produced as follows: C = {KG , P_m+kP_B}, where P_B is the users public key.

Step 6: Decrypt the cipher text using the method {Pm+ k P_B -nB (KG)= P_m+Kn_BG-nBKG} = P_m

The figure 1 shows an example of image encryption [4].

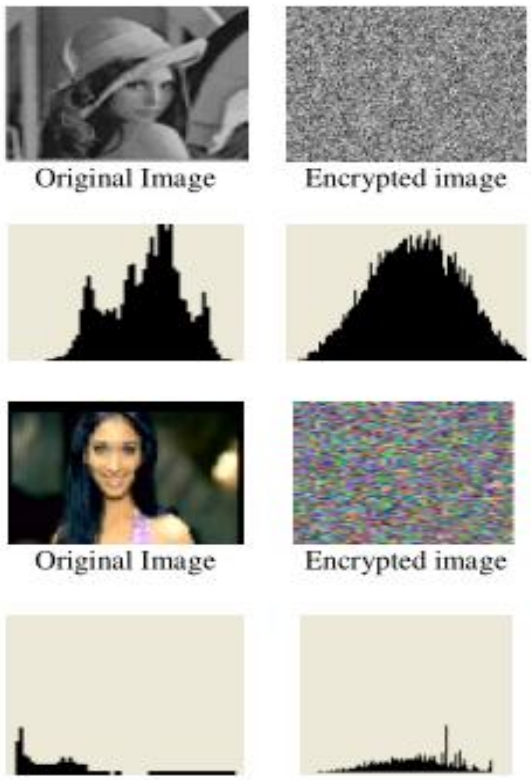


Fig. 1 Example of an image encryption [4].

V. AUDIO ENCRYPTION

The encryption of audio signals also has much importance in this era of 4G technological world. Even the data is text or image or audio, all are digital data. So the same type of encryption can be applied to audio data too. The encryption and decryption algorithm is described below [5]:

Step 1: Let 'X' be an audio input file

Step 2: Let 'm' be each value of audio file 'X', represent it as coordinates (X_m, Y_m) on the elliptic curve

Step 3: Let 'K' be the random positive integer, then $X_m = m*K + j$, where j = 0,1,2,... and $Y_m = \sqrt{(x3 + ax + b)}$

Step 4: Let 'G' be a point on the curve and Ep(a,b) be an elliptic group

Step 5: Sender 'A' chooses a secret integer 's', compute Q = s.G

Step 6: Receiver 'B' consists of public key Ep(a,b), and the points G and Q, s is kept private

Step 7: Let P_m be the plaintext message from A to B

Step 8: A selects a random positive integer k and produce the ciphertext $C_m = \{kG, P_m + kQ\}$

Step 9: Perform decryption using the method {Pm + kQ – s.(kG) = Pm + k(s.G) – s.(kG)} = Pm

VI. VIDEO ENCRYPTION

Secure video data transmission is extremely important nowadays, as we all use video conferencing, video broadcasting, video on demand etc. There are several techniques for the encryption of video signals. Encryption using ECC is one of the best and most popular techniques used. The encryption and decryption are performed using Rivest Cipher(RC5) code and ECC. RC5 has following suitable characteristics: it is a block cipher with varying block size (32, 64 or 128 bits), varying key size (0 to 2040 bits) and variable number of rounds (0 to 255) (so that the user can choose the level of security appropriate for his application). It is a fast block cipher with a simple and easy to analyse structure. It also has adaptable word size in order to suit processors of different word lengths and flexibility of changing the parameters easily [5]. Steps are as follows:

Encryption:

Step 1: Pre-processing using look up table

Step 2: Generate quadruples for all combinations.

Step 3: Encrypt quadruple using Electronic code book of RC5

Step 4: Look up table stores list of coefficients and the values encoded

Step 5: Select each frame and perform step 6 through step 7

Step 6: Consider AC1 to AC4, four consecutive coefficients

Step 7: Check for hit or miss with look up table, if hit then apply the algorithm of ECB mode with RC5 and ECC. If miss

Select DC coefficients as input and use CBC mode and RC5 to encrypt those values.

Decryption:
Step 1: At receiver side, generate look up table and the quadruples are encrypted.
Step 2: Interchange columns in the look up table
Step 3: Check whether value pairs are in correct order
Step 4: Perform RC5 decryption followed by CBC mode; same table is used for AC coefficients.

VII. MULTIMEDIA ENCRYPTION

The security in computer networks is a topic of powerful research due to the increasing use of the computers or laptops in modern times and their interconnection between the networks of all kinds and sizes, regularly by internet [6]. The combination of encryption methods has various advantages. One is that a connection channel is established between two users' set of equipments. Users then have the ability to communicate through hybrid encryption. Asymmetric encryption can slow down the encryption process, but with the simultaneous use of symmetric encryption, both forms of encryptions are enhanced. The result is the added security of the transmittal process along with overall improved system performance [7].

By all of these possibilities we can exchange the information and access the data which are stored in various multimedia which belongs to text, image, audio and video data. All comes under digital data. This paper describes a common technique to encrypt multimedia data using ECC. Initially multimedia data is preprocessed. Preprocessing means, if the data is a textual data we can covert to cipher using TDMRC. If the data is other than text, that means image, audio or video preprocessing involves conversion of image to pixels and audio/video to text and then applies TDMRC and ECC for encryption. The ECC can yield a level of security with a 164 –bit key that other systems require a 1024-bit hey to achieve, due to that ECC helps to establish equivalent security with lower computing power and battery resources. [8].

ECC provides the highest strength-per-bit of any cryptosystem known today with smaller key sizes like RSA, resulting in faster computations, lower power consumption and memory. It also provides a methodology for obtaining high-speed, efficient and scalable implementation of protocols for authentication and key agreement [9].

The proposed algorithm is as follows:
Steps:
Step 1: Obtain the digital version of multimedia data, which will be the plaintext.
Step 2: Choose an Elliptic curve E(a,b)
Step 3: Obtain the first character of plaintext
Step 4: Encrypt using TDMRC
Step 5: Let p1 be the ASCII value of first character of the plain text.
Step 6: Let p2 be the value substituted with the equivalent value in the first random series.
Step 7: Let P be the poly alphabetic coefficient used in the generation of TDMRC code.
Step 8: Find the product of p2 and 2P, x=p2*2P
Step 9: Solve y for x = (p2*2P) +1, x = (p2*2P) +2, x = (p2*2P) +3 and so on until y is obtained
Step 10: The point (x,y) on the elliptic curve will correspond to the first character in the plain text
Step 11: Repeat the procedure until all characters are covered
Step 12: Encrypt using ECC and send the two cipher text points to the receiver.
Step 13: Then the receiver will decrypt the cipher text to the point (x,y).
Step 14: Decode the point (x,y) to the number p2
Step 15: Apply TDMRC decryption algorithm to obtain the plain text character.

VIII. CONCLUSIONS

Since we are using a hybrid method for encryption, it ensures good efficiency and good performance. The convenience of using this method is due to the symmetric scheme and efficiency is achieved through the asymmetric scheme. The research in this area has high scope, since we are using mobile applications, smart cards, cloud computing etc. ECC has remarkable roles in cloud computing and end to end encryption in the transmission of encrypted text messages in mobile communication. In this work, various types of digital data are encrypted using ECC. The work can be extended to the area of cloud computing and mobile applications also.

REFERENCES

[1] Tawalbeh, L, Mowafi, M, Aljoby W, Use of elliptic curve cryptography for multimedia encryption, IET Information Security, Vol. 7, 2013
[2] Laiphrakpam Dolendro Singh, Khumanthem Manglem Singh, Implementation of Text Encryption using Elliptic Curve Cryptography, Procedia Computer Science, Vol. 54, 2015
[3] Cimi Thomas M, Varghese Paul, Secure Method For Embedding Plaintext On An Elliptic Curve Using Tdmrc Code And Koblitz, Vol. 84, 2016
[4] Gupta, Kamlesh Silakari, Sanjay Gupta, Ranu Khan, Suhel A., An ethical way for image encryption using ECC, 1st International Conference on Computational Intelligence, Communication Systems and Networks, CICSYN 2009, Pages 342-345
[5] Lekha Bhandari, Avinash Wadhe, Speeding up Video Encryption using Elliptic Curve Cryptography (ECC), International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-2, Issue-3)

[6] Rahul Singh, Ritu Chauhan, Vinit Kumar Gunjan, Pooja Singh, Implementation of Elliptic Curve Cryptography for Audio Based Application, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 1, January – 2014

[7] Bala, ChDurga, VijayaKumar, B PrasannaBabu, D Nethaji, A Noval Security Method For Implanting A Plaintext On Elliptic Curve Cryptography By Using Tdmrc Code, International Journal of Innovative Research in Science and Engineering, Vol. No. 2, Issue 05, May 2016

[8] Al-khalidi, Saeed Q Y, Hybrid encryption/decryption technique using new public key and symmetric key algorithm, Int. J. Information and Computer Security, Vol. 6, No. 4, 2014

[9] Mulani, Karim Shahajhan, Ramchandra, Nimbalkar Ravi, Wi-Fi security using Elliptical Curve Cryptography, International Journal of Science and Research (IJSR), Vol. No. 3, Issue 5, Pages 567-571

[10] Shaikh, A P, Enhanced Security Algorithm using Hybrid Encryption and ECC, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. IV (May-Jun. 2014), PP 80-85

