International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 7, Issue 11, November 2018)

A Novel Approach towards designing highly secure Cryptography Encryption Algorithm

Neeraj Singh[1], Prof. Nitin Choudhary[2]

[1]*M.tech Scholar,* [2]*Assistant Professor, Computer Science & Engineering, Kopal Institute of Science & Technology*

Abstract: **Information security is a progressing challenge for designers and programmers. To battle diverse assaults by programmers, there is a need for more reliable security innovations. In this research work a low complexity security algorithm is created. Utilizing different confounding variable elements is the quality of this calculation and makes retrieval of unique message by attacker more troublesome. I have first implemented DSEA [12] algorithm and found that the algorithm is easy to break or guess the keyword as there are only 26 different combinations of key is used. Then i implemented the algorithm which overcome the problem of DSEA [12] algorithm and also improve the outcomes. In this research I used 256 key combinations that make recovery of original message by attackers more difficult. All letters of key ought to be changed over into ASCII binary format keeping in mind the end goal to be utilized by security algorithm in the circular left rotation operation. The outcomes appear that our proposed security algorithm has less complexity as compare to Data Structure Encryption Algorithm based on circular queue to enhance data security (DSEA) (2018).**

Keywords **- Encryption, decryption, plain text, cipher text, symmetric key and Crytography.**

I. INTRODUCTION

We live in a large World in terms of physical boundaries but in terms of communication, this world become too small. By this communication system transmission of different type of data from one location to another location become easier. At one end this is very an enormous thing but at another end there is also a high risk of information leakage. Hundred percent controlling of this information leakage is very hard, so there is multiple method of information hiding through which information can be changed before sending.

These information hiding methods are called encryption. Different encryption methods are introduced time by time. Each such method has their own copouts between security and time complexity. Cryptography means not only providing information security, but rather one set of techniques. It is the study of mathematical techniques which keeps the aspect of information security, like privacy, integrity of data and entity authentication. Confidentially means keeping information covert from all and only see it the authorized one. Data integrity means to ensure that the information reached to the receiver in unaltered form. There are some characteristics of cryptographic algorithm: security, performance, and ease of implementation.

Security defined to defeat the objective by an upper bound of work. Performance means the efficiency of an algorithm calculated in a specific mode of an operation. There are many points of security: Security service, security mechanism, and security attack. Security service means a service that increases the data processing system security and information transfers of an organization. Security mechanism means that are designed to detect, prevent, or recover from a security attacks. Security attack means any action that harm security of information owned by an organization. Encryption means the process of converting information or data from plaintext to cipher text. A small or large piece of information, usually consist of a number is called key, that allows a receiver. There is also second key also allows a receiver to decode messages sent to him or her. There are some types of encryption. These include classical techniques, modern techniques, and public-key encryption techniques. Classical techniques again categorized in substitution and transposition techniques. Substitution techniques are again categorized in Caesar cipher, mono-alphabetic cipher and poly alphabetic cipher. Block cipher, stream cipher and DES algorithm comes under the modern techniques. In Public-key encryption the RSA algorithm is there. Digital Signatures is also a part of cryptography that look like in functionality of hand-written signature and Digital Certificates that related to an unique ID -card or other related to office. There are some applications of cryptography based on communication, identification, electronic commerce, key recovery identification and remote access. For securing information and protecting data, modern cryptography provides essential techniques.

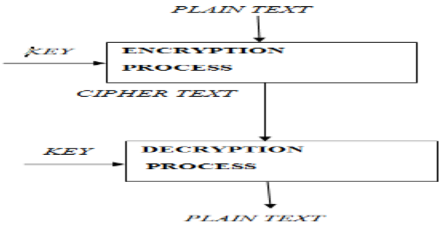


Figure 1: Encryption and Decryption

1.1 *Introductory Terms*

- *Encryption:* when a mathematical process is applied on plain text to transform it in a cipher text then these process is called encryption.

- *Decryption:* It is a process of converting (unscrambling) files or documents from an encrypted form (cipher text) to an unencrypted form (plaintext). It is opposite of encryption technique.
- *Plain Text:* Plaintext is unencrypted text (clear text), the original message or filet o which an encryption algorithm is applied.
- *Cipher Text:* It is a form of plain text comes from encrypted message or data, scrambled into unreadable form.
- *Symmetric Key:* Sharing of same key for communication by both sender and receiver.

1.2 Cryptographic Algorithm categories

There are main two types of cryptographic algorithm.

- Symmetric key
- Asymmetric key

1.2.1 Symmetric key

- Sender and Receiver share a same key.
- A undisclosed piece of information used to encrypt or decrypt the message.
- If a key is covert, than only sender or receiver can read the message
- If Alice and bank each has secret key, than they may send each other private message.
- The task of privately choosing a key before communication however can be problematic.

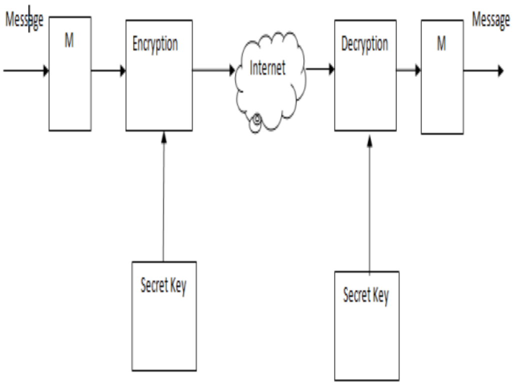


Figure 2: Process of Symmetric Key Encryption Algorithm

1.2.2 Asymmetric key:

- Defining the algorithm for solving the key exchange problem which uses two keys, each key is used to encrypt the message.
- If one is used to encrypt a message, another key must be used to decrypt it.
- This makes it possible to receive secure message by simply publishing one key (public key) and keeping another secret (private key).
- Any one may encrypt a message using public key, but only the owner of the public key is able to read it.
- In this way Alice may send private message to owner of a key-pair (the bank) by encrypting it using their public-key. Only bank can decrypt it.

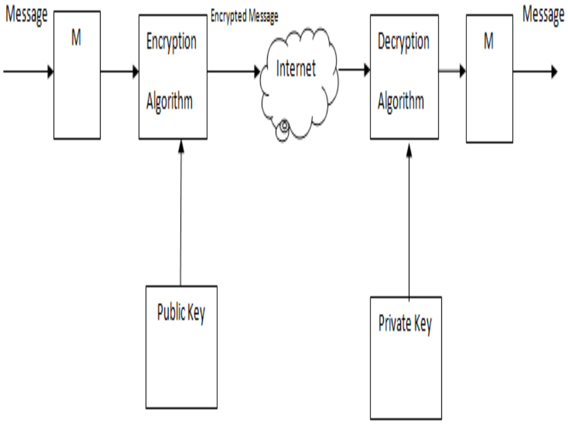


Figure 3: Process of Asymmetric Key Encryption Algorithm

1.3Goals of cryptography

The main goals of cryptography are [11]

- *Confidentially or privacy:* Keeping information secret from all and give access to those who are authorized to see it. Confidentially means protection of transmitted data from passive attacks .
- *Data integrity:* Ensuring that information has not altered by an unauthorized or unknown means. One must have the ability to detect insertion or some substitution in information by illicit parties. This insertion, deletion, and substitution is called Data manipulation.
- *Authentication:* It is a service associated with identification. This function applies to both entities and information.
- *Non-repudiation:* It prevents denying of message from either sender or receiver. Thus, whenever any message is transfer then receiver prove it that the message was send by the suspected sender. Similarly, when a message is received, the sender can prove the suspected receiver is receiving that message.

1.4 Application of cryptography

- Secrecy in Transmission
- Secrecy in Storage space
- Integrity in message Transmission
- Integrity in Storage
- Authentication of Identity
- Credentialing Systems
- Electronic Signatures
- Electronic Cash
- Threshold Systems
- Systems Using Changing Keys
- Hardware to Support Cryptography

II. Literature Survey

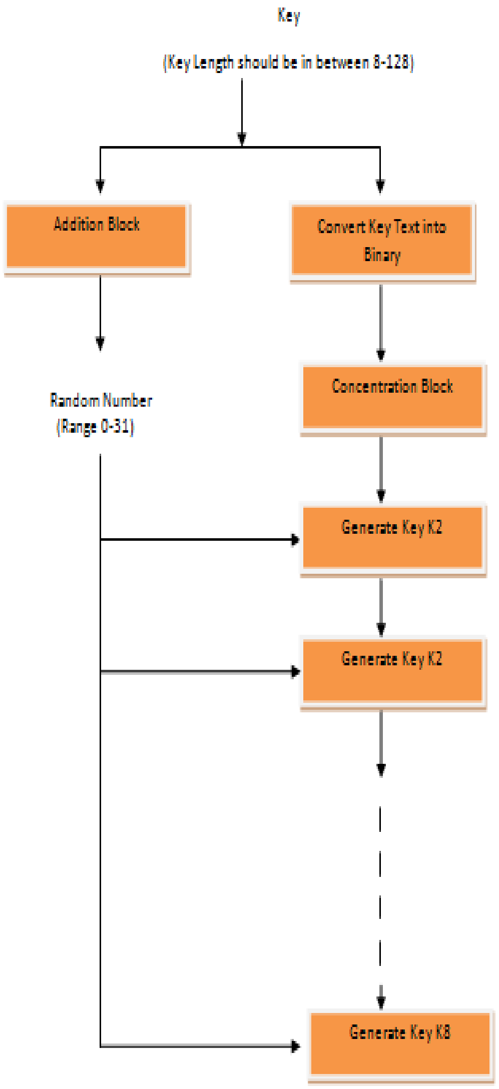
Many existing researchers have proposed various methods to encrypt the information. Some proposed an algorithm in which circular queue as data structure is used to encrypt the data some applied operation on circular array and some applied double encryption and decryption concept to provide better security on their data .

Circular queue is a data structure can be employed in the information security to make ciphered message more difficult to decipher. For instance, the authors of paper [5] developed an algorithm that uses the shifting and replacing operations of bi-column-bi-row for circular queue to increase security. A random number was used in this algorithm to control the shifting between the row and column, eventually this lead to increase the complexity of plaintext decryption. In the same vein, an elliptic curve algorithm was designed based on matrix scrambling using circular queue [6]. In this research also utilizes shifting process to accomplish the encryption and the decryption of the text. In addition, a multiple circular arrays algorithm was developed to encrypt data using three circular arrays. This algorithm enabled the shifting (elements in the outer or inner array), swapping (elements among the circular arrays) and XORing (for encrypting the text) based on generating random number [7]. In contrast, a double encryption technique is proposed, which means the transmitter encrypts the text two times that leads the receiver decrypt the cipher text twice using public key [8].

Also, an elliptic curve algorithm is developed to produce a cipher text [9]. Actually, in this work the text firstly formed into ASCII code, and then the prime number and random number are chosen and formed into binary format. Where the "0" representation of the prime number is responsible of shifting the row/column in upward and left respectively. In addition, a multiple access circular queues algorithm is proposed with variable length in [10].

In this work different numbers of rotations are applied to the circular queues, swapping the elements in the same queue and XORing the elements with generating key number. The authors recommended that these processes would make a secure plaintext over the transmission line. On the other hand, Fibonacci sequence is mostly used for image encryption. A text to image encryption algorithm is designed using Fibonacci sequence [11]. This algorithm firstly converts the plaintext using Fibonacci sequence, and then the Unicode is converted to hexadecimal number and a RGB matrix. Finally, a shuffling operation is made to obtain the image to be sent.

III. Proposed Method



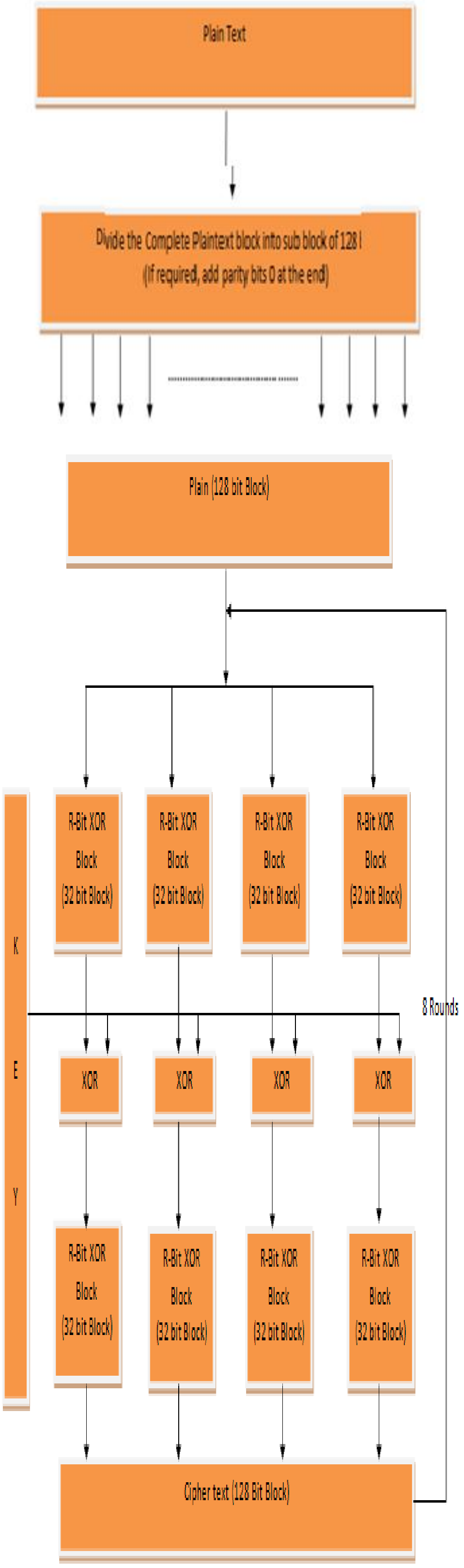

Plain Text
Divide the Complete Plaintext block into sub block of 128 l
(If required, add parity bits 0 at the end)
Plain (128 bit Block)
K
E
Y
R-Bit XOR Block (32 bit Block)
R-Bit XOR Block (32 bit Block)
R-Bit XOR Block (32 bit Block)
R-Bit XOR Block (32 bit Block)
8 Rounds
XOR
XOR
XOR
XOR
R-Bit XOR Block (32 bit Block)
R-Bit XOR Block (32 bit Block)
R-Bit XOR Block (32 bit Block)
R-Bit XOR Block (32 bit Block)
Cipher text (128 Bit Block)

Figure 4: Block diagram of Proposed Algorithm

3.1Proposed Algorithm:

3.1.1 Encryption Process:

Step1: Taking a Plaintext and arbitrary length key (Max 16 Characters) as an input.

Step2: Generate 8 different key of 128 bit from the given key.

- *Steps of generating Keys are as follow:*

a. Generate a Pseudo Random Number by passing an input key into addition block. Addition block add ASCII value of all the characters in key and last modulo of 32 is calculated of the resultant value of addition block. This value is random number (RN).
b. Now, convert all the characters of keys into binary format.
c. Now, if the length of key is less than 128 bit than make it equal to 128 by xoring all bit with its next bit and append with the key. Repeat this step till it become equal to 128 bit key.
d. Now, Generate the 8 different keys, by performing circular left rotation by RN bits on key by following method.

K[0] = leftrotate1(Key, RN);

K[1] = leftrotate1(K[0], RN);

K[2] = leftrotate1(K[1], RN);

K[3] = leftrotate1(K[2], RN);

K[4] = leftrotate1(K[3], RN);

K[5] = leftrotate1(K[4], RN);

K[6] = leftrotate1(K[5], RN);

K[7] = leftrotate1(K[6], RN);

Step 3: Now, convert the plaintext into binary format and then divide it in to number of chunks equal to 128 bits. If the last chunk having less bits than pad ‘0’ to make it equal to 128 bit.

Now, there is only one chunk is possible also it contains less bit than 128 hence pad ‘0’ to make it equal to 128 bit.

Step 4 Repeat the following steps for each chunk

a. Divide a chunk into four equal sub-block and each block have 32 bits.
b. All four chunks passed to R-Bit XOR which xor all bits by its next RN bit.
c. Now, taking key first Key K[0] and divide into 4 equal chunks of 32 bit and xor with plaintext sub block as shown in figure.
d. Again pass the result to R-Bit XOR.

Step-5 Repeat step 4, eight times and the result is ciphertext of first chunk and finally after getting ciphertext of all chunks result will again convert into text format.

3.1.2 Decryption Process:

Decryption algorithm is just a reverse process of encryption algorithm.

IV. Result Analysis

There are multiple researchers that work on many encryption and decryption algorithm to make it better in terms of security, space & time evaluation. Here I experimentally evaluate DSEA algorithm [12] and Proposed an algorithm and compare it in terms of time and space complexity.

4.1 Evaluation Method and Experimental Result of DSEA & Proposed algorithm

Encryption algorithm plays a very important role in network information security. It is essential to evaluate the performance of encryption algorithms. Usually the evaluation includes three parts: security, space and time efficiency. We analyzed the **DSEA algorithm** [7] and proposed algorithm on two parameters. In this section, we discussed the experimental results on **DSEA algorithm** [12] and **proposed algorithm** on two parameters security & time with comparison graph.

A. Encryption Speed Evaluation

The encryption speed is considered the computation quantity that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption speed is used to measure the throughput per unit time of an encryption scheme. The encryption speed is calculated as the total plaintext in bytes divided by the encryption time. The main work for encryption speed evaluation is to observe the performed encryption time for certain plaintext. Table 1 show the encryption time of DSEA algorithm [12] and proposed algorithm on different file size.

Table1:
Encryption Time and throughput of DSEA Algorithm and proposed algorithm

File Size in KB	**Algorithm**	
	Execution Time in Second	
	DSEA	Proposed Algorithm
	Encryption Time (in Sec)	Encryption Time (in Sec)
10 KB	0.031	0.612
20 KB	0.109	2.273

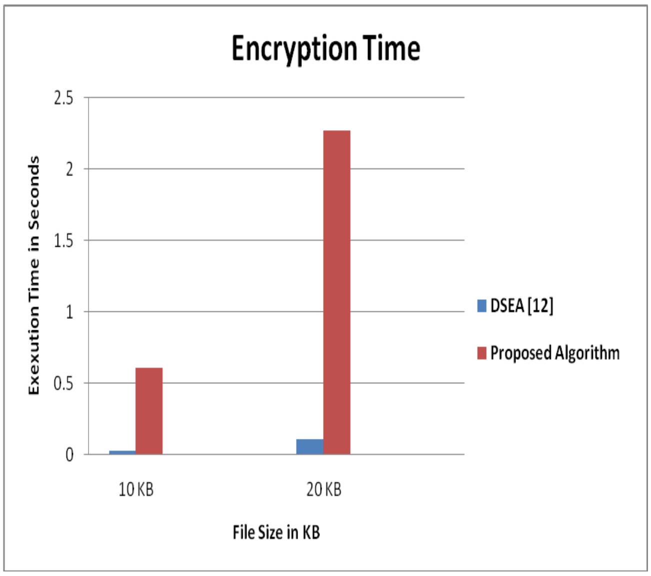


Figure 5: Encryption Time of DSEA algorithm and Proposed Algorithm

Here, it is clearly seen that as file size increases, the encryption speed (throughput) of algorithm decreases. Here our algorithm justify that because our algorithm is more secure as compare to DSEA so it takes some more time in encryption as compared to DSEA algorithm.

B. Encryption Security

Encryption security considers the strength of encryption algorithm. As discussed, key strength of DSEA is not powerful as compare to our proposed Algorithm. For analyzing the strength of encryption algorithm, Avalanche Effect is calculated. According to the avalanche effect, on changing the single bit in key 50% bits of cipher text must change. The algorithm close to avalanche effect is more secure against cryptanalysis. Table 2 shows the avalanche effect of DSEA algorithm [12] and proposed algorithm.

Table 2:
Avalanche Effect of DSEA & Proposed algorithm

Algorithm		
Avalanche Effect		
Sample	DSEA Algorithm	Proposed Algorithm
Sample-1	42.26 %	49.44%

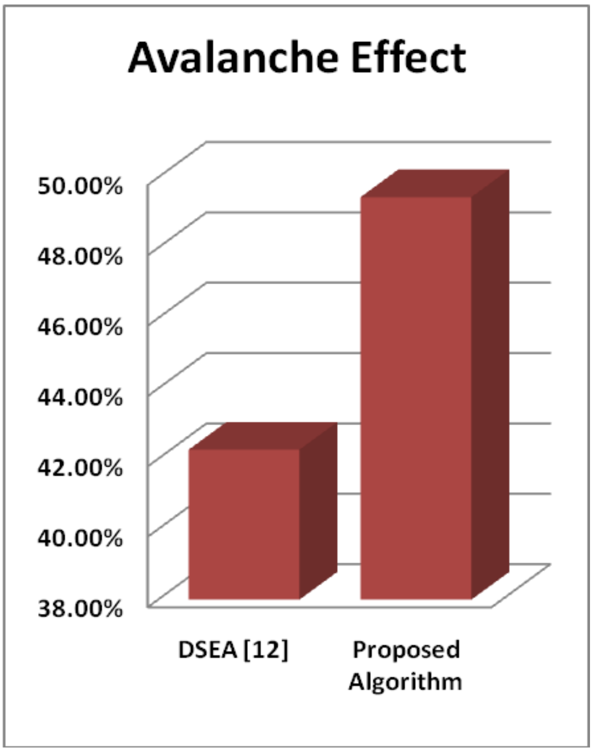


Figure 6: Avalanche Effect of DSEA algorithm and Proposed Algorithm

Here, on analyzing the avalanche effect, it is clear from table 2 and figure-6 that robustness of the DSEA algorithm is low as its avalanche effect is very low and our proposed algorithm is very robust.

V. Conclusion & Future Scope

With the projectile like growth of technologies in the field of computers and internet, security of data is an important concern in today's life. In this thesis, I have studied lots of cryptographic algorithms and proposed an improved algorithm and analyzed it with DSEA [12]. Cryptography has been known and practiced for centuries. Previously, people would use manual methods for encrypting data. But after the arrival of variety of techniques, the entire method of data hiding has been modified. Cryptography has totally overtaken the old traditional methods in recent world of computers and internet. Also with the arrival of new methods, the attackers have invented newer techniques to break the code. This in turn gives rise to invention of more secure methods which are even more complex. This work aims to develop an algorithm which provides more security to the confidential data by first encrypt it by applying a new secure encryption algorithm.

To sum up, all the previous techniques are useful for real-time encryption application. Each technique is different in its way, and suitable for different applications. New encryption technique is developing everyday therefore prompt and secure conventional encryption techniques will always work out with high rate of security. Here i show the result of proposed algorithm implemented in .net frame work. Following point of proposed Algorithm that makes it fit for sending secure data over the channel.

- The encryption speed (throughput) of algorithm not decreases as file size increases.
- Avalanche effect showed that the key strength of Proposed Algorithm is very much powerful.

Results prove that our proposed algorithm shows the better result from DSEA in term of security.

We can use our algorithm in many application such as cloud computing, and real time application like banking services and online payment gateway.

Future scope of this research work is to make it more efficient in terms of security, time and space. It can also be integrated with other algorithm to get more benefits.

REFERENCES

[1] Kahate, Atul., "Cryptography and Network Security", TataMcGraw-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 Key Management-Part 1: General (Revision 3)", Computer Security Division (InformationTechnology Laboratory), 2016.

[5] Wu, Suli, Yang Zhang, and Xu Jing. "A Novel EncryptionAlgorithm based on Shifting and Exchanging Rule of bi-column bi-row Circular Queue", IEEE International Conference on Computer Science and Software Engineering, Vol. 3 , 2008.

[6] Amounas, Fatima., "An Elliptic Curve Cryptography based on Matrix Scrambling Method", IEEE International Conference on Network Security and Systems (JNS2), 2012.

[7] S. S. D. Pushpa R. Suri, "A Cipher based on Multiple Circular Arrays", International Journal of Computer Science Issues(IJCSI), Vol. 10, No. 5, pp. 165-175, 2013.

[8] Merkle, Ralph C., and Martin E. Hellman. "On the Security of Multiple Encryption", Communications of the ACM, Vol. 24,No.7, 465-467, 1981.

[9] Hankerson, Darrel, Alfred J. Menezes, and ScottVanstone," Guide to Elliptic Curve Cryptography", Springer Science and Business Media, 2015.

[10] S. Phull and S. Som, "Symmetric Cryptography using Multiple Access Circular Queues (MACQ)", Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, 2016.

[11] 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.

[12] Ali N. Albu-Rghaif ; Abbood Kirebut Jassim ; Ali J. Abboud "Data Encryption A data structure encryption algorithm based on circular queue to enhance data security", 1st International Scientific Conference of Engineering Sciences - 3rd Scientific Conference of Engineering Science (ISCES),. 79-82, 10-11 jan 2018.