International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Enhancement of Data Security using Circular Queue Based Encryption Algorithm

K. Harini, N. Pravallika, K. Sashi Rekha

ABSTRACT: ***Data security is a progressing provocation for designers and Hackers. To battle different attacks by hackers, there is a need for increasingly solid security advancements. In this proposed system, a low complexity circular queue data structure security algorithm can be created. Numerous complicating variable components are used to enhance the quality of this algorithm and make recuperation of original message for hackers, becomes progressively troublesome. These tunable components are the size of the circular queue, the start of the picked keyword letter and the various portrayals of a number are in the Fibonacci manner. All letters ought to be changed over into ASCII binary configuration so as to be utilized by security algorithm in the sensible and shift operations. The outcomes demonstrate that our proposed security algorithm has half low complexity than analyzed multiple circular queues algorithm (MCQA). Fibonacci manner and variable number of difficult factors in this algorithm give adaptability in changing the security of the algorithm as per the conditions. Circular queue is an data structure can be utilized in the data security to make figured message progressively hard to disentangle. For example, a calculation that utilizes the moving and supplanting tasks of bi-section bi-push for round line to expand security. An irregular number was utilized in this algorithm to control the moving between the line and section, in the end this lead to expand the unpredictability of plaintext decrypting.***

Keywords: Data security, hacking, adaptable, complicating variable, Circular Queue

I. INTRODUCTION

Circular Queue may be a linear system within which the operations area unit performed supported FIFO (First in First Out) principle and therefore the last position is connected back to the first position to make a circle. It is also called 'Circular Queue'.

Data security refers to the method of protective knowledge from unauthorized access and knowledge corruption throughout its lifecycle. Data security includes encryption, tokenization, and key management practices that shield knowledge across all applications and platforms. Information security is one of extreme vital points in the arranged network.

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
K. Harini*, B. Tech, Department of computer science and technologies (CSE), saveetha school of engineering, Chennai, India.
N. Pravallika, B. Tech, Department of computer science and technologies (CSE), saveetha school of engineering, Chennai , India.
Sashi Rekha.K, Associate Professor in the Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India.

The significance of this subject has a place with a few current issues incorporating various types' assaults in digital systems administration condition, rupturing the security of clients and expanding use of web for electronic exchanges. The principle Devices of information security are cryptography, steganography, watermarking and information honesty calculations. Initially, cryptography calculations are grouped into symmetric and Asymmetric. The symmetric calculations utilize single basic key for both sender and collector while deviated algorithms utilize two keys for every client. Open key cryptography is a case of Asymmetric algorithms that include utilize open and private keys. Furthermore, steganography is another significant apparatus to shroud data inside a spread bearer to ensure data. Thirdly, watermarking is the security mechanical assembly to check the legitimacy of the data. In conclusion, information honesty calculations speak to the apparatuses that test the uprightness of the information. They incorporate hash work, message validation codes (MAC) and computerized marks. To whole up, data security assumes a noteworthy job in insurance and legitimacy of information and applications running in PC systems. It enables individuals to convey or exchange information electronically without stresses of misdirection. Likewise, guarantee the respectability of the message and validness of the sender. Besides, this paper presents information security calculation which depends on the roundabout line information structure and numerous difficult elements. It tends to be connected to a few applications including correspondence systems, informing administrations, versatile applications. The remainder of this paper is composed as pursues. Area II abridges encryption and decoding calculations. Segment III demonstrates the structure of our proposed model of utilizing roundabout line to upgrade data security. Segment IV displays the exploratory outcomes and investigation. Segment V is utilized to clarify ends and future work.

II. RELATED WORK

Circular Queue is a data structure can be utilized in the data security to make figured message progressively hard to interpret. For example, the creators of paper built up a calculation that utilizes the moving and supplanting activities of bi-section bi-push for roundabout line to expand security. An irregular number was utilized in this calculation to control the moving between the line and segment, in the long run this lead to expand the multifaceted nature of plaintext decoding. In a similar vein, an elliptic bend calculation was planned dependent on network scrambling utilizing round line.

In this exploration additionally uses moving procedure to achieve the encryption and the unscrambling of the content. What's more, a various roundabout exhibits calculation was created to scramble information utilizing three round clusters. This calculation empowered the moving (components in the external or inward cluster), swapping (components among the roundabout exhibits) and XORing (for scrambling the content) in light of producing irregular number. Interestingly, a twofold encryption twofold unscrambling procedure is proposed, which implies the transmitter encodes the content multiple times that drives the beneficiary decode the figure message twice utilizing open key. Likewise, an elliptic bend calculation is created to deliver a figure content. In reality, in this work the content right off the bat shaped into ASCII code, and afterward the prime number and arbitrary number are picked and framed into twofold organization. Where the "0" portrayal of the prime number is mindful of moving the line/segment in upward and left individually. Also, a various access round lines calculation is proposed with variable length in. In this work; distinctive quantities of turns are connected to the round lines, swapping the components in a similar line and XORing the components with creating key number. The creators suggested that these procedures would make a protected plaintext over the transmission line. Then again, Fibonacci arrangement is for the most part utilized for picture encryption. A content to picture encryption calculation is structured utilizing Fibonacci arrangement. This calculation right off the bat changes over the plaintext utilizing Fibonacci grouping, and afterward the Unicode is changed over to hexadecimal number and a RGB network. At long last, a rearranging activity is made to get the picture to be sent.

Utilizing round line in this examination gives a few factors that make the encryption/decoding process progressively troublesome for meddlers to unscramble the cipher text. In addition, these elements are settled upon by both sender and recipient before the encryption procedure. These components can be outlined as pursues:

- The span of the round line is variable.
- The start of the watchword letter is variable.
- The portrayal number in the Fibonacci design.

III. EXISTING SYSTEM:

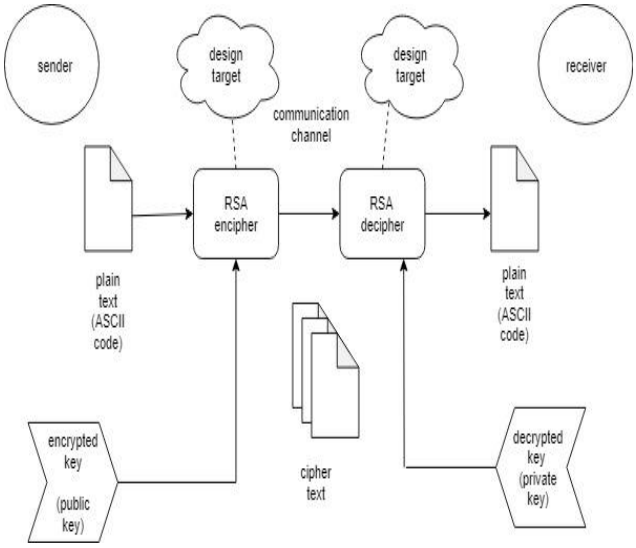
There are several forms of security technology available, but encryption is one that every data computer users should know about.

The technology comes in several forms with key size and strength usually being the most important variations in one selection from succeeding.

1. One of the existing algorithms in data security is RSA.
2. RSA is an example for Asymmetric tool in data security.
3. Unlike triple DES, RSA is taken into account associate degree uneven rule thanks to its use of a combine of keys.

For encrypting the data, we will use public key and for decrypting the data we will use private key

DIAGRAM:



IV. PROPOSED SYSTEM

In this field, the proposed algorithm is illustrated thoroughly. It is primarily based principally on using a circular queue arrangement in secret writing and cryptography processes. At the start, a circular queue that employed in our projected rule is shown in Fig 1. The "n" during this figure refers to the scale of the circular queue and also the plaintext is shown within the circular queue. The letters within the core of the circle represents the keyword letters to be shifted to the correct and left so XORed with plaintext to get cipher text.

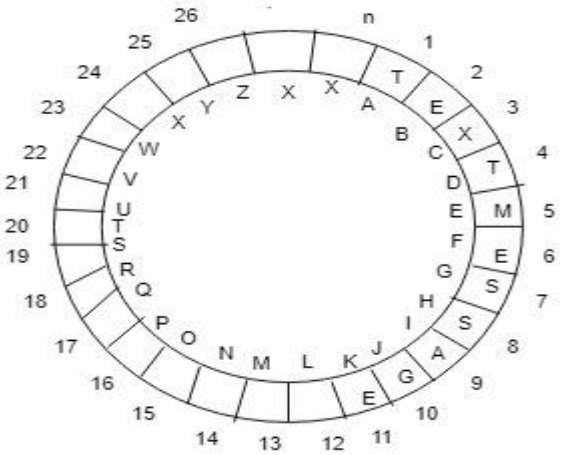


Fig. 1 Circular Queue representation

Utilizing round line in this examination gives a few factors that make the encryption/decoding process progressively troublesome for meddlers to unscramble the cipher text. In addition, these elements are settled upon by both sender and recipient before the encryption procedure. These components can be outlined as pursues:

1.The span of the round line is variable.
2.The start of the watchword letter is variable.
3.The portrayal number in the Fibonacci design.

In the data security we have two process. They are:

1. ENCRYPTION PROCESS
2. DECRYPTION PROCESS

V. ENCRYPTION PROCESS

To scramble a record or other data put away in a PC intends to change over it into a mystery code with the goal that it can't be utilized or comprehended until it is decoded or unscrambled. You should need to scramble a document on the off chance that it contained a mystery equation for another development, or some money related plans that your rivals would love to think about ahead of time. When you scramble something, the PC will request that you set up a secret word. From that point forward, nobody will most likely understand the data except if they have a similar secret key. Encryption conceals your information from inquisitive eyes. This is a procedure of encoding information to keep unapproved individual from survey or changing it. The principle highlights of information encryption are:

1.Forestalls undesirable access to records and email messages

2. Most grounded dimensions of encryption are hard to break.

The encryption procedure starts by conveying plaintext letters in the round line. At that point these letters and watchword letters are changed over to their identical 8 bits ASCII code and XORed with one another. From that point forward, the resultants are spoken to as decimal numbers. At long last, these numbers are shown into Fibonacci arrangement to be sent as a figure content, as delineated.

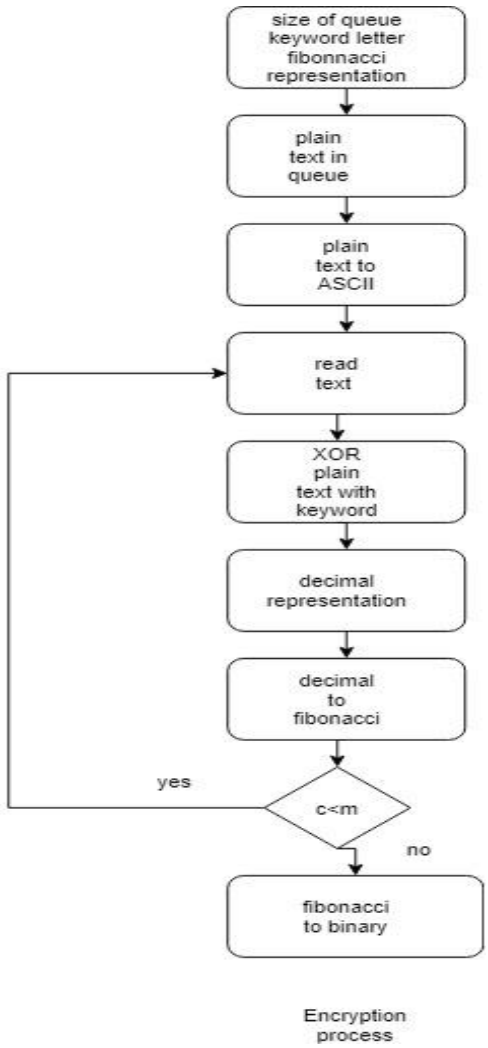


Fig. 2 Encryption process Let us consider below text message as example,

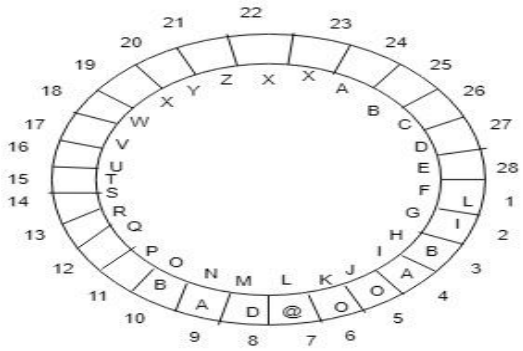


Fig. 3 Sample Example ("LIBAOO@DAB")

Given example below illustrates the secret writing method in a very range of steps. Let take the primary name of the authors as a plaintext "LIBAOO@DAB".As shown in Fig. 2 earlier, the sender and receiver ought to agree on 3 factors. The values of these factors in this example as follows:

factor1: the size of circular queue is 28 as shown in Fig. 3.

factor2: the keyword letter started with letter "F" as shown in Fig.3.

factor3: the illustration of the number is that the first illustration.

Steps for Encryption process:

STEP 1: Rewrite the plaintext and keyword letters into the ASCII code

Letters	ASCII Code							
L	0	1	0	0	1	1	0	0
I	0	1	0	0	1	0	0	1
B	0	1	0	0	0	0	1	0
A	0	1	0	0	0	0	0	1
O	0	1	0	0	1	1	1	1
O	0	1	0	0	1	1	1	1
@	0	1	0	0	0	0	0	0
D	0	1	0	0	0	1	0	0
A	0	1	0	0	0	0	0	1
B	0	1	0	0	0	0	1	0

Step 2: Perform XOR operation with the plaintext letters and keyword letters.

Plain letter	**L**	0 1 0 0 1 1 0 0
Keyword letter	**F**	0 1 0 0 0 1 1 0
Encrypted letter		0 0 0 0 1 0 1 0

Plain letter	**I**	0 1 0 0 1 0 0 1
Keyword letter	**G**	0 1 0 0 0 1 1 1
Encrypted letter		0 0 0 0 1 1 1 0

Plain letter	**B**	0 1 0 0 0 0 1 0
Keyword letter	**H**	0 1 0 0 1 0 0 0
Encrypted letter		0 0 0 0 1 0 1 0

Plain letter	**A**	0 1 0 0 0 0 0 1
Keyword letter	**I**	0 1 0 0 1 0 0 1
Encrypted letter		0 0 0 0 1 0 0 0

Plain letter	**O**	0 1 0 0 1 1 1 1
Keyword letter	**J**	0 1 0 0 1 0 1 0
Encrypted letter		0 0 0 0 0 1 0 1

Plain letter	**O**	0 1 0 0 1 1 1 1
Keyword letter	**K**	0 1 0 0 1 0 1 1
Encrypted letter		0 0 0 0 0 1 0 0

Plain letter	**@**	0 1 0 0 0 0 0 0
Keyword letter	**L**	0 1 0 0 1 1 0 0
Encrypted letter		0 0 0 0 1 1 0 0

Plain letter	**D**	0 1 0 0 0 1 0 0
Keyword letter	**M**	0 1 0 0 1 1 0 1
Encrypted letter		0 0 0 0 1 0 0 1

Plain letter	**A**	0 1 0 0 0 0 0 1
Keyword letter	**N**	0 1 0 0 1 1 1 0
Encrypted letter		0 0 0 0 1 1 1 1

Plain letter	**B**	0 1 0 0 0 0 1 0
Keyword letter	**O**	0 1 0 0 1 1 1 1
Encrypted letter		0 0 0 0 1 1 0 1

Step 3: convert the encrypted outputs as decimal numbers.

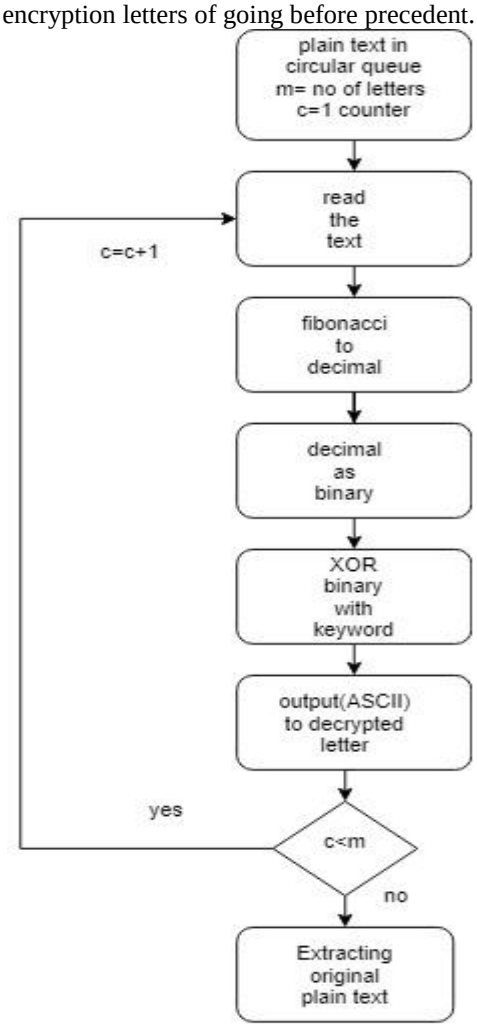
Encrypted letter	Decimal number
0 0 0 0 1 0 1 0	10
0 0 0 0 1 1 1 0	14
0 0 0 0 1 0 1 0	10
0 0 0 0 1 0 0 0	8
0 0 0 0 0 1 0 1	5
0 0 0 0 0 1 0 0	4
0 0 0 0 1 1 0 0	12
0 0 0 0 1 0 0 1	9
0 0 0 0 1 1 1 1	15
0 0 0 0 1 1 0 1	13

Step 4: converting the decimal numbers into Fibonacci format to be sent as binary numbers.

Decimal number	Fibonacci format 21 13 8 5 3 2 1 1
10	0 0 1 0 0 1 0 0
14	0 1 0 0 0 0 0 1
10	0 0 1 0 0 1 0 0
8	0 0 1 0 0 0 0 0
5	0 0 0 1 0 0 0 0
4	0 0 0 0 1 0 0 1
12	0 0 1 0 1 0 0 1
9	0 0 1 0 0 0 0 1
15	0 0 1 1 0 1 0 0
13	0 0 1 0 1 1 0 0

VI. DECRYPTION PROCESS:

Decryption process is translating scrambled data so that is can be accessed again by approved clients. To make the information private, data (plain content) is encoded utilizing a specific algorithm and a secret key. After encryption process, plain content gets changed over into cipher text. To decode the cipher text, similar algorithm is utilized and toward the end the first information is acquired once more. The decryption process is the invert activity of encryption to recoup the first message. In the wake of getting the cipher text in Fibonacci design, it changed over back to the decimal number as appeared. At that point, these numbers are XORed with keyword letter as per their areas. In the long run, the first message is re-established. The key point in this procedure is to play out the change procedure of the Fibonacci number cautiously. To exhibit the decoding procedure, we have utilized encryption letters of going before precedent.



decryption process

From the last step of Encryption process, the message is decrypted by the following steps

The steps of Decryption process are:

Step 1: The received encrypted message (Fibonacci number) is converted to decimal number

Fibonacci format 21 13 8 5 3 2 1 1	Decimal number
0 0 1 0 0 1 0 0	10
0 1 0 0 0 0 0 1	14
0 0 1 0 0 1 0 0	10
0 0 1 0 0 0 0 0	8
0 0 0 1 0 0 0 0	5
0 0 0 0 1 0 0 1	4
0 0 1 0 1 0 0 1	12
0 0 1 0 0 0 0 1	9
0 0 1 1 0 1 0 0	15
0 0 1 0 1 1 0 0	13

Step 2: Decimal number is converted to binary format.

Decimal number	Binary format
10	0 0 0 0 1 0 1 0
14	0 0 0 0 1 1 1 0
10	0 0 0 0 1 0 1 0
8	0 0 0 0 1 0 0 0
5	0 0 0 0 0 1 0 1
4	0 0 0 0 0 1 0 0
12	0 0 0 0 1 1 0 0
9	0 0 0 0 1 0 0 1
15	0 0 0 0 1 1 1 1
13	0 0 0 0 1 1 0 1

Step 3: Perform XOR operation between the binary numbers and the keyword letters.

Binary number	**10**	0 0 0 0 1 0 1 0
Keyword letter	**F**	0 1 0 0 0 1 1 0
Decrypted letter		0 1 0 0 1 1 0 0

Binary number	**14**	0 0 0 0 1 1 1 0
Keyword letter	**G**	0 1 0 0 0 1 1 1
Decrypted letter		0 1 0 0 1 0 0 1

Binary number	**10**	0 0 0 0 1 0 1 0
Keyword letter	**H**	0 1 0 0 1 0 0 0
Decrypted letter		0 1 0 0 0 0 1 0

Binary number	**8**	0 0 0 0 1 0 0 0
Keyword letter	**I**	0 1 0 0 1 0 0 1
Decrypted letter		0 1 0 0 0 0 0 1

Binary number	**5**	0 0 0 0 0 1 0 1
Keyword letter	**J**	0 1 0 0 1 0 1 0
Decrypted letter		0 1 0 0 1 1 1 1

Binary number	**4**	0 0 0 0 0 1 0 0
Keyword letter	**K**	0 1 0 0 1 0 1 1
Decrypted letter		0 1 0 0 1 1 1 1

Binary number	**12**	0 0 0 0 1 1 0 0
Keyword letter	**L**	0 1 0 0 1 1 0 0
Decrypted letter		0 1 0 0 0 0 0 0

Binary number	**9**	0 0 0 0 1 0 0 1
Keyword letter	**M**	0 1 0 0 1 1 0 1
Decrypted letter		0 1 0 0 0 1 0 0

Binary number	**15**	0 0 0 0 1 1 1 1
Keyword letter	**N**	0 1 0 0 1 1 1 0
Decrypted letter		0 1 0 0 0 0 0 1

Binary number	**13**	0 0 0 0 1 1 0 1
Keyword letter	**O**	0 1 0 0 1 1 1 1
Decrypted letter		0 1 0 0 0 0 1 0

Step 4: Rewrite the XOR output which represent the ASCII code of the plaintext to original message.

XOR output	Letter
0 1 0 0 1 1 0 0	L
0 1 0 0 1 0 0 1	I
0 1 0 0 0 0 1 0	B
0 1 0 0 0 0 0 1	A
0 1 0 0 1 1 1 1	O
0 1 0 0 1 1 1 1	O
0 1 0 0 0 0 0 0	@
0 1 0 0 0 1 0 0	D
0 1 0 0 0 0 0 1	A
0 1 0 0 0 0 1 0	B

VII. SECURITY ANALYSIS:

Security examination is the investigation of tradable money related instruments called securities. It manages finding the correct estimation of individual securities (i.e., stocks and bonds). These are generally grouped into obligation securities, values, or some half and half of the two. Tradable credit subsidiaries are additionally securities. Wares or fates contracts are not securities. They are recognized from securities by the way that their execution isn't subject to the administration or exercises of an outside or outsider. So as to investigation the security execution of our encryption/decoding calculation, let accept busybodies have the cipher text as represented in the precedent. They endeavour to unscramble the message by changing over these paired digits to the ASCII code. Thus, the outcome as pursues:

Original message	If hacker decodes message to binary	Decoded message by hacker
L	00100100	$
I	01000001	A
B	00001001	Space
A	00100000	Space
O	00001000	BS
O	00000100	EOT
@	00100000	Space
D	00100100	$
A	00001001	HT
B	00100000	!

If the hacker hacks the message, the message decoded by the hacker is different from the original message if the proposed algorithm is followed.

The recuperated message by meddlers is entirely unexpected from unique message and such outcome demonstrates trouble of certain sorts of assaults, for example, measurable and straight. Such accomplishment of trouble is ascribed to the difficult components of variable line measure, variable key size and diverse Fibonacci design portrayals. Therefore, our proposed calculation is fulfilling required privately by utilizing variable size components. In addition, Fibonacci group adds greater intricacy to the decoding procedure. Moreover it exhibits another case of our encryption calculation, where the image "… "Is a reached out of the ASCII code and has no portrayal. Choices on these agreements are anyway viewed as securities, since execution is presently subject to the exercises of an outsider. The examination of different tradable money related instruments is called security investigation. Security examination assists a money related master or a security examiner with determining. The examination of different tradable money related instruments is called security investigation.

Security examination assists a money related master or a security examiner with determining the estimation of benefits in a portfolio.

VIII. CONCLUSION:

In this examination another information structure based security calculation is proposed. The noteworthiness of this calculation is utilizing roundabout line and Fibonacci arrangement to be sent as a figure content. The unscrambling procedure is trying because of the use of variable elements. Also, our calculation offers adaptable size tenable system. The most significant issue is the understanding among sender and recipient to change round line estimate, watchword letter/image and the portrayal of the Fibonacci number before foundation of association. Moreover, our calculation is quicker than MACQ calculation because of low multifaceted nature of the encryption/unscrambling forms. We need to specify that proposed calculation is utilized for instant messages. Nonetheless, we will intend to encode different kinds of information such pictures, voice and video utilizing this calculation. In this exploration another data structure based security calculation is proposed. The significance of this algorithm is utilizing circular queue and Fibonacci grouping to be sent as a cipher content. The decryption process is challenging because of the utilization of variable components. In addition this algorithm offers adaptable size tuneable component. The most important issue is the agreement between sender and receiver to change circular queue size, keyword letter/symbol and the representation of the Fibonacci number before establishment of connection.

REFERENCES

1. Kahate, Atul., "Cryptography and Network Security", Tata McGraw-Hill Education, 2013.
2. Ali J. Abboud, "Multifactor Authentication For Software Protection", Diyala Journal of Engineering Sciences, Vol. 08, No. 04, Special Issue, 2015.
3. Ali J. Abboud ,"Protecting Documents Using Visual Cryptography", International Journal of Engineering Research and General Science ,2015.
4. E. Barker, W. Barker, W. Burr, W. Polk and M. Smid, "Recommendation for Ke Management-Part 1: General(Revision 3)", Computer Security Division.
5. P. Agarwal, N. Agarwal and R. Saxena, "Data Encryption Through Fibonacci Sequence and Unicode Characters", MIT International Journal of Computer Science and Information Technology, Vol. 5, No. 2, pp. 79-82, August 2015
6. Hankerson, Darrel, Alfred J. Menezes, and Scott Vanstone," Guide to Elliptic Curve Cryptography", Springer and Business Media, 2015.
7. Wei and S. Zhang, "Using auto-generated materials to facilitate instructors' offline 151-152.
8. S. Zhang, "An Auto-Generation Approach to Create Visualization Teaching Materials for Data Structures andAlgorithms in MS-PPT Format," International Journal of Information and Education Technology vol. 5, no. 9, pp. 714-718, 2015.
9. R. S. Baker, M. Boilen, M. T. Goodrich, R. Tamassia, andB. A. Stibel, "Testers and visualizers for teaching data structures," SIGCSE Bull., vol. 31, pp. 261-265, 1999.
10. C. Tao and T. Sobh, "A tool for data visualization andvisualization and user-defined algorithm animation," in user-defined algorithm animation," in Frontiers inEducation Conference, 2001. 31st Annual, 2001, pp. TID2 Vol.1.
11. R.d.V. Virseda, "A visualization tool for tutoring the interactive learning of data structuresand algorithmic schemes," in Proceedings of the 41st ACM technical symposium on Computer science education (SIGCSE '10). ACM, Milwaukee, Wisconsin, USA,187-191.
12. E. Barker, W. Barker, W. Burr, W. Polk and M. Smid, "Recommendation for Ke Management-Part 1: General (Revision 3)", Computer Security Division (Information Technology Laboratory), 2016.
13. Wu, Suli, Yang Zhang, and Xu Jing. "A Novel Rule of Encryption Algorithm based on Shifting and Exchanging bi-column bi-row Circular Queue", IEEE International Conference on Computer Science and Software Engineering, Vol. 3. , 2008.
14. Amounas, Fatima., "An Elliptic Curve based on Matrix based on Matrix Scramblin Method", IEEE International Scramblin Method", IEEE International Conference on Network Security and Systems (JNS2), 2012.
15. I. Bezakova, J. E. Heliotis, and S. P. Strout, "Board game strategies in introductory computer science," in Proceeding of the 44th ACM technical symposium on Computerscience education (SIGCSE '13). ACM, Denver, Colorado, USA, 17-22.
16. Lawrence, "Teaching data structures using competitive games," Education, IEEE Transactions on, vol. 47, pp. 459466, 2004.

AUTHORS PROFILE

K. Harini, B. Tech, Department of computer science and technologies (CSE), saveetha school of engineering, Chennai.

N. Pravallika, B. Tech, Department of computer science and technologies (CSE), saveetha school of engineering, Chennai

SASHI REKHA.K is an Associate Professor in the Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai with 14.9 years of teaching experience and 2 years of industrial experience. She graduated her B.E from Madras University, M.E., from Anna University and currently Pursuing Ph.D. from Anna University in Computer Science and Engineering. Her research interests are Distributed Computing and Network Security. Her research contributions have culminated in 14 publications which include 4 International Journals, 10 International Conferences and 4 National Conferences.