ISSN 2278-3091

Volume 8, No.5, September - October 2019

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse106852019.pdf

https://doi.org/10.30534/ijatcse/2019/106852019

A New Circle based Symmetric key Encryption Technique for Text Data

Sailaja K L[1], Srinivasa Rao P [2], Ramesh Kumar P [3]

[1, 3]Department of Computer Science & Engineering, VR Siddhartha Engineering College, Vijayawada, INDIA

[2] Department of CS&SE, AU College of Engineering, Andhra University, Visakhapatnam, INDIA

[1]sailaja0905@gmail.com, [2] peri.srinivasarao@yahoo.co.in, [3] send2rameshkumar@gmail.com

ABSTRACT

Cryptography helps to send data from a sender to a receiver by providing confidentiality and integrity and it is carried out in two different phases – encryption and decryption. So many cryptographic algorithms are proposed for encryption and decryption process. All these algorithms come under either symmetric key cryptography or asymmetric key cryptography. A lot of research is going on these cryptographic algorithms and different approaches have been applied on them. Among all, geometrical approach is one of the most prominent cryptographic techniques. The proposed chakra based Text crypto system is based on chakra symmetric key encryption algorithm [1]. Here the encryption process is applied on Text data of different extensions which is considered as plain text and the corresponding cipher text is generated by the principle of circle generation and rotation. It works with less computational complexity and more confidentiality.

Key words: Cryptography, Cartesian coordinate, encryption, geometric cryptography

1. INTRODUCTION

Information plays major role in all aspects. With the fast development of technology, huge volumes of data are produced and providing security to these data during communication is most essential. Therefore vast research is going on cryptography algorithms. Transmitted text and images have different applications like military, medical, commercial etc. Therefore it is very essential to encrypt the text / image data before transmission via network to maintain security and accessing by unauthorized persons. The circle based encryption process provides a new and efficient way to encrypt the Text data.

2. RELATED WORK

In [2], the authors proposed a hybrid of public key crypto system by combining ECC – for key encryption & digital signature and AES for confidentiality. The main parameters are 192 bit key length, 12 iterations and different types of attacks. With this, the competency is increased and failures are minimized. The cache timing attack correlates the timing details for encryption using known and unknown key and this algorithm prevents the weaknesses posed by timing side channel attack. So many authors work with the Text encryption scheme.

With the advantage of high security with lesser key size the authors used elliptic curve cryptography [3] for text encryption. Here the ASCII values of the plain text are paired up and these values are given as input to the scheme. This procedure avoids mapping which is a costly affair and the common lookup tables need not be distributed to the sender and receiver. This algorithm accepts any type of script consisting of ASCII values. The authors performed key space analysis and key sensitivity analysis which gives better results. The strength of the scheme is analyzed with different attacks and time complexity is also evaluated. This algorithm also reduces the bandwidth utilization.

In article [4], the authors briefly described ECC key exchange, encryption and decryption of both text and images and a detailed explanation of implementing Elliptic Curve Cryptography on text document in C++. The proposed scheme is straightforward and utilized all security features of elliptic curves and is applicable to all ASCII characters.

The article [5] proposed by Maria et.al implemented by ECC. The authors first transformed the message into an affine point on the elliptic curve over the finite field and demonstrated the method of encryption and decryption of a text message. The proposed scheme is almost infeasible to challenge a brute force attack to crack the cryptosystem using ECC.

In [6] the same authors presented the implementation of Elliptic Curve Cryptography and demonstrated encryption and decryption process of a text message and image files in spatial domain by getting security using Comparative Linear Congruential Generator for good random number generation. This allows the cracking of cipher text nearly impossible for the brute force attack. In this article, a Nonce based Elliptic Curve Cryptosystem is proposed. The proposed scheme reduces the processing time, improves the computation speed, less power utilization and less storage necessities. These facilities allow the execution of security system in mobiles, smart cards and other small devices.

.3. METHODOLOGY

3.1 Proposed Scheme

The Text encryption algorithm works based on the geometrical circle properties and transformations – translation & rotation. Here the input plain text is converted into its corresponding binary pattern.

3.2 Encryption Process

The Encryption process is a symmetric key encryption where same key used by the sender and the receiver. This scheme consists of the following parameters as the key – X_L, Y_L are the dimensions of the encryption grid, r – radius of the circle, a -random angle at which the circle is rotated. Based on the above key inputs, a random key is generated by the encryption algorithm.

Encryption Algorithm

1. Input the TEXT to be encrypted.(.txt, .doc, .py, .docx, .pdf)
2. Convert the Text file into sequence of binary patterns.
3. Print the length of the input file Len(File);
4. Enter X_L, Y_L dimensions of the encryption grid;
   If (X_L, $Y_{L)}$ < $_{Len}$(File)
   Then
   Reenter X_L, Y_L
   4.1 Enter the radius of the circle r
   4.2 Create an empty grid and fill it with random bits (0,1)
   4.3 Fill the grid with the Text input string
   4.4 Find the center of the circle (X_C, Y_C) based on the input circle radii;
   4.5 No of circles are generated with random angles(o,90,180,270,360)
   4.6 Generate the circumference point of each circle based on Bresenham circle generation algorithm.
   4.7 Create encrypted file with the file form (enc.)

Generate the key based on the parameters X_L, $Y_{L,}$ r, Image size, random rotation angle.

3.3 Decryption Process

Since this is a symmetric key encryption process, the key which is generated during encryption process is used for decryption also.

Decryption Algorithm

1. Enter the encrypted Text file enc.txt
2. Enter the key string
3. Divide the key into XL, YL, radius, length of the input bits and array of random rotations.
4. Sort the circles based on the XL, YL location.
5. Read each circle and reverse the circle center point XC, YC and circumference point.
6. Rotate each circle in anti clockwise direction based on the key.
7. Save the decrypted file decrypt.txt

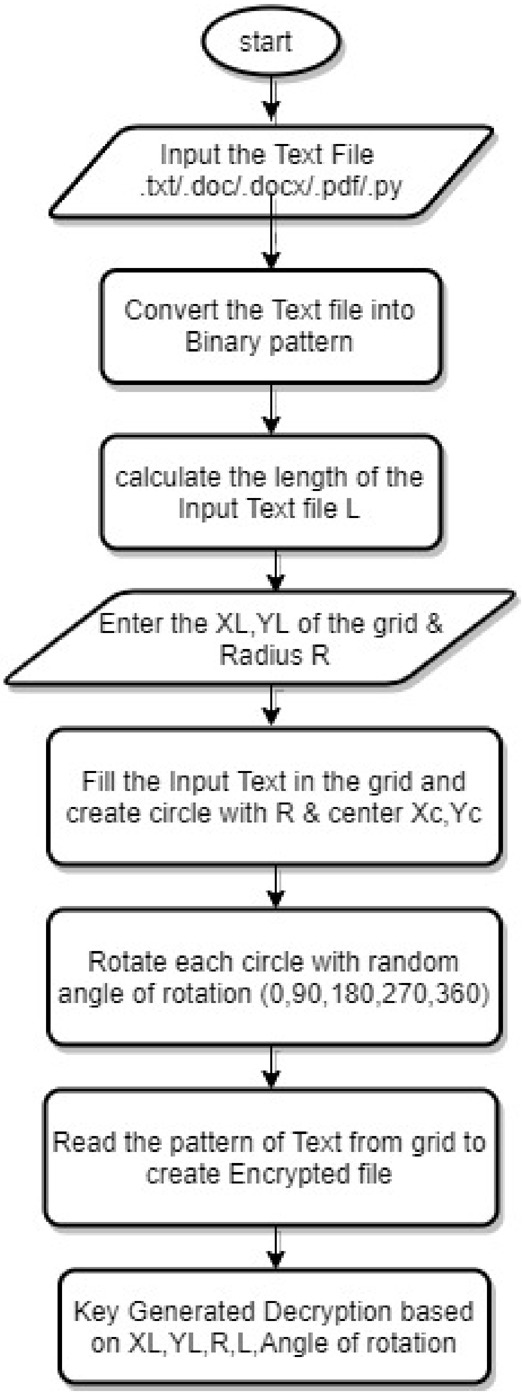
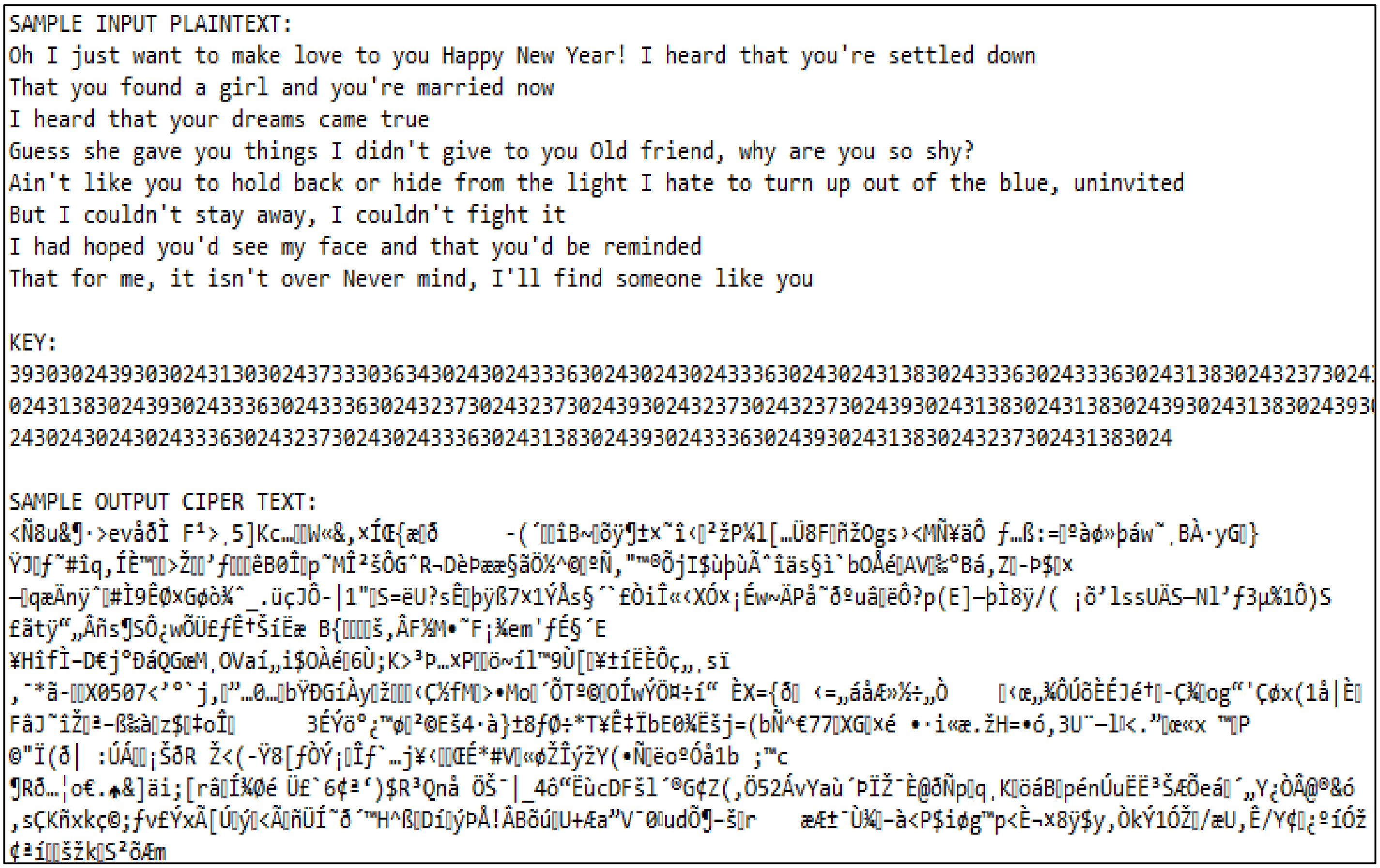

start
Input the Text File .txt/.doc/.docx/.pdf/.py
Convert the Text file into Binary pattern
calculate the length of the Input Text file L
Enter the XL,YL of the grid & Radius R
Fill the Input Text in the grid and create circle with R & center Xc,Yc
Rotate each circle with random angle of rotation (0,90,180,270,360)
Read the pattern of Text from grid to create Encrypted file
Key Generated Decryption based on XL,YL,R,L,Angle of rotation

Figure 1: Flow chart of the proposed Encryption Process

Table 1: Sample Key Parameters

File Name & Type	Plain Text Size	Key Parameters (XL, YL ,r)	No. of Circle generated	Rotation Angle of each circle	Key generated	Encrypted Text Size
Adele.txt	89.1KB	(900,900,100)	41	[360, 270, 0, 0, 360, 360, 360, 90, 180, 270, 180, 90, 270, 0, 180, 0, 90, 180, 90, 360, 180, 360, 180, 0, 270, 0, 270, 270, 360, 270, 180, 0, 90, 0, 180, 270, 270, 360, 270, 90, 270]	393030243930302431303024373330363430243336302432373024302430243336302433363024393024313830243237302431383024393024323730243024313830243024393024313830243930243336302431383024333630243138302430243237302430243237302432373024333630243237302431383024302439302430243138302432373024323730243336302432373024393024323730 24	147KB
Word.docx	14.1KB	(400,400,50)	41	[360, 270, 360, 270, 0, 90, 90, 90, 180, 90, 0, 180, 180, 0, 360, 90, 0, 180, 360, 0, 360, 0, 180, 0, 0, 0, 270, 270, 0, 180, 360, 270, 360, 90, 90, 360, 360, 360, 90, 270, 90]	343030243430302435302439373132302433363024323730243336302432373024302439302439302439302431383024393024302431383024313830243024333630243930243024313830243336302430243336302430243138302430243024302432373024323730243024313830243336302432373024333630243930243930243336302433363024333630243930243237302439302 4	31.4KB
Pdf.pdf	210KB	(1300,1300,500)	5	[360, 180, 270, 360, 270]	313330302431333030243530302431363736353630243336302431383024323730243336302432373024	662 KB



```
SAMPLE INPUT PLAINTEXT:
Oh I just want to make love to you Happy New Year! I heard that you're settled down
That you found a girl and you're married now
I heard that your dreams came true
Guess she gave you things I didn't give to you Old friend, why are you so shy?
Ain't like you to hold back or hide from the light I hate to turn up out of the blue, uninvited
But I couldn't stay away, I couldn't fight it
I had hoped you'd see my face and that you'd be reminded
That for me, it isn't over Never mind, I'll find someone like you

KEY:
39303024393030243130302437333036343024302433363024302430243336302430243138302433363024333630243138302432373024
024313830243930243336302433363024323730243237302439302432373024323730243930243138302431383024393024313830243930
2430243024302433363024323730243024333630243138302439302433363024393024313830243237302431383024

SAMPLE OUTPUT CIPER TEXT:
<Ñ8u&¶·>evåðÌ F¹>¸5]Kc…▯▯W«&,xÍŒ{æ▯ð      -(´▯▯îB~▯õÿ¶±x˜î‹▯²žP%l[…Ü8F▯ñžOgs›<MÑ¥äÔ ƒ…ß:=▯ºàø»þáw˜¸BÀ·yG▯}
ŸJ▯ƒ˜#îq,ÍÈ™▯▯>Ž▯▯’ƒ▯▯▯êB0Î▯p˜MÎ²šÔGˆR¬DèÞææ§ãÖ%^©▯ºÑ,"™®ÕjI$ùþùÃˆîäs§ì`bOÅé▯AV▯‰°Bá,Z▯-Þ$▯x
—▯qæÄnÿˆ▯#Ì9ÊØxGøò%ˆ_.üçJÔ-|1"▯S=ëU?sÊ▯þÿß7x1ÝÅs§ˆˆ£ÒiÎ«‹XÓx¡Éw~ÄPåˆðºuâ▯ëÔ?p(E]—þÌ8ÿ/( ¡õ’lssUÄS—Nl’ƒ3µ%1Ô)S
£ãtÿ“„Âñs¶SÔ¿wÕÜ£ƒÊ†ŠíËæ B{▯▯▯▯š,ÂF%M•˜F¡¾em'ƒÉ§´E
¥HîfÌ-D€j°ÐáQGœM¸OVaí„i$OÀé▯6Ù;K>³Þ…xP▯▯ö~íl™9Ù[▯¥±íËÈÔç„¸sï
,¯*ã-▯▯X0507<’°`j,▯”…0…▯bŸÐGíÀy▯ž▯▯▯‹Ç%fM▯>•Mo▯´ÕTº©▯OÍwÝÖ¤÷í“ ÈX={ð▯ ‹=„áåÆ»½÷„Ò    ▯‹œ„¾ÔÚõÈÉJé†▯-Ç¾▯og“'Çøx(1å|È▯
FâJ˜îŽ▯ª–ß‰à▯z$▯‡oÎ▯      3ÉÝö°¿™ø▯²©Eš4·à}±8ƒØ÷*T¥Ê‡ÏbE0¾Ëšj=(bÑ^€77▯XG▯xé •·i«æ.žH=•ó,3U¨—l▯<.”▯œ«x ™▯P
©"Ï(ð| :ÚÁ▯▯¡ŠðR Ž<(-Ÿ8[ƒÒÝ¡▯Îƒ`…j¥‹▯▯ŒÉ*#V▯«øŽÎýžY(•Ñ▯ëoºÓå1b ;™c
¶Rð…¦o€.♠&]äi;[râ▯Í¾Øé Ü£`6¢ª‘)$R³Qnå ÖŠ¯|_4ô“ËùcDFšl´®G¢Z(,Ö52ÁvYaù´ÞÏŽ¯È@ðÑp▯q¸K▯öáB▯pénÚuËË³ŠÆÕeá▯´„Y¿ÒÂ@®&ó
,sÇKñxkç©;ƒv£ÝxÃ[Ú▯ý▯<Ã▯ñÜÍ˜ð´™H^ß▯Dí▯ýÞÅ!ÂBõú▯U+Æa”V¯0▯udÕ¶-š▯r    æÆ±¯Ù¾▯-à<P$iøg™p<È¬x8ÿ$y,ÒkÝ1ÓŽ▯/æU,Ê/Y¢▯¿ºíÓž
¢ªí▯▯šžk▯S²õÆm
```

Figure 2: Sample Output of the Encryption Scheme.

4. RESULT AND DISCUSSION

For Texts of different formats and different sizes, the key size, key parameters, size of the encrypted text, No of circles generated and rotation angles are presented in Table I. The sample data is taken from the Kaggle data set [7] and the encryption technique is applied on different input texts and the result is presented.

5. CONCLUSION

In this paper, a symmetric encryption and decryption scheme of text data based on the properties of the circle is implemented. The input is a Text data of different sizes and formats. The main strength of this algorithm is the key itself – X_L,Y_L, radius and rotation angles. The key is generated during the encryption process to encrypt the text data. After that the same key is used for decryption process. Hence the proposed algorithm is more secure. This scheme is tested on Kaggle dataset and the experimental results on different size and formats of text are mentioned. The security efficiency is good.

REFERENCES

1. Kumar, P. Ramesh, et al. **"Chakra: A new approach for symmetric key encryption."** 2012 World Congress on Information and Communication Technologies. IEEE, 2012. https://doi.org/10.1109/WICT.2012.6409170
2. Mathur, Nishtha, and Rajesh Bansode. **"AES based text encryption using 12 rounds with dynamic key selection."** Procedia Computer Science 79 (2016): 1036-1043. https://doi.org/10.1016/j.procs.2016.03.131
3. Singh, Laiphrakpam Dolendro, and Khumanthem Manglem Singh. **"Implementation of text encryption using elliptic curve cryptography."** Procedia Computer Science 54 (2015): 73-82. https://doi.org/10.1016/j.procs.2015.06.009
4. Kolhekar, Megha, and Anita Jadhav**. "Implementation of elliptic curve cryptography on text and image."** International Journal of Enterprise Computing and Business Systems 1.2 (2011)
5. S. Maria Celestin Vigila and K. Muneeswaran, **Implementation of Text based Cryptosystem using Elliptic Curve Cryptography,** International Conference on Advanced Computing, IEEE, pp. 82–85, December (2009)
6. Vigila, S. Maria Celestin, and K. Muneeswaran. **"Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications**." IJ Network Security 14.4 (2012): 236-242
7. Paul Mooney**, Song Lyrics Poetry and Lyrics (TXT files)** https://www.kaggle.com/paultimothymooney/poetry
8. Priyanka Thakur, Rajiv Shrivastava **”A Review on Text Based Emotion Recognition System**” International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE),PP 67-71, Volume 7 No. 5 (2018) https://doi.org/10.30534/ijatcse/2018/01752018
9. Azreen Azman, Mostafa Alksher, Eissa Alshari3, Razali Yaakob and Shyamala Doraisamy “**Optimization of Idea Mining Model based on Text Position Weight”**, International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE),PP 120-125, Volume 8 No. 1.4 S.I (2019) https://doi.org/10.30534/ijatcse/2019/1881.42019