IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-2 E-ISSN: 2347-2693

LFSR Based Block Cipher Technique for Text

Sakshi Dubey[1*], Darpan Anand[2], Jayash Sharma[3]

[1*]Dept. Of Computer Science Engineering, HITM, AKTU, Agra, India
[2] Dept. Of Computer Science Engineering, HITM, AKTU, Agra, India
[3] Dept. Of Computer Science Engineering, HITM, AKTU, Agra, India

[*]*Corresponding Author:* Sakshidubey.19dec@gmail.com, *Tel.: +91-7351197808*

Abstract**--** In the world of cryptography there are a lot of techniques and their simultaneous operations, which are used for making our data transmission better, secure and fast. Today to get more and more data transmission capabilities, people tend to compromise security of their data due to non availability of better cryptography techniques to suit different needs of their data transmission. Keeping this requirement of enhanced security in mind, some new techniques are making their way in cryptography, which are reliable, fast and give better data security for transmission of different kind of data (i.e. Text, Images, Videos etc.). In this paper, authors are proposing a cryptography method for enhanced encryption and decryption with help of LFSR (linear feedback shift register), which can reliably give much desired security with more speed. In this paper the method is used only for text, it could be further modified for 2D as well as 3D images.

Keywords: LFSR (Linear Feedback Shift Register); Encryption; Decryption; Cipher text; Block cipher**.**

I. INTRODUCTION

Today increasing amount of data and information are transmitted over internet through insecure channel. It has created a digital environment in which digital information are easy to transmit, modify and distribute. Data security requirements are of high importance (i.e. integrity, confidentiality, availability) during data transmission over the internet. Cryptography can be used to ensure that the content of the data are very securely transmitted and would not be altered [1]. The main goal of cryptography is privacy of messages in insecure channels. The main purpose of encryption and decryption is to encode and decode the message which could not be read by unauthorised person and hackers.

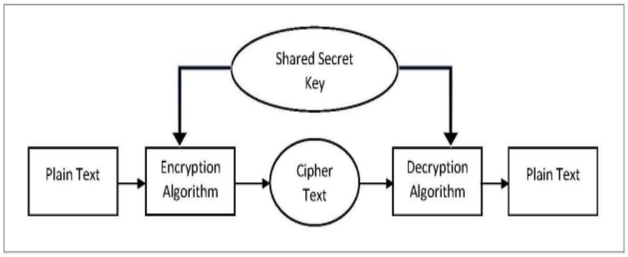

Figure1. Block diagram of symmetric key cryptography

Cryptography is a technique of using some computations and analytics for encryption and decryption of data, it enables you to store important data and transmit by insecure channel so it cannot be read or written by anyone except receiver. It has two techniques which will discuss in further section. One of them has shown in the above diagram that is symmetric key cryptography. Only one key is used in this scheme that is shared by both sender and receiver and used to encryption and decryption algorithm. Data that can be read and understand without any special measure that is called Plaintext or Cleartext. The method of hiding the data from others is called Encryption. Encrypting plaintext, gives us unreadable & meaningless pattern known as Cipher text. The process of reversing cipher text into plaintext is known as Decryption. Symmetric key cryptography has many algorithms for encryption and decryption and many of them have some drawbacks. To achieve better results with less efforts new method is introduced that is LFSR method, which explained in this paper, is simple as well as easy for computation and more secure rather than other symmetric cryptography schemes. A Linear Feedback Shift Register (LFSR) is a kind of sequential shift register including computational logic that approaches to pseudorandom cycle via a binary value sequence [2]. This paper focus on 16 random bit LFSR with XOR function. Many algorithms and mechanisms have been developed for symmetric cryptography with less computational work and more effective. Some of them will discuss in coming sections.

Rest of the paper is organised as follows, Section I contains Introduction, Section II contains Literature review, Section III describes Proposed method in detail, Section IV comprises of Result and Analysis part and section V concludes research work with Future Scope.

II. LITERATURE REVIEW

Cryptographic algorithms are extremely effective to transfer a lot of data with less computation and efforts. Two types of algorithms are symmetric and asymmetric algorithms are based on stream cipher and block cipher which provides bit by bit encryption and block encryption respectively. It consist various mathematical techniques to avoid hacking of the content of encrypted message [3]. Cryptography techniques provide security of information and categorised in two categories of schemes, which are symmetric cryptography and asymmetric cryptography.

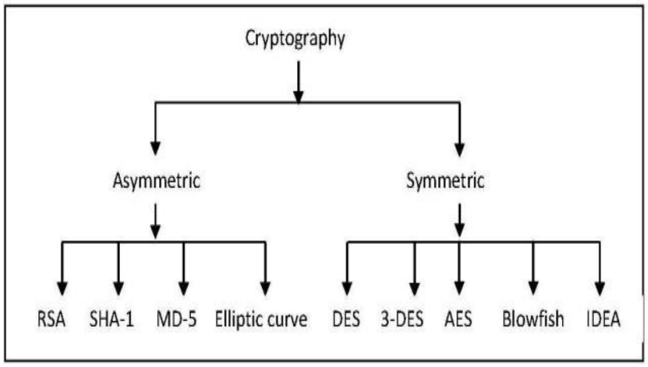

Figure 2. Classification of cryptography techniques.

In symmetric cryptography scheme, sender sends the data and receiver receives that same data in encrypt form and decrypt the data on receiver side with help of a private key. Keys need to be exchanged between users, which mean, key is in the shared form in encryption and decryption. On the other hand asymmetric cryptography does the same work with different keys (public and private keys), one key is used to encrypt the message and another key is used to decrypt the message. There are many techniques for security of information in symmetric cryptography such as DES, TRIPLE DES, AES, BLOWFISH, and IDEA etc.

Some symmetric key algorithms are given as follows:

1. Data Encryption Standard (DES) - it was designed by IBM in 1976 for the National Bureau of Standards (NBS). DES consists of a encryption formula that is employed in a system and network protect from cryptanalysis attacks[4]. DES algorithm is a block cipher that use same key for encryption and decryption [5]. Here plain text is of 64 bits data block which is controlled by 56 bit of data key and produce 64 bit cipher text. Similarly 64 bit cipher text is used as an input for decryption process with the help of 56 bit of data key and gets 64 bit plaintext.
2. Triple DES- Triple Data Encryption Standard was developed in 1999 by IBM which is used to prevent man in the middle attack. Triple DES is better than DES because of triple strong algorithm [6]. The original DES cipher's key size is 56 bit but to increase the computational power and security triple DES is developed. It provides security against such attacks because to use of tree times of encryption and decryption with tree keys with the length of 192 bits. Triple DES runs tree times slower than DES but it is more secure.
3. Advanced Encryption Standard(AES)-
AES is a block cipher encryption method with the variable key length and several rounds of encryption [7]. Block size is fixed and the key length of 128, 192, 256 bits whereas Rijndael can be specified with key and block size is any multiple of 32 bits with minimum of 128 bits and maximum of 256 bits. AES is a non feistel cipher that encrypts and decrypt a data block of size 128 bits with 10, 12 and 14 rounds and key size is depends upon rounds. A round of AES consists of four operations: Sub byte operation, Shift rows operation, mixed column operation and Add round key operation. It is more comfortable to implement with low and high level language.
4. Rivest Cipher 4(RC4) - the cryptographic stream cipher RC4 is designed by Ronald L. Rivest [8] in 1987 for RSA data security. This is a stream cipher, symmetric key algorithm; here data stream is simply XOR with generated key sequence [5]. Encryption and decryption both can be done by this algorithm. Variable key length is used to initialize a 256 bit state table, and this table is used to generate pseudo random bits and then generate pseudo random stream, which is XORed with the plaintext to give the ciphertext [9].
5. Blowfish Algorithm- it is a block cipher encryption algorithm which is safely and effectively used for securing of data. It has variable key length which is 32 to 448 bits, which makes it ideal for data security. This symmetric key algorithm was developed by Bruce Schneier in 1993 [6] and included in a large number of cipher suits and encryption products. Blowfish contains 64bit block size with any length of key up to 448 bits. This algorithm divides into two parts: a key expansion part and a data encryption part. With the variable key length blowfish is relatively simple to implement

Asymmetric cryptography schemes types are RSA, ElGamal, SHA-1, MD-5, ELLIPTIC CURVE CRYPTOGRAPHY etc. This scheme is different from symmetric key because two keys (public and private) are used in asymmetric method.

Public key is shared by everyone in system by private key kept secret by authenticated user.

1. RSA (River, Shamir, Adleman) - RSA stands for River Shamir Adleman which is introduced in 1977 [10]. It is asymmetric cryptographic algorithm used for encryption and decryption with two different types of key, one is public and another is private key [11]. Public key is open for everyone and seen by every person but private key kept secret by authenticated used. RSA provide confidentiality, integrity, availability, non repudiation of data [12].
2. ElGamal- ElGamal algorithm is introduced in 1985[13]. This algorithm based on Diffie Hellman Key Exchange algorithm as an alternative of RSA for public key encryption. It is used in Digital Signature Generation algorithm [14]. It has the advantage the same plaintext gives a different cipher text each time it is encrypted and has a disadvantage that the cipher text is twice as long as the plaintext.
3. ECC (Elliptic Curve Cryptography) - ECC stands for Elliptic Curve Cryptography introduced in 1985 by Neal Koblitz and Victor S. Miller. The applications of ECC are encryption, digital signature and pseudo-random generators [15] etc.
4. MD 5- MD 5 stands for Message Digest was developed by Ron Rivest. This method produce 128 message digest from a variable length message. It is quite fast than other versions of MD [16].
5. SHA 1- SHA stands for Secure Hash Algorithm developed by National Institute of Standards and Technology (NIST). It is the modified version of MD5. This algorithm uses a message as input with maximum length (less than 2^{64} bits) and produces 160 bit message-digest as output [18].

This section provides an overview of similar work done by various authors. Tang Songsheng, Ma Xianzhen [18] (2010) provide block cipher DES algorithm with one advantage space utilization very efficiently but due to the small key size it can be break very easily[7] .AES algorithm is also provided by Tang Songsheng that is more secure than DES in various differential cryptanalysis. Wenxue, et al [19] give RSA algorithm with different approaches, he emphasizes on security of key and information, but here is a disadvantage of weak key generation. Suli Wang, Ganlai Liu [8] (2011) perform RSA algorithm with portable components. Suli Wang made this algorithm efficient and reusable with wide development aspects. It comprises high security and communication between both parties is easy in insecure environment. All over cost is high with this method.

Jawahar Thakur et al [5] [2011] show the comparison among three symmetric key cryptography algorithms: DES, AES, Blowfish. He compares the performance of all three algorithms on the behalf of behaviour and data load that is used for encryption and decryption. The comparison is based on the three parameters: key size, block size and speed [6]. Shashi Mehtotra Seth et al. [2011] give the comparative study of these three algorithms based on memory usages, output bytes and computation time. A cryptographic technique is used for various experiments. Experimental results are used to study the effectiveness and accuracy of all algorithms [20].

G. Ramesh et al [2012] give the comparison among five algorithms such as DES, 3DES, AES, UMARAM, UR5 based on throughput, power consumption and encryption running time. According to the author UR5 gives the better experimental results over all algorithms [21].

Jitendra Singh Laser et al [22] [2016] analyse the conventional algorithms based on their pros and cons. This paper offers the future work opportunities in field of cryptographic techniques.

Md. Alam Hossian et al [23] [2016] elaborate the basic features (key size and block size) of symmetric, asymmetric and hashing algorithms. We implemented firewall for encrypted techniques like BLOWFISH, RC4, DES, AES, RSA algorithms and give the comparison based on their running time of encryption and decryption of different file size.

Dr. D Vimal Kumar et al [24] [2016] analyse the difference among all encryption techniques not considering the mathematical theory behind an algorithm, the best algorithm are those that are well-documented & well-known, because they are always well-studied and well tested [6].

III. PROPOSED METHOD

In cryptography there is a concern about more security and less running time in communication channel so there is a method which is fitted for this requirement that is LFSR. This LFSR technique is used for encryption and decryption without data alteration. Firstly should know about LFSR, it is a sequential shift register including combinational logic that approaches to pseudorandom cycle via a binary value sequence [2]. For example 16 random bits LFSR generate with polynomial $x^{16}+x^{14}+x^{13}+x^{11}+1$ and corresponding diagram given below [25]. The bit positions which is called taps, affects the next state. In this diagram block 16, 14, 13 and 11 are taps. The right most bit is output bit in LFSR. The taps get XOR'd with the output bit sequentially and then feedback goes into the leftmost bit. In this system, the rightmost sequence of bits is called output stream. An m-sequence (which cycles through all possible 2^n-1 states within the shift register except all zero bit state) is produced by maximum length LFSR. If it contains all zero then it will never change.

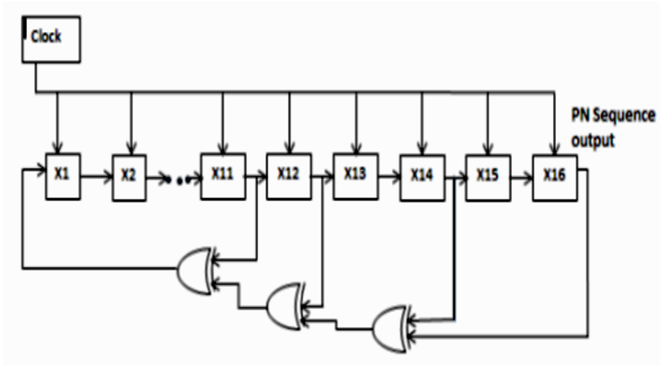

Figure 3. LFSR of 16 bit

This method is based on block cipher where a message is divided into blocks and one by one block is processed. Key1 is used for encryption and decryption for first block and for next block the LFSR of key 1 is used, for the next block LFSR of key2 is used and so on, the diagram is given below.

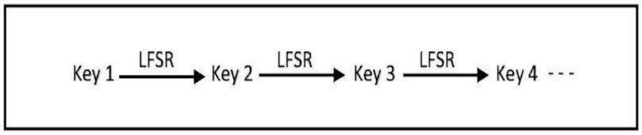

Figure 4. LFSR applies on key

In this method the absolute block length is the multiple of key length and relative block length. Key length and relative block length are free in size. Here the original message is divided into blocks and the block size is depends upon key length and relative block length.

Encryption and decryption of blocks are given below.

ENCRYPTION: Suppose the key length is 3 Unicode character and relative block length is 2 Unicode character so the block size will be 6 Unicode character .i.e.

Absolute Block Length = key length * Relative Block

So firstly take 1st block for processing with 6 Unicode character and first half of this block is XOR with key and get half cipher ext and another half cipher text is done by XOR of first half cipher text and second half plaintext as shown in this above Figure.

DECRYPTION: Decryption of message is little bit differ from encryption method, here first half of cipher text is XOR with key and get first half plaintext and another second half of plaintext is getting XOR of first and second half of cipher text as shown in this above diagram.

Now first block is processed and encryption and decryption is done and for next block the key will be different. In other words the LFSR of key will be use and rest method is same for encryption and decryption. Here we are using random 16 bit LFSR which we have discussed previously with Figure 3. This LFSR method gives the secure message transmission with less integrity. Block diagram of LFSR based encryption and decryption given below.

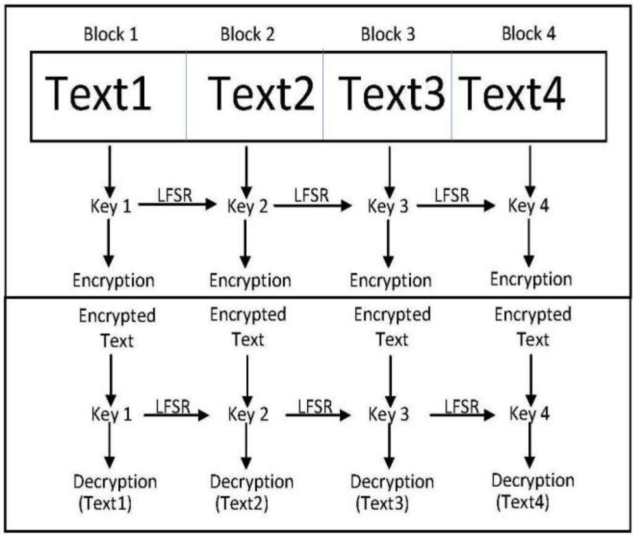

Figure 5. Block diagram of LFSR based encryption and decryption

This above diagram explains the whole process of proposed method. Here text is considered as an input which is used for encryption and after that decryption with LFSR of key. Original text is divided into blocks and one by one block will process. At first take block1 which is used to encrypt message by using key1. That encrypted message is used to decrypt by key1. In next step block2 will take to process, same procedure will work by with different key. Key should be LFSR of previous key as shown in Figure4. By this way the whole message is encrypt and decrypt on the receiver side. This is symmetric key approach because of this, only one key is used at initial but LFSR concept makes it secure and effective. Algorithm of this process is given below.

ALGORITHM:

1. Take an input as string // take any sentence as input

2.Key={K1,K2,K3}, Plaintext={P1,P2,P3,P4,P5,P6} , Cipher text={C1,C2,C3,C4,C5,C6} // key are divided into three part, plain text and cipher text also show in P1 to P6 and C1 to C6 respectively.

3. Divide the string into blocks // string which has taken an input is divided into blocks.

4. Take 1st block for processing //first block has taken to encryption.

5. 1st block is divided into two equal halves. // first block is divide and it can consider P1 to P3 and P4 to P6.

6. $P1 \oplus K1=C1$, $P2 \oplus K2=C2$, $P3 \oplus K3=C3$

$C1 \oplus P4=C4$, $C2 \oplus P5=C5$, $C3 \oplus P6=C6$ //first half plaintext is XOR with key and first half of cipher text is XOR with second half of plaintext.

7. Get cipher text //result shows cipher text.

8. This cipher text is going to decrypt // this cipher text used an input (plaintext) for further process to get decryption.

9. $C1 \oplus K1=P1$, $C2 \oplus K2=P2$, $C3 \oplus K3=P3$

$C4 \oplus C1=P4$, $C5 \oplus C2=P5$, $C6 \oplus C3=P6$ //first half and second half of cipher text is XOR with key and first half of cipher text respectively.

10. Get plaintext //combine all P1 to P6 and get plaint text

11. Now LFSR of key is used // for the next block new key (LFSR of previous key) is used and rest all same.

12. Next block is divided into two equal halves //next input block is divided into two equal halves.

13. Go to step 5

14. All blocks are processed //whole plaintext is convert into cipher text by encryption and again cipher text is convert into plaintext by decryption.

The above algorithm can be understood in better way by the following example of LFSR technique in cryptography. Suppose a sentence is taken as an input that is “ALICE SEND MESAGE TO MICHAL” , this input is divided into equal number of four blocks and very first block can be consider for further process. At initial take first block and apply key (K) which is already known and describe in [K1, K2, K3]. Plaintext of first block is describe in [P1 to P6] which depends upon number of letters present in first block. Plaintext is XOR with key and gets ciphertext [C1 to C6]:

ENCRYPTION:

$P1 \oplus K1=C1$, $P2 \oplus K2=C2$, $P3 \oplus K3=C3$

$C1 \oplus P4=C4$, $C2 \oplus P5=C5$, $C3 \oplus P6=C6$

This ciphertext is work as an input for decryption and XOR with key to get original first block and we can say plaintext that is [P1 to P6]

DECRYPTION:

$C1 \oplus K1=P1$, $C2 \oplus K2=P2$, $C3 \oplus K3=P3$

$C4 \oplus C1=P4$, $C5 \oplus C2=P5$, $C6 \oplus C3=P6$

Now for further process take second block for encryption and decryption. All process are same with small difference that is in second time the initial key is not use, LFSR of initial key is used which shown in Figureure4. Ne key is derived from LFSR which gives the security for this algorithm. Key will be different is each and every block, all the time key will change for next encryption and decryption. By this way all message is convert in encrypted message (cipher text) and this same message can get by decryption of cipher text on the receiver side

EXAMPLE:

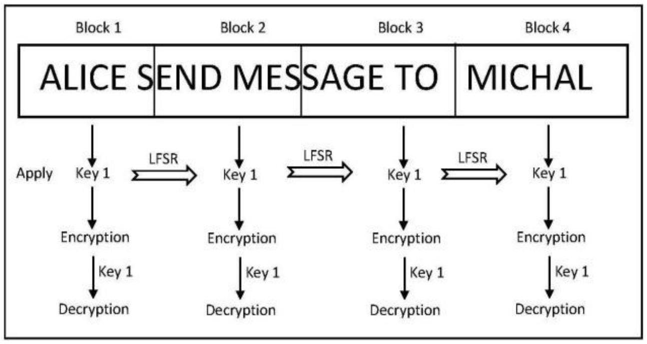

Figure 6. Cryptography using LFSR

Procedure of 1st block

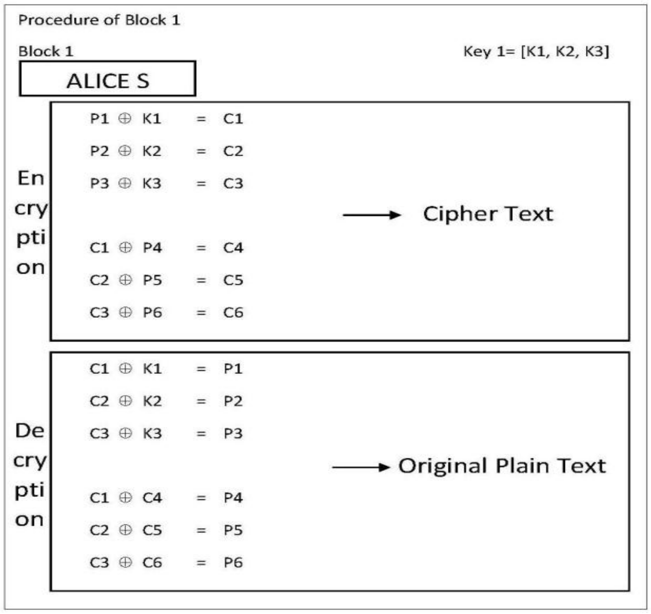

Figure 7. Procedure of 1st block

IV. RESULT AND ANALYSIS

Now, we demonstrate the performance of our proposed method, it is well good in running time and gives better security in cryptography. According to this given table as key size increase, running time is decrease simultaneously. Here we are showing a table to elaborate some parameters such as key size, data size and running time. This table easily show the running time depends upon key size and data size. Here T2 indicates two Unicode characters of key, T4 indicates four Unicode characters of key and T8 indicates eight Unicode characters of key and data size start with 10kb and increase up to 100mb and more than that. Here data size is shown in this table that means, 10kb data file size takes 0.00036 seconds for encryption with two Unicode character of key, if four Unicode character of key is taken so, 0.000347 seconds will require and 0.000303 seconds require for eight Unicode characters of key. Other data size and key size relation mention in given table. It shows some decimal values, indicates running time in seconds which depend upon key size and data size.

Key Size / Data Size	T2	T4	T8
10kb	0.00036	0.000347	0.000303
100kb	0.000508	0.000440	0.000389
1mb	0.00122	0.00108	0.000982
10mb	0.00324	0.00292	0.00256
100mb	0.00636	0.00560	0.00504
100mb>	0.01052	0.008333	0.00790

Table 1. Comparison based on running time

The performance of this method is better which can proof by this following curve, shows the linear behaviour of LFSR. Red line shows key size of 2 which means two Unicode characters; green line shows key size of 4, means four Unicode characters and blue line shows key size of 8, means eight Unicode characters. Here time has taken in milliseconds on Y-axis and no. Of characters has taken in Unicode character on X-axis on the behalf of both parameter the performance of graph has shown in Figure 8. This graph shows some points which is not exactly linear but show linear behaviour.

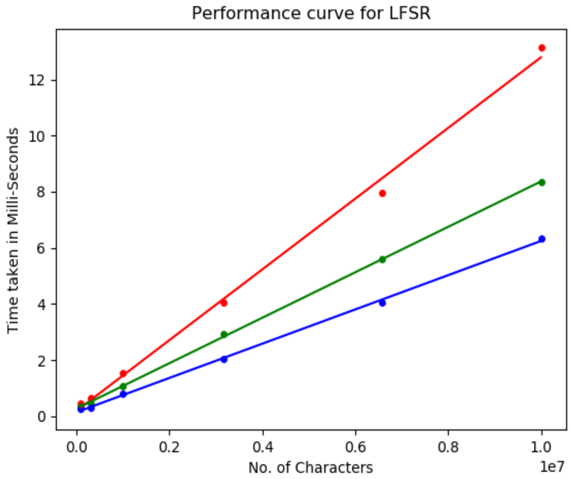

Figure8. Performance curve for LFSR

The performance curve shows number of character on X-axis in decimal which means 0.2(0.2 * 10^6 or 2e6), 0.4(0.4 * 10^6 or 4e6) and so on.

Serial (linear) procedure of LFSR: here all description in terms of Unicode character.

Absolute key length=KL

Relative key length=RL Absolute block length=Key length * Relative length

LFSR is a method to apply key only, it produce $K^{/}$ (new key) from K (old key).

Let this transformation be $K_i \rightarrow K_{i+1}$

Suppose initial key to be K_0 and XOR indicated by" ⊕".

Also assume, there are N blocks, and then execution timeline can be denoted as:

$$K_0 \oplus (P_0^0 , P_0^1 , ...P_0^{R-1}) \rightarrow (C_0^1 , C_0^1 , ...C_0^{R-1})$$

$$K_1 \oplus (P_1^0 , P_1^1 , ...P_1^{R-1}) \rightarrow (C_1^0 , C_1^1 , ...C_1^{R-1})$$

$$K_2 \oplus (P_2^0 , P_2^1 ,............P_2^{R-1}) \rightarrow (C_2^0 , C_2^1 , ...C_2^{R-1})$$

.

.

.

$$K_N \oplus (P_N^0 , P_N^1 ,.........P_N^{R-1}) \rightarrow (C_N^0 , C_N^1 ,.............C_N^{R-1})$$

At first sight, $K_i \rightarrow K_{i+1}$ seems inherently serial like traversing a linked list, but if we can save current key value in the system to be applied in a block and perform LFSR to generate next key without XORing current key to block on which it is to be applied, we can get significant speed up using parallelism, both work can run simultaneously. According to this procedure the algorithm can be better than many other methods.

Theoretically if the results are reviewed, we can find that the algorithm is better than DES algorithm because of two factors. First one is, its circular LFSR pattern , DES algorithm contains 56 bits of key in each and every round of encryption and decryption. Key size is fixed in DES but LFSR method provides variable key length. Second one is running time; DES takes much time in encryption and decryption [26] than LFSR algorithm. It provides security from attacks because attacker has difficulty to crack this circular way. In every next block, key change its digits by LFSR and this way makes it strong.

V. CONCLUSION

As per shown data in result we can conclude here that given LFSR algorithm is clocking better running time than previously used DES algorithm described in past researches. This work has illustrated that LFSR technique is good in reference of security and running time. Running time is the major factor to show effectiveness of any algorithm. In this paper 16 bit LFSR is given for encryption and decryption. This method is block cipher method which is used for text but images can also be use for encryption and decryption. This is safe because we cannot design neural network for LFSR due to its circular pattern. LFSR pattern is better than many other algorithms in many references. The future work could be to improve the security of retrieval of encoded message in communication channel. Here block cipher LFSR method is used for text, but it can be extend for images of both 2 Dimensional and 3 Dimensional patterns also with more security and can be extend with less running time.

REFERENCES

[1]. A. Joseph Amalraj, Dr.J. John Raybin Jose, "*A Survey Paper of Cryptography Techniques*" Issue.8, August 2016.

[2]. Rohit S and Vinay G "*A Novel to Stage Binary image Security system Using (2, 2) Visual Cryptography Scheme*", ISSN: 2250-3005.

[3]. Prof. Mukund R.Joshi , Renuka Avinash Karkade, "*Network Security With Cryptography*" , Issue.1 , January 2015

[4]. A. Balasubramani, Ch.D.V Subba Rao, "*Image Security Implementing Steganography and Cryptographic Methods*", International Journal of Computer Science and Engineering, Volume.6, Issue.1, January 2018.

[5]. Jawahar Thakur, Nagesh Kumar, "*Des, Aes And Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis*" International Journal Of Emerging Technology And Advanced Engineering, Volume 1, Issue 1, November 2011.

[6]. Sonia Rani, Harpreet Kaur, "*Technical Review on Symmetric and Asymmetric Cryptography Algorithms*." Vol.8, May 2017.

[7]. Mini Malhotra, Aman Singh, "*Study of various Cryptographic Algorithms*", Vol.1, Issue 3, November 2013.

[8]. Wang, Suli; Liu, Ganlai, "*File encryption and decryption system based on RSA algorithm*", Computational and Information Sciences (ICCIS), pp. 797 – 800, 2011.

[9]. Suresh, V., and C. Saraswathy. "*Separable reversible data hiding using Rc4 algorithm*", 2013 International Conference on Pattern Recognition Informatics and Mobile Engineering, 2013.

[10]. R. L. Rivest, A. Shamir, and L. Adleman "*A Method for Obtaining Digital Signatures and Public- Key Cryptosystems*." Communications of the ACM, vol. 26, no. 1, pp. 96–99, 1983

[11]. Faiqa Maqsood, Muhammad Ahmed, Muhammad Mumtaz, Munam Ali. "*Cryptography: A Comparative Analysis for Modern Techniques*", International Journal of Advanced Computer Science and Applications, 2017

[12]. M. E. Student, "*Algorithms for Secure Cloud*," vol. 3, no. 6, pp. 1–9, 2014

[13]. P. Nalwaya, V. P. Saxena, and P. Nalwaya, "*A cryptographic approach based on integrating running key in feedback mode of elgamal system*," Proc. - 2014 6th Int. Conf. Comput. Intell. Commun. Networks, CICN 2014, pp. 719–724, 2014.

[14]. X. Li, X. Shen, and H. Chen, "*ElGamal digital signature algorithm of adding a random number*," J. Networks, vol. 6, no. 5, pp. 774–782, 2011

[15]. M. S. Anoop, "*Elliptic Curve Cryptography," Infosecwriters*, pp. 1–11, 2015

[16]. Alok Kumar Kasgar, Mukesh Kumar Dhariwal,"*A Review Paper Of Message Digest 5(MD5)*", Volume 1, Issue 4, December 2013

[17]. Chaitya B. Shah, Drashti R. Panchal, "*Secured Hash Algorithm-1: Review Paper*", Volume 2, Issue X, October 2014.

[18]. Tang Songsheng, Ma Xianzhen,"*Research of typical block cipher algorithm*", Computer, Mechatronics, Control and Electronic Engineering (CMCE), pp. 319 – 321, 2010.

[19]. Wenxue Tan ; Wang Xiping ; Jinju Xi ; Meisen Pan , "*A mechanism of quantitating the security strength of RSA key*", Electronic Commerce and Security (ISECS), pp. 357 – 361, 2010.

[20]. Aarti Devi, Ankush Sharma, Anamika Rangra, "*Performance Analysis Of Symmetric Key Algorithms: Des, Aes And Blowfish For Image Encryption And Decryption*" International Journal Of Engineering And Computer Science Volume 4 Issue 6 June 2015

[21]. G. Ramesh1 Dr. R. Umarani, "P*erformance Analysis of Most Common Symmetrical Encryption Algorithms*" International Journal of Power Control Signal and Computation (IJPCSC) Vol 3. No 1. Jan-Mar 2012.

[22]. Jitendra Singh Laser, Viny Jain, "*A Comparative Survey Of Various Cryptographic Techniques*" International Research Journal Of Engineering And Technology (IRJET), Volume: 03 Issue: 03 | Mar-2016

[23]. Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, "*Performance Analysis Of Different Cryptography Algorithms*", International Journal Of Advanced Research In Computer Science And Software Engineering Volume 6, Issue 3, March 2016.

[24]. Dr. D. Vimal Kumar, Mrs. J. Divya Jose, "*Over View of Cryptographic Algorithms for Information Security*" International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 5, May 2016.

[25]. Siddesh Gaonkar, "*Design Of 8bit, 16bit and 32bit LFSR For PN Sequence Generation Using VHDL*", Issue 31(September, 2015)

[26]. Sumitra, "*Comparative Analysis of AES and DES Security Algorithms*", Volume 3, Issue 1, January 2013.

Authors Profile

Ms. Sakshi dubey received her B. Tech. At the Hindustan Institute of Technology and Manangement. She is doing her M. Tech. From Hindustan Institute of Technology and Management and doing her research in cryptography techniques. She is author of a review paper on Modern cryptography techniques.

Mr. Darpan Anand received his M.Tech. at the Dayalbagh Educational Institute. He is research Scholar at Dr. A.P.J. Abdul Kalam Technical University, Lucknow, India. He is an Assistant Professor at the Department of Computer Science Engineering, Hindustan Institute of Technology and Management, India. His research interests include information security, security in e-governance, computer network, distributed computing, machine learning, etc. He is author of a great deal of research studies published at national and international journals, conference proceedings.

Jayash Kumar Sharma received his Master in Technology in Computer Science & Engineering at Dr. A P J Abdul Kalam Technical University, India. He is also a Ph.D. research Scholar at Rajasthan Technical University, India. Currently he is working with Hindustan Institute of Technology & Management, India as an Assistant Professor at the Department of Computer Science & Engineering. His research interests include Pattern Recognition, Image Processing, Machine Learning, Information Security.