ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Multi -Way Encryption Using Elliptic Curve Cryptography

Dr. Nilambar Sethi [1], Binayak Panda [2]

Associate Professor, Department of Computer Science & Engineering, GIET, Gunupur, Odisha, India [1]

Assistant Professor, Department of Computer Science & Engineering, GIET, Gunupur, Odisha, India[2]

ABSTRACT: Once a purpose steps out of the limits of a single-computer box, its peripheral communication is immediately uncovered to a mass of outside observers with an assortment of intention, good or bad. In order to protect sensitive data while these are en route, applications call up different methods. Thus, cryptography mechanisms form a groundwork upon which many important aspects of a solid security system are built. Cryptography is the science of writing in secret code and is an ancient art. In Symmetric Key and Asymmetric Key, Symmetric key algorithms are the quickest and most commonly used type of encryption. This paper describes multi-way encryption technique for data encryption-decryption using elliptic curve. So a new method based on both cryptography and format of message like text to image or image to text, which overcome each other's weaknesses and make difficult for the intruders to attack or steal sensitive information is being proposed.

KEYWORDS: Cryptography, Elliptic curve, Symmetric Key, Asymmetric Key, Encryption, Decryption.

I. INTRODUCTION

"Cryptography" derives from the Greek word kruptos, meaning "hidden" and graphian means writing. Cryptography is the science of encrypting and decrypting information. The growth of modern communication technologies imposes a particular means of security mechanisms in particular in case of data networks [2]. The network security is becoming more important as the volume of data being exchanged over the Internet increases day by day [1]. The network security is becoming more important as the volume of data being exchanged over the Internet increases day by day [2]. Cryptography is the art of transmitting the data safely over the Internet by applying some cryptographic algorithms so that it will be difficult for an attacker to attack or steal some confidential or private information [14]. The key to hiding data is to devise a hiding (encryption) mechanism that is very difficult to reverse (i.e., to find the original data) without using the decryption key. It is a substitution cipher, a special type of private key cryptography. Given a general description of the private key cryptography, it is called symmetric key cryptography. [1] Usually, the harder it is to discover the key, the more secure the mechanism. In symmetric (also called "secret-key" and, unfortunately, "private key") encryption, the same key (or another key fairly easily computed from the first) is used for both encryption and decryption.

In asymmetric (also called "public-key") encryption, one key is used for encryption and another for decryption. Public key cryptography not only solved the problem of sending the encryption key to the other party by a secure transmission mode. In public key cryptography, each of users is required to publish his /her private key directly accessible to each one. In cryptosystem different type of attack may be come to get the original message [10].to avoid this attack the different types of encrypted mechanism are developing like multilevel and multiphase encryption [4, 7, 1].Some are also using the compression technique to mosque the data in channel [9].Different algorithms are there to encrypt the message [14].elliptic curve public key cryptosystem is one of the technique to secure the data which is using the smaller key size [10]. There are many types of attack may be occurs like Security Threats, Virus assault, Unauthorized Access, Data stealing and cryptography attacks, Unauthorized application installations, application-Level Attacks in our network. This paper we are trying to deal with multi-way encryption using symmetric Key cryptography technique. A new Symmetric Key cryptographic idea has been proposed in this paper which encrypts the text to image and image to text.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

II. TYPES OF CRYPTOGRAPHY

The modern cryptography is classified into two types -Symmetric Key Cryptography and Asymmetric Key Cryptography.

A. Symmetric Key Cryptography: In Symmetric Key algorithms, a single key is used for both encryption and decryption process. Both the parties must agree on the secret key before the actual exchange of data takes place. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data categories –Stream Ciphers and Block Ciphers. A stream cipher breaks the plaintext X into successive characters or bits x1, x2, and enciphers each xi with the ith element ki of a key stream K = k1,k2. . . whereas , a block cipher breaks X into successive blocks (each block is typically several characters long.) X1, X2 . . . . . and enciphers each Xi with the same key K; that is , EK(X) = EK(X1)EK(X2) . . .

B. Asymmetric Cryptography: Asymmetric: Cryptography refers to a cryptographic system requiring two separate keys, one to encrypt and one to decrypt. One of these keys is published or public and the other is private. Public key algorithms, unlike symmetric key algorithms, do not require a secure initial exchange of secret keys between the people. Public-key cryptography is used as a method of assuring the confidentiality, authenticity and non-reputability.

III. REVIEW OF VARIOUS CRYPTOGRAPHIC TECHNIQUES [3]

(A) DES: The Data Encryption Standard (DES) is symmetric-key cryptography. It is a block cipher that enciphers 64-bit blocks of data with a 56-bit key and eight bits are used for checking parity.

(B) AES: AES is a symmetric key block cipher and is fast in both software and hardware. AES has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. AES is essentially a substitution permutation network.

(C) Diffie–Hellman Key Exchange (DHKE): It is a specific method of exchanging cryptographic keys. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

(D) RSA: Like other cryptography RSA is a public-key cryptosystem. In RSA, the encryption key is public and differs from the decryption key which is kept secret. Messages encrypted with the public key can only be decrypted using the private key.

(E) ElGamal Encryption: The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. We consider the El Gamal encryption scheme over the group Z□p , where p is a prime.

(F) Elliptic Curves: Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography. Elliptic curve has a hard exponential time challenge for an intruder to break into the system.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

TABLE -1 COMPARISION AMONG DIFFERENT CRYPTO SYSTEM

Cipher	Type	Bit Length	Possible attacks
DES	Symmetric Key	56 bits	Brute force Attacks , Differential and Linear Cryptanalysis
AES	Symmetric Key	128,192,256 bits	Known plaintext, Side channel attack
RSA	Asymmetric Key	1024 – 2048 bits (Based on no. of bit in N=p*q)	Brute Force Attacks , Side Channel Attacks
ElGamal Encryption	Asymmetric Key	1024 – 2048 bits	Chosen Ciphertext attacks.
Elliptic Curves	Asymmetric Key	160 – 256 bits	Pollard‟s Rho method

IV. PROPOSED APPROACH

Elliptic curve E over a field F defined as the set of all points in F × F that satisfy an equation of the form E y2 + axy + by = x3 + cx2 + dx + e along with a point at infinity 'O'. Where a, b, c, d, e belongs F. They are so named because they are described by cubic equation. Equation of the curve takes different forms based on the character of the field. Let the points P =(x1, y1) and Q =(x2,y2) be in the elliptic group Ep(a,b), and O is the point at infinity. The rules for addition over the elliptic group Esp(a, b) are:

P +O = O +P = P

If x2 = x1 and y2 = −y1, that is P =(x1, y1) and Q =(x2, y2) =(x1, −y1) =−P, then P +Q = O.

If Q =−P, then the sum P +Q =(x3, y3) is given by: $x3 = \lambda 2 - x1 - x2 \bmod p$ $y3 = \lambda(x1 - x3) - y1 \bmod p$ where $\lambda = y2 - y1 / x2 - x1$ if $P \neq Q$ $\lambda = 3\ x12 + a\ 2y1$ if P = Q .

The crucial property of an elliptic curve is that resultant point of two points after addition is a point on the elliptic curve. In mathematics, the point and the addition laws from a finite abelian group. We need to include an extra 'zero' point O. which does not satisfy the elliptic curve equation. This zero point is taken to be a fully paid of point of the curve. The order of curve is the number of distinct point on the curve, including the zero point. Having defined addition of two point, we can also define multiplication k*P where k is the positive integer and P is the point. For this we have to add P, k times [1]. Let P=211 is a prime number. EP(0,-4) which is equivalence to curve y2=x3-4; for F=(2,2), one can calculate that 240*F=O. If we carry on computing P+P+P…. for a long enough, since the number of curve point is finite, we must eventually get a result O. We will certainly have a * P=b*P for some a, b with b>a this implies that c*P= O where c=b-a .The least c for which this is true called order of the point, and c must divide the order of the curve. For good security, fixed point is chosen so that the order of the fixed point F is a large prime number.

A. Elliptic curve Encryption/ Decryption

Several approaches to encryption and decryption using elliptic curve have been analyzed in the literature. Here we discussed one method. First task in this system is to encode the plane text M to be send as an (x, y) point .It is the point PM that will be encrypted as a hypertext and subsequently decrypted. As there is constant need for a database of the elliptic curve points, a code to scan all Y coordinates that satisfy the elliptic curve equation for the given X co-ordinate has been included. Equation of the elliptic curve: $y2 \bmod p = (x3+ax+b) \bmod p$, Where, p is a prime number. The constants a and b are non negative integers smaller than the prime number p and must satisfy the condition: $4a3 + 27\ b2 \bmod p \neq 0$.

For Z29 = {1, 2, 3, 27, 28} the elliptic group Ep(a, b)=E29(2,1) thus include the points: E29(2,1)={ (0,1),(0,28),(1,2) ,(1,27) ,(2,10), ,(2,19), ,(3,11), ,(3,18) ,(5,7) ,(5,22) ,(8,6) ,(8,23) ,(9,9) ,(9,20) ,(10,8) ,(10,21) ,(11,7) ,(11,22) ,(12,10) ,(12,19) ,(13,7) ,(13,22) ,(15,10) ,(15,19) ,(19,5) ,(19,24) ,(21,13) ,(11,16) ,(23,11) ,(23,18) ,(25,4) ,(25,25) }

The first step consists in choosing a generator point, G ∈ Ep (a, b), such that the smallest value of n such that nG = O is a very large prime number. The elliptic group Ep(a , b) and the generator point G are made public. Each user select a private key, nA <n and compute the public key PA as: PA = nAG. G: The generator or base point. A distinct point of the curve which resembles the start of the curve. This is either given in point form G or as two separate integers gx and

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

gy , n is the order of the curve generator point G. For example: G= (0, 28), nA=3, (8,6) = 3(0, 28). So, PA= (8, 6) is the public key for private key 3.

B. **Rules for encryption and decryption**

Rule-1 is used to convert an integer into a corresponding elliptic curve points from our evaluated Elliptic curve points.
Rule-2 is used to convert an elliptic curve point into its corresponding integer.
Rule-3 does reverse operation same function as Rule-2
Rule-4 dose reverse operation same as Rule-1.

The text encryption procedure has used the in-built feature of Python to assign the ASCII value of a character to an integer variable when the latter is equated to the former. If user A wants to send to user B the message M which is encoded as the plaintext point PM = (21, 13) ∈ E29 (2,1). She must use user B public key to encrypt it. Suppose that user B secret key is nB = 3, then his public key will be: PB = nBG = 3(0, 28) PB = (8, 6) User A selects a random number k = 4 and uses user B's public key PB = (8, 6) to encrypt the message point into the cipher text pair of points: PC = [(kG),(PM + kPB)] PC = [(5 ,22),(2,10)]

Once receiving the cipher text pair of points, PC = [(5, 22), (2, 10)]], user B uses his private key, nB = 3, to compute the plaintext point, PM, as, (PM +kPB)−[nB(kG)] ie (PM+kPB)−[nB(kG)]=(21,13) and then maps the plaintext point PM = (21,13) back into the original plaintext message M. many author done the text encryption and decryption using Elliptic curve. Here we are trying to encrypt the image to text and text to image.

C. **Image Encryption Procedure**

The image encryption procedure is based on encrypting the image into a new string. This new string is decrypted at the receiver side to obtain the original string in the form of image.
Steps are:

1. Convert the image into a string S.
2. Convert the string into an elliptic curve point E using Rule-1
3. Encrypt the Elliptic curve point to a new point (E').
4. Using Rule-2, the new point is converted to a corresponding integer M.
5. This integer M is used to calculate the new encrypted string S´.

D. **Decryption Procedure**

1. The encrypted string S' and the page number (P) are read from the received files.
2. These 2 parameters are used to calculate the integer M.
3. Using Rule-4, the integer M is converted to encrypted elliptic curve point E'.
4. The point E' is decrypted to get the original point E.
5. By Rule-3, the original String S is obtained and can be converted into image

V. RESULT

The cipher text is not expressing anything about the object which has been encrypted. It creates an illusion of text to text encryption. This ensures a trivial security characteristic. The following result shows how the proposed approach takes input as an image and produces the out as a text.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Input is given in the fig-1:

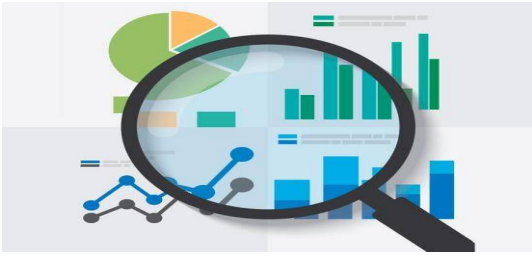

Fig-1

Output as a text given in the fig -2 after encryption:

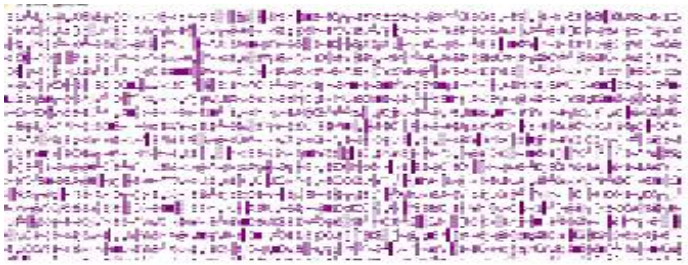

Fig-2

VI. CONCLUSION

In this paper, a very comprehensive review of the conventional approaches and techniques used in the security of transmitted data over the data networks has been given. The survey has been carried out related to public key cryptography. So, in order to overcome the lack of coverage of all the principles of security in those algorithms, a new idea has been proposed that would satisfy all the principles of security and also satisfy the requirements of cryptography. The proposed algorithm can be implemented in a security system as a future research work that would probably excel in comparison to the existing algorithms. The system would be tested on the basis of various test cases and the results would be compared with those of existing algorithms. Here we are trying to make little bit confusion to the attacker when it is encrypting text to image or image to text. The study of multi-way encryption aims to enhance the potential of upcoming encryption by merging multi-way, multilevel and multi phase cryptosystem,

REFERENCES

[1] Himanshu Gupta and Vinod Kumar Sharma" ***Multiphase Encryption: A New Concept in Modern Cryptography*** "Inter*national* Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013 pp638-640.

[2] Jidagam Venkata Karthik, B.Venkateshwar Reddy, "***Authentication of Secret Information in Image Steganography***", International Journal of Latest Trends in Engineering & Technology, Vol. 3(1), Sep 2013, pp. 97-104.

[3] Jyotirmoy Das "***A Study on Modern Cryptography and their Security Issues***" International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 10, October 2014,pp 320-324.

[4]K.Govinda1*, Dr.E.Sathiyamoorth "***Multilevel Cryptography Cryptography using graceful***", Journal of Global Research in Computer Science Volume 2, No. 7, July 2011, pp 1-5.

[5] Mini Malhotra, Aman Singh" ***Study of Various Cryptographic Algorithms***" International Journal of Scientific Engineering and Research (IJSER)" Volume 1 Issue 3, November 2013,pp77-88.

[6] Neal Koblitz, "***A course in Number theory and Cryptography***", Second Edition, Springer.

[7] **]**Rajesh R Mane1" ***A Review on Cryptography Algorithms, Attacks and Encryption Tools***" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 9, September 2015, pp 8509-8514.

[8] Ravi Sharma, "***Study of Latest Emerging Trends on Cyber Security and its challenges to Society***", International Journal of Scientific &Engineering Research, Volume 3, Issue 6, June-2012.

[9] *Sarita Kumari, **" A research Paper on Cryptography Encryption and Compression Techniques"** International Journal Of Engineering And Computer Science, Volume 6 Issue 4 April 2017, Page No. 20915-20919.*

[10] Sharad Kumar Verma and Dr. D.B. Ojha***" A Discussion on Elliptic Curve Cryptography and Its Applications***" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012,pp74-77.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

[11] S. William, *Cryptography and Network Security: Principles and Practice*, 2nd edition, Prentice-Hall, Inc, 1999. pp 23-50.
[12] Siddharth Ghansela, ***"Network Security: Attacks, Tools and Techniques***", www.ijarcsse.com, Volume 3, Issue 6, June 2013.
[13] Taher ElGamal ***"A public key cryptosystem and a signature scheme based on discrete logarithms***". IEEE Transactions on Information Theory, 31(4):, 1985, pp 469- 472.
[14] Vipula Madhukar Wajgade, Dr. Suresh Kumar, "***Stegocrypto - A Review of Steganography Techniques using Cryptography***", International Journal of Computer Science & Engineering Technology, ISSN: 2229-3345, Vol. 4, 2013, pp. 423-426.
[15] W. Diffie and M. Hellman***," New directions in cryptography***", IEEE Trans. Info., vol. 22, no. 6, Nov. 1976. , pp. 644-654.