ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 1, 2025

SECURITY ENHANCEMENT OF INFORMATION USING MULTILAYERED CRYPTOGRAPHIC ALGORITHM

MUDUMALA DEEPTHI [1] , NALLAGOTI SUKEERTHI [2] , PATTAN SHAHANAZ THABASSUM [3] , SHAIK SHAHEENA [4] , SHAIK SHAMSHAD [5] , K. MADHAVI [6]

[12345]UG STUDENTS, DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING, DR.K.V.SUBBA REDDY INSTITUTE OF TECHNOLOGY, KURNOOL,AP, INDIA.

[6]ASSOCIATE PROFESSOR, DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING, DR.K.V.SUBBA REDDY INSTITUTE OF TECHNOLOGY, KURNOOL,AP, INDIA.

Abstract: This project presents data security enhancement using the multilayer linear feedback shift register (LFSR) cryptographic technique to overcome the problem of data hacking. The information security is achieved with a One Time Pad (OTP) algorithm developed in multilayer which defines the signal transmission in the medium. The Pseudorandom Noise (PN) sequence created by the primitive polynomial is used to get the seed values that are used to characterize OTP functionality. The single-layered LFSR cryptography is analyzed with a cascaded LFSR cryptography technique to prove the security of digitized data. The authentication key generation circuits for various levels of bit handling in data communication systems are implemented in LFSR cascaded cryptography in both encryption and decryption process. The cascaded multilayer cryptography is analyzed for improved data security and the results based on operating frequency, power consumption, delay, and memory usage prove that it suits well for developing modern network-based applications.

1. INTRODUCTION

In the data communication process, hacking has become a great threat, which leads to the loss of information during the transmission causing insecurity. This data hacking affects the user and confidentiality during the data handling process. Data security is achieved using various techniques in the data handling process. The most familiar method used to overcome this problem is cryptography. Cryptography is the process of encrypting the data with the help of the key which is generated by the transmitter [3,4]. The receiver wants to decrypt the data with the key to read the data. Key may be common to both transmitter and receiver. Symmetric cryptography is the cryptographic technique that uses the same key for both encryption and decryption. Key used for both encryption and decryption is the private key which should be secret for both transmitter and the receiver [7]. This

symmetric cryptography includes various algorithms such as AES algorithm [12], DES algorithm [14], Triple DES algorithm [8], Blowfish algorithm [6, 15], etc., For AES algorithm block size will be 128 bit and the key length will be 256 bit, which is the longest key. For DES algorithm, block size will be 64 bit and the key length will be 56 bit, which is the smallest key. In the triple DES algorithm, the block size will be 64 bit and the key length will be 112 bit or 168 bit, which is a shorter key compared to the AES algorithm. Asymmetric cryptography [10,16] is the cryptographic technique which uses the different key for encryption and decryption. Key used for encryption is the public key and the key used for the decryption is the private key. Asymmetric cryptography includes RSA algorithm, HASH algorithm, Digital signature algorithm, etc.

The modern cryptographic technique includes the development of the Linear Feedback Shift Register (LFSR) system [2]. This Linear Feedback Shift Register is used for the encryption and the decryption process. Key used for encryption and decryption will be Pseudo noise sequences generated by a feedback shift register and the combinational logic [5]. The Pseudo noise sequence [1] is generated at the output of the last flip flop in the shift register. There are many types of ciphers are available to generate the one-time pad (OTP) to provide a secure cryptosystem [10]. LFSR is used for generating the pseudo-random number generator which is used in stream ciphers especially in military cryptography due to its simple construction. LFSR is a linear system. To enhance the data security level, the multilayer technique is presented. Multilayer cryptographic technique [3, 9, 11] is the process of encrypting the already encrypted information one or more by using the same algorithm or using different algorithms.

Data security is importance in present time as lots of information is being communicated via network. A suitable methodology for privacy transformation is best to make a data protected over network. Different methods are implemented in order to protect the sensitive data. Now a days most of the data is secured by the technique of encryption and certificates. Most of methods are based on cryptography technique. Multi-level encryption is a new concept that is used for making the system more secure than existing cryptosystems. Multi level encryption is the process of encrypting the plain text with one or more time with same

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

of different no of keys. It makes the process more complex and powerful than existing.

CRYPTOGRAPHY AND TYPES

Cryptography: It is a technique to which information is send in a secure manner so that only authorized user is able to receive this information. It refers to the scrambling of the data and make it meaningless for the third party during transmission There are three basic components of cryptography system

Plain text : Source / information/data / original message

Key : Necessary for encryption process.

Cypher text : Unrecognized data /encrypted data / encrypted message

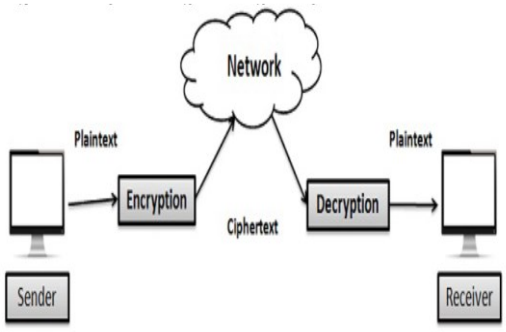

Fig 1: Encryption Decryption Process

The original message is then encoded using encryption algorithm. This process is called encryption. The reverse process to get back the encrypted data into plain text by using decryption algorithm. This process is called decryption. The process of decryption is reverse that of encryption. Cryptography is used to achieve following objectives:

Confidentiality : Confidentiality means to the keep information secret / private.

2. LITERATURE SURVEY

Exploring the Potential of Threshold Logic for Cryptography-Related Operations by Alessandro Cilardo

Motivated by the emerging interest in new VLSI processes and technologies, such as Resonant Tunneling Diodes (RTDs), Single-Electron Tunneling (SET), Quantum Cellular Automata (QCA), and Tunneling Phase Logic (TPL), this paper explores the application of the non-Boolean computational paradigms enabled by such new technologies. In particular, we consider Threshold Logic functions, directly implementable as primitive gates in the above-mentioned technologies, and study their application to the domain of cryptographic computing. From a theoretical perspective, we present a study on the computational power of linear threshold functions related to modular reduction and multiplication, the central operations in many cryptosystems such as RSA and Elliptic Curve Cryptography. We establish an optimal bound to the delay of a threshold logic circuit implementing Montgomery modular reduction and multiplication. In particular, we show that fixed-modulus Montgomery reduction can be implemented

as a polynomial-size depth-2 threshold circuit, while Montgomery multiplication can be implemented as a depth-3 circuit. We also propose an architecture for Montgomery modular reduction and multiplication, which ensures feasible O(n ^{2}) area requirements, preserving the properties of constant latency and a low architectural critical path independent of the input size n. We compare this result with existing polynomial-size solutions based on the Boolean computational model, showing that the presented approach has intrinsically better architectural delay and latency, both O(1).

FPGA based N-bit LFSR to generate random sequence number by Babitha P. K, Thushara T, Dechakka M. P.

Random number generators are most prominently used in the area of communication to provide security for information systems through pseudo random sequences. It also applicable for key generation in cryptography applications and signature analyzer to generate test patterns for Built-In-Self Test. In conventional method, random numbers are generated by a reference value i.e., seed value, using a XOR gate. The new proposed methods present a linear feedback shift register (LFSR) which generates an arbitrary number based on XOR, XNOR gates with and without seed value using multiplexer. Multiplexer is append to generate a random value at user defined state in runtime. Hardware complexity and power consumption is reduced by replacing the multiplexer with tristate buffers. Result analysis indicates that proposed LFSR with and without seed value gives a better performance, low power consumption and improves more randomness in runtime with Partial Reconfiguration (PR). Resource utilization for standard XOR based LFSR is compared with proposed LFSR using XOR and XNOR logic. Proposed method is designed in Verilog HDL, simulated with ISE Simulator, synthesized and implemented using Xilinx ISE, targeted for Spartan3E XC3S500E-FG320-4 and Virtex-5

XUPV5LX-110T architecture.

A multilayered Secure for Transmission of Sensitive Information based on Steganalysis by Divya Jenifer D' Souza, Minu P Abraham

We propose a multilayered secure scheme to transfer sensitive text over an unreliable network. The secret text is first encrypted using the AES algorithm. The cipher text produced is hidden in an audio file. The audio file is in turn encrypted in parallel

using the concept of Shamir's technique based on CRT to maximize resource utilization. These, audio shares are sent over different channels in the network for security. Experimental results show that, even if certain shares got lost over network, audio files could be recovered at the receiver with the remaining shares without sender needing to resend the file.

An efficient chaos pseudo-random number generator applied to video encryption by HuiXua, Xiaojun Tonga, XianwenMenga

Traditional cipher systems are not appropriate for video encryption due to the high computation overhead. Video encryption must take account of the trade-off of both data security and real-time performance. In this paper, an efficient chaos pseudo-random number generator is designed to generate key stream for encrypting video syntax elements of H.264/AVC. In view of the efficiency and security, the intra-prediction mode (IPM), signs of trailing ones (T1s), signs of non-zero (NZ) coefficients, signs of motion vector difference (MVD) are chosen for selective encryption. The proposed scheme provides sufficient protection for the video commercial value. Experimental results demonstrate that the course of encryption will not affect the coding efficiency of H.264/AVC by keeping exactly the same bitrate and negligible time overhead. Security analysis shows that the proposed scheme has the ability to resist malicious attacks.

Computing Seeds for LFSR-Based Test Generation FromNontest Cubes by IrithPomeranz

In test data compression methods that are based on the use of a linear-feedback shift register (LFSR), a seed that produces a test for a target fault is computed based on a test cube for the fault. With a given LFSR, a seed may not exist for a given test cube, even though a seed may exist for a different test cube that detects the same fault. This issue is addressed in this brief by computing seeds for LFSR-based test generation without using test cubes. Instead, the procedure described in this brief is based on the use of nontest cubes. A nontest cube for a fault must be avoided in any test or test cube for the fault in order to allow the fault to be detected. Therefore, nontest cubes do not limit the ability of the procedure to compute seeds with a given LFSR. Experimental results demonstrate the advantages that the use of nontest cubes provides, and the associated computational cost.

3. EXISTING SYSTEM

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

LFSR cryptography is illustrated in Figure 1, where both the encryption and the decryption is done only by the EXOR operation [4,5,13]. EXOR operation between the plain text and random key for the encryption process and the EXOR operation is done between the ciphertext and the random key for the decryption process.

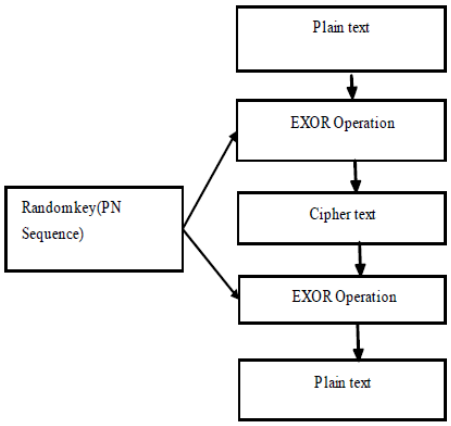

Figure 1: Existing LFSR cryptography

The highly emerging digital VLSI system design in the communication field requires fast generation of random patterns for error detection, VLSI circuits testing, data encryption and decryption. The test patterns for the above applications are generated by Linear Feedback Shift Register (LFSR). The 8 bit pattern generation circuit to generate a pattern X^7+X^5 +X^4+X^3+1 is shown in Figure 1. As the technology advances, the need for low power consumption circuit increases. Thus, the circuit is generally expected to be designed in such a way that it should consume less power, occupy minimum area with improved response time. The use of flip-flop with activated clock in the register design consumes more power which is not sufficient for high throughput, so pulsed latches are used in the place of flip-flops in this proposed work.

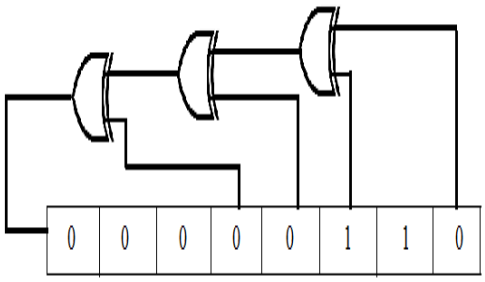

Figure 2. 8-bit LFSR circuit

For reducing the power consumption of the device, various methodologies are available in the literature. Dropping the number of transitions is one of the means for power optimization. Transitions are reduced by swapping the bits and applying clock to half part of the circuit. Clock gating is also employed for power optimization. Although various optimization techniques are implemented for minimizing the power consumption of the device, they are not eventually much effective by the means of reducing the response time and area. Like power optimization techniques, techniques for minimizing the area and increasing the

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

speed are also employed in [1]-[5]. The conventional method of serial to parallel architecture and pipelining algorithms are used to increase the speed of the shift register. Also calculation of output value only by considering the past feedback value in the transposed serial architecture, increases the speed. The transformation from long LFSR sequence to several short LFSR sequence in series reduces the overhead. Though several techniques are used to reduce the power, area and speed, they are not efficient in terms of critical path delay.

LFSR is a serially connected flip-flop configuration – shift register configuration – with feedbacks from certain flip-flop outputs – taps – that are XORed together –added in modulo 2 – and connect back to first flip-flop's input. The number and position of taps determine the length and sequence of generated PRBS pattern. An exemplary 8 stage LFSR with tap connections that provide maximum possible sequence length (2n-1 patterns)

4. PROPOSED LFSR CRYPTOGRAPHY

In this LFSR OTP encryption and decryption algorithm is used. LFSR OTP encryption is shown in Figure 4

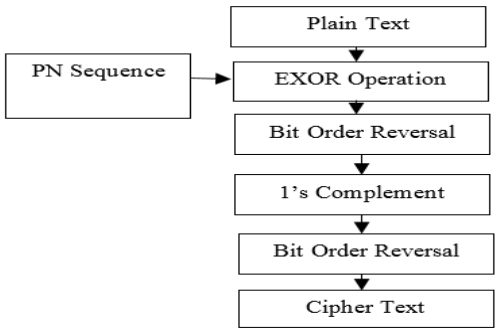

Figure 4: LFSR OTP encryption

The number of steps has been increased in both the encryption and the decryption process to attain the high security level of data. Here the OTP algorithm is presented in such a way that the process includes a Bit reversal process after the EXOR operation. The reversed sequence is performed with a 1's complement operation then once again the bit reversal operation is performed to get the Cipher text. This helps to improve security than a single layer. In the above proposed LFSR cryptography technique, multi-layers can be used to achieve higher security.

The LFSR OTP decryption is shown in Figure 2. Here the reverse process of the encryption process is performed to retrieve the original information. Then the sequence is made to experience the routine extraction process using the PN sequence. Without the knowledge of the OTP algorithm network hacking will be difficult on the information transmitted.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

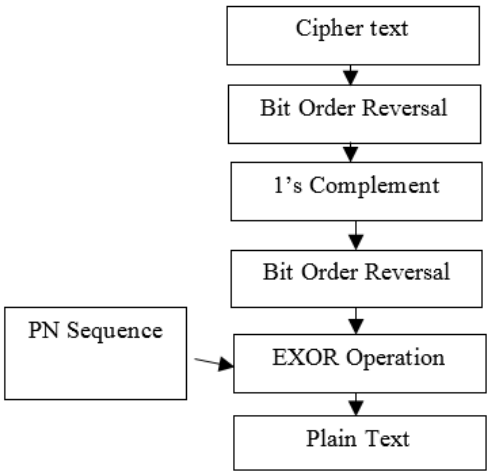

Figure 5: LFSR OTP decryption

5. MULTILAYER OR CASCADED CRYPTOGRAPHY

Multilayer or cascaded cryptography is the process of encrypting an already encrypted data into two or more times either by using the same or different algorithms.

Block diagram for the proposed multilayer cryptography is explained in Figure 6

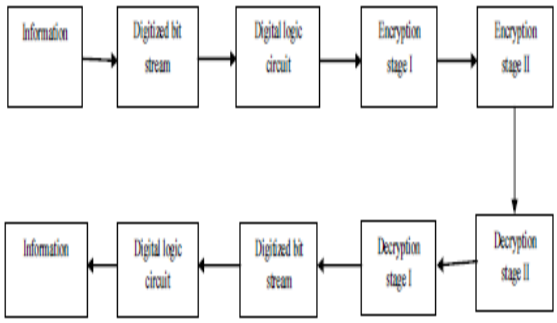

Figure 6: Block diagram

`

In this block diagram, information is the input image. The input image is then converted into the digitized bit stream. This bit stream is taken for the encryption and decryption stages. The resultant bit stream is then converted into the original image which is the input. Conversion of the image into bit stream and bit stream into an image is done by using the Matlab software. Simulink is used for linking the Matlab and the model SIM software.

6. MULTILAYER LFSR OTP ENCRYPTION ALGORITHM:

In this multilayer LFSR OTP encryption cipher text can be created by using the mathematical expression given as

$$\alpha = N\left[\{(\mu \oplus \gamma) >>> n\} >>> n\right]^{r} \quad ...(1)$$

Where, α = encrypted data,

N = number of layers,

>>> = circular right shift,

n = number of bits,

μ = PN sequence,

γ = input.

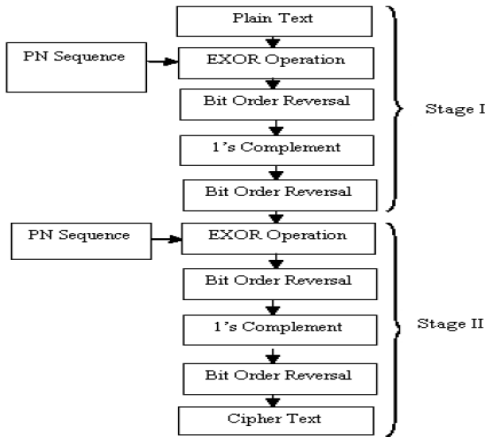

Figure 7 Two stages of LFSR OTP encryption

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

The equation provides the step by step process involved in the OTP algorithm. The first step, a plain text which is nothing but the PN sequence created in the LFSR operation is to be EXORed. The resultant value is taken and their bit order is reversed by using the circular shift register. Then, the obtained result is inverted by using the 1's complement logic. Again the bit order is reversed for the result obtained in the previous step. The resultant value is the cipher text for the stage I encryption. The resultant cipher text is the EXOR ed with the PN sequence which is the random key.

The output obtained in the above step is taken and fed into the circular shift register to reverse their bit order. Perform 1's complement for the output obtained by using the inverter logic.

Multilayer LFSR OTP Decryption algorithm:

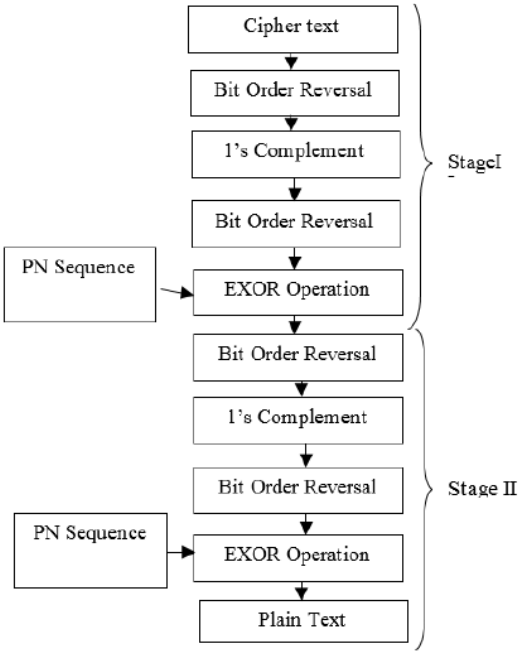

Figure 8 Two stages of LFSR OTP decryption

In this multilayer LFSR OTP decryption original plain text is retrieved by using the mathematical expression which is shown in the equation (2).

$$\beta = N\left[\{(\alpha >>> n)^{r}\} \oplus \mu\right] \quad \text{.....(2)}$$

Where,

β = decrypted data,

α = encrypted data,

n = number of shifts,

N = number of layers,

μ = PN sequence,

>>> = circular right shift

Equation (2) explains that the original plain text can be retrieved by using the following steps. In the first step, ciphertext which is nothing but the resultant value obtained in

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

the multilayer LFSR OTP encryption algorithm is taken and fed into the circular shift register to reverse the bit order. The next step is to perform 1's complement for the resultant value obtained in the previous step. The resultant value is taken and fed into the circular shift register to reverse the bit order. Then, the final result is taken and EXORed with PN sequence which is nothing but the random key. The resultant value is the stage I decryption. This value in the decryption stage I is taken and fed into the circular shift register to reverse the bit order. Subsequently, this performs 1's complement for the resultant value obtained in the previous step. The output obtained in the above step is taken and fed into the circular shift register to reverse their bit order. Again the EXOR operation is performed between the resultant value obtained in the above step and the PN sequence which is nothing but the random key generated by the LFSR. The resultant value is the original plain text for the stage II decryption. After the cryptography process, the final digitized bitstream is taken into Matlab. To attain the original image corresponding binary image of the resultant digitized bitstream is processed.

7. SIMULATION RESULTS

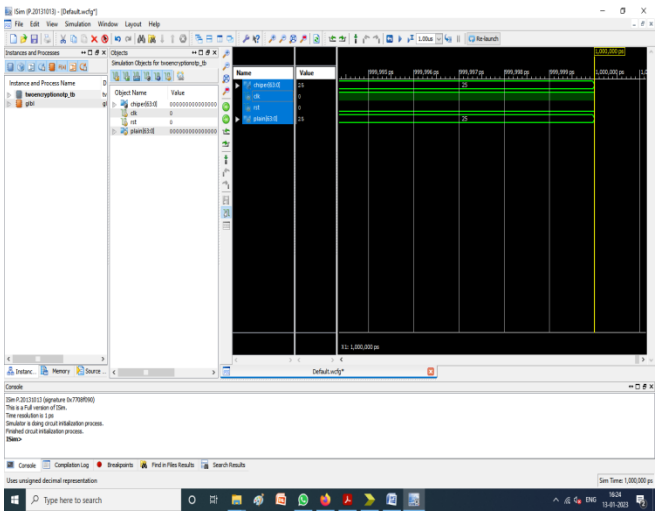

Fig 9 Simulation Result

8. CONCLUSION AND FUTURE WORK

The first layer and second layer of cryptography are completed with the help of the LFSR cryptographic technique. The cipher text for the LFSR cryptography is generated. Here both the encryption and the decryption process are done by the OTP algorithm. Due to this security of the data has been enhanced and the various cryptographic techniques have been summarized. The work focused on the design of effective single-layered cryptography as well as multilayer cryptography by using the LFSR cryptographic technique. Various levels of the bit handling process in the data communication system are implemented successfully through this LFSR cryptographic technique by generating the

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

authentication key. The concept of image processing is also implemented successfully in the Matlab software. The multilayered cryptography is compared with the single-layer cryptography to prove that the multilayered cryptography is better enough to enhance the data security level during the data transmission.

REFERENCES

[1] Alessandro Cilardo "Exploring the Potential of Threshold Logic for Cryptography-Related Operations" In IEEE Transactions On Computers, Vol. 60, No. 4, (April 2011).

[2] Dr.M.V. Sruthi "Exploring the Use of Symmetric Encryption for Remote User-Authentication in Wireless Networks " in 3rd International Conference on Smart Generation Computing, Communication and Networking

[3] Divya Jenifer D' Souza, Minu P Abraham "A multilayered Secure for Transmission of Sensitive Information based on Steganalysis" in ELSEIVER, Procedia computer science 78 (2016).

[4] HuiXua, Xiaojun Tonga, XianwenMenga, "An efficient chaos pseudo-random number generator applied to video encryption" in ELSEIVER, OPTIK 127 (2016).

[5] IrithPomeranz "Computing Seeds for LFSR-Based Test Generation FromNontest Cubes" in IEEE transactions on very large scale integration (vlsi) systems, vol. 24, no. 6, june 2016.

[6] Jawahar Thakur, Nagesh Kumar "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" in International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 1, Issue 2, December 2011)

[7] Mitali, Vijay Kumar and Arvind Sharma "A Survey on Various Cryptography Techniques" in International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 4, July-August 2014 ISSN 2278-6856.

[8] NouraAleisa "Comparison of the 3DES and AES Encryption Standards" in International Journal of Security and Its Applications Vol.9, No.7 (2015), ISSN: 1738-9976

[9] PushpLata, V. Anitha, "Multi-Layered Cryptographic Processor for Network Security" in International Journal of Scientific and Research Publications, Volume 2, Issue 10, October 2012 1 ISSN 2250-3153.

[10] Ritu Tripathi, Sanjay Agrawal "Comparative Study of Symmetric and

Asymmetric Cryptography Techniques" in International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853

[11] Sahil Agarwal, Barkha Khattar , Dr. Inder Singh, "multi-layered security for private Communication (using steganography and cryptography)" in International Journal of Advance Research In Science And Engineering IJARSE, Vol. No.4, Special Issue (01), March 2015 ISSN-2319-8354(E).

[12] ShraddhaSoni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma "Analysis and Comparison between AES and DES Cryptographic Algorithm" in International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012 ISSN:2277-3754.

[13] Sugitha,G A.Albert raj, A "CNLRA : Critical node and Link reconnect algorithm for wireless adhoc networks using graph theory" Asian Journal of Research in Social Science and Humanities Vol 6,no 8 , 2016,pp 1953-1963.

[14] Yashwantkumar, Rajatjoshi, Tameshwarmandavi, Simranbharti, Miss Roshni Rathour "Enhancing the Security of Data Using DES Algorithm along with Substitution Technique" in International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issue 10 Oct. 2016.

[15] Maria Jessi ,A,Albert Raj " A newfangled method to maintain Infrastructure and Mobility of Nodes by weigh based Clustering and Distributed Scheduling , International Journal of Printing & Packaging Allied Science,Vol 5, no 1 , 2017,pp 24-33 ISSN 2320- 4287.

[16] Bommi,A,Albert Raj "A Low Cost Image De-noising Implementation Using Low Area CSLA for Impulse Noise Removal" Journal of Circuits, Systems, and Computers Vol 27 no 4 2018,pp 1850060-1-20.