IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 1 ISSUE : 10 Print / Issue Publication Date: 10-Oct-2016

ISSN : 2455-2143

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 10, ISSN No. 2455-2143, Pages 84-88
Published Online August - September 2016 in IJEAST (http://www.ijeast.com)

AN IMPROVED CRYPTOGRAPHIC TECHNIQUE USING TWO DIMENSIONAL ROTATIONS: 2D ROTATION ALGORITHM

Preeti Poonia
Department of Computer Science & Engineering
BRCM CET, Bahal, MDU, India

Praveen Kantha
Department of Computer Science & Engineering
BRCM CET, Bahal, MDU, India

ABSTRACT: In recent day's drastic change in communication like social media network such as mobile communication and computer, all type of a data such as audio, video, images are used for the communication. More Security for that data is an important issue. Cryptography is the technique to transforming plain text (message) into one that is cipher text and then transforming the message back to its original form. Symmetric key Cryptography is a cryptographic approach where the sender and receiver of a message allocate a single, common key that is used to encrypt and decrypt the message Geometry based Cryptography is a new and emerging approach in the field of cryptography. It uses 2-D Rotation and performs geometric transformations on the object matrix to produce cipher text. This work focuses on the symmetric key Cryptography technique, using the concepts of 2-D rotation of object. The main focus in this paper is to produce an algorithm. The proposed algorithm is an improvement in the basic encryption algorithm in terms of accuracy and security.

Keywords – Symmetric key, 2-D Rotation, Substitution, Hill cipher, block cipher, stream cipher.

I. INTRODUCTION

In Cryptography technique, human-being is allowed to encrypt the data in such a technique that the decryption can be performed without the aid of sender. In the world, the network technology has been more advanced and popular ; there is a need to send much information via the Internet. At the same time, the security issues are a crucial problem in the transmission process. In symmetric key encryption, same key is shared by the sender & receiver. Text message are arranged in different 3*n matrices .When there is a need to send a message, the generated key as angle in rotation matrix. Again all the characters in the matrices are converted into hexadecimal. Now the data will be encrypted using rotation matrices. Then the encrypted message and Intermediate-key will be transmitted to the Destination. When the cipher-text reaches the Destination, the rotation key will be computed by using transpose matrix. Then the message will be decrypted.

Cryptography: Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.

Symmetric Cryptography: In the symmetric key encryption, same key is used for both encryption and decryption process. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encrypt them. The symmetric key encryption takes place in two modes either as the block ciphers or as the stream ciphers. The **block cipher** mode provides, whole data is divided into number of blocks. This is based on the block length and the key is provided for encryption. In the case of the **stream ciphers** the data is divided as small as single bit and randomized then the encryption takes place. Symmetric key cryptosystems are much faster than the asymmetric key cryptosystems [7].

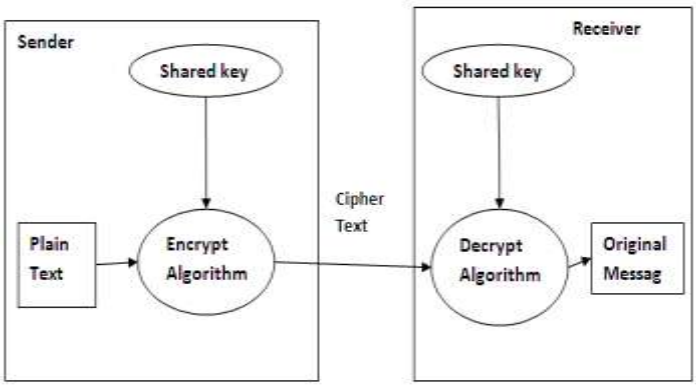


Figure 1: Symmetric cryptographic process

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 10, ISSN No. 2455-2143, Pages 84-88
Published Online August - September 2016 in IJEAST (http://www.ijeast.com)

Substitution Technique In Cryptography:

It is a technique in which the letter of plaintext are replace by other letters or by number or symbols .If the message is view as a series of bits, then substitution involve replace plaintext bit patterns with cipher text bit patterns. Mostly used substitution technique is – Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Cipher etc.

In this paper, introduce the idea form hill cipher technique ,In hill cipher used a matrix as a key and multiply by plaintext .In plaintext, each character is assigned a numerical value like: a=0, b=1,---------- z=25. It is denoted in terms of column vectors and matrices: C=KP, Where C and P are column vectors of length 3, representing the plaintext and the cipher text and K is a 3*3 matrix, which is the encryption key. After multiplication plain text and key apply mod 26. For the decryption process calculate the inverse of matrix K. The K^{-1} of a matrix K is defined by the equation is $K\,K^{-1}= I$ where I is the Identity matrix. K^{-1} is applied to the cipher text, and then the original text is find out for decryption: $P=D(K, C) =K^{-1}C= K^{-1}KP=P$.

Disadvantage: The inverse of a matrix doesn't always exist, but when it does it satisfies the proceeding equation.

In this work, developed algorithm to improve the some constraint introduce in hill cipher by which 2-D rotation matrix with angle.

1. **Two Dimensional Rotations:** In 2-D rotation, rotate the particular object at specific angle θ (theta) from its origin. In the Figure, the point P(x, y) is located at angle φ from the horizontal X coordinate with distance r from the origin.

The Rotation of P point to rotate at the angle θ. After Rotating a new point is P' (X', Y').

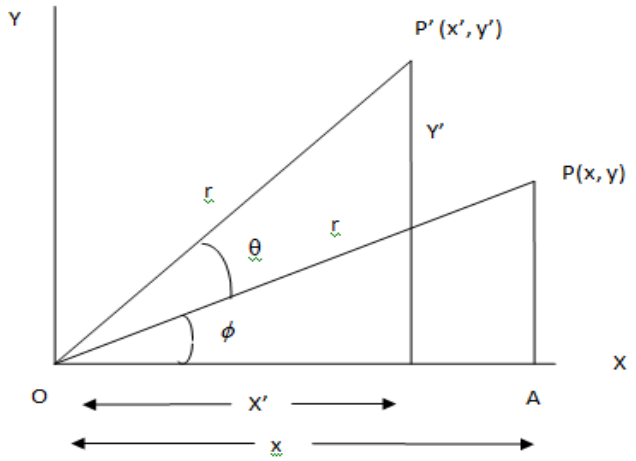


Figure 2: Rotation at point

The point P(x, y) can be represented as, In **Δ**OPA, cos ϕ=x/r, and sin ϕ=y/r , then

$x=r\cos\phi$ ---------- (1)

$y=r\sin\phi$ ---------- (2)

Similarly, the point P' (x', y') represent as in ΔOP'A', cos (θ+ ϕ) =x'/r and sin (θ+ ϕ) =y'/r, then

$x'=r\cos(\theta+\phi)=r\cos\theta\cos\phi - r\sin\phi\sin\theta$ then,

$x'=x\cos\theta - y\sin\theta$---------- (3)

$y'=r\sin(\theta+\phi)= r\sin\phi\cos\theta + r\cos\phi\sin\theta$ then,

$y'= y\cos\theta + x\sin\theta$---------- (4)

Representing the equation (3) and equation (4) in matrix form: In two dimensions every rotation matrix has the following form:

$$R(\theta) = \begin{matrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{matrix}$$

And three dimensions representation are

$$\begin{matrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{matrix}$$

2. Related work:

Deepti Rana et.al. [1] Examines that, cryptography is the science or art of transforming an intelligible message (plaintext) into one that is unintelligible (cipher text) and then transforming the message back to its original form. . Symmetric key Cryptography is a cryptographic approach where the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message Geometry based cryptography is a new and emerging approach in the field of cryptography. It uses geometric shapes such as circles; ellipses etc and perform geometric transformations on these figures to produce cipher text. The presented work focuses on the Symmetric key Cryptography technique, using the concepts of Cartesian coordinate geometry and circle generation. Chakra algorithm, for symmetric key cryptography, is used as the basis for this work with some modifications in it for better results. Chakra is a Sanskrit term which means a circle or a disc. It plays a key role in encryption of data. 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, generate circles on the grid and apply 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(Sx, Sy) and translation factors(Tx,Ty). The proposed

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 10, ISSN No. 2455-2143, Pages 84-88
Published Online August - September 2016 in IJEAST (http://www.ijeast.com)

algorithm is an improvement in the basic Chakra algorithm in terms of accuracy.

Swapnali Krushnarao Londhe et.al.[2] emphasis on, Privacy for that data is an important issue .Cryptography is one of the technique used for stopping unauthorized access and increasing integrity of that data. In this research encryption and decryption scheme is used based on image pixel shuffling and transposition. We can use cipher algorithm for generating key using RGB values of the pixel. For that purpose we use m*n size image on which different operations are performed. This algorithm was implemented in java language.

Mohammad Jabed Morshed Chowdhury et.al.[3], focus on Symmetric Key cryptography is one of the prominent means of secure data transfer through unreliable channel. It requires less overhead than Public Key Cryptosystem. We present here, 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.

Prerna Gaur et.al.[4] proposes a new method for security with symmetric key here 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 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.

II. PROPOSED METHODOLOGY

Here introduced a new advanced symmetric key cryptographic method. By this, introduced new manipulation method for data encryption and decryption of any text. The aim to develop some symmetric key methods where they have used 2D rotation matrix (2D transformation) for encryption and decryption methods. In the present work used a 3*n matrix which obtain from the ASCII value of plain text in a first row and use a random number for which find out second row and last row use the identical value If length of plaintext is less than three add required bogus (dummy) character and multiply this matrix with 2D rotation matrix and rotate with a random angle ɵ. Find out encrypted rotation text matrix. Now convert encrypted rotation matrix into hexadecimal (cipher text) and send to other end.

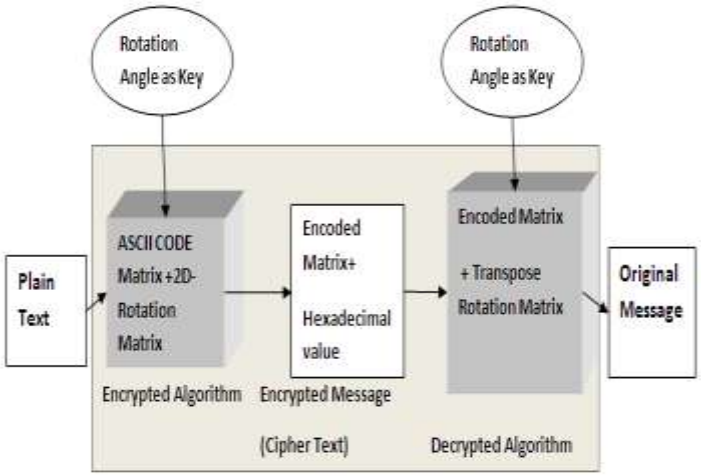


Figure 3: Block Diagram 2-D Rotation Algorithm for Cryptography Technique

Now perform reverse process on cipher text for decryption Convert receiving encrypted hexadecimal value in integer and generate 3*length (plaintext) array matrixes. Transpose of the 2-D Rotation matrix and multiply with new generated matrix then Convert ASCII value to character find out original text message.

III. ALGORITHM

2-D rotation Algorithm:

For Encryption

1. Input text message (plain text)
   Set msg: =plain text
   Theta: = random ɵ (1,360)
2. If length(msg)<3 then
   Add bogus (dummy) character into the plain text to make length equal to three
   End if
3. Generate ASCII value of each character of msg.
   asciivalue[i]=ascii(msg[i]) for all i=1 to length(msg)
4. Create plain text Matrix of (3*length) of asciivalue

plaintext[i,j]=asciivalue[i] for all i=1& j=length(msg) //first row

plaintext[i,j]=asciivalue[i]+rand(1,n) for all i=2& j=length(msg) //second row

plaintext[i,j]=1 for all i=3& j=length(msg) //To make homogeneous Matrix to assign one

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 10, ISSN No. 2455-2143, Pages 84-88
Published Online August - September 2016 in IJEAST (http://www.ijeast.com)

5. Multiplication of 2-D rotation matrix with plaintext matrix

Rotation_plaintext= Rotation_matrix(ɵ)* plain_text matrix(3*length(msg))

6. Convert the Rotation_plaintext matrix into hexadecimal values.

Cipher text=hexadecimal (Rotation_plaintext matrix) //encrypted message

2 -D rotation Algorithm:

For Decryption.

1. Convert encrypted hexadecimal Text to numeric array

Ciphet_Text[i,j]= hexadecimaltonumeric(i)

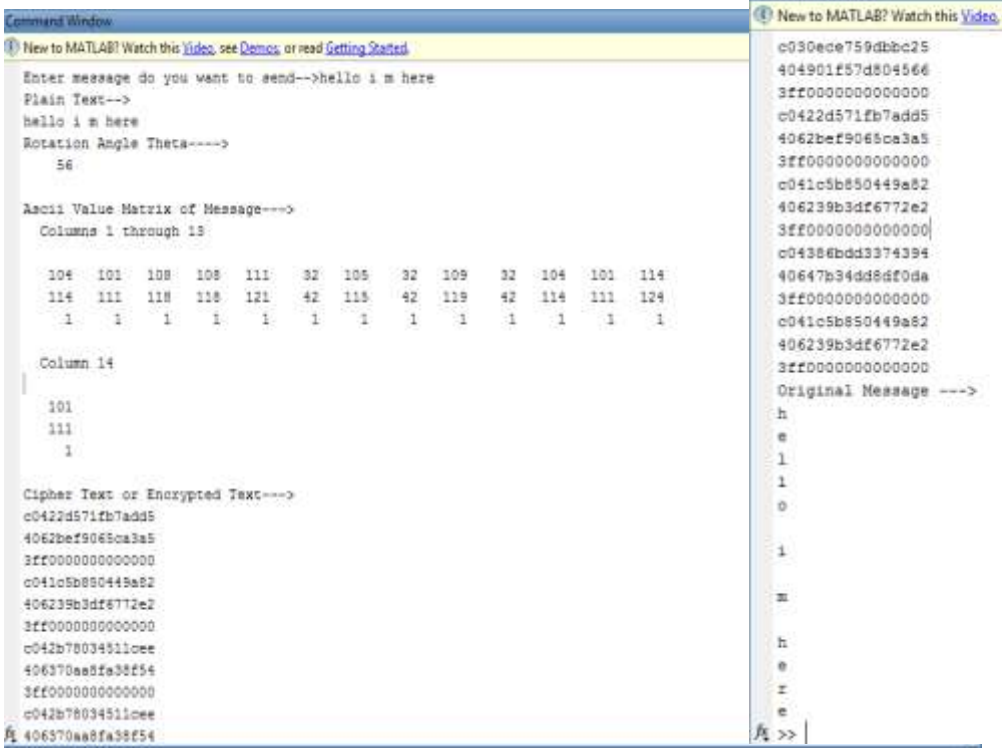
2. Transpose of Rotation matrix.
3. Multiplication of transpose rotation matrix and cipher text matrix

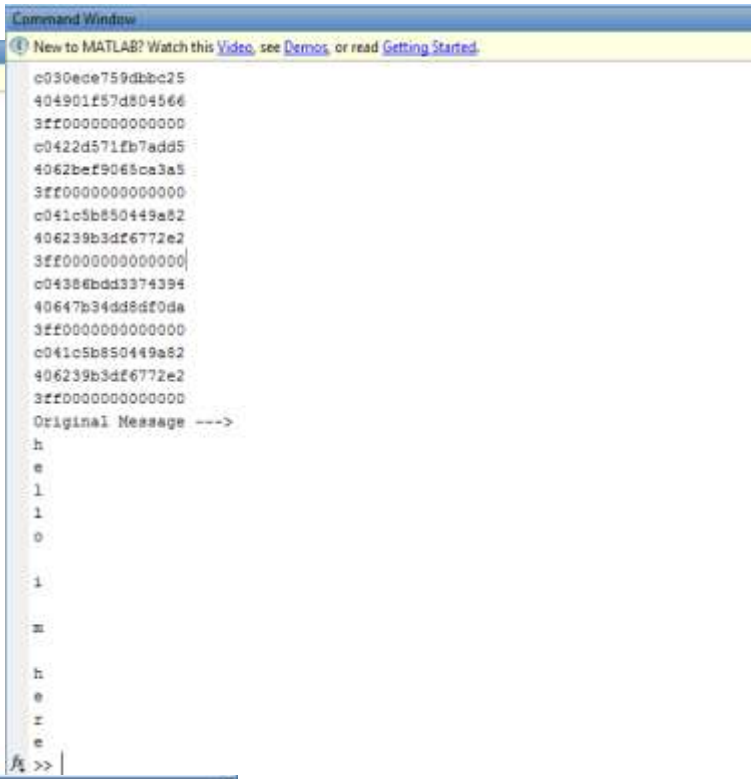
original_asciivalue[i,j]= Transpose_Rotation_matrix(ɵ)* Cipher_Text matrix(3*length(msg))

4. Convert original _asciivalue[i,j] into character for all i=1 & j=1to length(msg)
5. Find original text message.

3. **Experimental work**:

To the encryption and decryption 2-D Rotation algorithm work depict in figure and tool used MATLAB VER R2011.





IV. CONCLUSION

This paper presents a cryptographic key generation algorithm on a 2D transformation using 2D rotation matrix and ASCII value of plain text. The size of text using as an input. And encrypt the message and generate the key. In proposed cipher algorithm in each stage different keys are generated using the different rotation angle values on which different operations are performed. In future we can combines different cryptography method and generate a new hybrid technique for key generation.

V. REFERENCE

[1] Deepti Rana, Shivani Saluja, "A Modified Approach for Symmetric Key Cryptography Using Circles" ," 2014 International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Issue 12, December 2014.

[2]Swapnali Krushnarao Londhe,Megha Dilip Jagtap, Ranjeet Ravindra Shinde, P.P. Belsare , " A Cryptographic Key Generation on a 2D Graphics using RGB pixel Shuffling and Transposition", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 17, Issue 6, Ver. IV (Nov – Dec. 2015).

[3]Chowdhury ,M.J.M.,"A New Symmetric Key Encryption Algorithm based on 2-d Geometry","2009 International Conference on Electronic Computer Technology",2009.

[4] Prerna Gaur,Dr. Paramjeet Singh,"Geometry Based Symmetric Key Cryptography Using Ellipse", International Journal of Application or Innovation in Engineering & Management (IJAIEM),Vol.2, Issue 6",2013.

[5] Donald Hearn, Pauline Baker; " Computer Graphics: C version",Pearson Education; 2005.

[6]. Pratik Shrivastava, Retesh jain, K.S.Raghu Wanshi, A modified. Approach of key manipulation in cryptography using 2D graphics Image, 2014.

[7] Mohit Mittal, "Performance Evaluation of Cryptographic Algorithms", International Journal of Computer Applications, ISSN 0975-8887.

[8]P.Ramesh Kumar,S.S. Dhenakaran,K.L. Sailaja,P.Saikishore, "CHAKRA: A New approach For Symmetric key Cryptography" ,"2012 World Congress on Information and Communication Technologies"(IEEE Journal),2012.

[9]Computer Graphics Principles and Practices second edition by James D. Foley, Andeies van Dam, Stevan K. Feiner and Johb F. Hughes, Addision Wesley.

[10] William Stallings "Cryptography and Network Security: Principles and Practices", PHI Learning Private Limited, Forth Edition, 2009, pp 64 – 86.

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143