GEOMETRY IN CRYPTOGRAPHY: A REVIEW

Preeti Singh[1], Praveen Shende[2], Rahul Singh[3]

[1]*M. Tech Scholar, CSE Department, CSIT, Durg, India*
[2]*Assistant Professor, CSE Department, CSIT, Durg, India*
[3]*M. Tech Scholar, CSE Department, CSIT, Durg, India*

Abstract

In the infancy of Cryptography Mono-alphabetic Substitution Ciphers were considered good enough to baffle any potential attackers but with the advancements in technology & the upsurge of computing power those methods have become trivial. Even the very complex methods of encryption are vulnerable to the brute force attacks of contemporary computers and with Quantum computing on the horizon even the current state of the art cryptosystems are at risk. Lots of research is being done and every possible field is being explored in order to create that elusive unbreakable cipher. Among other subjects, Geometry is also being applied and various ciphers based on the properties of different geometrical figures have been developed. This paper ventures to investigate the recent research applying the concept of geometry to boost the caliber of pre-existing cryptosystems enhance the understanding of the subject.

Keywords: *Cryptography, Geometry, Encryption, Decryption, ECC, Circle, Chakra, Ellipse, Hyperbola, HCCS*

----------***----------

1. INTRODUCTION

Secrets are as old as the Human Civilization and for centuries people have been using the art and science that is Cryptography. Julius Caesar is credited with one of the first Ciphers ever created, that we still have records of. Earlier this science was used mainly for political or military purposes but in today's world when the whole world has become a global village and, information is so much more important the ever before, it is so much more relevant and noteworthy. Although military use is still more critical but as almost everyone is using the internet for communication, Cryptography has become much more commonplace. The process of cryptography consists of two phases, Encryption & Decryption. Encryption is the process of converting the plain text (the information) to a form that is illegible to any intruder or attacker. This form is called the cipher text. Decryption is the reverse process that converts the cipher text to plain text. Both the phases use some "key" and "algorithm" to achieve their goal, which are predefined. Fig. 1 depicts the whole process. A key is used and an algorithm is applied to render the information illegible to any unintended observer. A reverse algorithm and the same or a different key are applied to recover the information from the encrypted data. On the basis of whether one or two keys are used Cryptography can be categorized in two.

- Symmetric Key Cryptography
- Asymmetric Key Cryptography

Symmetric Key Cryptography is the model where one key is used for both encryption and decryption. This is also called "Secret Key Cryptography" as the key secret and known only to the sender & the recipient. Asymmetric Key Cryptography is also called "Public Key Cryptography" as it uses different keys for encryption and decryption. The encryption key is public knowledge but the decryption key is only known to the receiver. There are numerous techniques being used currently for encryption and decryption. But there is always a need for newer and stronger ciphers. There are many different approaches that have been applied to create algorithms spreading a range of mathematical fields. Geometry is a field that hasn't been explored that much. Although a very prominent technique based on geometry exists, the Elliptic Curve Cryptography (ECC), there also exist some not as famous mechanisms.

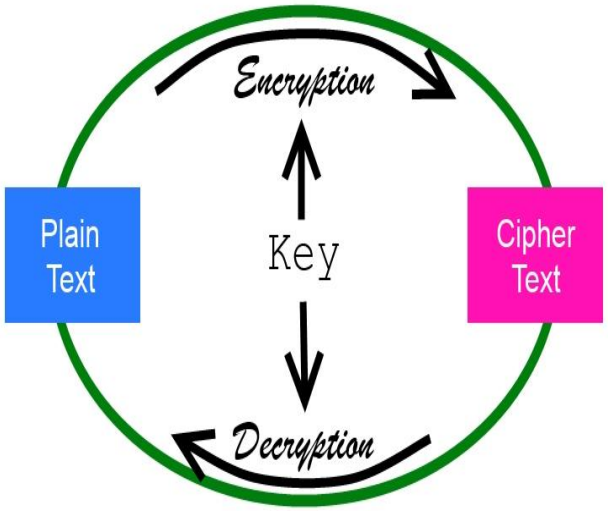

Fig 1: Cryptography Process

2. RELATED WORK

There has been some research on applying geometry in the field of Cryptography. But it is not the most explored area. This section of the paper attempts to review the recent research literature akin to the topic of this work.

Elliptic curve cryptography is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography is the same level of security provided by keys of smaller size. In 1985, Elliptic Curve Cryptography (ECC) was proposed independently by cryptographers Victor Miller (IBM) and Neal Koblitz (University of Washington). ECC is based on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). Elliptic curves combine number theory and algebraic geometry. These curves can be defined over any field of numbers (i.e., real, integer, complex) although we generally see them used over finite fields for applications in cryptography [16]. An elliptic curve consists of the set of real numbers (x, y) that satisfies the equation:

$$y^2 = x^3 + ax + b \qquad \text{...eq. (1)}$$

The set of all of the solutions to the equation forms the elliptic curve. Changing a & b, changes the shape of the curve, and small changes in these parameters can result in major changes in the set of (x, y) solutions. Fig. 2 Illustrates an Elliptic Curve.

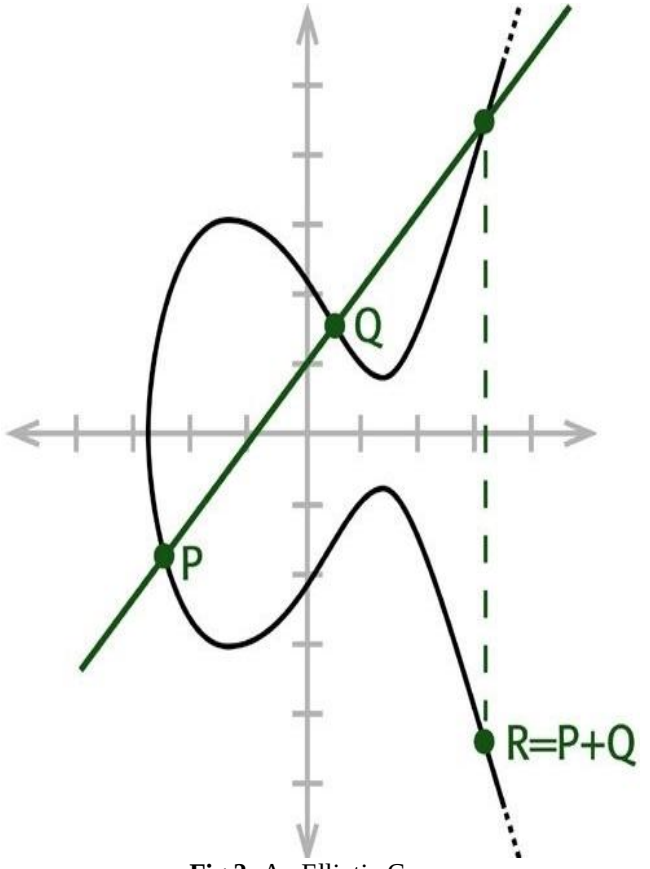

Fig 2: An Elliptic Curve

Choudhury M.J.M. & Pal T. presented an approach for encryption based on the geometry of circle in the paper titled, "A New Symmetric Key Encryption Algorithm based on 2d Geometry", which was inspired by Elliptic Curve Cryptography (ECC) in [1]. This new symmetric encryption scheme is based on the geometry of a circle. Both the users share a secret key which consists of two geometric points:

- The center of the circle
- A secret point on the circle perimeter.

This algorithm can encrypt/ decrypt as many message symbols as its diameter. If the length of the diameter is the largest integer of n bits (2^n) then it can successfully encrypt/decrypt 2^n distinct message symbols. And the computations are in real value domains rather than integer domains. First the message point is randomized and the representation of the randomized message point is determined on the circle. Then, the circle-centered angle that is obtained by traversing along the perimeter of the circle from the secret point to the message point in the counter-clockwise direction represents the encrypted value. The encrypted message is the circle-centered angle and it is transmitted through the network. This value is always less or equal to 2π. Upon receiving the encrypted message, the receiving entity decrypts the message by traversing along the circle's perimeter from the secret point by an angle equal to the encrypted message.

Kumar, Dhenakaran, Sailaja, & SaiKishore presented another encryption algorithm based on circled in "Chakra: A new approach for symmetric key encryption" [2]. This algorithm is a symmetric key encryption technique. It is a process of encrypting the data with the concepts of Cartesian Co-ordinate Geometry and circle generation. The process considers the translation and rotation of axis when the data is grouped into circles each circle holds the portion of data. The Cartesian axis will be migrated to the respective centers circles and rotated by certain angle. The collection of angle with which each individual circle is rotated; the co-ordinates to which it is swapped, the size of the square grid the radius of the circle hold the symmetric key. Unlike the other current algorithms, in Chakra Algorithm we will not directly change the data instead location of data [2].

Bac, Binh & Quynh presented a paper titled "New Algebraic Structure Based on Cyclic Geometric Progressions over Polynomial Ring Applied for Cryptography" [3]. This paper presents a proposed cryptosystem that 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 [3].

Chatterjee, Nath et al. have proposed a new combined cryptographic method called TTJSA in [4]. This is a combination of MSA and NJJSAA which were developed

by Nath et al. and a generalized Vernam Cipher Method. The above three methods are applied in random order on any given plain text for a number of times to get the ultimate cipher text file [4]. They modified the standard Vernam Cipher Method for all characters (ASCII code 0-255) with randomized keypad, and have also introduced a feedback mechanism. They also claim that the method is extremely secure and almost unbreakable.

In [5], Gaur & Singh also based their work on geometry, but not of a circle but an ellipse. Here elliptic shape geometry is defined to generate the dynamic key so as to perform the symmetric encryption of input text. Based on the geometric elliptic figure's properties and length and breadth of Cartesian plain the key is generated. Once the area is 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 is 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 obtained from the work.

Rana & Saluja, in [6] presented A Modified Approach for Symmetric Key Cryptography Using Circles. This work is based on the "Chakra" algorithm from [2] & focuses on the Symmetric key Cryptography technique, using the concepts of Cartesian coordinate geometry and circle generation. Data is grouped into circles and each circle holds a portion of data. An improved geometric cryptographic algorithm is developed, that considers data into a 2- dimensional data grid, generates circles on the grid and applies some geometric transformations over data. This encryption technique adapts hybrid geometric transformations,(i.e., translation followed by scaling) of the circumference points of every circle by some scaling factors(S_x, S_y) and translation factors(T_x,T_y).

Shamshad et al. have also based their work on the "Chakra" algorithm but applied this to the encryption of watermarked images. To provide double protection, after the watermarking process, the watermarked image tends to go through an encryption process using Chakra [7]. The authors proposed digital image watermarking on different types of images by converting the image format into JPEG-LS, which produces a better result on image transmission through Internet. To provide a two layered security, the watermarked JPEG-LS image is encrypted using Chakra-Symmetric Key Encryption Standard.

Kaur, Singh & Garg proposed a Public Key Encryption Mechanism that is based on the geometry of the sphere. Sphere is locus of point in space which moves in such a way that its distance from fixed point always remain constant, where fixed point is the center of the sphere and constant distance is the radius of sphere [8]. In this system public key and private key are generated by using the property of Sphere. A point which lie on the sphere is chosen as the private key and the center of sphere (fixed point) is taken as the public key. This key management provides more security against attacks.

Rasmi & Paul published a paper titled, "A Hybrid Crypto System based on a new Circle Symmetric key Algorithm and RSA with CRT Asymmetric key Algorithm for E-commerce Applications" [9]. The authors present a hybrid cryptographic system that combines both the symmetric key algorithm, which uses the properties of a circle and asymmetric-key algorithm of RSA with CRT. The circle symmetric key algorithm is based on 2-d geometry using property of circle, and circle-centered angle. This is based on the work done in [1]. It is a block cipher technique but has the advantage of producing fixed size encrypted messages in all cases. The asymmetric algorithm is RSA with CRT which improves the performance of the basic RSA algorithm by four.

A new public key cryptography system based on hyperbolic curve over finite field was proposed by Liu et al. in [10]. They propose a new technology that improves Diffie-Hellman's safeness and keeps its good property. It is called "Hyperbolic Curve Cryptography System" (HCCS) which is based on the properties of a hyperbolic curve over a finite field. HCCS has a solid Abel group structure whose order is diverse over finite field and the system is secure which is mainly based on the Discrete Logarithmic Problem (DLP) and hardness of solving fundamental solution [10]. The claim is made that compared with Diffie-Hellman, this process has same calculation complexity but it is more flexible.

3. CONCLUSION

Cryptography, as a field of scientific research is as exciting as it is longstanding. Researchers are working on numerous new ciphers all around the world. This paper is an attempt to shed some light on the convergence of geometry & cryptography. Ten different research papers were overviewed & various cryptography algorithms based on the properties of different geometrical figures were examined. Application of geometry in cryptography is a field with much scope for research & has the potential to yield some intriguing ciphers.

REFERENCES

[1] Chowdhury, M.J.M.; Pal, T., "A New Symmetric Key Encryption Algorithm Based on 2-d Geometry," Electronic Computer Technology, 2009 International Conference on , vol., no., pp.541,544, 20-22 Feb. 2009, doi: 10.1109/ICECT.2009.130

[2] Kumar, P.R.; Dhenakaran, S.S.; Sailaja, K.L.; SaiKishore, P., "Chakra: A new approach for symmetric key encryption," Information and Communication Technologies (WICT), 2012 World Congress on , vol., no., pp.727,732, Oct. 30 2012-Nov. 2 2012, doi: 10.1109/WICT.2012.6409170

[3] Dang Hoai Bac; Nguyen Binh; Nguyen Xuan Quynh, "New Algebraic Structure Based on Cyclic Geometric Progressions over Polynomial Ring Applied for Cryptography," Computational Intelligence and Security Workshops, 2007. CISW 2007. International Conference on , vol., no.,

pp.777,780, 15-19 Dec. 2007, doi: 10.1109/CISW.2007.4425610

[4] Chatterjee, T.; Das, T.; Dey, S.; Nath, A.; Nath, J., "Symmetric key cryptosystem using combined cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm," Information and Communication Technologies (WICT), 2011 World Congress on , vol., no., pp.1175,1180, 11-14 Dec. 2011, doi: 10.1109/WICT.2011.6141415

[5] Gaur P., Singh P., "Geometry Based Symmetric Key Cryptography Using Ellipse", IJAIEM Volume 2, Issue 7, July 2013 ISSN 2319 – 4847, pg: 1-6

[6] Rana D., Saluja S., "A Modified Approach for Symmetric Key Cryptography Using Circles", IJIRSET, Vol. 3, Issue 12, December 2014, ISSN: 2319-8753, DOI: 10.15680/IJIRSET.2014.0312083

[7] Shamshad Sk, Sailaja K.L., Rameshkumar P., "Encryption of Watermarked Images using Chakra Symmetric Key Approach", IJARCSSE, Volume 3, Issue 11, November 2013, ISSN: 2277 128X, pg 569-575

[8] Kaur G., Singh S., Garg A., "ACBS: Asymmetric Cryptography Based on SPHERE", IJARCSSE, Volume 4, Issue 3, March 2014, ISSN: 2277 128X, pg: 430-433

[9] Rasmi P S., Paul V., "A Hybrid Crypto System based on a new CircleSymmetric key Algorithm and RSA with CRT Asymmetric key Algorithm for E-commerce Applications", International Conference on VLSI, Communication & Instrumentation (ICVCI) 2011, Proceedings published by International Journal of Computer Applications® (IJCA)

[10] Liu X., Zheng Q., Yang J., Wang L., Zhang T., Li T., Wang R., "A new public key cryptography system based on hyperbolic curve over finite field", 3rd International Conference on Multimedia Technology（ICMT 2013)

[11] Singh P., Shende P., "Symmetric Key Cryptography: Current Trends", IJCSMC, Vol. 3, Issue. 12, December 2014, pg.410 – 415, ISSN 2320–088X

[12] Stallings W., "Cryptography and Network Security: Principles and Practices", 4'th Ed., Pearson Education 2006, ISBN: 81-7758-774-9

[13] Hearn D., Baker M.P., "Computer Graphics: C Version" 3'rd Edition, Pearson Education, 1997, ISBN: 0-13-530924-7

[14] Mao W., "Modern Cryptography: Theory and Practice", © 2004 Hewlett-Packard Professional Books, Pearson Education, ISBN: 978-81-317-0212-3

[15] Singh S., "The Code Book: The Secret History of Codes and Code-Breaking", © Author 1999, Fourth Estate, ISBN: 978-0-00-745308-5

[16] Kessler G.C., An Overview of Cryptography, http://www.garykessler.net/library/crypto.html, Accesed Feb 2015

[17] Elliptic Curve Cryptography on Wikipedia, http://en.wikipedia.org/wiki/Elliptic_curve_cryptography, Accessed Feb 2015

BIOGRAPHIES

Miss. Preeti Singh received M.Sc. (Computer Science) in the year 2011 and is pursuing M. Tech (CS) from Chhatrapati Shivaji Institute of Technology (CSIT), Durg, CG, India and working as an Assistant Professor at CGVVM, Bhilai. Her research interests are Cryptography, Green Computing, Databases and Data Mining.

Mr. Praveen Shende received M. Tech. (Computer Sc.) in year 2014 from Chhatrapati Shivaji Institute of Technology (CSIT), Durg, CG, India. His interests are Programming Languages (Java, PHP, Zoomla), Cloud Computing and DBMS, Computer Networks, Computer System Architecture.

Mr. Rahul Singh received B.E. (Computer Science) in the year 2010 and is pursuing M. Tech. (CS) from Chhatrapati Shivaji Institute of Technology (CSIT), Durg, CG, India and working as an Assistant Professor at CGVVM, Bhilai. His research interests include Programming Standards, Compilers, Cloud Computing, Cryptography and NLP.