Technium Vol. 4, No. 9 pp.89-101 (2022)
ISSN: 2668-778X
www.techniumscience.com

A Review of the Blowfish Algorithm Modifications in Terms of Execution Time and Security

Raghad Abdul Hadi Abdul Qader[1*], Auday H. Saeed AL-Wattar[2]

[1*,2] Department of Computer Sciences, College of Computer Sciences and Mathematics, University of Mosul, Mosul, IRAQ

[1*]Raghad.sulyman@ uomosul.edu.iq ,[2]Ahsa.alwattar@uomosul.edu.iq

Abstract. Data has become increasingly popular for advanced digital content transmission. Researchers are concerned about the protection of data. The transmission of digital data over a network has made multimedia data vulnerable to various threats, including unauthorized access and network hacking. As a result, the data must be protected with encryption methods based on symmetric encryption algorithms, which will ensure the data security. The Blowfish encryption algorithm is one of the most well-known cryptographic algorithms. However, each of the current algorithms has its own set of advantages and disadvantages. However, there are several drawbacks to using this algorithm, including complex computational operations, fixed (S-Box) and pattern issues, which can arise while dealing with more complex data, including texts. Many academics have sought to increase the algorithm's efficiency. The modifications to the Blowfish algorithms provided by researchers in prior works are summarized in this publication.

Keywords. Cryptography, Blowfish Algorithm, Symmetric Encryption, S-Box , Execution Time.

I. Introduction

Over the last few years, computer and internet technology have evolved at a breakneck rate. Many facets of everyday life, including commerce and education, now depend on data (such as texts).

The science of cryptography is commonly used for network security [1;2]. Cryptography is a technique for sending confidential data over

Technium Vol. 4, No. 9 pp.89-101 (2022)
ISSN: 2668-778X
www.techniumscience.com

vulnerable networks, such as the internet [3;4]. Confidentiality, integrity, authentication, and non-repudiation are essential aspects of cryptography [5;2]. The plaintext refers to the original message, while the ciphertext refers to the coded message. Encryption is translating plaintext to ciphertext; decryption is the process of recovering the plaintext from the ciphertext [6].The following are the two types of cryptographic algorithms: (i) Symmetric Key Cryptography, in which a single key is used to encrypt and decrypt data. (ii) Asymmetric Key Cryptography [7], in which one key is used for encryption and the other for decryption. Based on their operations, symmetric key cryptography is divided into two classes. [8]: A stream cipher encrypts a digital data stream bit by bit or byte by byte. (ii) Block Cipher: A block cipher reads a block of plaintext in its entirety and uses it to create a ciphertext block of equal length [6].

This paper shows modifications to the (BLOWFISH) algorithm performed by researchers in previous studies and compares them in terms of execution time and level security. The following is a breakdown of the paper's structure: Section II contains a summary of the Blowfish algorithm; Section III contains a review of the literature; Section IV contains a discussion; and Section V contains the conclusion.

II. Blowfish algorithm

Blowfish is a symmetric block cipher with a Feistel network that uses basic 16-time enciphering and deciphering functions. The Blowfish algorithm's strength comes from its subkey generation as well as its simple confusion and diffusion-based nature [9].

Technium Vol. 4, No. 9 pp.89-101 (2022)
ISSN: 2668-778X
www.techniumscience.com

The Blowfish cipher employs 18 (32-bit) permutation arrays, referred to as P-Boxes, and four (32-bit) substitution boxes, referred to as S-Boxes, each with 256 entries. The Blowfish cipher work is summarized in the following: It divides the (64-bit) block into two (32-bit) blocks, the left of which is XORed with the first Subarray P1 and the result is fed into a function called F-function. Substitution operations are carried out within the F-function, converting (32-bit) blocks into another (32-bit) block. As a result, the (32-bit) entries XORed with the right half, serving as the left half for the next round. Figures 1, 2 display the Feistel structure of the Blowfish algorithm with 16 rounds of encryption. The Blowfish of encryption is described in the algorithm (1):

Input: Plain text (64-bit) and from P1 to P18

Output: Result Ciphertext (64-bit)

Divide plain text into two sections, each with 32-bit XLeft and XRight values;

for i=1 to 16 do

XLeft = XLeft XOR Pi;

XRight = F(XLeft) XOR XRight;

XLeft and XRight should be swapped;

End

XRight = XRight XOR P17;

XLeft = XLeft XOR P18;

XLeft and XRight should be combined (ciphertext);

Algorithm (1) : Blowfish [9]

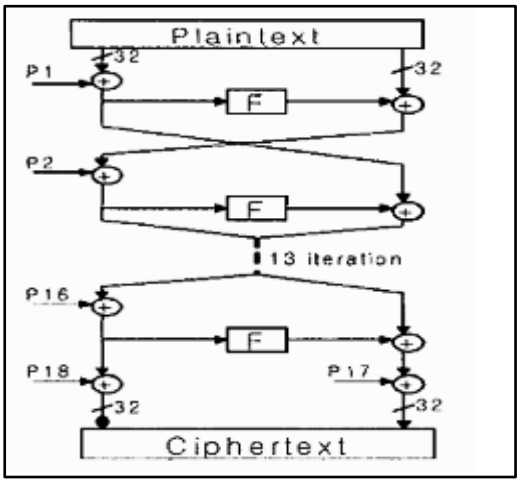

Figure 1:-Blowfish algorithm[9]

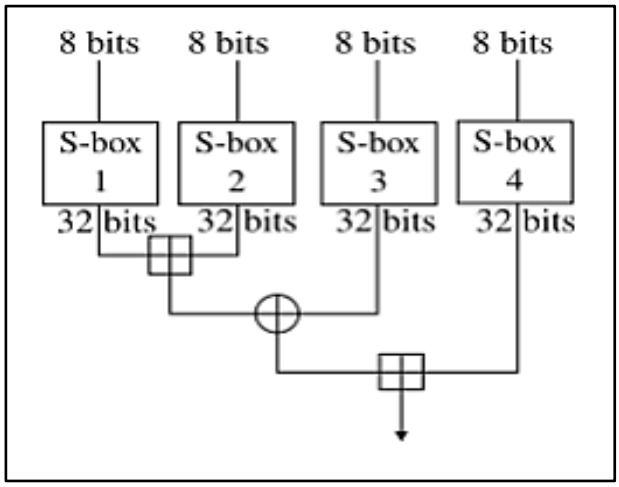

Figure 2:- S-Boxes (Blowfish) [9]

The Decrypting process uses the Blowfish algorithm, where the already encrypted message is decrypted using the same key used at the encryption time. The decrypting process is like encryption except that in decrypting, P1, P2, ..., P18 is used in adverse order [7].

III. Literature Reviews

For this research, we found, examined, and reviewed about 40 journal and conference papers on the blowfish algorithm's progress over the years. In this paper, we concentrate on papers published between 2011 and 2020. Based on this literature review, we were able to define relevant parameter in the Blowfish algorithm: execution time . Table 1 describes the cited publication and proposed methods for modifying the Blowfish algorithm for data such as texts. The modified Blowfish algorithm's measures of degree of security and execution time and the specification of the proposed techniques and data sizes were among the 20 studies highlighted. The time it takes to perform the encryption and decryption procedures determines the execution time. The results of the

original Blowfish algorithm are also compared to those of the modified Blowfish method in the table.

Table 1 : Includes a summary of the modifications made to the algorithm

	Proposed Methods/ Security/Data	Original Blowfish/ Execution Time		Modified Blowfish/ Execution Time	
		Encryption	Decryption	Encryption	Decryption
1	The Blowfish Algorithm may be enhanced by switching to a (128-bit) block cipher and constructing a new (S-Box) function to create (64-bit) data from a (8-bit) input./ powerful Security/(0-500)mb[14]	(13980- 45696) ns	(14752- 214371) ns	(144714- 315707) ns	(136424- 381983) ns
2	During encryption and decryption, reducing the number of rounds and increasing the block length with a fixed length with the addition of a transformation process on selected rounds. / Moderate Security/(17951-64682)kb for encryption and (47873-172505)kb for decryption [13]	(13.40-32.64) ms	(13.87-34.16) ms	(1.74-5.34) ms	(1.72-3.12) ms
3	That uses a 128-bit key and a 128-bit block size with a smaller number of (S-Boxes) for less memory use/High security/(10-1000)kb[15]	(51.10-3999.40) ms	(91.80-8070.90) ms	(96.40-5085.40) ms	(153.75-1018375) ms
4	The supported block size increased from 64 to 128 bits./ Increased security/ 128-bits, 256-bits, 512-bits, 1024-bits inputs respectively Using both the dynamic selection encryption methods well as randomly defined rounds for cipher function execution[16]	0.24 ms 0.26 ms 0.52 ms 0.95 ms	0.15 ms 0.26 ms 0.45 ms 0.87 ms	(0.12-0.14) ms (0.20-0.20) ms (0.38-0.37) ms (0.74-0.73) ms	(0.11-0.13) ms (0.20-0.19) ms (0.37-0.36) ms (0.69-0.69) ms
5	The number of Feistel rounds was reduced to 14, and the block size was increased to 128 bits with variable key	(13.3968-32.6392) ms	(13.8716- 34.1564) ms	(1.7448- 5.3418) ms	(1.7159- 3.1236) ms

	length. and shifting system on selected rounds /Moderate Security /(17951- 64682)kb for encryption and (47873-172505)kb for decryption[17]				
6	This study employed Fisher-Yates Shuffle (FYS), for permutation of (S-Box), and a modified (F-function) was used to improve the technique to handle this problem./ Moderate Security/ different file formats[12]	(2845.78-774037.50) ms	(233,714.41-4,538,285.29) ms	(2406.78-625193.74) ms	(10,641.78-3,435,559.24) ms
7	by combining the Blowfish and the Runge-Kutta (RK) method to improve the efficiency of the Blowfish cryptography algorithm by adding parallel processing techniques and making modifications to the Feistel (F) feature of Blowfish./high security/(50-208942)bytes[18]	(0.7586- 63.2736) ms	(0.7602-63.159) ms	(0.7932- 67.3147) ms	(0.7948- 67.3096) ms
8	By modifying the Feistel (F) function, MS-Blowfish combines Blowfish and the Mixed strategy(MS) to boost the efficiency of the Blowfish cryptography algorithm./more security/(50- 208942) mb [21]	(0.7586- 63.2736) ms	(0.7602- 63.159) ms	(1.0458- 87.9248) ms	(1.0482- 88.0193) ms
9	The use of two functions, F1 and F2, by decrease the rounds, make algorithm structure more complex for the attacker./ more security/(7-23591)kb[19]	-	-	(1.26- 3.37) sec	(1.22-4.41) sec
10	A new key and (S-Box) creation method was built based on the Self Synchronization Stream Cipher (SSS) algorithm, with the key generation process for this algorithm being updated to work with the Blowfish algorithm/ Moderate Security/(1-15)kb [11]	(7-63) sec	(7-63) sec	(16-72) sec	(16-72) sec
11	The original Blowfish method was modified by dividing the four (S-Boxes) into two (S-Boxes). / Moderate Security/(41-82)bytes[10]	(5.42- 6.53) ms	(0.82- 1.51) ms	(5.00- 6.36) ms	(0.85- 1.45) ms
12	A random number between 0 and 65535 can be generated,				

	then sets the flag's value to zero. Furthermore, finally, adjust the flag value to zero after converting the random number to 16-bit binary form and finding the positions with 0 inputs. The (F-function) does not work if the flag is 1, but it does work if the flag is 0./high security/(3-21)kb[20]	(3.54-28.28) ms	(3.53-27.99)ms	(1.77- 19.06) ms	(1.73- 17.99) ms

IV. Discussion

This paper presents a description of the alteration methods as well as a comparison of the results. The execution time and degree of security are the parameters that affect the algorithm's efficiency. The size of the data used in the proposed methods by researchers, on the other hand, varies significantly. As a result of these differences, comparing the proposed work in terms of output parameters is difficult.

A. Execution Time

The length of the encryption and decryption processes is referred to as execution time, and it is used to calculate the speed of the Blowfish algorithm. By comparing the processing times of the original Blowfish algorithm to those of the modified algorithm, the efficiency of the encryption and decryption processes can be compared.

Another new approach is introduced in [10]. The goal is to decrease the four S-Boxes in the original Blowfish method to two S-Boxes in order to improve performance and data security. When compared to original methods, the key benefit of modified Blowfish is that the execution time is lowered to 0.2 milliseconds. The authors of [11] created an (S-Box) creation method based on the Self Synchronization Stream Cipher (SSS) algorithm, with the key generation process modified to operate with the Blowfish algorithm.

Technium Vol. 4, No. 9 pp.89-101 (2022)
ISSN: 2668-778X
www.techniumscience.com

According to the suggested algorithm's time performance study, the improved method is quicker than the previous algorithm. The suggested technique outperforms the existing algorithm in terms of time, requiring just 272 iterations to create the subkeys compared to 521 iterations for the prior algorithm. The replacement and permutation of variables in the Blowfish algorithm's Substitution Box (S-Box) still has problems in [12], impacting the algorithm's encryption and decryption. To overcome this difficulty, researchers employed Fisher Yates Shuffle (FYS), for (S-Box) permutation and a modified (F-function), to accelerate the Blowfish method.

The Blowfish algorithm was modified in [13] by lowering the number of rounds and increasing block length with a fixed length during encryption and decryption, as well as implementing a transformation mechanism on chosen rounds to increase performance. The Blowfish algorithm has significantly reduced the execution time while maintaining the encryption file content's sophistication. In [14], the modified Blowfish method uses a lot of memory, which is one of its drawbacks. The memory capacity of the new Blowfish algorithm is two to three times that of the old Blowfish algorithm. The modified algorithm may demand more memory than the original algorithm. In [15], although the updated method is somewhat slower than Blowfish, this is due to the larger input block size.

The level of protection is a critical criterion for evaluating the Blowfish algorithm's efficiency. The majority of previous research has suggested methods for modifying the Blowfish algorithm's level of

security. There are essential differences in the degree of protection for the modified algorithms in the current analysis. The differences occur due to the various techniques suggested by researchers in these papers and the modified phase of the Blowfish algorithm. The highest levels of protection are demonstrated in [14,15,16,18,19, 20, and 21], which focused on the measures that influence the algorithm's security level. In [21] this work integrates Blowfish with the Mixed strategy (MS) to improve the efficiency of the Blowfish encryption method. results indicate that the Avalanche effect of modified Blowfish is (62.1ms) much better than Blowfish algorithm (57.1ms).So it is clear that modified Blowfish algorithm is very strong, secure and unbreakable than the Blowfish algorithm. In [18] by combining the Blowfish and the Runge-Kutta (RK) method to improve the efficiency of the Blowfish cryptography algorithm by adding parallel processing techniques and making modifications to the Feistel (F) feature of Blowfish. results indicate that the Avalanche effect of modified Blowfish is (60ms) much better than Blowfish algorithm (57ms). In [15] that uses a 128-bit key and a 128-bit block size with a smaller number of (S-Boxes) for less memory use. The Blowfish has a 47.14% avalanche, and the modified Blowfish is at 52.86%. The higher the avalanche percentage, the higher will be the security.

Vaibhav Poonia and Dr Narendra Singh Yadav [22] proposed another modification by combining the XOR and the original algorithm and adapting the (F-function) to different instances, and the original Blowfish algorithm was improved. After examining the Blowfish algorithm's (F-function) changes, we can see that the majority of the changes make the original Blowfish algorithm the most secure.

Other studies built dynamic 3D (S-Boxes), dynamic (P-Boxes), and F-functions to boost Blowfish key generation and reduce the time needed to generate sub keys [23]. The generation of elements achieved reduced time complexity in all studies involving the processing of sub keys, even though the methods used were completely different from the original algorithm. Some Blowfish modifications focused on changing the number of rounds to increase speed and, in turn, improve protection [24] [13] [17] [19]. Although a minimum of 5 rounds was stated, no minimum number was specified [25]. Also, modify was used to reduce the number of S-Boxes from four to two [10] [15]. Several researchers have tried to increase the block size of Blowfish to 128 bits [14] [15] [16] [17] [26] [27], but the results show a need for more memory but more security.

In [28], the authors present a new method for improving the Blowfish algorithm's efficiency, and this is achieved by developing a new structure for each of the original algorithm's 16 rounds. This paper suggests adding a key and replacing the old XOR with a new operation to increase the robustness of the Blowfish algorithm and make it more resistant to intruders. Multiple secrete keys are used in this structure to generate these multiple keys efficiently. The theory of Cellular Automata (CA) is applied. The suggested approach provides excellent encryption and is extremely resistant to efforts to crack the cryptography key. Another paper describes a new method for improving the security of the Blowfish algorithm by replacing the pre-defined XOR operation with a new operation called "#". Blowfish will perform better against any intrusion if we add a key and replace the old XOR with the new operation

"#." This advanced Blowfish algorithm is more energy-efficient and stable, using less battery power [29].

V. Conclusion

Between 2011 and 2020, researchers worldwide made new changes to the Blowfish algorithm, which are reviewed and discussed in this paper. Processing speed and execution time are among the performance parameter discussed in this paper. According to this analysis, the Blowfish algorithm still has space for improvement. As a result, research that proposes a novel approach to improving the efficiency of the Blowfish algorithm, which has high resistance to attacks, network hacking, and unauthorized access, is valuable.

Reference

[1] Sumedha Kaushik & Ankur Singhal "Network Security Using Cryptographic Techniques," International Journal of Advanced Research and Computer Science and Software Engineering (IJARCSSE), Volume 2, Issue 12, December 2012.

[2] Anand Kumar M and Dr. S. Karthikeyan, "Investigating the Efficiency of Blowfish and Rejindael Algorithms", International Journal of Computer Network and Information Security, pp. 22-28, 2012.

[3] Obaida Mohammad Awad Al-Hazaimeh, "Design of a New Block Cipher Algorithm", Network and Complex Systems, Vol. 3, No. 8, pp. 1-5, 2013.

[4] Ali M Alshahrani, "Different Data Block Size Using to Evaluate the Performance Between Different Symmetric Key Algorithms", International Journal of Computer Networks and Communications, Vol. 6, No. 2, pp. 89-97, 2014.

[5] K. Acharya, M. Sajwan, and S. Bhargaya, "Analysis of Cryptographic Algorithms for Network Security" International Journal of Computer Applications Technology and Research., vol. 3, issue no. 2, pp.130- 135–8887, 2013.

[6] William Stallings, "Cryptography and Network Security", Fifth Edition, Pearson Publication, Prentice hall, 2013.

[7] Landge, I.A.: "VHDL based Blowfish implementation for secured embedded system design", pp. 3–7, 2017.

[8] Manikandan G, Rajendran P, Chakarapani K, Krishnan G and Sundarganesh G, "A Modified Crypto Scheme for Enhancing Data Security", Journal of Theoretical and Applied Information Technology, Vol. 35, No.2, pp.149-154, 2012.

[9] Milind Mathur and Ayush Kesarwani, “Comparison Between DES, 3DES, RC2, RC6, BLOWFISH AND AES” Proceedings of National Conference on New Horizons in IT - NCNHIT 2013.

[10] Christina and Joe Irudayaraj, "Optimized Blowfish Encryption Technique" ; International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2014.

[11] Tayseer S. Atia; "Development Of A New Algorithm For Key And S-Box Generation In Blowfish Algorithm" ; Journal of Engineering Science and Technology Vol. 9, No. 4, 2014 .

[12] R. Corpuz, B. Gerardo, and R. Medina, “A modified approach of blowfish algorithm based on s-box permutation using shuffle algorithm”, pp. 140–145, 2018.

[13] Godfrey L. Dulla et al., "A unique message encryption technique based on enhanced blowfish algorithm" To cite this article, 2019 .

[14] Ashokkumar Kothandan, "Modified Blowfish Algorithm to Enhance its Performance and Security"; School of Computing National College of Ireland; 2020.

[15] Theda Flare G. Quilala , Ariel M. Sison and Ruji P. Medina, "Modified Blowfish Algorithm" , 2018.

[16] A. R. Reyes, E. Festijo, and R. Medina, “Blowfish-128: A modified blowfish algorithm that supports 128-bit block size,” 2018.

[17] Godfrey L. Dulla, Bobby D Gerardo, Ruji P. Medina, "An Enhanced Blowfish (eBf) Algorithm for Securing x64FileMessage Content";; Technological Institute of the Philippines; 2018.

[18] B. Shamina Ross, V. Josephraj, "Performance Enhancement of Blowfish Encryption Using RK-Blowfish Technique"; International Journal of Applied Engineering Research; ISSN 0973-4562 Volume 12, Number 20, 2017.

[19] Rohan Kumar, Rahul Thakkar and Manoj Kumar; " Simulated Analysis and Enhancement of Blowfish Algorithm" ; IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. II, 2015.

[20] Monika Agrawal and Pradeep Mishra, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm"; International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-6, August, 2012.

[21] Joseph Raj and Shamina Ross; "Enhancement Of Blowfish Encryption In Terms Of Security Using Mixed Strategy Technique"; 1Dept. of Computer Science, Kamaraj College, Thoothukudi-628003, INDIA 2Dept. of Computer Applications, Scott Christian College, Nagercoil-629001, INDIA; 2016

[22] Vaibhav Poonia and Dr. Narendra Singh Yadav; "Analysis of modified Blowfish Algorithm in different cases with various parameters"; International Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, ISSN 2091-2730, 2015.

[23] Ashwak Mahmood Alabaichi, "A Dynamic 3D S-Box based on Cylindrical Coordinate System for Blowfish Algorithm"; Indian Journal of Science and Technology, Vol 8(30), DOI: 10.17485/ijst/2015/v8i30/86800, November 2015

[24] P. Patel, R. Patel, and N. Patel, “Integrated ECC and Blowfish for Smartphone Security,” Procedia Comput. Sci., vol. 78, pp. 210–216, 2016.

[25] R. Patel and P. Kamboj, “Security Enhancement of Blowfish Block Cipher,” pp. 231–2382016.

[26] N. J. Oishi, A. Mahamud, and Asaduzzaman, “Short paper: enhancing Wi-Fi security using a hybrid algorithm of blowfish and RC6”; International Conference on Networking Systems and Security; pp. 1–5, 2016.

[27] A. M. Alabaichi, R. Mahmood, F. Ahmad, and M. S. Mechee, "Randomness Analysis on Blowfish Block Cipher Using ECB and CBC Modes"; J. Appl. Sci., vol. 13, no. 6, pp. 768–789, Jun. 2013.

[28] Afaf M. Ali Al-Neaimi and Rehab F. Hassan, "New Approach for Modifying Blowfish Algorithm by Using Multiple Keys" ; IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.3, March 2011.

[29] Gurjeevan Singh, Ashwani Kumar, K. S. Sandha, "A Study of New Trends in Blowfish Algorithm"; International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, 2011.