Technique to Enhance Information Security Using Hybrid Geometric Cryptography: A Review

Sapna Rani
M.Tech(CSE), NCCE, Israna, Panipat, Haryana, India.

Sukhbir Singh
Professor of Computer Sciences, NCCE, Israna, Panipat, Haryana, India.

Abstract – Cryptography is the science or art of transforming any data (plaintext) into one that is not understandable by unauthorized person (cipher text) and then transforming the message back to its original form(plaintext).Here, the information is encoded to some other form so that the intermediate user cannot understand and read it. Data security plays a important role in businesses over the internet. Two cryptographic approaches can be used for it. First is symmetric key encryption and second is asymmetric key encryption. In this paper, we present the hybrid cryptography approach by using two geometrical shapes i.e. rectangle and the ellipse. The transformation operations will be applied on these two shapes alternatively to encode the information and to make data transmission reliable.

Index Terms – Hybrid Cryptography, Symmetric key approach, Transformation Operations.

1. INTRODUCTION

Cryptography is a Greek word which means "secret writing". It is an art and approach of transforming messages so as to make them secure and protect them from cyber attacks. Cryptography involves two steps, first step is the process of encryption and second is the process of decryption. The process is shown as.

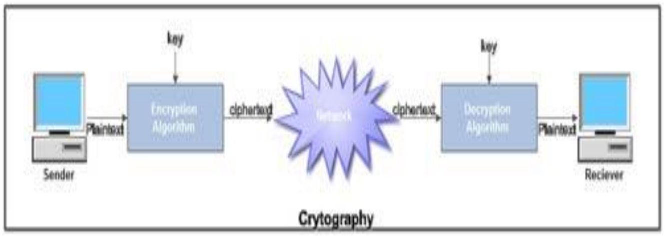

Fig1: Cryptography process

In this approach of cryptography, encryption is the process of encoding messages (or information) in such a way that unauthorized persons or hackers cannot read and misuse it, but that only the authorized persons can read it. In an encryption method, the message or information (called as plaintext) is encrypted using an encryption algorithm, transforming it into an unreadable cipher text. This is usually done by making use of an encryption key, which specifies how the message is to be encoded. And it makes sure that can see the cipher text should not be able to identify anything about the original message.

An authorized party will only be able to decode the cipher text using a decryption method, which usually requires a secret decryption key that unauthorized person do not have access to. For security purposes, 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 used for encryption and decryption, there are mainly two types of algorithms which are as follows [5].

Asymmetric Encryption: It is also called as public key encryption. Each of the communicating entity has its own private and public keys, in which one is used for encryption (public key) and the other is used for decryption (private key). It is computationally infeasible and very difficult to determine the decryption key (private key) given only knowledge of the cryptographic algorithm and the encryption key as in [6].Only the person having the private can decrypt the message.

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

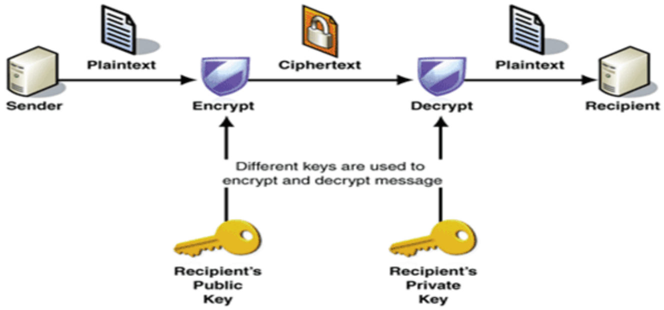

Fig.2: Asymmetric Key Encryption

Symmetric Key Encryption: also know as private key encryption. With symmetric cryptography (or symmetric-key encryption), the same key is used for both encryption and decryption as shown in Fig 3. Symmetric key encryption is very crucial because it is relatively inexpensive to produce a strong key for these ciphers, the keys tend to be much smaller for the level of protection they afford and the algorithms are relatively inexpensive to process. Therefore, implementing symmetric cryptography (especially with hardware) can be highly effective because you do not experience any significant time delay as a result of the encryption and decryption. Symmetric cryptography also ensures authentication because data encrypted with one symmetric key cannot be decrypted with any other symmetric key. Therefore, as long as we will keep the symmetric key secret to the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.

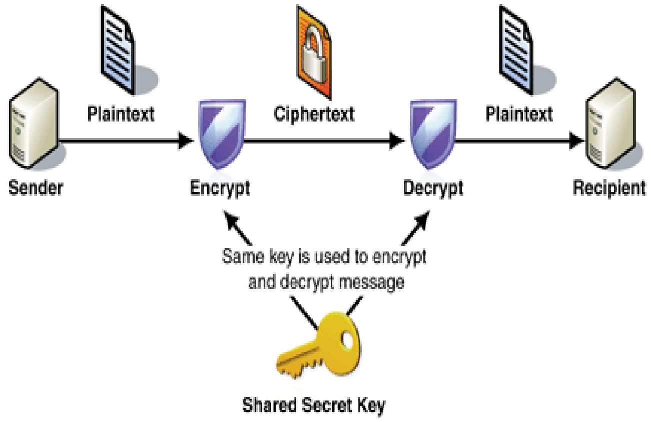

Fig.3: Symmetric Key Encryption

2. RELATED WORK

There has always been a need of securely transfer the message secretly and also keep it as an ever last secure b/w two communicating parties. So the Cryptographers always try to find out such an encryption algorithm that fulfils such need of the peoples. So there are several research of the different great minded person that leads the way toward the unbreakable secure system. Frank Miller in 1882 was the first to describe the one-time pad (a provable secure system) for securing telegraphy.

In 1917, Gilbert Vernam (of AT&T Corporation) invented an electrical one time pad system. Each character in a message was electrically combined with a character on a paper tape key. In the early 1920s, three German cryptographers (Werner Kunze, Rudolf Schauffler and Erich Langlotz), who were basically involved in breaking systems, realized that they could never be broken if a separate randomly chosen additive number was used for every code group. The German foreign office put this system into operation by 1923. Later a new assumption came into focus that leads to a highly secure way of communication. This was the idea of Bounded Storage Model. This Idea was described by U. Maurer with a paper Conditionally-perfect secrecy and approvable-secure randomized cipher.

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. It's limitation is that it's computationally complex.

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.

In year 2013, Prerna Gaur performed a work “Geometry Based Symmetric Key Encryption Using Ellipse” implement 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 2014, Author proposed a symmetric key encryption algorithm termed as A Modified Approach for Symmetric Key Cryptography Using Circles, algorithm is an improvement in the basic Chakra algorithm for symmetric key cryptography. This encryption technique adapts combined transformations, (i.e., translation followed by scaling) of circumference points of every circle by some scaling factor (Sx , Sy) and translation factor (Tx,Ty).

In the proposed approach, there will be no use of sine and cosine functions, thus minimizing the probability of precision errors due to irrational numbers. So, the presented work will be more effective in terms of accuracy. The presented work is about to perform the symmetric cryptography by using two geometric figures and we have selected the ellipse and rectangles as the geometric figures. Geometric operations will be applied on both figures alternatively to encode the information and information will be stored on boundaries of the shapes in bit form. Key generated here will be more complex and very difficult to predict.

3. PROPOSED WORK

In this presented hybrid geometric cryptography approach, some geographical shape has been taken as a cover to place the information and a series of geometric transformation operations will be applied to encode the information. The presented work is defined to achieve the information security travelling over the internet. The work is here defined as the hybrid cryptography approach with the specification of two shapes i.e. ellipse and the rectangle. These shapes will be placed in some geographical area alternatively and information will be stored on boundaries of the shapes in the form of bits. The transforming operations on these two shapes will be applied separately. For ellipse rotation and translation will be applied in series whereas for rectangle these operations will be applied in reverse order. Flow work shows the cryptographic model applied in this work to perform the hybrid geometric cryptography. According to this cryptography technique firstly we will take the input in the textual form. The input is then analyzed under the geometric adaptation. For this analysis, the text is converted into the bit form. Based on this, bit adaptive size is required to store the data in bit form. After that the required number of bits and relatively required size of canvas will be identified. The area based split on is here done to identify the number of possible shapes that can be drawn over this geographical area. From this analysis the actual key will be generated to perform the cryptography. After the key is generated, the next work is to generate these shapes alternatively over some defined geographical area. This shape generation process is repeated till the complete geographical area has not been covered. Finally the bit adaptive model is applied to store the data at identified locations.

The flow of work is defined as:

Step 1: Accept the Input Text

Step 2: Analyze the Text and identify the geometric dimensions

Step 3: Generate the Key for ellipse and rectangle separately

Step 4: Generate these shapes alternatively over the geographical area

Step 5: Store the data on bounds of these shapes

Step 6: Apply alternative transformations on these shapes

Step 7: Collect data in binary form to obtain cryptographic text

The standard model applied as the symmetric key cryptography approach. This proposed approach is defined with specification of geometrical constraints so that the geometric adaptive cryptography is obtained from the work. The presented work model is here defined under the specification of the input text, key and the obtained algorithm. As the plain text is input, the analysis is here performed to generate the key. This dynamic key formation model has improved the strength of work. Once the encoding is done, the data is transmitted and on the receiver side the decoding process is applied. The decoding is here done using the same key and the final normal text is obtained from the work. The key strength of this adapted model includes the alternate shape adaptive data storage. In this work, two shapes are considered called ellipse and the rectangle. These shapes are drawn on the geographical area in a sequence. Once the shape is drawn, the next work is to store the data on these locations. The data is stored here in bit form. After obtaining the shape adaptive data storage, the next work is to perform the encoding. In this work geometric transformation is applied to perform the encoding. In this work two methods are applied to perform encoding. These methods are scaling the rotation algorithms. These algorithms are applied on each location of the stored data bit and the encoded data bits are obtained. Finally the data is retrieved and converted back to the secret form. Here key adaptive cryptography model is shown in figure 4. The figure showed the key generation and the role of key in encryption and decryption process. The figure shows that the algorithm adaptive model is here applied to perform encoding and decoding of data. The work is processed into two parts:

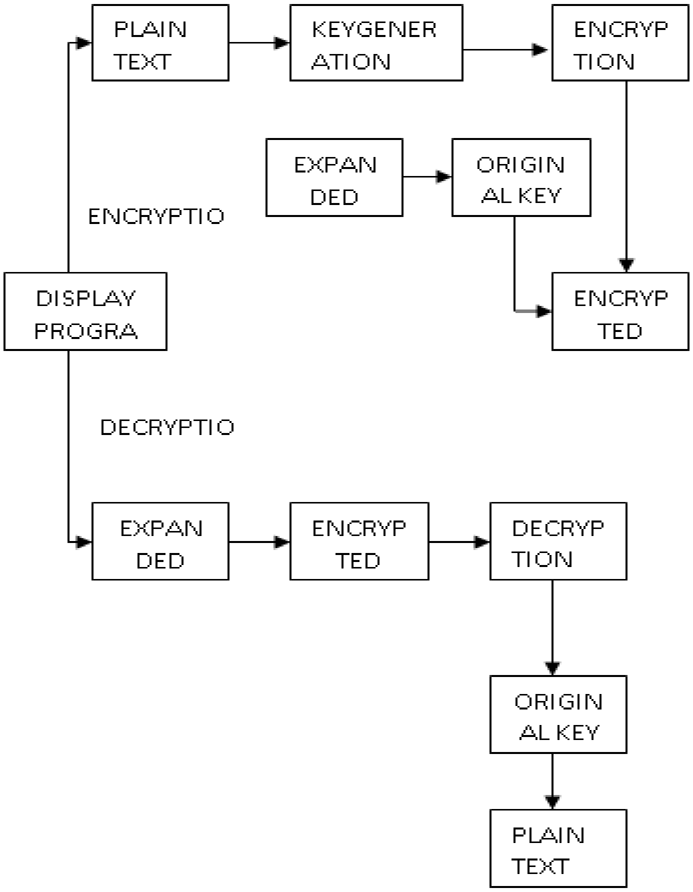

Figure 4: Expended Cryptographic Model

In this part, the text file is selected, this file contain the data to be encrypted. This processing includes the analyses for geometrical shapes and also performs key generation as per the parameters of ellipse and rectangle. The text file data converted into binary shape in order to store the data on the boundary required in next part of processing.

1) Geometric Area Processing

In this part, we generate ellipses and rectangles in hybrid manner using key generated in previous step then we record the data on the bound of these shapes. Now the encoding is performed. After encoding our information, we can get our original data by using decoding scheme in vice-versa manner.

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].

$(x^{'}, y^{'}) = ((xCOSa-ySIN\ a), (xSINa +yCOSa))$

4. ALGORITHM

Key Generation: The key generation is here done in dynamic way. The generation is here done adaptive to the input message

Algorithm (message)

/*message is the plain input text on which the encoding algorithm is applied*/

```
{
    1. Binmessage=ToBinary(message)
       [Transform the input message to binary form]
    2. Len=GetLength(Binmessage)
       [Get the size of message I terms of bits]
    3. Define the static key parameters in terms of individual shape size
    4. eSize=GetReqBit(keyparameers,ellipse)
       [Get the number of bits required to draw the ellipse]
    5. rSize=GetReqBit(keyparameers,rectangle)
       [Get the number of bits required to draw the rectangle]
    6. key=AnalyzeSize(eSize, rSize,Len)
       [Get the geographical Parameters based on these size]
    7. return key
}
```

Area Draw:

Once the key is obtained, the next work is to generate the geometric shapes alternatively to perform the encoding. The drawing algorithm is shown in the figure

GeometricDraw(message,key)

/*message is the input plain text message which is encoded in this presented work, key is the geometric key using which encoding is performed*/

```
{
    1. [AreaX, AreaY, shapeW, ShapeH]=GetKeyParameters(key)
       [Obtained the geographical ara parameters in terms of maximum required area size and the shape constraints]
    2. For x=1 to AreaX [Step shapeW]
       [Identify the shape adaptive locations on the geographical area respective to x axis]
       {
    3. For y=1 to AreaY [Step shapeH]
       [Identify the shape adaptive locations on the geographical area respective to y axis]
       {
    4. If (shapecount=Even)
       [Check for shape adaptively]
       {
    5. DrawRectangle(x,y,shapeW,shapeH)
       [draw the rectangle shape]
       }
    6. Else
       {
    7. DrawEllipse(x,y,shapeW,shapeH)
       [draw the ellipse shape]
```

```
        }
        }
}}
```

5. CONCLUSION

In this paper, a new approach of cryptography is used which is based on geometric figures. Here the random plain text bits are placed on ellipses and rectangles and on these two shapes, two operations are applied alternatively that is translation and rotation to obtain cipher text. In the previous techniques, the ellipse was used as the basic geometric figure to perform the cryptography. But due to 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 makes the use of more complex geometric figures i.e. ellipses and rectangles. We are expecting a high level of reliability from this work.

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

[4] http://www.cryptographyworld.com/concepts.htm

[5] Trisha Chatterjee," Symmetric key Cryptosystem using combined Cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm", 978-1-4673-0125-1@ 2011 IEEE (pp 1179)

[6] Wasim A Al-Hamdani," Elliptic Curve for Data protection", (pp 1-14)

[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] Parisa Kaghazgaran," Secure Two Party Comparison over Encrypted Data", 2011 World Congress on Information and Communication Technologies 978-1-4673-0125-1@ 2011 IEEE (pp 1127-1130)

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