Advanced Encryption Standard (AES) Using Pseudorandom Binary Sequence (PRBS) As a Key, Simulated In MATLAB

Suparba Tapna

Dept. of Electronics and Communication Engineering
Durgapur Institute of Advanced Technology and Management
Durgapur, India
suparbadrgvy788@gmail.com

Amiya Karmakar

Dept. of Computer Science and Engineering
Maulana Abul Kalam Azad University of Technology, West Bengal
Kalyani, India
amiya.karmakar@rediffmail.com

Abstract — Cryptographic cipher strength, highly depends on the statistical performance of its generated key stream. The generated key stream is constructed stochastically for the statistical behavior of secure key. This enormous behavior proves that the level of security proffered by the cipher. When the key behaves as a random nature, it increases the encryption performance of high-quality key stream. Many key generation techniques use a pseudorandom binary sequence as a key due to its randomness in nature. Keeping with this view, in this paper pseudorandom binary sequence generated key is applied in encryption & decryption of text & images, which is tested by frequency (monobit) test.

Keywords - AES, Computer security, Cryptography, Decryption, Encryption, Matlab, NIST, Pseudorandom binary sequence (PRBS), P-value, Random number, Symmetric key cryptography.

I. INTRODUCTION

Modern communication technology mostly uses wireless networks. To avoid illegal usage & unauthorized access of information and data must be transferred over secure communication channels [14]. The security strength can be increased by a cryptosystem which will be developed & established. The maximal security system depends on the cryptographic methods which provide the necessary security to the user's sensitive data to prevent illicit usage. The key challenge in the cryptographic standard is to create sequences with steep randomness and statistical properties. The Pseudorandom binary sequence is used in encryption technique to strength the security. The good quality key ensures that the better security offered by block cipher [11]. Apart from the cryptography, pseudorandom binary sequence (PRBS) is applied in the areas of digital communication system [13] such as a direct sequence spread spectrum (DSSS), CDMA technique, sampling [1] [3] [5] [6] [8] [15] etc. The Pseudorandom binary sequence is equally relevant & most significant in many fields for better security [10] [18].

II. DESCRIPTION OF AES

The need for coming up with a new cryptographic algorithm due to weakness in DES. The 56-bit keys of DES are no longer considered safe against massive cyber-attacks in the areas of email password, online payment transaction, E-commerce password, net banking etc. [20]. AES is to be hinged on 128-bit blocks, with 128-bit keys. AES is to consider more protected than others, encryption algorithm mainly due to its variable key length (likes 128-bit, 192 bit, 256 bit key [7, 17]). The variable key length changes the security level low-high without any confusion [19]. It is very much hard to the hackers to make the possibility of encryption strength by applying a key which randomly generates bit sequences. A randomly generated variable key increases the performance level of cryptographic methods [12]. Now a day's cryptographic standard is very much important.

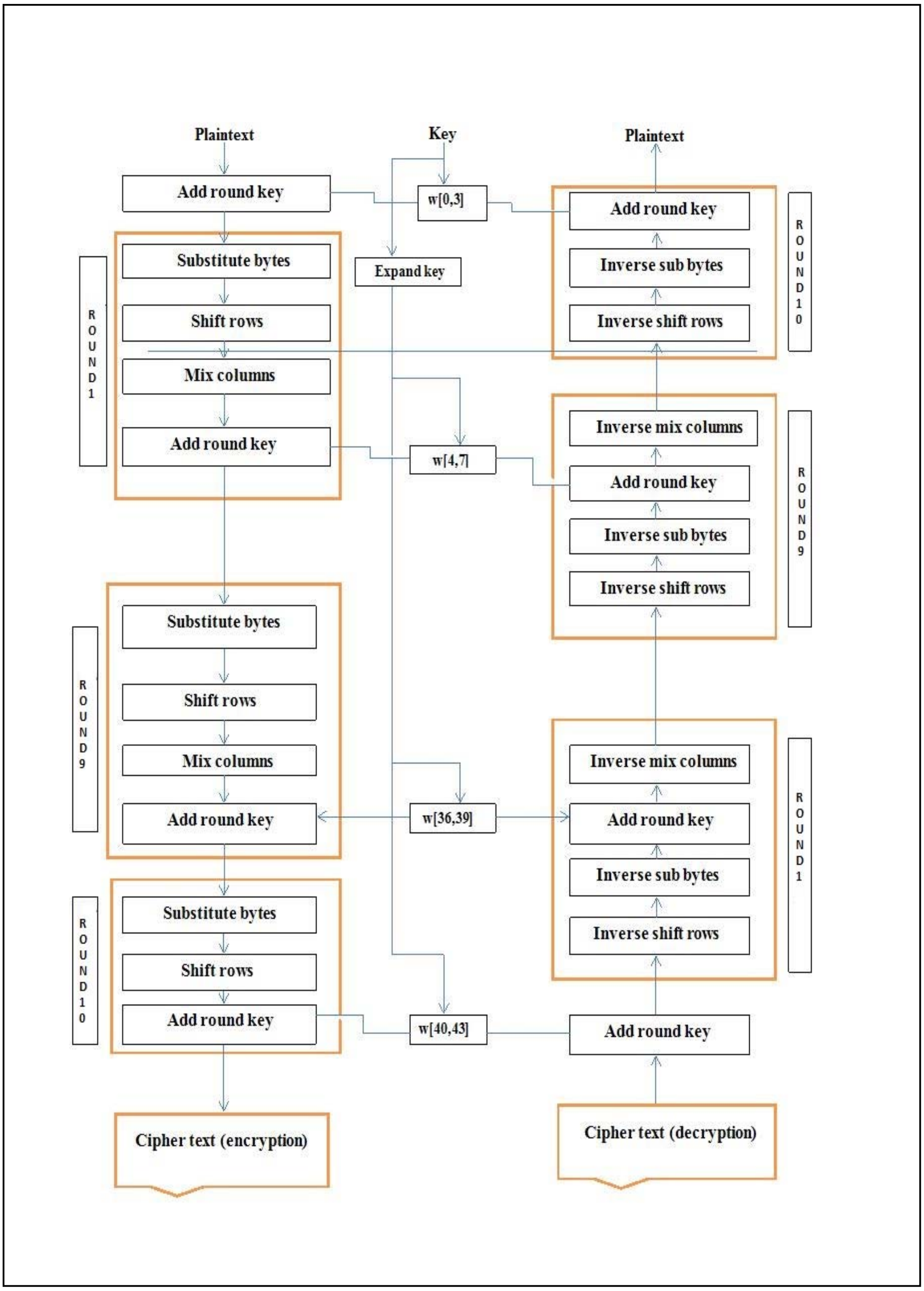


Figure 1. The architecture of AES [1]

III. PSEUDORANDOM BINARY SEQUENCE

A pseudo random binary sequence generated number is widely used in many areas such as telecommunication, computer simulation, encryption, statistical sampling, gaming, gambling, correlation technique and cryptography [13]. In cryptographic technique, a pseudo random binary sequence must be cryptographically consistent to any type of attacks. A string of unpredictable random numbers is required for some cryptographic components like PRBS key generation, authentication, etc. A fault in the randomly generated bit stream or numbers may bring about a complete failure of the whole process. So, the security of randomly generated bits for cryptographic application needs to be checked using NIST standard statistical test suite.

The circuit for generating pseudo random binary sequence consisting of a shift register with the output taps feeding a or gate. A pseudo random binary sequence generator circuit is shown in Figure 2.

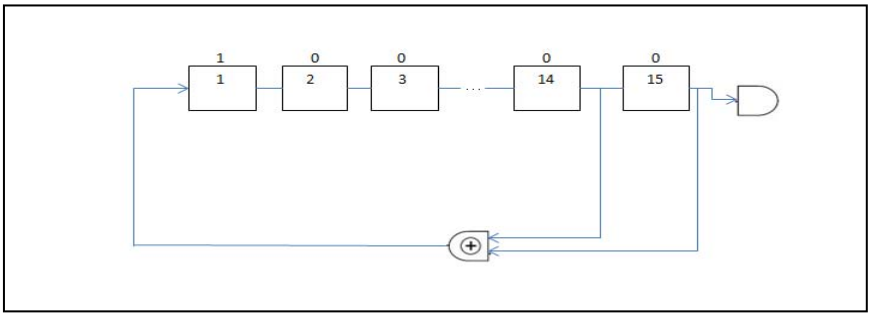


Figure 2. Pseudorandom binary sequence generator circuit

IV. PROPOSED WORK

A. AES algorithm with PR-sequence as a key

The following architecture depicts the complete operation of AES in the blocks and it is also shown the pseudorandom binary sequence applied as a secure key.

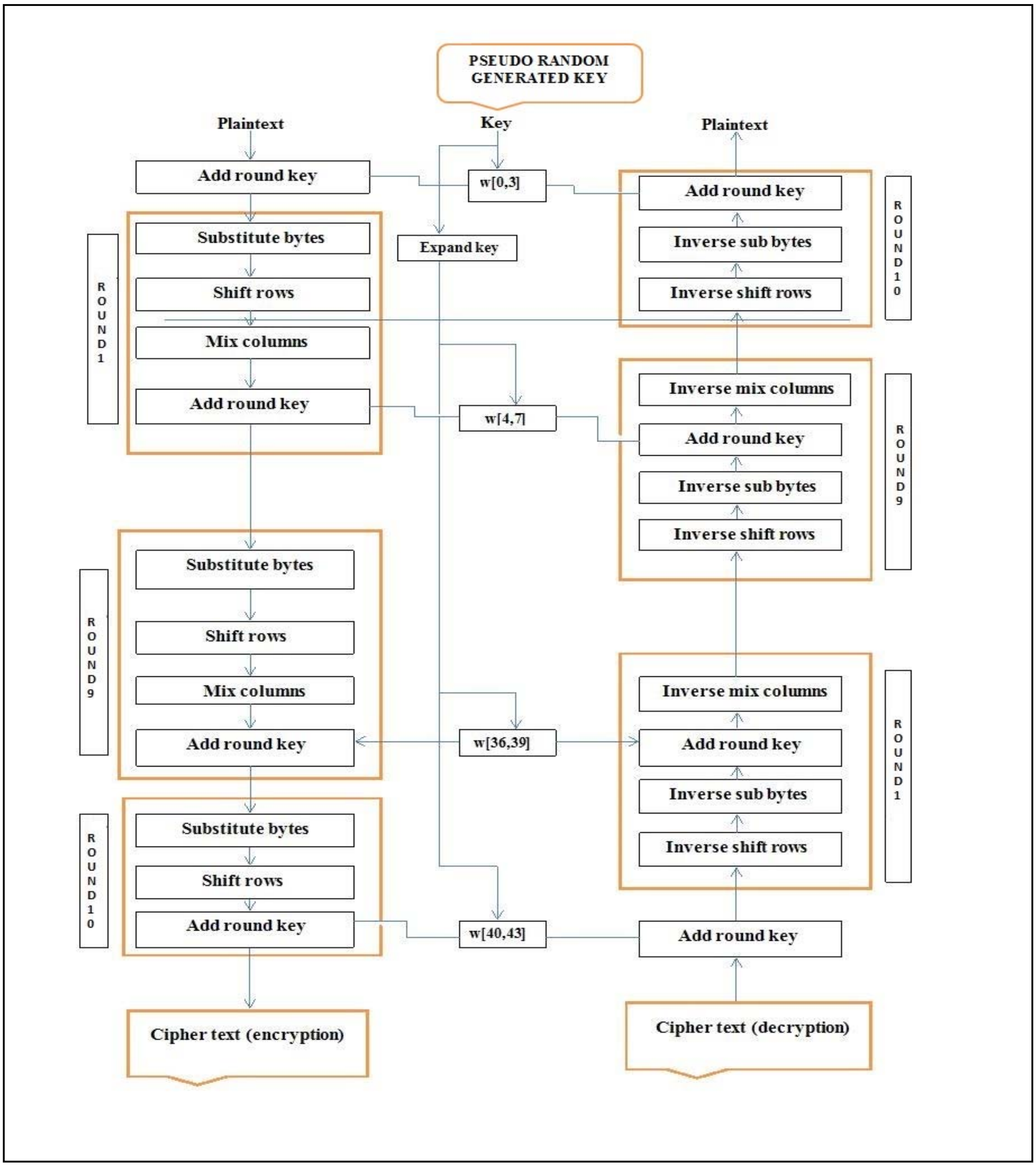


Figure 3. Architecture of AES with PR-sequence as a key

Advanced Encryption Standard (AES) implement is done by using a key encryption & decryption for image & text by existing key & output sequence which is a pseudorandom binary sequence (PRBS) generated. Comparison is made by the following parameters: Time Complexity, Security, etc. In this paper, by using the existing key & Pseudo random binary sequence generated key, which is more time consuming & have better security.

B. Block diagram of implemented PR-sequence as a key

The main implementation is described in following block diagram. The key is random. The encryption & decryption of text & images are performed by randomly generated key. During each simulation, different cipher texts have been formed. The strength of security increases at every simulation for randomly generated bit stream [9].

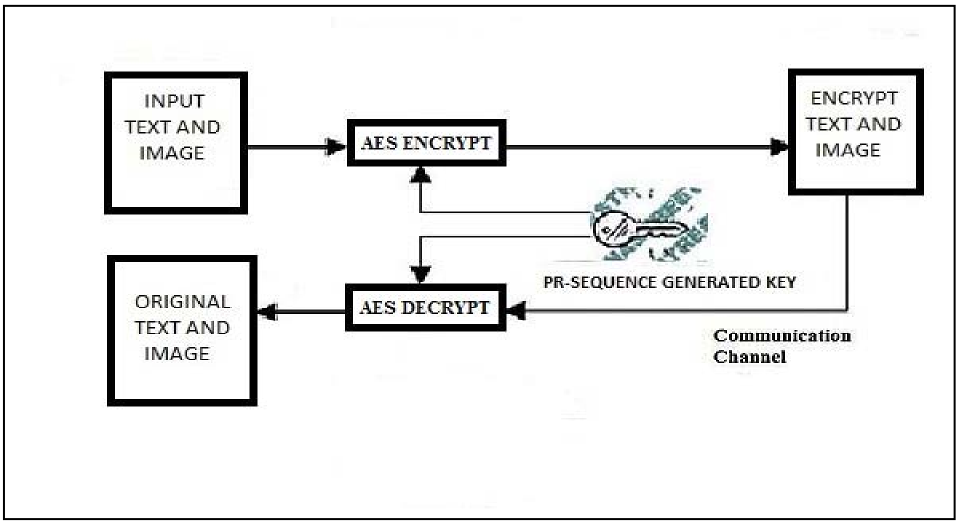


Figure 4. Proposed block diagram of implementation

V. SIMULATION RESULTS USING MATLAB

A. Pseudorandom binary sequence (PRBS) generation

In the pictorial view of pseudorandom binary sequence is briefly elaborates that the generated sequence has been applied on AES 128-bit encryption & decryption for text & images. In this paper, the PR sequence generator is simulated in MATLAB & the simulated output represent as 128-bit secure key.

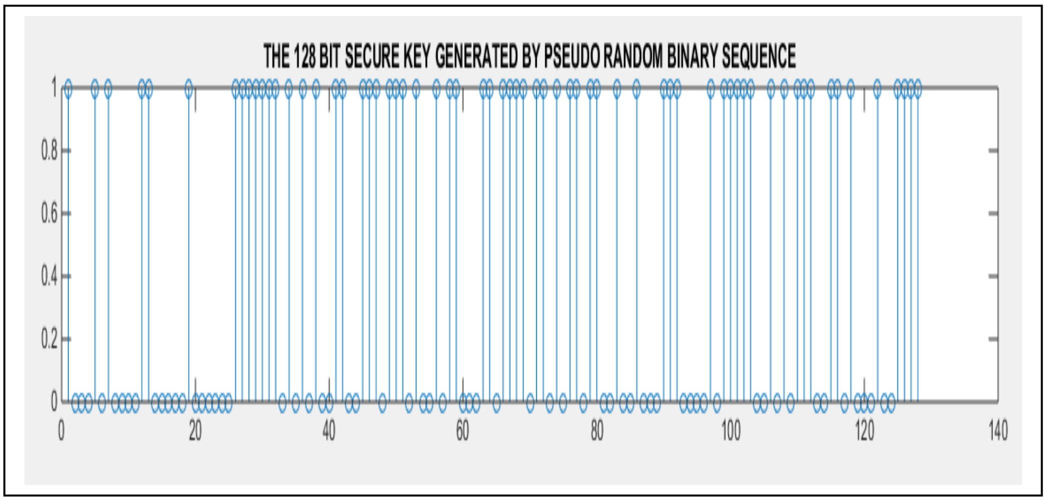
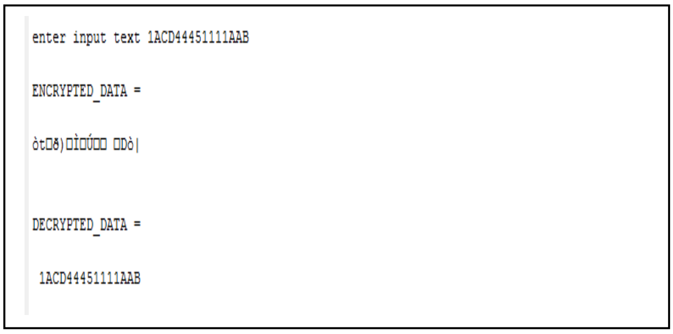


Figure 5. Pseudorandom binary sequence generation

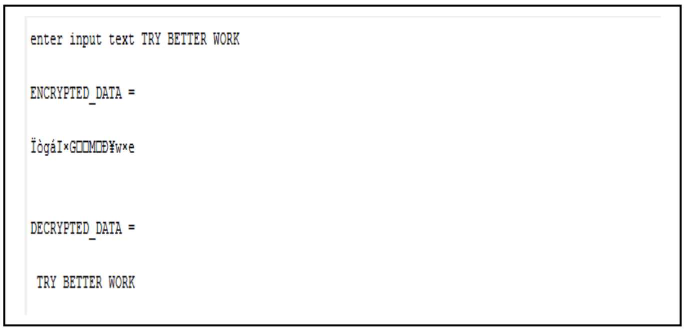
B. Pseudorandom sequence applied to AES architecture as a key

The application of a pseudorandom sequence as a key is implemented in MATLAB. In the following picture analyses that, the input texts are 16-bit hex number and plain message. The key is pseudo random & acts as a secure key. During simulation, the encrypted data is in the following & the decrypted data is getting back to plain text. Hence, encryption & decryption are successfully performed by randomly generated bit stream.



```
enter input text 1ACD44451111AAB

ENCRYPTED_DATA =

òt□ð)□Ì□Ú□□ □Dò|


DECRYPTED_DATA =

 1ACD44451111AAB
```

Figure 6. Simulation of 16 bit hex as text



```
enter input text TRY BETTER WORK

ENCRYPTED_DATA =

ÏògáI×G□□M□Ð¥w×e


DECRYPTED_DATA =

 TRY BETTER WORK
```

Figure 7. Simulation of plain message as text

The Figure [Figure 8.] Depicts the image encryption [4] & decryption using randomly generated key. The key is random and operated in backbend position at each & every simulation. The encryption & decryption are performed in a short interval of time. As a result, due to the performance of encryption & decryption using pseudo random binary sequence generated key, the cipher also changes periodically.

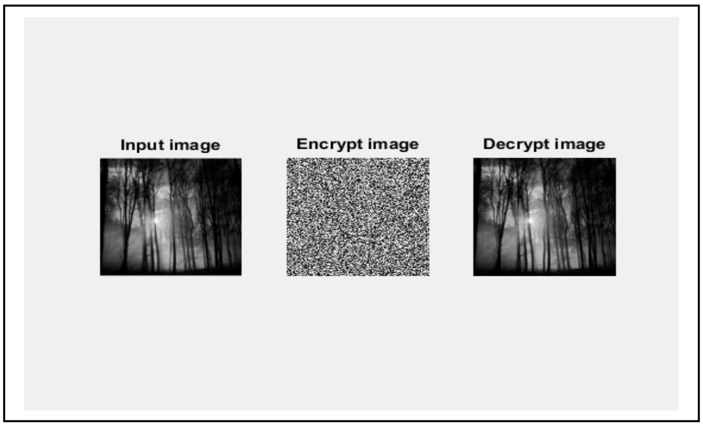


Figure 8. Simulation of an image

PSNR is important to analyze the quality of an image being formed. The peak signal to noise ratio (PSNR) during the encryption & decryption performance of an image is given by the following [Table I.].

TABLE I. PEAK SIGNAL TO NOISE RATIO(PSNR) OF AN IMAGE

Image	Original image (PSNR)	Encrypted image (PSNR)
forest.jpg	7.1411	7.1608

C. Randomness testing of pseudorandom binary sequence (frequency monobit test)

To substantiate the randomness in performance of pseudo random sequence, the test for randomness of the statistical test suite (STS) by the National institute of standards and technology (NIST) [2] are produced. The generated pseudorandom sequences undergo the random property tests like Frequency, Block frequency, serial, Cu sum, runs, FFT, etc. The key sequence which is generated by the pseudo random sequence generator behaves randomly in nature for 200 observations.

Here the NIST standard test used is frequency (monobit) test. The above test follows the decision rule (at the 1% level); it said that, if p value $\geqslant$ 0.01 the sequence is purely random otherwise the sequence is not random [2]. The average p value at the end of 200 observations is 0.534181074 and it can be told that the P-value came is better than any other experimental work related to pseudorandom binary sequence-based cryptography. Therefore, the pseudorandom binary sequence based key sequence is more random in nature.

TABLE II. RESULT OF NIST STS RANDOMNESS ANALYSIS

Randomness test	**P-value**	
Frequency Test	***In [16]***	***This paper***
	0.382778	0.534181074

In this paper all the observed p-value found by NIST frequency mono bit test plots in a graph using MATLAB tool. The change of the random bit generation is observed, and it is achieved from the graph that most of the p-values comes lie above on the existing p-value though few are under the existing p-values. It is shown that the probability value after 200th observation comes to reaching at 0.534181074, which is above the existing value 0.382778 [16] in Figure 9**.**

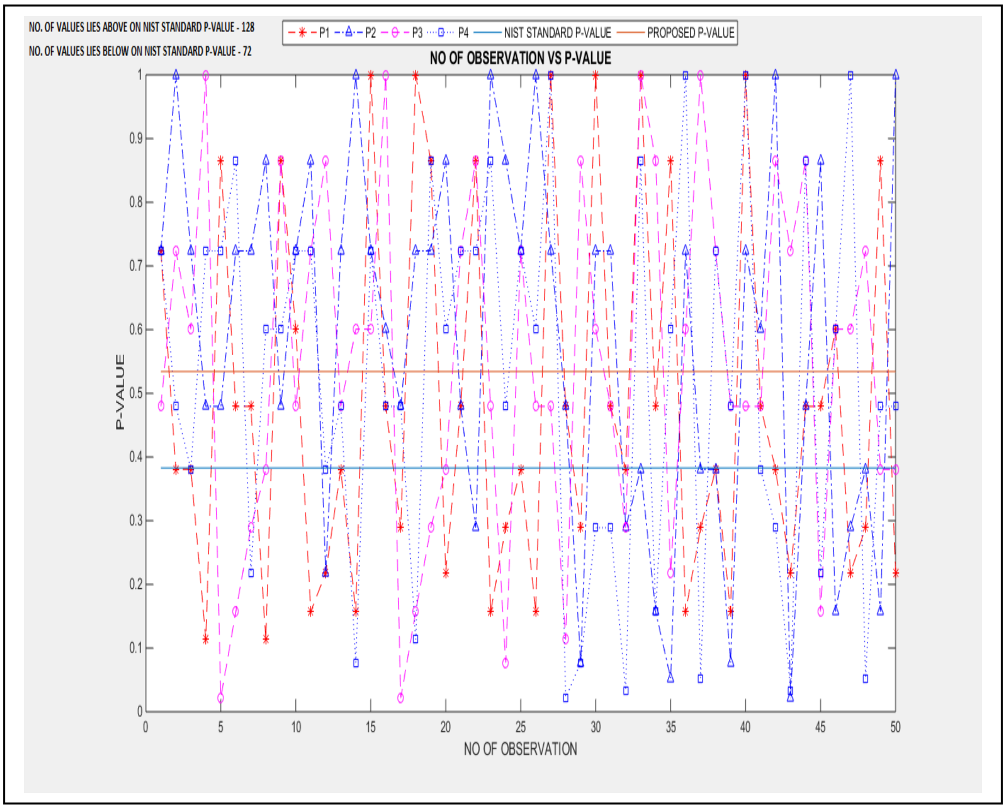


Figure 9. No. Of observation Vs. P-value graph

The graph represents the brown line which follows the average p-values (0.534181074) and the below the blue line denotes a P-value (0.382778) [16] for NIST STS randomness analysis.

1) Comparative analysis of time complexity: It is noticed from a MATLAB simulation that the execution time during encryption & decryption using stochastic (randomly) generated key sequence is less than an existing one. Hence, it can be inferred that, the time complexity of AES (proposed key generation by pseudo random binary sequence) is less than AES (existing).

TABLE III. COMPARISON TABLE FOR TIME COMPLEXITY ANALYSIS

Algorithms	Time complexity	Remarks
AES (Existing)	0.104	Less
AES (PRB Sequence)	0.065	Better

2) Comparative analysis of randomness & security: In case of security for AES encryption & decryption by PR-sequence (having a NIST randomness test p-value of 0.534181074) is better protected than existing (having a NIST randomness test p-value of 0.382778) encryption & decryption technique. In every instance of the simulation and with a short interval of time, different bit sequence gets generated randomly, therefore continuous change in the key with high randomness at each time and also the cipher changes repeatedly (which is shown in Fig. 4. & Fig. 5.). Thus, true randomness is maintained, which can influence the security level of the cryptosystem to a large extent producing a better random cryptography.

TABLE IV. COMPARISON TABLE FOR RANDOMNESS AND SECURITY

Parameters	Existing Work	Proposed work
Key size	128 bits	128 bits
Frequency monobit test for randomness	0.382778 [16]	0.534181074
Possible combination to crack	2^128	2^128 (Random)
Remarks	Average	Better

VI. CONCLUSION

A pseudorandom binary sequence is utilized as an encryption & the decryption key with high randomness and ergodicity. The overall circumstances describe that PR sequence is well protected than any other implementation in cryptography. The nature of high randomness indicates that the better security offered by the cipher, which enhances most of the cases like cyber security, vulnerability etc. To be better protected & well suited. The algorithm is programmed in MATLAB language on a 64-bit computer. Hence outstanding performance is achieved. From proposed work, the time complexity (0.065) is faster than existing (0.104) one and in case of security analysis, i.e. pseudorandom binary sequence based key generation is more secure than existing encryption and decryption technique.

ACKNOWLEDGMENT

The authors would like to express their thanks to the department of Computer Science and Engineering, Maulana Abul Kalam Azad University of Technology, West Bengal, Kalyani for the constant infrastructure support. The authors also greatly acknowledge the support of others faculty member of Department of CSE.

REFERENCES

[1] J. Daemen and V. Rijmen, “The block ciphers Rijndael, Smart Card research and cryptographic Applications”, Springer-Verilog, pp. 288-296, LNCS 1820.

[2] A. Rukhin, et al. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”, NIST Special Publication 800-22, 2001.

[3] A. Meneze, P. Van Oorschot, and S. Vanstone,” Handbook Of Applied Cryptography”, CRC Press, p. 81-83, New York, 1997.

[4] M. Kar, M. K. Mandal, D. Nandi, A. Kumar & S. Banik, “Bit-plane Encrypted Image Cryptosystem Using Chaotic, Quadratic, and Cubic Maps,” IETE Tech. Rev., Vol. 33, pp. 651-661, Feb. 2016.

[5] H. Niederreiter and A. Winterhof, “On a New Class of Inversive Pseudorandom Numbers for Parallelized Simulation Methods”, Periodica Mathematica Hungarica, vol. 42, no. 1 - 2, pp. 77--87, 2001.

[6] T. Siegenthaler,’ Decrypting a Class of Stream Ciphers Using Ciphertext Only’, ieee transactions on computers, vol. C-34, no. 1, January 1985.

[7] Heba Abunahla,Dina Shehada, Chan Yeob Yeun,Baker Mohammad, and Maguy Abi Jaoude, “ Novel secret key generation techniques using memristor devices”,AIP Advances 6,025107,pp.1-10,2016.

[8] S. Y. Hwang, G. Y. Park, D. H. Kim and K. S. Jhang, “Efficient Implementation of a Pseudorandom Sequence Generator for High Speed Data Communications”, ETRI Journal, vol. 32, no. 2, pp. 222-- 229, 2010.

[9] N. Ruggeri, “Principles of Pseudo-Random Number Generation in Cryptography”, 2nd edition, august 26, 2006.

[10] K. Chandra Sekhar, K. Saritha Raj, “An Efficient Pseudo Random Number Generator for Cryptographic Applications”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-4 Issue 1, October 2014.

[11] Alka P. Sawlikar, Dr. Z. J. Khan, Dr. S. G. Akojwar, “ Security Level Enhancement in Noisy Environment”, International Journal of Scientific, Engineering and Technology (ISSN: 2277-1581) Volume No.2, Issue No.10, pp: 1044-1048 1 Oct. 2013.

[12] R. Latif and M. Hussain, “Hardware-Based Random Number Generation in Wireless Sensor Networks”, Advances in Information Security and Assurance, LNCS, vol. 5576, pp. 732--740, 2009.

[13] Alka Sawlikar, Manisha Sharma,’ Analysis of Different Pseudo Noise Sequences’, International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 2, Oct, 2011.

[14] R. Mita, G. Palumbo and M. Poli, “Pseudo-random Sequence Generators with Improved Inviolability Performance”, IEEE Proceedings- Circuits, Devices and Systems, vol. 153, issue 4, pp. 375--382, 2006.

[15] E. Cruselles, M. Soriano, and J. L. Melus, “Uncorrelated PN sequences generator for spreading codes in CDMA systems”, Sixth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, vol. 3, pp. 1335--1340, 1995.

[16] Ahmad and Farooq, “Chaos Based PN Sequence Generator for Cryptographic Applications”, International Conference Signal Processing and Communication Technologies, pp. 83-86, 2011.

[17] J. Nechvatal, ET. Al., Report on “The Development of the Advanced Encryption Standard (AES)”, National Institute of Standards and Technology, pp. 1-7, October 2, 2000.

[18] Ch. Ravi Sankar, P Rambabu,”Random key generation for advance encryption Standard (AES) Using rmprng algorithm”, ieee conference, Vol-3, no 11 (2014).

[19] Shaanban Sahmoud,Wisam Elmasry and Shadi Abudalfa, “Enhancement The Security of AES Against Modern Attacks By Using Variable Key Block Cipher”, International Arab Journal of e-Technology, Vol. 3, No. 1, January 2013.

[20] Garry C. Kessler, “An Overview of cryptography”, ISDN, 4th edition (McGraw-Hill, 1998).