International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2023.9.8.1

E-ISSN : 2454-6135

Volume.9, No. 8
August - 2023

Improved Blowfish Algorithm for Text Encryption Using DNA and Linear Feedback Shift Registers (LFSR)

Raghda Sattar Jabbar [1*], Israa Shihab Ahmed [2] and Saadi Mohammed Saadi [3]

[1]Assistant Teacher, [2] Teacher, [3]Assistant Teacher

[1] Department of Quality Assurance and University Performance, Mustansiriyah University

[2] Informatics Institute for Postgraduate studies, Iraqi Commission for Computers and Informatics

[3] Ministry of Education

Baghdad-Iraq

ABSTRACT

The Blowfish algorithm is a popular way to protect information by scrambling it. It is known for being strong and fast. The strength and randomness of the encryption key are very important for the security of Blowfish. This paper suggests a new way to make the key generation process better in the Blowfish algorithm by using Linear Feedback Shift Registers (LFSRs) and DNA Algorithm. LFSRs are basic but effective machines that create sequences that look random but are not truly random. The DNA algorithm is used to make it harder for others to guess the correct key. To make the Blowfish algorithm better, we are combining the LFSR and DNA Algorithm in the key generation stage. This will make it more secure and efficient. The security of Blowfish greatly depends on how strong and random the encryption key is. It also explains the benefits and things to think about when using these methods. The paper includes experiments to test if this approach works well.

Key Words: Blowfish Algorithm, DNA Algorithm, Encryption, Linear Feedback Shift Registers (LFSR), Security.

1. Introduction

Internet communication is very important for sending lots of information in different areas. Some data might be sent through a channel that is not secure from the person sending it to the person receiving it. The private and public sectors use various techniques and methods to keep important data safe from unauthorized access as the security of electronic information is very important. Cryptography is a very important and well-known way to protect data from attackers. It does this by using two important actions called Encryption and Decryption [1,2]. Encryption means converting or encoding data so that it becomes difficult for unauthorized people to understand or access the original information [3]. This part can change regular information into an unreadable form. The next thing that needs to be done by the person in charge is decryption. Decryption is the process of transforming secret code into regular words without leaving any words out from the original text [4]. Cryptography uses math and changes things around to do certain tasks, and it can do this with or without a key [1,4]. Modern cryptography helps to keep information secret, ensures that it has not been changed or tampered with, ensures that the sender cannot deny sending the information, and verifies the identity of the sender. Nowadays, there are many ways to protect and decode important information. These techniques fall into one of three categories. Symmetric cryptography is the name of the first kind. This indicates that the data is encrypted and decrypted using the same key. The second one uses an encryption technique known as asymmetric cryptography. When using this type of cryptography, two distinct keys are used to both conceal and reveal information. In contrast to other hash functions that require a key, a cryptographic hash function is utilized to combine data without the usage of a key [2,5]. The symmetric key is significantly faster and more efficient than the asymmetric. AES, Blowfish, Simplified Data Encryption Standard (S-DES), and 3DES are a few of the popular symmetric algorithms. This paper's main goal is to present a novel hybrid technique for text encryption that combines the DNA, LFSR, and BLOWFISH algorithms. The structure of this paper is as follows: A description of the cryptographic algorithm is given in section 2. The Proposed Method is presented in section 3. Implementation of the proposed method is presented in Section 4. Section 5, Experimental Results are presented in this section. In section 6, provide a conclusion.

2. Overview of Cryptographic Algorithm of DNA, LFSR and BLOWFISH Algorithm

In this section, the concepts of DNA, LFSR, and BLOWFISH algorithms will be explained in detail:

A-Linear Feedback Shift Registers (LFSRs) [6,7]:

LFSRs are registers that create sequences of random-like numbers using a specific method. They are made up of a bunch of switches and special gates. The feedback path is made up of taps that control how the shifting and XORing is done. LFSRs are commonly used in many different situations when you need to generate random numbers that are not truly random. The LFSR structure is shown in Figure 1.

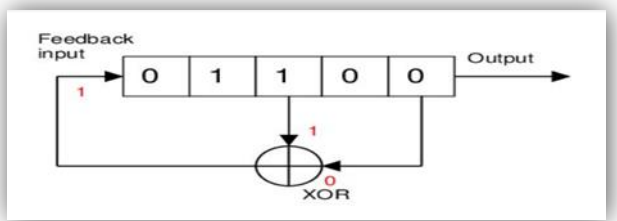

Figure 1: Functional Principle of a LFSR [8].

B- DNA Algorithm [9,10,11]:

DNA cryptography is a part of biology that can hold a lot of information. It can keep track of details about living things. Living things have special DNA information. It is when information is stored, processed at the same time, and transmitted in a very safe way. DNA cryptography uses a method called one-time-pads scheme. Cryptography and molecular biology need to come together to make data transmission and hiding more secure. A plain message is changed into DNA sequences. DNA sequences become more potent or effective when they are joined or paired with the nucleotide bases A-T and C-G. We need DNA cryptography technology to ensure information security and keep data safe and hidden. Genetic information is written down using letters (G, A, T, C). Adenine, Thymine, Guanine, and Cytosine are pairs of building blocks that stick together to keep the DNA structure in a spiral shape. They are connected to a sugar and a phosphate. DNA strands stick together with the help of hydrogen bonds. The letters A and T in DNA stick together with a weak bond made of two hydrogen atoms. The letters C and G in DNA stick together with a stronger bond made of three hydrogen atoms.

C- Blowfish Algorithm(BA) [12,13,14]

The Blowfish algorithm is a way to scramble data using a specific method created by Bruce Schneider. This is a type of encryption method called a symmetric block cipher. It uses something called a Feistel network, The Blowfish algorithm which is like a pattern for how the encryption is done. It repeats a simple process of encrypting and decrypting 16 times. Every Feistel structure has different benefits, especially when used in machines. When decrypting the coded message, all you need to do is reverse the order of the key schedule. The Blowfish algorithm can be split into two parts: key expansion and data encryption. The key expansion process involves using sub-keys that are created from the P-array and S-boxes. This requires precomputation before encrypting or decrypting data. The P-array has eighteen sets of numbers called sub-keys, and each sub-key is made up of 32-bits. These sub-keys are named P1, P2, and so on. A key with a maximum size of 448 bits is divided into smaller components in this section of the text called sub-key arrays. The maximum size of these sub-key arrays is 4168 bytes. Each of the four 32-bit S-boxes has 256 entries:

DOI : 10.31695/IJERAT.2023.9.8.1

S1,0, S1,1,. . , S1,255,

S2,0, S2,1,. . , S2,255,

S3,0, S3,1,. . , S3,255,

S4,0, S4,1,. . , S4,255

This text outlines the formula used to determine these sub-keys:

1. We begin by assembling the P-array. Then, we build up the four S-boxes using a specified string that consists of the digits of pi represented by numbers and letters.

2. XOR P1 with the key's first 32 bits. The next 32 bits of the key are XORed with P2. Continue doing this until all P14 bits of the key have been used. Up until all of the P-array bits have been XORed along with the key bits, the cycle repeats again for each bit of the key.

3. Using the sub-keys outlined in steps 1 and 2, the BA is used to encrypt a string of just zeros in step 3

4. The outcome of step 3 is used to swap P1 and P2 as in step 3.

5. Use the Blowfish technique to encrypt the output of step 3 using changed sub-keys.

6. P3 and P4 are substituted using the outcome of step 5 in step 6.

7. The output is constantly changing as the procedure continues, switching every component of the P-array before switching the four S-Boxes.

A 64-bit block element of plain text is converted to a 64-bit cipher text to begin data encryption. First, the 64-bit segment is split into two identically sized segments that serve as the basis for the BA. The first 32-bit block portion must be combined with the first P-array using XOR as the next step. The F function receives the 32-bit data obtained in step 2 and organizes it into a 32-bit segment. The following step is an XOR operation to merge it with another chunk of the 32-bit block (R) from the 64-bit plaintext split. The 32-bit parts L and R are switched for further rounds of the BA after the XOR operation is complete. This image displays. I'm outlining the 16-round BA's organizational structure. The information is 64-bit data with the name X. There are two portions to this data, each with 32 bits. These components are known as XL and XR. Data encryption and decryption are identical processes; however, they involve separate procedures. P18s are applied in the reverse hierarchy.as depicted in figure 2.

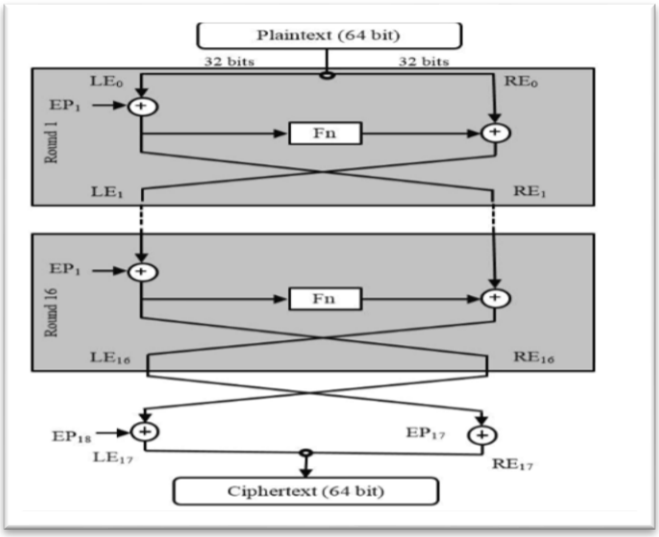

Figure2: Blowfish Algorithm [15].

DOI : 10.31695/IJERAT.2023.9.8.1

3. THE PROPOSED METHOD

In this section, we will cover the architecture of the proposed method will be explained, which is the methodological framework that represents how to encode the text massage based on the optimized algorithm, as shown in figure 3, which represents a detailed diagram of the proposed method.

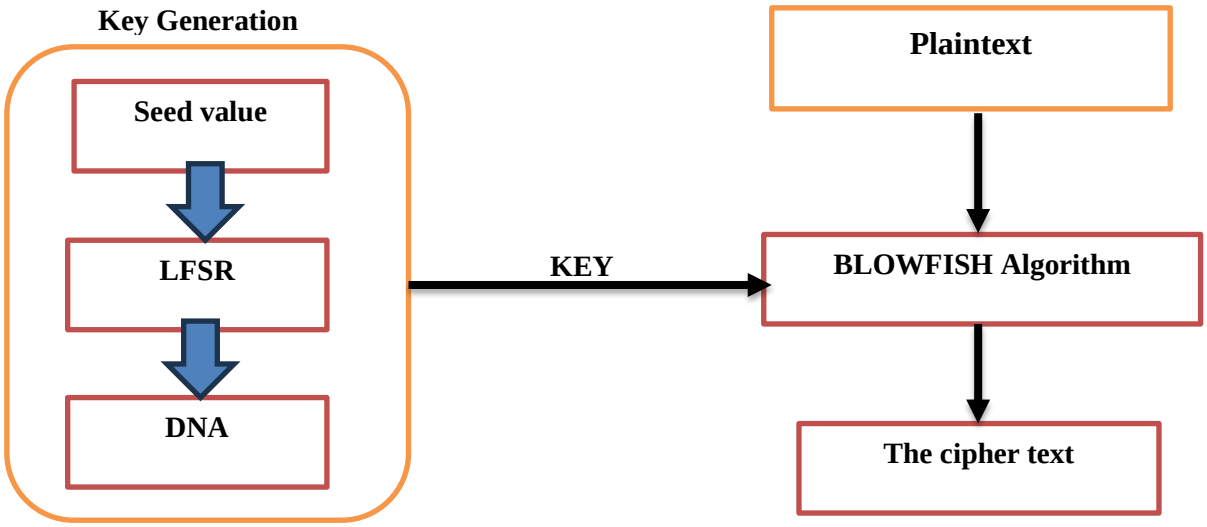

Figure3: Encryption Process

4. IMPLEMENTATION OF THE PROPOSED METHOD

The new method uses the LFSR and DNA Algorithm to create a key for the blowfish algorithm. In order to make the key generation process in Blowfish better, LFSRs and DNA algorithm can be used to create key which helps to increase randomness and make the keys harder to predict. There are five steps in the process of generating a key.

A. Key Generation Stage

1- Starting point: The LFSR is set to begin with a certain initial value called the seed. The seed value is a secret code that only the person sending a message and the person receiving it know. The seed value decides where the shift register begins.as shown in figure 4.

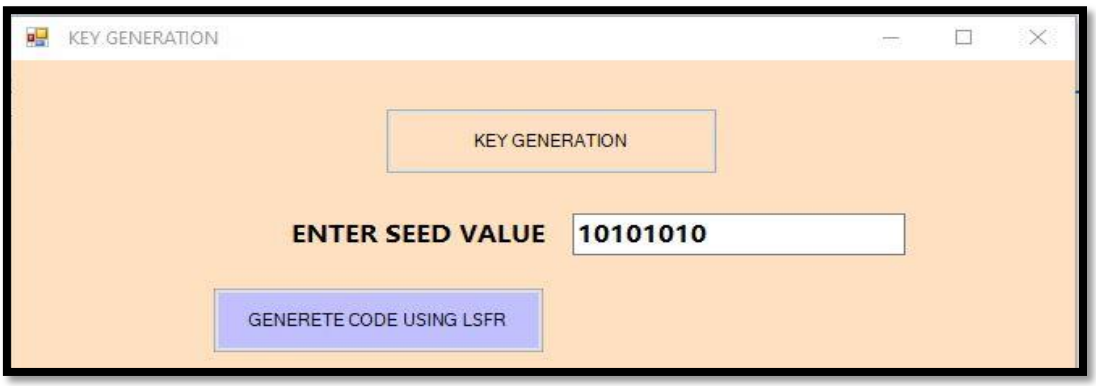

Figure 4: Seed Value

2- Feedback mechanism: The LFSR uses a way of giving back information to generate a sequence of random bits that aren't truly random. The feedback system uses a math function with a certain level of complexity. The function creates a new bit using the information in the shift register. The LFSR produces a series of computer-generated random bits, which are then used as a secret key in the blowfish algorithm.

DOI : 10.31695/IJERAT.2023.9.8.1

3- Key expansion: The LFSR output is made longer to match the key length needed for the blowfish algorithm. To make the key longer, we repeat a sequence of random bits until the desired length is reached. Then key will be generated as shown in figure 5.

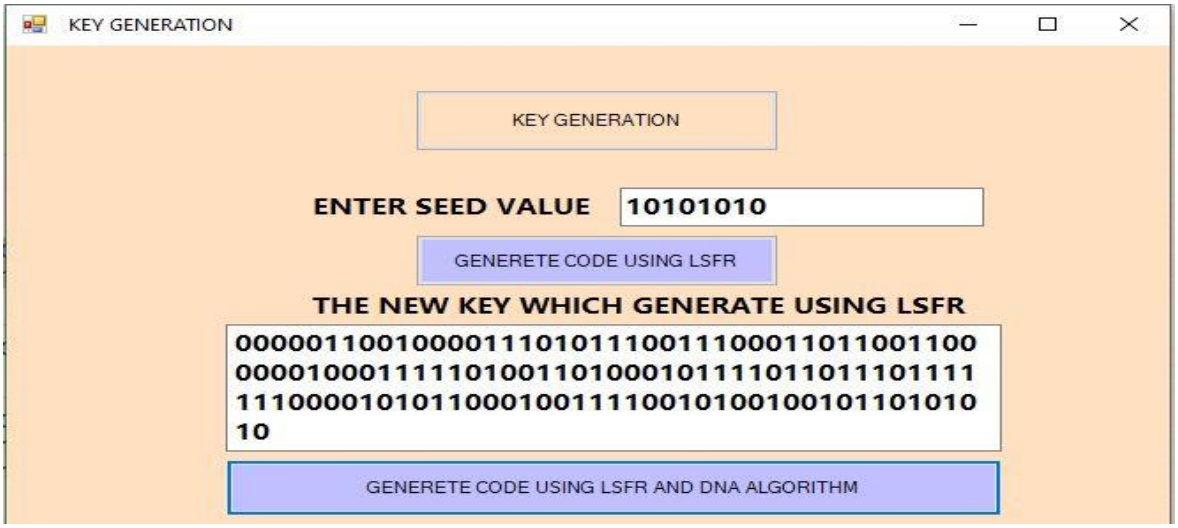

Figure 5: Key Using LSFR

4- Output operation of LFSR is represented in DNA bases format. Representation is a way of showing something using numbers or symbols. In this case, we use the letters A, T, C, and G and assign them specific number combinations: A is 00, T is 01, C is 10, and G is 11.

5- Now complement the DNA bases as: A=T; T=A; C=G; G=C . The result key is then used as the key for the blowfish algorithm. Then convert the result key to string as shown in figure6.

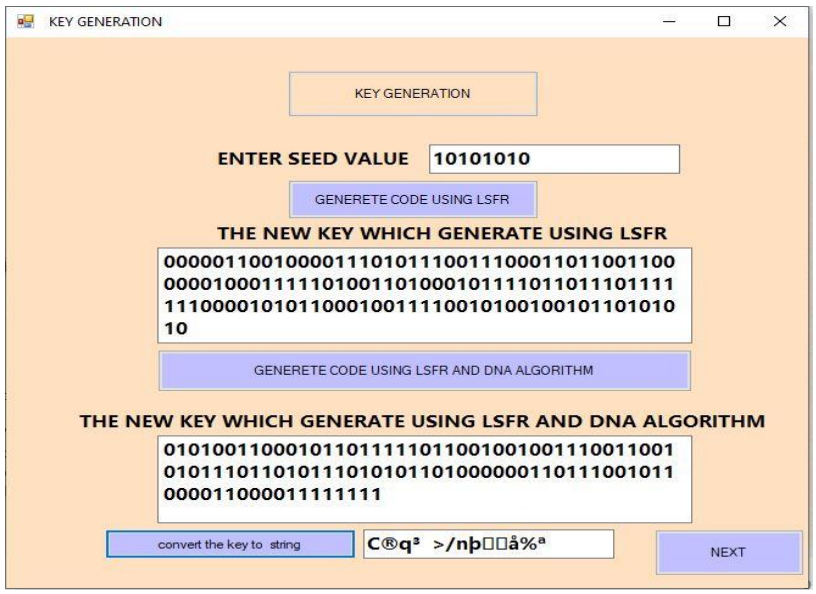

Figure 6: Key After DNA Algorithm

A. **Encryption process: -**After find the key we must enter the plain text then click (encrypt) to encrypt the string using the blowfish algorithm as shown in the figure 7 &8.

DOI : 10.31695/IJERAT.2023.9.8.1

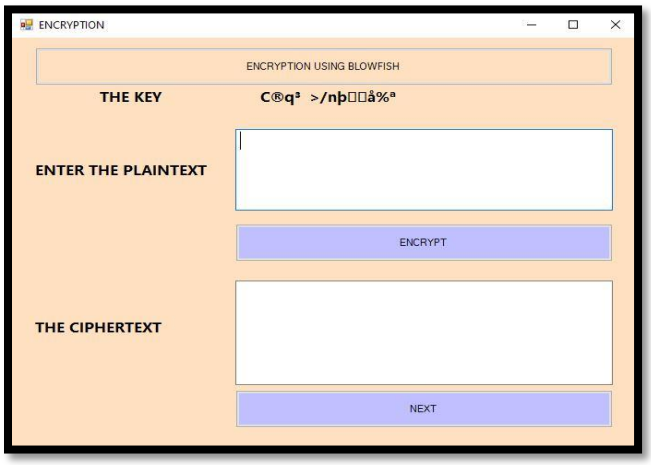

Figure 7: Window Main

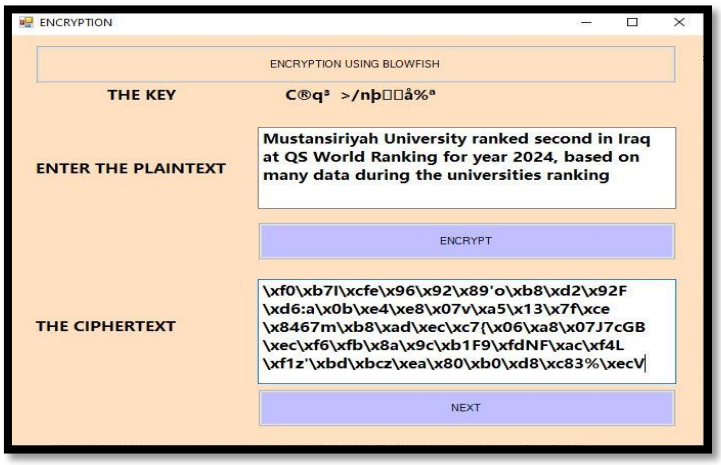

Figure 8: Encryption Process

B. Decryption process: -

In this part, the decryption process involves using the same key to decode the cipher text, so when you press the decryption button, the original text will appear as shown in Figures 9 and 10.

Figure 9: Cipher Text

Figure 10: Decryption Process.

5. EXPERIMENTAL RESULTS

There are a lot of tests to assess the quality of cryptographic and security analysis methods. For the encryption, the plaintext within Figure 11(A) is utilized. In Figure 11 (B), the encrypted text whose cipher is produced with the help of the utilization of the proposed method appears, the data is successfully encrypted because the text is like symbols and numbers so we can't normally interpret it. In Figure 11 (C), the encrypted text whose cipher is produced with traditional blowfish. The decrypted text appears in Figure 11(D).

DOI : 10.31695/IJERAT.2023.9.8.1

encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as cipher text. Ideally, only authorized parties can decipher a cipher text back to plaintext and access the original information

Figure 11-(A)Plaintext

\xecge\x12\xb0\x0en\x93(rj\x89\xa4\x16\xf6\xdc\xb2\xd4L\xcd5C\xae\xb1\x10O\x8f\xa7V\xcf\x06\x1c\xf1\xe9$\xfeCIK\x99\xfbLoj}\xca\rL1W\xe5\xad\xd5\x0c\xda`\x90C\nw)\xa5\xd8\xe7\xc3\x19\xc1\x84\x90\xa8\xd0\xaf\x8e/r\xd3\xc3\xa5\n`\x0f\xf7\xc1\xd2\xc9M\xe6`[\xd0\x06\xe9x\xa6\xbaI]\x8e\x94\xd7\x06\xa8\x8f\xcd7)\xcf\xc1\xaaVGy\xe9p\xe1\x10o\xbb\ngt\x16\xa1~\x02\xed2G\xb0_\xc2i\x1a\xae\x9ewu\xaa\xff\xcc79W\xda@6\xad{\xfdC\xf9\x1c\x7f2\x1b\xe0\xf9\xb2j\xb4\xbaEG\xc5\xed\xee"B\x02q\xd6\xb9:\xc7\nU\xa8\xc5V\xe4\x9b\xdb\xffN\xc6!\xd5\xffZg\xdc(\xbd\xc5\x08.\r\x93v\xf2\xe5\xc1\x1a\xb6\xd0e\x94\xa1\x94@u\x90\xed\n@\x88\"\x19}Y\xea\xb63\xd6z\xe1\xda\xf6\xa0\xcd\xcb\x9c.L\x8a\x93V\x01\x19.hu\xfc\r\xea\n\x9c\xca2FL\x1dM\x0f\xf4h\x07Y\xad2\xedq\xd9o,8\xa3vp{\x95\"\xd8\xa2G\x0f_I#ik\x11,8\x02m1\xcd\x11j\xb86\xaa\x1bc\xfb\xbc\x86\x12\x02\\\xff\xfc\xe32\x92d\xcfz\xf5\xcf

Figure 11-(B) Cipher text Using Proposed Method

Z6jXCQICQov4Opr3iXmwzXnfCCrWBg9DSAAI3cCKAxPr7xfDHMqGeAdpEeOac27c+DTw11PH7Xl0rEKx7LHS14epsPktWhrkOZCZJwGN2y/2lX3E4lzFS5FJNvaSxS25XRuP2fndl33F/oVUtZ2pKzoZFHOFoTFjMcJhRhaoeHWmuaBF8pJoFWfMrZUgs4LQUvxLMtYwziDIN7p0OcETpD6bTNqE8K6JQALgBx0IJ6PB6WjgQgJqIpdBz5GHkFDE1awmHCkIoOGDRC46TW48ynjLuCRj0IUrLOBBJTY4Re2bqXxLDTAmDhbGWgoCHiKKbwmOpqL1U6Xaw/rXZw/+03xPwIPnA86bIDsXPk7hgLKQwLRXS6cWNh7WXMnXa1UsobaylgThAUzFLp6ORG3cCQ==

Figure 11-(C) Cipher text Using Traditional Blowfish

encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as cipher text. Ideally, only authorized parties can decipher a cipher text back to plaintext and access the original information

Figure 11- (D) decrypted text information.

DOI : 10.31695/IJERAT.2023.9.8.1

Histogram analysis can be used to evaluate the statistical analysis of both the plaintext and encrypted form. The histogram can provide information to find the secret key, the plaintext, or both. The histogram cannot be examined to learn anything about the plaintext if the histogram content is not evenly distributed across the scale. Figure 12 (A, B, and C) each show the histogram of the plaintext characters and the encrypted text separately. As is immediately apparent, the suggested method's histogram has a homogeneous cipher text, making the proposed system resistant to both frequency and histogram attacks.

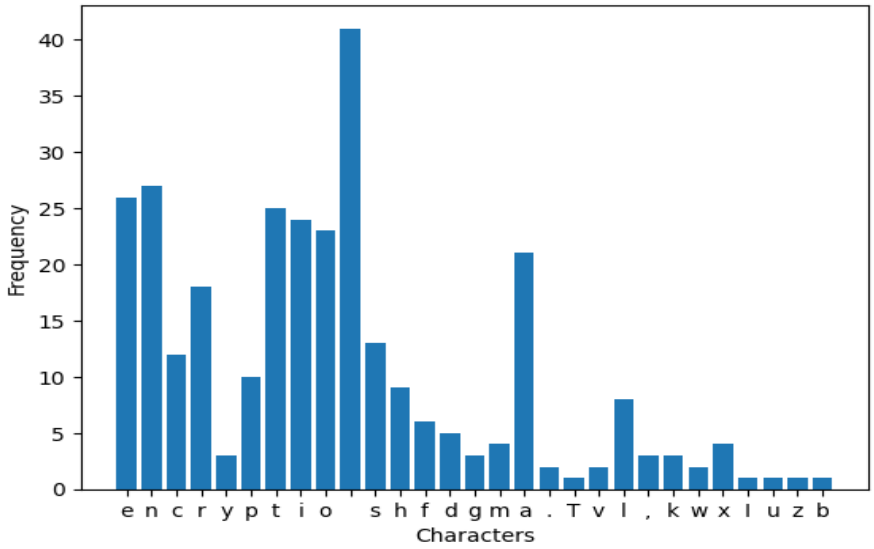

Figure 12(A) Plaintext Histogram.

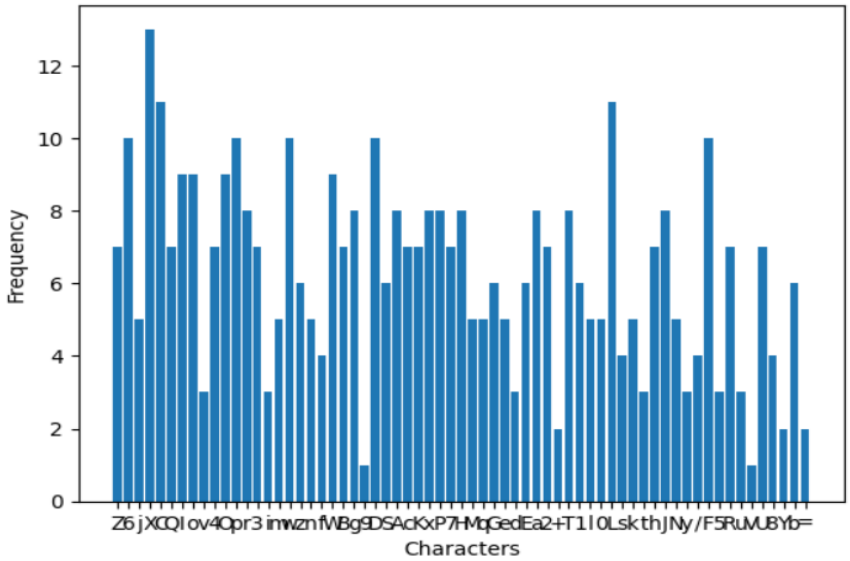

Figure 12(B)Cipher Text Histogram

DOI : 10.31695/IJERAT.2023.9.8.1

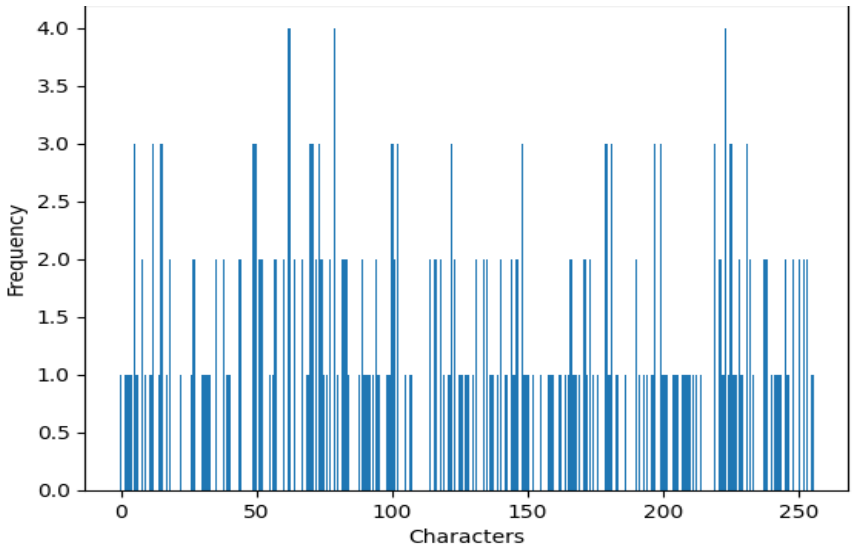

Figure 12(C) Cipher Text Using Traditional Blowfish

Information entropy for the suggested method is (7.229), whereas it was (5.886) for the conventional blowfish method based on the same text. A notion from information theory called information entropy measures how random or uncertain a batch of data is. More randomness and unpredictability are indicated by a higher entropy rating. The technique suggested to make it more difficult for an adversary to decipher, encryption aims for high unpredictability to reduce or eliminate dependency between the key and the cipher text.

6. CONCLUSION

In conclusion, this paper proposes utilizing LFSRs for key generation in the Blowfish algorithm, aiming to enhance its security and efficiency. Combining LFSR and DNA algorithm with Blowfish key generation has many advantages:

- Improved Randomness: LFSRs create fake random sequences that have good statistical qualities, making encryption keys stronger and harder to predict.
- The LFSR and DNA Algorithm-generated keys make it harder for hackers to guess or find the key, protecting against attacks that try to figure out the key by guessing or using known information.
- Efficiency: LFSR and DNA Algorithm have a simple way of working in computers and can quickly create keys, making them important for encrypting things in real-time or when needing to process a lot of information.
- By generating pseudorandom sequences using LFSRs, the randomness and unpredictability of encryption keys can be improved.

7. ACKNOWLEDGMENT

The author would like to thank Mustansiriyah University (www. uomustansiriyah.edu.iq) , Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics (https://iips.edu.iq/) , and the Ministry of Education - Gifted Care Authority (www.https: //epedu.gov.iq/) , Baghdad - Iraq for its support in the present this work.

DOI : 10.31695/IJERAT.2023.9.8.1

REFERENCES

[1] Abdullah, A. M., & Aziz, R. H. H. (2016, June). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm., International Journal of Computer Applications, Vol. 143 No.4 (pp. 11-17).

[2] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).

[3] Al-Shabi, M. A. (2019). A survey on symmetric and asymmetric cryptography algorithms in information security. International Journal of Scientific and Research Publications (IJSRP), 9(3), 576-589.

[4] Pianykh, O.S. (2012). DICOM Security. In: Digital Imaging and Communications in Medicine (DICOM). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-10850-1_11.

[5] Harba, E. S. I. (2017). Secure data encryption through a combination of AES, RSA and HMAC. Engineering, Technology & Applied Science Research, 7(4), 1781-1785.

[6] Canteaut, A. (2011). Linear Feedback Shift Register. In: van Tilborg, H.C.A., Jajodia, S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5906 5_357.

[7] Xiao, G., Lu, M., Qin, L. et al. New field of cryptography: DNA cryptography. CHINESE SCI BULL 51, 1413–1420 (2006). https://doi.org/10.1007/s11434-006-2012-5.

[8] Trein, J & As, Th & Schwarzbacher, & Hoppe, B.. (2023). The Development of a Binary Pseudo Random Number Generator with Controllable Output Density. 13-14.

[9]Bhowmik, A., Karforma, S. Linear feedback shift register and integer theory: a state-of-art approach in security issues over e-commerce. Electron Commer Res 22, 1–21 (2022). https://doi.org/10.1007/s10660-021 09477-w.

[10] Das, A., Sarma, S.K., Deka, S. (2021). Data Security with DNA Cryptography. In: Ao, SI., Gelman, L., Kim, H.K. (eds) Transactions on Engineering Technologies. Springer, Singapore. https://doi.org/10.1007/978- 981-15-8273-8_13.

[11] Anam, B., Sakib, K., Hossain, M. A., & Dahal, K. (2010). Review on the Advancements of DNA Cryptography. arXiv preprint arXiv:1010.0186.

[12] Rao, Shirole & K, Jyothi. (2022). Secret Key Generation using Genetic Algorithm for the Hybrid Blowfish Encryption and Substitution Ciphers. 1-5.

[13] Alabaichi, A., Ahmad, F., & Mahmod, R. (2013, September). Security analysis of blowfish algorithm. In 2013 Second International Conference on Informatics & Applications (ICIA) (pp. 12-18). IEEE.

[14] S. Manku and K. Vasanth, "Blowfish encryption algorithm forinformation security," ARPN Journal of Engineering and AppliedSciences, vol. 10, no. 10, pp. 4717–4719, 2015.

[15] Mushtaq, Muhammad & Jamel, Sapiee & Disina, Abdulkadir & Pindar, Zahraddeen & Shakir, Nur & Ma Deris, Mustafa. (2017). A Survey on the Cryptographic Encryption Algorithms. International Journal o Advanced Computer Science and Applications. 8. 333-344. 10.14569/IJACSA.2017.081141.

DOI : 10.31695/IJERAT.2023.9.8.1