Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.1 – 6

REVIEW ARTICLE

A Review of Geometry Based Symmetric Key Encryption Using Ellipse

Prerna Gaur[1], Dr. Paramjit Singh[2]
[1]Computer Science and Engineering Department, PDM College of Engineering, Bahadurgarh, Haryana, India
[2]Professor of Computer Sciences, PDM College of Engineering, Bahadurgarh, Haryana, India

[1] prernagaur4@gmail.com; [2] director_engg@pdm.ac.in

Abstract— Cryptography is the way to secure the data to achieve higher reliability during the communication process. There exist a number of cryptographic approaches. This paper defines a geometry based Symmetric cryptography algorithm that is used to encrypt the input data. As the name suggests the approach is based on the geometric figure to perform the cryptography. In this work, we will define an elliptic shape geometry to generate the dynamic key so as to perform the dynamic symmetric encryption of input text. Based on the geometric elliptic figure's properties the key will be generated and by using the key parameters the length and breadth of Cartesian plain will be defined. Once the area will be defined, the next work is to define a group of ellipses and to perform the translation and rotation of axis. By extracting the pixel positions on these ellipses and to place the input data respectively to these locations the cryptography will be performed. The actual work of this algorithm is to change the data locations instead of changing the data. The secure and reliable encoding of the data is expected from the work.

Key Terms: - Encryption; Symmetric Key Encryption; Ellipse Generation; Translation; Rotation

I. INTRODUCTION

In cryptography, **encryption** is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an **encryption scheme**, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a **decryption** algorithm, which usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys as in [8].There are several ways of classifying cryptographic algorithms. Based on the number of keys employed for encryption and decryption, there are mainly two types of algorithms as in [5].

Asymmetric Encryption: It's also known as public key encryption. Each communicating entity has its own private key and public key. One is used for encryption and the other for decryption. It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key as in [6].

In public key cryptography the encryption key is public but the decryption key is private.

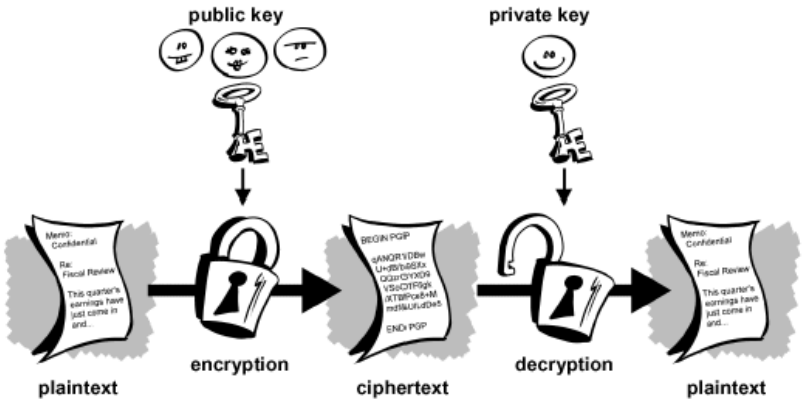

Fig. 1 Public Key Encryption

The problem of public key cryptosystem is that one has to do massive computation for encrypting any plain text. Due to massive computation the public key cryptosystem may not be suitable in securing data in ad hoc sensor networks as in [2].

Symmetric Encryption: The same key is used for both encryption and decryption and it is shared between the two communicating parties. In symmetric key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher-text to the receiver. The receiver applies the same key (or rule-set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver as in [3].

The merit of 'symmetric key cryptography' is that the key management is very simple as one key is used for encryption as well as for decryption. In case of symmetric key cryptography the key is secret as in [2].

Fig. 2 Symmetric Encryption

II. RELATED WORK

In 2007, Reference [1] proposed cryptosystem based on a new algebraic structure with simple and flexible properties. This cryptosystem is constructed from Cyclic Geometric Progressions over polynomial ring in finite field, in which it is considered as a poly alphabetic cipher. Simple scheme for cryptosystem using the cyclic geometric progression over polynomial ring is described. The new structure of multiplicative group and Cyclic over polynomial ring is also mentioned in this paper. With all characteristics of CGPs and the efficiency in the implementation, the newly proposed method may be very practical to use in the on-line computer system. For instance, strong requirement of data security and reliability by using mobile telephone to transmit data, voice and image across the sky can be greatly satisfied with the scheme. It's limitation is that it's computationally complex. According to Hoai Bac et al. "Our techniques have a number of crucial advantages. They are provably

secure: they provide provable secrecy for encryption. The algorithms we present are simple, fast and easily implemented in terms of encryption as well as decryption."

In 2009, Reference [3] explained that Symmetric Key Cryptography is one of the prominent means of secure data transfer through unreliable channel. It requires less overhead than Public Key Cryptosystem. They presented a new algorithm based on 2-d geometry using property of circle, and circle-centered angle. It is a block cipher technique but has the advantage of producing fixed size encrypted messages in all cases. It incorporates low computational complexity with fairly high confidentiality than the previous techniques.

In 2012, Reference [7] proposed a symmetric key encryption algorithm known as Chakra Algorithm. It's a process of encrypting the data with the concepts of Cartesian Co-ordinate Geometry and circle generation. This technique also uses circle as the geometric figure like the previous one but in this the key is much more complex than previous technique's.

According to this " The process considers the translation and rotation of axis when the data is grouped in circles each circle holds a portion of data. Unlike the other current algorithms, in Chakra Algorithm we will not directly change the data instead location of data. Here the random plaintext bits are placed on the fixed size Cartesian grid and the circles generated at origin and translated to consent circle center. The encryption technique adapts rotation of circumference points with some angle for all circles. The drawbacks in chakra algorithm are the sine and cosine functions used during rotation of a circle which mostly give irrational numbers making it difficult to store the original value. A circle is rotated by 45° then the point (1,1) becomes (0,1.414..) the irrational numbers causing the problem. The rotational angle (90°, 180° etc.) are only possibilities where both sine and cosine functions are rational numbers".

III. OVERVIEW OF ALGORITHM

The presented work is about to perform the symmetric cryptography by using the geometric elliptical figure. The presented approach is based on the geometric figure based cryptography and we have selected the ellipse as the geometric figure. Based on the defined figure's geometry analysis the dynamic key as well as the dynamic key cryptography will be implemented. The presented work will be implemented in two major stages, first to analyse the geometric figure and based on the initial analysis the dynamic symmetric key will be generated. Now based on these parameters the cryptography work area will be defined in terms of rectangular axis. The area will be extended on each side based on the horizontal and vertical radius of the geometric figure.

To identify the elliptic boundary area the bresenhams ellipse drawing algorithm will be implemented. The obtained pixel positions will be elected as the positions to locate the data values. In same way the whole plain area will be covered by the intersecting ellipses. Now we have to perform the basic transformations on these ellipses in terms of rotation defined at a particular angle and the transformation of the actual data will be performed. The main objective of the work is to change the location of data instead of changing the data values so that a safe cryptography will be performed.

Key: The key mainly consists of 3 parts

- Major axis and Minor axis of ellipse
- Length and Breadth of the Cartesian plain
- Array of angles each ellipse is rotated

The basic steps involved in the work are given as under.

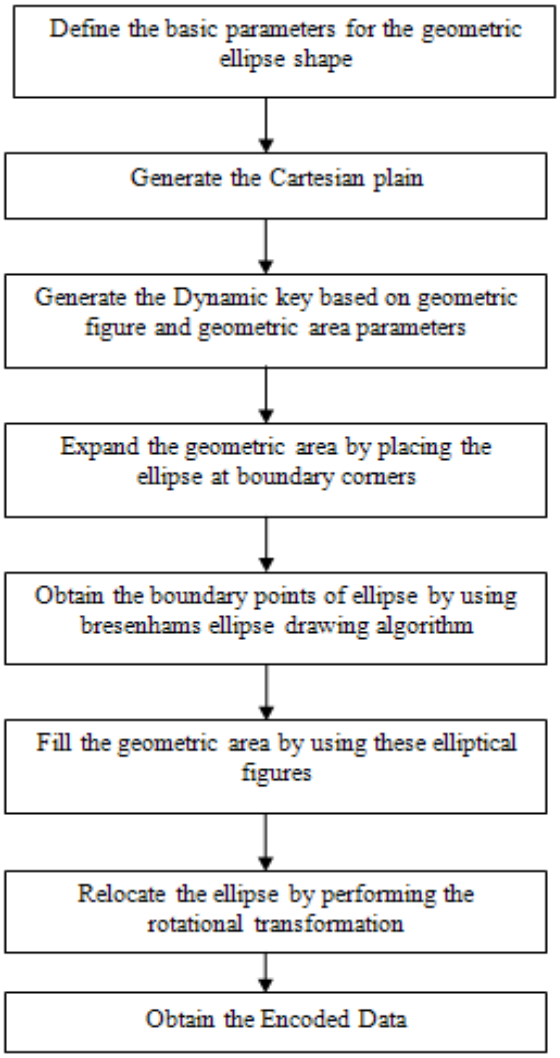

Fig. 3 Flow Diagram of proposed approach

This encryption technique is based on the principles of the Cartesian system given below.

A) Translation of Cartesian Co-ordinates:- A Translation is applied to any object by repositioning it along a straight line path from one co-ordinate location to another.

B) Rotation of Cartesian Co-ordinates:- A 2-dimensional rotation is applied to an object by repositioning it along a circular path in X- Y plane.

A) Translation: - Let (x,y) be a random point in a Cartesian plain and (a,b) be a point to which the axis is moved to then the resultant coordinate will be (x',y') given by the following formula [3].

$$(x', y') = (x + a, y + b)$$

B) Rotation: - Let (x,y) be a random point in the Cartesian plain and the plain is rotated by θ then the new coordinates are given below [3].

$$(x', y') = ((x\cos\theta - y\sin\theta), (x\sin\theta + y\cos\theta))$$

IV. NEW SYMMETRIC KEY ALGORITHM

It's a modern symmetry key encryption technique, which uses the concepts of Cartesian coordinate and ellipse transformation (rotation & translation). Data types used in the algorithm are :-

1. X-Length (XL): Length of the x-axis in the Cartesian plane.
2. Y-Length (YL): Length of the y-axis in the Cartesian plane.
3. Length of major axis (2a) and minor axis (2b) of ellipse.
4. Point(x, y, data bit): A point data type consists of three parameters its x and y coordinate and the data bit(0 or 1) that is present in that location. Grid is a collection of points. An ellipse is a portion of grid
5. P: Length of bit stream of plain text (bit 0 or 1).
6. Ellipse: User defined data class contains Ellipse Center (xc, yc), X-Coordinate and Y-Coordinate.

The major steps of algorithm are explained below:-

Step 1: Collect data from the sender: XL: X-Length, YL:Y-Length, 2a: major axis, 2b: minor axis, , P-Plaintext (stream of bits).

Step 2: Create Cartesian Grid plain (XL*YL)

Step 3: Generate ellipses using Bresenhams ellipse drawing algorithm .

Step 4: Add 1 bit of data at every integral Cartesian point that lies on ellipse.

Step 5: Perform translation and rotation of these ellipses so that bit position is changed.

Step 6: Cipher text is obtained.

A. Bresenhams Ellipse Drawing Algorithm

Step 1: Start the process.

Step 2: Input two radii i.e rx , ry and ellipse center (xc,yc) and obtain the first point on the circumference of an ellipse centered on the origin (x0,y0) = (0,ry).

Initialize "x" and "y" as below:-

$x = 0$

$y = ry$

Step 3: Calculate the initial value of the decision parameter as

$Px = 0$

$Py = 2 * rx^2 * y$

$P = ry^2 - (rx^2 * ry) + (0.25 * rx^2)$

Step 4: while $Px < Py$

[Repeat steps 5 to 7]

Step 5: $Px = Px + 2 * ry^2$ and $x = x + 1$

Step 6: If $P < 0$

$P = P + ry^2 + Px$

else

$Py = Py - 2 * rx^2$

$P = P + ry^2 + Px - Py$

$y = y - 1$

Step 7: Draw Points for 4 octants

Step 8: $P = ry^2 * (x + 0.5)^2 + rx^2 (y - 1)^2 - rx^2 * ry^2$

Step 9: While $y > 0$

[Repeat steps 10 to 12]

Step 10: $Py = Py - 2 * rx^2$ and $y = y - 1$

Step 11: if $P > 0$

$P = P + rx^2 - Py$

else

$Px = Px + 2 * ry^2$

$P = P + rx^2 - Py + Px$

$x = x + 1$

Step 12: Draw Points for 4 octants

Step 13: Exit

V. DECRYPTION ALGORITHM

Note all the information collected from the key, the receiver will know what is the size of the grid i.e. length and breadth of Cartesian plane , anti-rotate ellipse by how much angle i.e. rotate by -θ for every θ . Since all are invertible function at the end plain text is achieved [7].

VI. CONCLUSION

In this paper a new approach for symmetric Encryption using the concept of Cartesian Plotting, ellipse generation and translation, rotation is introduced. Here the random plaintext bits are placed on ellipses and these ellipses are translated and rotated to obtain cipher text. In the previous techniques, the circle is used as the basic geometric figure to perform the cryptography. But because of less number of dimensions and the easier algorithmic approach it has the more chances to reveal the information under some applied attack. But the present paper is about the use of more complex geometric figure i.e. ellipse and the algorithmic approach so that high level of reliability is expected from the work.

ACKNOWLEDGEMENT

Prof. (Dr.) Paramjit Singh is the professor in Department of Computer Science and Engineering at PDM College of Engineering, Bahadurgarh, Haryana. I am specially grateful for his guidance and contributions by generously giving his time and carefully reviewing this manuscript.

REFERENCES

[1] Bac Dang Hoai , Nguyen Binh , Nguyen Xuan Quynh "New Algebraic Structure Based on Cyclic Geometric Progressions over Polynomial Ring Applied for Cryptography" International Conference on Computational Intelligence and Security Workshops, 0-7695-3073-7/07,2007.

[2] Chatterjee Trisha, Tamodeep Das, Shayan Dey, Asoke Nath, Joyshree Nath" Symmetric key Cryptosystem using combined Cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm", 978-1-4673-0125-1 , IEEE (pp 1179),2011.

[3] Chowdhury M.J.M. , Pal Tapas "A New Symmetric Key Encryption Algorithm Base on 2-d Geometry", Proceeding of the International Conference on Electronic Computer Technology, pages: 541-544,2009.

[4] Cryptography. [online]. Available : http://library.thinkquest.org/C0126342/secret.htm.

[5] Forouzan A. Behrouj , Data Communication and Networking , 4th Edition, Tata McGraw Hill Company, 2006.

[6] Answers on History of Cryptography. [online]. Available : http://www.answers.com/topic/history of cryptography ,written on 2007.

[7] Kumar P.Ramesh, S.S.Dhenakaran, K.L.Sailaja, P.SaiKishore Virtus "CHAKRA:A New Approach for Symmetric Key Encryption", IEEE, 978-1-4673-4804-1,2012.

[8] Stallings William, Cryptography and Network Security, 3rd Edition, Prentice-Hall Inc., 2005.

