ISSN 2278-3091
Volume 9, No.1.3, 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse7091.32020.pdf
https://doi.org/10.30534/ijatcse/2020/7091.32020

A New Design of Permutation Function Using Spiral Fibonacci in Block Cipher

Kamsiah Mohamed [1], Fakariah Hani Hj. Mohd Ali [2], Suriyani Ariffin [3]
[1] Department of Computing, Universiti Selangor, Malaysia, kamsh@unisel.edu.my
[2]Faculty of Computer Sciences and Mathematical Sciences, UiTM, Malaysia, fakariah@tmsk.uitm.edu.my
[3]Faculty of Computer Sciences and Mathematical Sciences, UiTM, Malaysia, suriyani@tmsk.uitm.edu.my

ABSTRACT

Cryptography is an important part of information security that covers the investigation of algorithms and protocols for secure information. With the advance of technology, a new design of cryptographic algorithm is required to fulfil the new system requirements. This paper emphasizes on the new design of permutation function for improving security in modern block ciphers. The Spiral Fibonacci method is designed to rearrange or permute inputs of bits through the substitution boxes. Then, the experiment was conducted between the Spiral Fibonacci in the proposed block cipher and the ShiftRow in the Advanced Encryption Standard cipher. The correlation coefficient technique is used to examine the diffusion property of the new design of permutation function. The results showed that the values of Spiral Fibonacci indicate low correlation between plaintext and ciphertext. Thus, the proposed block cipher improved diffusion property between the plaintext and ciphertext.

Key words : block cipher, cryptography, diffusion, Spiral Fibonacci

1. INTRODUCTION

Nowadays cryptography plays an important role in protecting the information, making it secure and immune to attacks. Cryptography helps to send a message from a sender to a receiver by providing confidentiality and integrity and it is carried out in two different techniques – encryption and decryption [1]. Encryption technique can be accomplished by encrypting messages to make them unreadable when transmitting the message across any vulnerable network. Encryption can be divided into two types of key that are symmetric and asymmetric key algorithm. A symmetric or private key algorithm is effective at transforming a lot of data and computational less intensive than asymmetric key algorithm [2]. A symmetric key algorithm consists of traditional cipher and modern cipher. Traditional cipher is designed based on the substitution cipher and the transposition cipher such as the Caesar cipher, the Rail Fence cipher and the Playfair cipher. However, secure symmetric key encryption is related to the modern block cipher. A block cipher is known as a deterministic algorithm with fixed groups of bits, called blocks with unchanging transformation [3]. In a modern block cipher, a key only allows partial mapping of possible inputs to possible outputs [4]. The PRESENT cipher, Data Encryption Standard (DES) and Advanced Encryption Standard (AES), for example, operates on the basis of the substitution key. Therefore, a modern block cipher is built from a combination of substitution function and permutation function. This paper focuses on permutation function in a block cipher. The permutation function process is required to rearrange the bits obtained from the substitution function. However, common permutation functions are used in block ciphers are circular shift and swap. A study by [5] stated that a good cipher should behave like a random permutation. The byte permutation is more complicated as it covers the entire block [6][7]. Hence, a secure permutation is very significant to make an attacker difficult to determine the structure of any other elements. Therefore, this paper proposes enhancement from current cryptography design of permutation function based on Spiral Fibonacci to improve security of block cipher. In addition, the Spiral Fibonacci is considered flexible because it can be seen in clockwise direction or counter clockwise direction. For example, the number of clockwise spirals on the face of a sunflower will always be a Fibonacci sequence. Besides, the greatness of the creator of nature can be felt from the arrangement of leaves to plants to the human body. Therefore, this paper found that the concept of Spiral Fibonacci can be applied in permutation function to improve the cryptographic algorithm. The paper is structured according to the following. An overview of the permutation function is presented in Section 2. Next, Section 3 explains the Spiral Fibonacci in nature and the proposed design of permutation function. Section 4 presents obtained results and analysis of permutation function. The paper concludes in Section 5.

2. OVERVIEW OF PERMUTATION FUNCTION

A permutation can be defined as *[n]* is a one-to-one function between *[n]* and *[n]*, where S_n is the set of all *[n]* permutations [8]. Permutation function is a technique used to specify a diffusion property [9]. In addition, diffusion can be accomplished by repeatedly applying permutation of data. A study by [10] found that the 128-bit software block cipher DSDP had eight key-dependent permutation boxes designed to avoid differential and linear cryptanalysis. Then, [11] suggested bidirectional diffusion and implementation of a plaintext orbit turbulence mechanism to enhance the diffusion technique. Another study by [12] proposed permutation function based on the Cube and Slide to improve the 3D-AES block cipher. A study by [13] proposed the permutation shuffling technique to increase the diffusion capability of the cipher. Then, [14] introduced a dynamic method for permutation in the Serpent block cipher algorithm. The result showed that the dynamic method has good randomness compared with a classical Serpent algorithm. Thus, it can reduce the number of round and time usage. However, the dynamic method has sensitivity to any change in the key since it uses chaotic map in the key round generation. Therefore, many techniques were proposed to increase the security of the permutation function in order resist from cryptanalysis attack.

2.1 ShiftRow in AES Permutation Function

The Rijndael algorithm was chosen as the latest standard which was named as the AES by the National Institute of Standards and Technology (NIST) in 2001. Since then, AES has become the most widely used block ciphers in cryptographic applications. However, cryptanalysis of the strength of Rijndael has not stopped after the announcement and official publication of the AES. The security of AES depends on the substitution and permutation function. For substitution function, AES used substitution transformation to substitute a byte. The SubByte transformation is a single nonlinear transformation where each input byte is replaced by the output of the "S-box" function being applied to byte. In SubByte transformation, each byte (8-bit) of a data block is converted to another block using S-box. For a permutation function, the State is arranged in an array and then performs a circular shift for each row. The ShiftRow transformation is a linear process of diffusion on a row. In ShiftRow, the State's rows are rotated cyclically over various offsets [15]. It permutes the bytes and to the left is the shift. For the State's first row is not shifted, the second row is one byte shifted, the third row is two bytes shifted; and the last row is three bytes shifted to the left. The State array process is shown in Fig. 1.

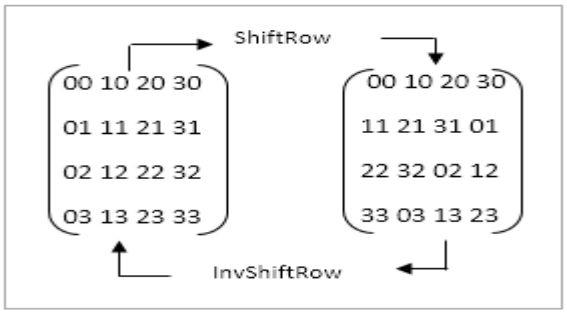

Figure 1: ShiftRow and InvShiftRow Transformation

The ShiftRow transformation is designed based on the simple structure. However, a study by [16] found that no structured approach for analyzing the influence of the ShiftRow. In another study, [17] improved the transformation of ShiftRow by the use of array shift mapping irrespective of movement and rotation of each element in order. Therefore, improved ShiftRow in AES block cipher will increase performance of an algorithm.

3. SPIRAL FIBONACCI IN NATURE

The Fibonacci sequence's or series mathematical ideas have long been admired for their simplicity and beauty, such as the golden ratio, spirals, and self-like curves, but no-one can really understand why they resonate so intensely in the art and nature world. In 1202, Leonardo of Pisa [18] is an Italian mathematician who discovered the first recursive number of sequences involving the growth of a hypothetical rabbit population based on idealized assumptions. After each month he found that the number of pairs of rabbits increased from 1 to 2, 3, 5, 8, 13 etc. Thus, he showed that the series progressed by adding the two previous numbers (in mathematical terms, $F_n = F_{n-1} + F_{n-2}$) , a series that in principle could continue indefinitely. Then, in 1875[19] a mathematical demonstration was presented that the helical arrangement of the leaves on a branch in Fibonacci proportions was an effective way of collecting a maximum amount of sunlight with a few leaves. After that, scientists have successfully established Fibonacci spiral patterns in the laboratory and found that an elastically incoherent bi-layer structure. scientists have successfully established Fibonacci spiral patterns in the laboratory and found that an elastically incoherent bi-layer structure may trigger Fibonacci pattern spirals. For example, the Fibonacci spirals were found to be the least elastic energy configuration [20]. The pattern occurs in plants, shell shape and sea shell. A nautilus shell cross-section shows the spiral curve of the shell, and the inner chambers that the animal uses contribute to growing it. For instance, an ear cochlea is a spiral of the Fibonacci, like the umbilical cord spiral. This spiral follows a precise mathematical pattern based on the Fibonacci sequences as shown in Figure 2.

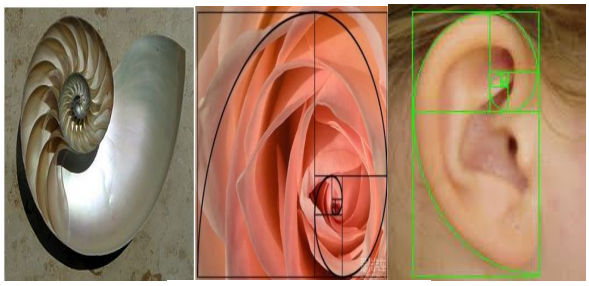

Figure 2: Spiral Fibonacci

In 2011, a study by [21] found that the structure of the coronary arterial tree follows a Fibonacci distribution. They stated that the Fibonacci number theory is useful in developing an innovative bio mathematical model of the coronary system as well as new techniques in cardiac arterial. Then, in 2013 [22] reported that a new phenomenon occurs within the cardiac cycle of the human heart beat where the golden ratio of Phi (φ) 1.618 occurs. The time intervals for the systolic and diastolic phases are considered to vary with the measurement process. Nevertheless, [23] found that the lack of statistical and well-documented empirical evidence makes an accurate description of the golden spiral to be difficult to assess. In addition, the Fibonacci sequence is closely associated with the unique proportional properties known as the golden section. Golden section preferences are seen as an important part of human appearance and beauty and as a result of the exceptional proportions of growth patterns in living things like animals and plants [24]. The Fibonacci sequence also can be seen in the deoxyribonucleic acid (DNA). A study by [25] has shown that the order of DNA replication in cells is also based on the Fibonacci series. Then, [26] found that the nucleic acid bases organization in the DNA sequence has an order (called the DNA SUPRA code) that fits the Fibonacci sequence. Spiral Fibonacci's rule is special and fascinating, as it can be found in many living things around the world. Therefore, a beauty of Spiral Fibonacci in nature inspired the study to enhancement from current cryptography design permutation function.

3.1 Proposed Spiral Fibonacci Design in Permutation Function

The permutation function should ideally satisfy the three goals which are being general-purpose and flexible, be simple to enforce and have good cryptographic properties [27]. The study found that Spiral Fibonacci's characteristics fulfilled the three goals proposed above. The Spiral Fibonacci is a set of connected quarter-circles drawn within an array of squares with Fibonacci dimensional sequence as shown in Figure 3.

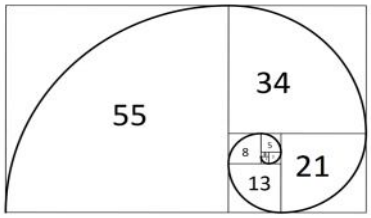

Figure 3: Spiral Fibonacci concept

The permutation function process requires rearranging the bits obtained from the substitution function. In the permutation function, the initial data which is the block matrix in sub byte will be diffused based on the logarithmic *spiral* or *SpiralFibonacci*. In the *SpiralFibonacci()* transformation, the bytes is permutated based on the spiral matrix by different offsets in a State. Figure 4 shows the Spiral Fibonacci algorithm is performed based on the anticlockwise rotation. It starts with the 4x4 square matrix consisting of $\mathbf{A_{2,1}}$, $\mathbf{A_{2,2}}$, $\mathbf{A_{1,2}}$, $\mathbf{A_{1,1}}$ coordinate becomes $\mathbf{A'_{0,0}}$,$\mathbf{A'_{1,0}}$, $\mathbf{A'_{2,0}}$, $\mathbf{A'_{3,0}}$. The elements will be accessed as follows: **A[r][c]**, where 'r' will go from **0** to **3** (A[ ][ ] is the array). The above processes will repeat till the matrix filled in 'n*n' values.

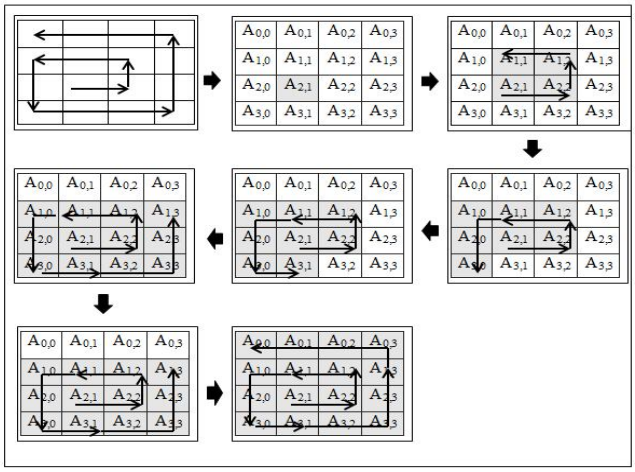

Figure 4: Spiral Fibonacci in Permutation Function

Figure 5 shows the flow of an encryption algorithm for the proposed block cipher. For the encryption algorithm, the user enters the input data which is called as plaintext. Then, plaintext is XORed with the cipher key. Thus, each element in a State was substituted byte by byte in the S-box which is called SubByte. The S-box used in this paper is based on [28]. After all elements were substituted, the elements are permute based on the Spiral Fibonacci function. Then, the elements are transformed into a MixColumn operation similar to the AES concept. After that, the elements of the MixColumn are XORed with the AddRoundKey to produce the ciphertext.

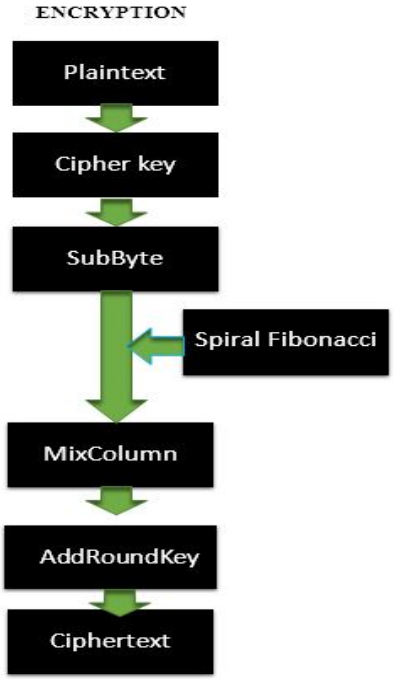

Figure 5: Encryption in Proposed Block Cipher

4. ANALYSIS OF PERMUTATION FUNCTION

The correlation coefficient technique is used in this paper to test the diffusion property of the new permutation function design. Correlation is a non-deterministic relationship that investigates the degree of linear correlation between two variables. It denotes the degree to be independent for evaluating the linear combinations of input bits and output bits. According to [29] a good cryptographic algorithm would make the correlation coefficient between plaintext and ciphertext is very low. The experiment was performed only on the permutation function between the Spiral Fibonacci function and the ShiftRow function in the AES block cipher. The objective is to recognize low linear relationship between the two variables in block ciphers which are plaintext and ciphertext. The experiment examined the correlation coefficient for 128 sequences of ShiftRow (AES block cipher) and Spiral Fibonacci (the proposed block cipher) is recorded. The results showed that none of Spiral Fibonacci's value is close to + 1 or -1, which implies a weak non-linear positive (or negative) relation. It means that low linear relationships exist between the plaintext and the ciphertext for Spiral Fibonacci. Table 1 shows the value of correlation coefficient. The result of correlation coefficient between the ShiftRow and the Spiral Fibonacci is shown in Table 2.

Table 1: Value of Correlation Coefficient

Value	Meaning
0-0.09	No relationship
0.1-0.3	Low relationship
0.3-0.5	Medium relationship
0.5-1.0	Strong relationship

Table 2: Correlation Coefficient Result between ShiftRow and Spiral Fibonacci

#Seq	ShiftRow	SpiralFibonacci	#Seq	ShiftRow	Spiral Fibonacci
1	0.2811	0.0567	73	0.2118	0.1529
2	0.0789	0.1248	74	0.125	0.2063
3	-0.0315	0.0291	75	0.1429	0.1867
4	0.2667	0.0984	76	0.0882	0.0227
5	0.0882	0.1803	77	0.2322	0.1529
6	0.2805	-0.0186	78	0.3118	0.0935
7	0.2784	-0.1005	79	0.1873	0.1544
8	0.0464	0.0623	80	0.1529	0.1429
9	0.1873	0.0588	81	0.3725	0.2451
10	0.3083	0.217	82	0.1903	0.0882
11	0.3712	0.0828	83	0.3358	0.0623
12	0.234	-0.0022	84	-0.1611	0.0542
13	0.1148	0.1867	85	0.1843	-0.0376
14	0.2749	0.1992	86	0.218	0.0333
15	0.2725	0.0616	87	0.3725	0.0918
16	0.214	0.2498	88	0.3943	-0.1275
17	0.2811	0.1231	89	0.3042	0.0857
18	1.0	-0.001	90	0.2188	0.2188
19	0.217	0.156	91	0.2093	0.2811
20	0.1248	0.1554	92	0.2797	-0.0121
21	0.4039	0.0156	93	0.2454	0.1231
22	0.2409	0.1873	94	0.218	0.2498
23	0.3431	0.0275	95	0.2312	0.1216
24	0.4999	0.1364	96	0.3305	0.0291
25	0.2667	0.0935	97	0.2483	-0.0121
26	0.4682	0.2498	98	0.2177	-0.0521
27	0.2483	0.146	99	0.2797	0.1216
28	0.2784	0.1144	100	0.2749	0.0616
29	0.1144	0.0	101	0.2498	0.0511
30	0.3276	0.0929	102	0.1903	0.3624
31	0.3423	0.0935	103	0.3042	0.0567
32	0.0604	0.1867	104	0.3522	0.1511
33	0.4353	0.1875	105	0.25	0.1255
34	0.4057	0.214	106	0.1488	0.1873
35	0.5624	0.1867	107	0.0625	-0.0315
36	0.1248	0.2749	108	0.3123	0.0755
37	0.2797	-0.0741	109	0.2471	0.0918
38	0.0918	0.1241	110	0.2768	0.217
39	0.1875	0.0313	111	0.2483	0.1196
40	0.2811	-0.0304	112	0.2454	0.146
41	0.0253	0.1511	113	0.2433	0.311
42	0.214	0.0588	114	0.3118	0.1529
43	0.1579	0.1843	115	0.9218	0.1867
44	0.1216	0.1511	116	0.2157	0.1488
45	0.4061	0.0542	117	0.1248	0.1231
46	0.2813	0.1544	118	0.319	0.1248
47	0.1511	0.0542	119	0.1544	0.1777
48	0.1138	0.0275	120	0.311	-0.0353
49	0.4688	0.1488	121	0.3379	0.1241
50	0.2797	0.0567	122	0.156	0.1544
51	0.3748	0.2186	107	0.0625	-0.0315
52	0.3522	0.0588	108	0.3123	0.0755
53	0.3333	0.0929	109	0.2471	0.0918

54	0.2483	0.3125	110	0.2768	0.217
55	0.3695	0.0253	111	0.2483	0.1196
56	0.2483	0.1544	112	0.2454	0.146
57	0.3305	0.2454	113	0.2433	0.311
58	0.25	0.0902	114	0.3118	0.1529
59	0.2409	0.1248	115	0.9218	0.1867
60	0.2093	0.0291	116	0.2157	0.1488
61	0.156	0.1857	117	0.1248	0.1231
62	0.3358	0.156	118	0.319	0.1248
63	0.2768	0.1231	119	0.1544	0.1777
64	0.2797	0.1196	120	0.311	-0.0353
65	0.3423	0.1554	121	0.3379	0.1241
66	0.2186	0.2186	122	0.156	0.1544
67	0.203	0.031	123	0.3305	0.1196
68	0.2805	0.1467	124	0.3123	0.1216
69	0.2483	0.1392	125	0.2797	0.0511
70	0.0567	-0.001	126	0.25	0.1711
71	1.0	0.1511	127	0.1248	0.1857
72	0.3123	0.214	128	0.1875	0.25

Figure 6 shows that the correlation coefficient values of Spiral Fibonacci are near to 0, which means that low correlation coefficient exist between plaintext and ciphertext. In #Seq 29, the minimum value is 0.0 and in #Seq 102 the maximum value is 0.3624. In ShiftRow function, the result indicates that 1.6 % correlation values is +1, representing a strong positive linear relationship. Nevertheless, the percentage of the value between 0.5 to 1.0 is considered very small. Therefore, AES block cipher resists from linear cryptanalysis attack. From the results, it can be inferred that there is an improved performance of the proposed block cipher algorithm based on diffusion property. Thus, low correlation exists between plaintext and ciphertext. It is essential to make it harder for an attacker to attack the block cipher. This is because it is difficult for an attacker to recognize input and output if the correlation is small. As a result, the Spiral Fibonacci feature in the proposed block cipher can withstand linear cryptanalysis attack.

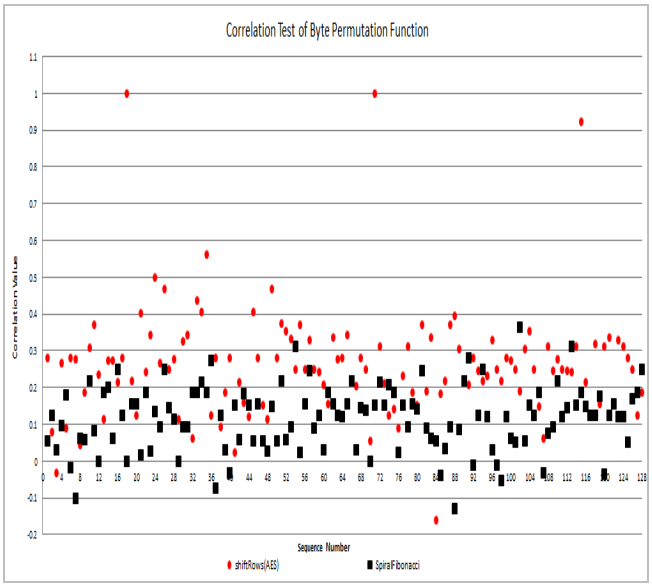

Figure 6: Result of ShiftRow and Spiral Fibonacci

5. CONCLUSION

This paper proposes an enhancement from current cryptography design of permutation function to improve the security of block cipher. Permutation function is an important part in a block cipher to rearrange the bits obtained from the substitution function. Therefore, the Spiral Fibonacci technique is designed to be used in the permutation function. The comparison was made between the ShiftRow and the Spiral Fibonacci. The correlation coefficient technique examines the cryptographic properties of the permutation function based on Spiral Fibonacci. The results showed that the range of values for the Spiral Fibonacci correlation coefficient is 0.0 to 0.3. A value of zero means that the two variables does not have a relationship. It indicates that there is no linear relation or very weak linear relationship between the variables. Therefore, it is difficult for the attacker to deduce the relation between plaintext and ciphertext in a block cipher.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the research support provided by the Universiti Teknologi MARA (UiTM).

REFERENCES

1. K. L. Sailaja, R. P. Srinivasa, P. K. Ramesh. **A new circle based symmetric key encryption technique for text data.** *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 8, pp. 2573-2576, September - October 2019. https://doi.org/10.30534/ijatcse/2019/106852019
2. M. Ghanti and S. K. Bandyopadhyay. **A proposed method for cryptography using random key and rotation of text.** *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 6, pp. 18-22, March-April 2017.
3. H. Cheng and Q. Ding. **Overview of the block cipher.** *Second International Conference on Instrumentation, Measurement, Computer, Communication and Control* (pp. 1628-1631). IEEE.2012.
4. A. Forouzan. **Cryptography and Network Security Forouzan**, *Tata McGraw Hill Publishing Company Limited*. 2008.
5. T. Tiessen, C. Rechberger and L. R. Knudsen. **Secure Block Ciphers-Cryptanalysis and Design**. 2017.
6. S. Ariffin, R. Mahmod, A. Jaafar, M. Rezal, M., and K. Ariffin. **An immune system-inspired byte permutation function to improve confusion performance of round transformation in symmetric encryption scheme.** *In Computer Science and its Applications* pp. 339-351. 2012. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-5699-1_34
7. N. H. Zakaria. **A Block Cipher Based On Genetic Algorithm Approach**, Ph.D. dissertation, Universiti Putra Malaysia, 2017.

8. E. Clark. **Elementary Abstract Algebra**. In: Elementary Abstract Algebra, Vol. 74, Department of Mathematics, University of South Florida, pp. 9-21, 2001.
9. A. Menezes, P. Oorschot, P. and S. **Vanstone, Handbook of Applied Cryptography**. CRC Press, Inc. 1997.
10. R. Zhang, and L. Chen. **A block cipher using key-dependent S-box and P-boxes.** IEEE International Symposium on Industrial Electronics, 1463–1468. 2008.
11. C. Fu, J.J. Chen, H. Zou, W. H. Meng,Y.F. Zhan and Y.W. Yu. **A chaos-based digital image encryption scheme with an improved diffusion strategy.** Optics Express, 20(3), 2363-2378.2012. https://doi.org/10.1364/OE.20.002363
12. S. Ariffin**. Secure block cipher inspired by the human immune system**. Ph.D. dissertation, Universiti Putra Malaysia, 2012.
13. A. Altaleb, M. S. Saeed, I. Hussain and M. Aslam**. An algorithm for the construction of substitution box for block ciphers based on projective general linear group.** *AIP Advances*, *7*(3), 035116. 2017.
14. I. A. Yousif. **Proposed A Permutation and Substitution Methods of Serpent Block Cipher.** *Ibn AL-Haitham Journal For Pure and Applied Science*, *32*(2), 131-144. 2019.
15. J. Daemen, and V. Rijmen. **AES proposal: Rijndael.** 1999.
16. C. Beierle, P., Jovanovic, M.M. Lauridsen, G. Leander, G. and C. Rechberger. **Analyzing permutations for AES-like ciphers: Understanding ShiftRows.** In *Cryptographers' Track at the RSA Conference* (pp. 37-58). Springer, Cham. 2015. https://doi.org/10.1007/978-3-319-16715-2_3
17. R. Riyaldhi, and A. Kurniawan. **Improvement of advanced encryption standard algorithm with shift row and S. box modification mapping in mix column.** *Procedia computer science*, *116*, 401-407. 2017.
18. Pomeraz, V. (1970). **Leonardo of Pisa. James Joyce Quarterly**, 7(2), 148-150.
19. J. Wiesner. **Bemerkungen u$ber Rationale und Irrationale Divergenzen**. Flora LVIII, 113–115, 139–143. 1875.
20. L. Chaorong, J. Ailing, and C. Zexian. **Stressed Fibonacci spiral patterns of definite chirality**. *Applied Physics Letters* 90, 164102 .2007.
21. H. Ashrafian and T. Athanasiou. **Fibonacci series and coronary anatomy.** Heart, Lung and Circulation, 20(7), pp.483-484. 2011.
22. G. Yetkin, N. Sivri, K. Yalta and E. Yetkin, E. **Golden Ratio Is Beating in Our Heart.** *International journal of cardiology*, 168(5), pp. 4926-4927.2013. https://doi.org/10.1016/j.ijcard.2013.07.090
23. D. Persaud and J. P. O'Leary**. Fibonacci Series, Golden Proportions, and the Human Biology**. 2015.
24. J. Kapusta. **The Square, the Circle and the Golden Proportion: A New Class of Geometrical Constructions**. WEB Journal FORMA 2004, Vol. 19, pp. 293-313.
25. D. S. Robertson. **Cellular Configuration of DNA And Cell Division. Medical Hypotheses,** 57(3), pp. 344-353.2001.
26. J. C. Perez. **Deciphering Hidden DNA Meta-Codes-The Great Unification & Master Code of Biology.** *Journal of Glycomics & Lipidomics*, 5(2), 1.2015.
27. R.B. Lee, Z. J. Shi, Y. L. Yin, R. L. Rivest, and M. J. Robshaw. **On permutation operations in cipher design.** In *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004.* (Vol. 2, pp. 569-577). IEEE. 2004.
28. K. Mohamed, F. H.H. M. Ali, S. Ariffin, S., N. H. Zakaria and M.N. M. Pauzi. **An Improved AES S-box Based on Fibonacci Numbers and Prime Factor**. *IJ Network Security, 20(6), 1206-1214. 2018.*
29. Z. H. A. O. Guosheng and W. A. N. G. Jian, **Security analysis and enhanced design of a dynamic block cipher.** *China Communications*, *13*(1), 150-160. 2016. https://doi.org/10.1109/CC.2016.7405712