Ahmed Abd Ali Abdulkadhim *et al*, International Journal of Computer Science and Mobile Applications,
Vol.10 Issue. 8, August- 2022, pg. 42-50 **ISSN: 2321-8363**
Impact Factor: 6.308
(An Open Accessible, Fully Refereed and Peer Reviewed Journal)

Subject Review: Data Encryption using Block Cipher Algorithm

Ahmed Abd Ali Abdulkadhim[1]; Dena Nadir George[2]; Arkan Mohammed Radi[3]
[1] ahmed_198@uomustansiriyah.edu.iq
[2] dena.my@uomustansiriyah.edu.iq
[3] arkanrady20@gmail.com

DOI: 10.5281/zenodo.6992617

Abstract: ***The process of "Block ciphering" is basically responsible about encrypting data in blocks; this is done via deterministic and special algorithm with a symmetrical key. Such a cipher is able to encrypts blocks of (128 bit) with a programmed key length of about: 128, 192, or 256 bits. This paper analyses most of the known block cipher algorithms such as, H through two factors (Algorithm specifications, function and round).***
Keywords: Data encryption, block cipher, security algorithms

1. Introduction

In the encryption system, the message or information that is called as plain text is encrypted, using an encryption algorithm. This results in the formation of an encrypted text that cannot be read unless it is decrypted. Nowadays, in digital communications, information security is very important. The development of Internet and multimedia technology requires a secure algorithm to protect multimedia contents such as images, audio, video and others.

Sensitive information also requires protection from unauthorized persons such as medical and legal records, credit ratings, trademarks and voice mail. Encryption is a method of hiding information in digital communications that maintains the integrity, confidentiality and credibility of multimedia and text information [1]. Now our modern world is witnessing a development and flourishment in using the multimedia, software and also the Internet services. With increasing the distribution of the imaging information and data, security risks and threats also come into the picture. Block cipher is a method that uses an algorithm and a cipher key to encrypt data in blocks to produce a cipher text. The stream cipher type is able to, encrypt (1 bit) of data all at once. While in a block cipher type, the entire block is processed simultaneously. Most modern block ciphers are designed to encrypt data in blocks of fixed size either 64 or 128 bits. Paper analyses most of the known block cipher algorithms through following two factors

First factor: Algorithm specifications.
Second factor: function and round.

2. FIRST FACTOR A SPECIFICATIONS

2-1-DES

In this algorithm, the encryption is a (64 bits) length of a plain, simple text which can produce a (64 bits) length cipher text. In the decryption stage, it takes a block with a (64 bits) length and produces a (64 bits) length plaintext using the same key in both encryption and decryption. [2]

2-2-Triple DES

The name of this algorithm came as (triple DES), since its applying a (DES) encryption 3 times to a data block to encrypt and decrypt - encrypt. A 64-bit block is encrypted using a key of length 112 or 168 bits because the DES algorithm is vulnerable to brute force attacks and various cryptanalysis attacks. This necessitated the design of the triple DES algorithm to provide a new mechanism to protect against attacks and increase the size of the key. Without the need to design a new algorithm. [3]

2-3-Rc5

This algorithm is suitable for hardware and software implementation. This algorithm is characterized by block size parameters with an inconstant key and rounds number, and this gives an algorithm a flexibility and strong security. [4]

2-4-Camellia

Camellia algorithm is characterized by using a structure of (18-rounds) Feistel for keys with (128- bit), and another one with (24-rounds) Feistel for keys with (192- and 256-bits). This including extra inputs and outputs whitening's [5]

2-5-Skipjack:

This algorithm encodes a block of data with a length of 64 bits and also decrypts it to produce a text of 64 bits length The use of a key length of 80 bits. The difference involves the execution of 32 actions or the repetition of a complex non-linear function. Increasing the rounds number ensures a higher algorithm security. [6]

2-6-Twofish

It is a cipher block with symmetrical characteristics. It depends on the use of (128 bits) block's length with the ability to accept up to (256 bits) keys length. It can be as fast on (32-bits) as on (8-bits) CPUs such as the smart card and embedded chips, etc.., in addition to hardware. [7]

2-7-RC6

It is a parameterized RC5-like algorithm in which block and key sizes, and rounds number are vary, with a highest average key's size of about (2040 bits). The RC6 algorithms were arranged to match the requirements of the competition of Advanced Encryption Standard (AES). This algorithm has an appropriate (128 bits) size of

block and support key's size of about (128 and 192 and 256 bits). It offers an additional multiplicity which cannot be found in the RC5 algorithms [8].

2-8-blowfish

The blowfish algorithm is classified as a symmetric cipher block, it is used to encrypt data effectively. The key has a variable size ranging from about (32 to 448 bits). The algorithm of Blowfish is considered as a Feistel Network, which uses blocks of data with a length of (64 bits) and up to (448 bits) inconstant key's length is used. There are complicated stages that the algorithm goes through before the encryption is produced.[9]

3. SECOND FACTOR FUNCTION AND ROUND

3-1-DES

The DES algorithm uses 16 rounds and each round is a femal cipher, the important part or the heart of the algorithm is a function, and the function uses a 48-bit key This function consists of four sections: expand D-box, bleacher (add a switch), set of S-box and straight D-box as shown in the figure1.[10]

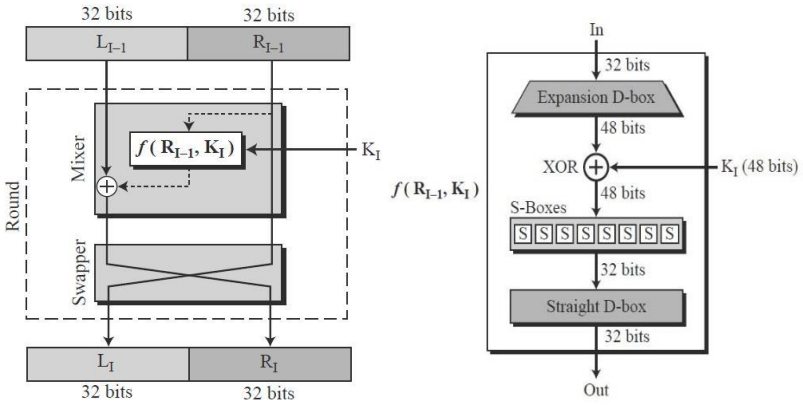

figure 1: illustrates the function and round of DES

3-2- **Triple DES**

A (56-bits) key is used in this algorithm, which isn't considered enough to encode important data. While, the triple-DES algorithm increases the size of the key by using an algorithm (3 times) with (3) various keys, until it reaches (168 bits). 3DES uses (3) DES keys (Key1, Key2, Key3) in the Encrypt-Decrypt- Encrypt (EDE) mode. It means that the K1 is encrypting a plain, simple text, followed by decrypting it with the K2, and finally, encryption is repeated with the K3. As seen in Figure 2.[12]

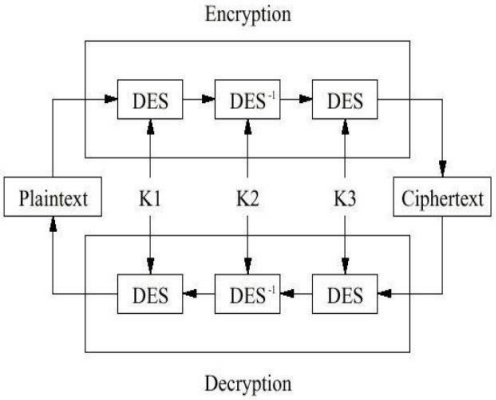

Figure 2: encryption and decryption of triple DES

3-3 RC5

The RC5 algorithm can be described as RC5-w/r/b Where w represents word's bits number and it's the parameter of RC5. The parameter's options to the algorithm are different. The number of its rounds is different with a repetitive structure The symbol r is the second parameter of the algorithm that represents the number of rounds. This algorithm uses a variable-length key, the key length denoted by b which is the third parameter of the algorithm. Where the number of r the number of rounds allowed is 0.1.....255, Where w allowed is 16, 32, and 64, but the standard value is 32 bits. Figure 3 shows structure of encryption RC5.[13]

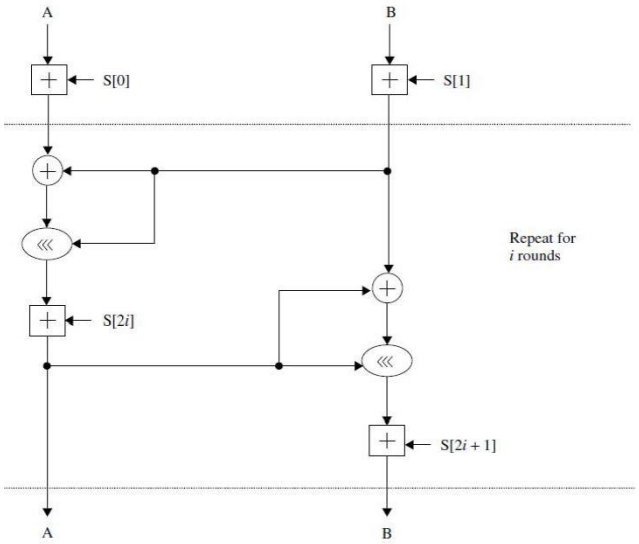

Figure 3: structure of encryption RC5

3-4-Camellia

This algorithm uses 18 rounds with a 128-bit key with a feistal structure and a feistal structure with 24 rounds for keys with (192 and 256-bits), with an extra I/O whitewashes and rational functions termed as tasks. FL and FL 1- functions are entered in every single round of the whole 6 rounds. A master table has (64-bits) sub keys kwt in which t=1;2;3;4 for I/O whitewash, ku in which u=1;2;r for round functions and klv in which v=1;2;;r=3-2 For FL and FL 1 functions of the secret K key. Figure 4 shows structure of encryption Camellia.[14]

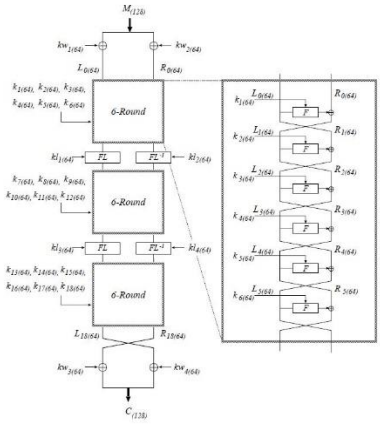

Figure 4: structure of encryption Camellia

3-5-Skipjack

This algorithm uses two different types of rounds, which makes the algorithm distinctly simple. Rounds are referred to as Round A and Round B. The encoding process is first applied by applying 8 rounds of A, then 8 rounds of B, and again 8 rounds of A and = 8 rounds of B. To 4 words with (16-bits). A non-linear switched switch can be applied by every round to 1 certain word from a block. Each cipher totally consists of (32) rounds. Figure 5 shows structure of encryption Skipjack .[15]

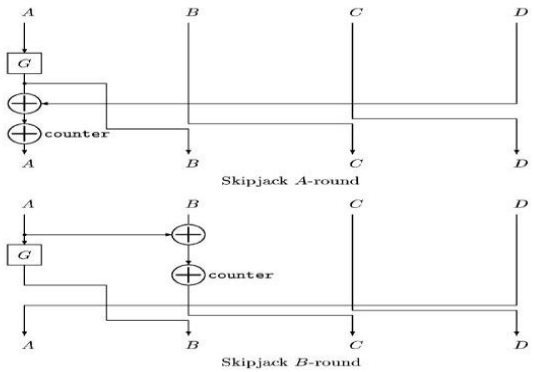

Figure 5: structure of encryption Skipjack

Ahmed Abd Ali Abdulkadhim *et al*, International Journal of Computer Science and Mobile Applications,
Vol.10 Issue. 8, August- 2022, pg. 42-50 **ISSN: 2321-8363**
Impact Factor: 6.308
(An Open Accessible, Fully Refereed and Peer Reviewed Journal)

3-6-Towfish algorithm

This 16-round algorithm uses a structure similar to a feistal and with an extra whitening for the inputs/outputs. An F function performs a switching depended mainly on a key of (64-bits) values where an operation is done with (3) arguments. (R0 and R1) represent the words of input, and (r) represents the number of the round that used to choose the suitable sub-keys. R0 is assigned to the g function, that produces T0, and R1 is rotated to the left (8 bits), then passed to the g function to produce T1, later T1 is combined with T0 in PHT. Figure 6 illustrates, Twofish is a Feistel network.[10]

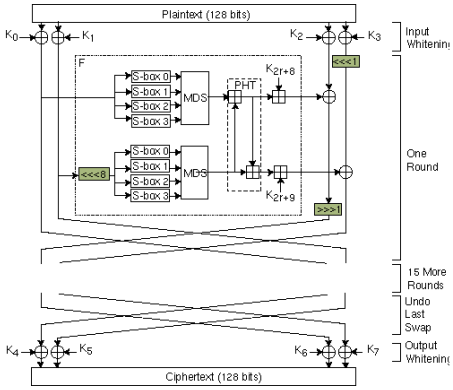

Figure 6:Twofish is a Feistel network

3-7- RC6

The RC6 algorithm is using a (128 bits) block's length and supporting key sizes of (128, 192 and 256 bits), respectively. It contains four registers of 32 bits length that help in the registration process [16], figure 7. The Feistel function of the RC6 algorithm.

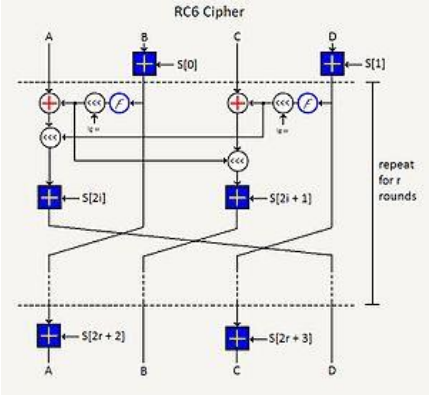

figure 7: The Feistel function of the RC6 algorithm.

3-8-blowfish

In this algorithm, the data is encrypted Via the Feistel network using 16 rounds and each round includes a switch dependent on the switch The operations used are XORs in addition to words with (32-bits). The opener expands (448 bits) as a maximum into the arrays of the sub key which are totaling (4168 bits).[11] figure 8. Shows Feistel network for blowfish

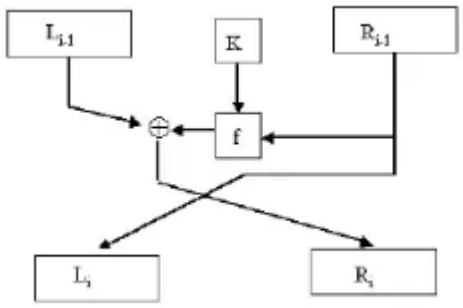

figure 8: Feistel network for blowfish

4. COMPARISON AMONG THE BLOCK CIPHER ALGORITHMS

Table 1 explain the comparison among block cipher algorithms.

Algorithm	Key length	Block size	Number Of round	Structure	Year	Ref.
DES	56 bits	64 bits	16	Balanced Feistel network	1977	[2]
3-DES	112 or 168 bits	64 bits	48 DES-equivalent rounds	Feistel network	1998	[3]
Blowfish	32–448 bits	64 bits	16	Feistel network	1993	[9]
Camellia	128, 192 or 256 bits	128 bits	18 or 24	Feistel network	2000	[5]

RC5	0 to 2040 bits	32, 64 or 128 bits (64 were suggested)	1-255	Feistel-like network	1994	[4]
RC6	128, 192, or 256 bits	128 bits	20	Feistel network	1998	[8]
Skipjack	80 bits	64 bits	32	unbalanced Feistel network	1980	[6]
Twofish	256	128	16	Feistel network	1998	[7]

5. Conclusion

In this paper, an analysis has been made of the majority of block cipher algorithms in terms of their specifications and security. An intensive analysis has been performed in this paper which has provided a detailed picture concerning the design of encryption algorithms. Where A block type ciphers are responsible about encrypting data in blocks, this is done via deterministic and special algorithm with a symmetrical key. In the current encryption type, a predeterminate key length of (128, 192, or 256 bits) was used along with a block cipher with a length of (128 bits). The advantages of block cipher are high spread and strong resistance without being detected. Although it has its advantages, it also has disadvantages, the speed of encryption and decryption is slow. Also, the problem of errors when one error occurs in one bit in the block leads to an error in the entire block, it can change the entire block

References

[1] Abdulkadhim, A. A. A., Jasim, Z. M., & Abood, Z. M. (2021). Security for Green Internet of Things Based On Cast Algorithm with Chaos. *Journal of Green Engineering*, *11*, 1-908.

[2] Bastanta, A., Nuryansyah, R., Nugroho, C. A., & Budiharto, W. (2021, October). Image data encryption using DES method. In 2021 1st International Conference on Computer Science and Artificial Intelligence (ICCSAI) (Vol. 1, pp. 130-135). IEEE.

[3] Rachmawati, D., Harahap, A. S., & Purba, R. N. (2018, November). A hybrid cryptosystem approach for data security by using triple DES algorithm and ElGamal algorithm. In *IOP Conference Series: Materials Science and Engineering* (Vol. 453, No. 1, p. 012018). IOP Publishing.

[4] Wai, H. Y., & Nwe, K. M. *Encryption and Decryption by using RC5 And DES Algorithms for Data*

File (Doctoral dissertation, MERAL Portal).

[5] Ci, C. W., Naziri, S. Z. M., Ismail, R. C., Hussin, R., Isa, M. N. M., & Basir, M. S. S. M. (2021, February). Crypto-core design using camellia cipher. In *Journal of Physics: Conference Series* (Vol. 1755, No. 1, p. 012019). IOP Publishing.

[6] Abduljabbar, H. A., Abdulkadhim, A. A. A., & Hashim, S. H. (2015). Adaptive Image Denoising Based on MACWM and NLEM Filters. , *16*(1), 53-64.

[7] Harahsheh, H., & Qatawneh, M. (2018). Performance evaluation of Twofish algorithm on IMAN1 supercomputer. *International Journal of Computer Applications*, *179*(50), 1-7.

[8] Paje, R. E. J., Sison, A. M., & Medina, R. P. (2019, January). Multidimensional key RC6 algorithm. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy* (pp. 33-38).

[9] Quilala, T. F. G., Sison, A. M., & Medina, R. P. (2018). Modified blowfish algorithm. *Indones. J. Electr. Eng. Comput. Sci*, *11*(3), 1027-1034.

[10] Hoomod, H. K. (2018, May). Fuzzy-cellular neural network for face recognition HCI Authentication. In *Journal of Physics: Conference Series* (Vol. 1003, No. 1, p. 012033). IOP Publishing.

[11] Hoomod, H. K., & Ali, A. A. (2019). New Technique for Internet of Things Security based on the Hybrid Mcrypton-Blowfish and Chaotic System. *Int. J. Sci. Res*, *8*(8), 650-652.

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

[13] Rivest, R. L. (1994, December). The RC5 encryption algorithm. In International Workshop on Fast Software Encryption (pp. 86-96). Springer, Berlin, Heidelberg.

[14] Mondal, T. K. (2011). Camellia. In Wild crop relatives: genomic and breeding resources (pp. 15-39). Springer, Berlin, Heidelberg.

[15] Wright, J. B. S., Naulaerts, J., & Henry, L. (2022). LIFE HISTORY OF SKIPJACK CAUGHT AROUND THE UK OVERSEAS TERRITORY OF ST HELENA, SOUTH ATLANTIC: REPORT FOR THE 2022 ICCAT SKIPJACK TUNA DATA PREPARATORY MEETING. Collect. Vol. Sci. Pap. ICCAT, 79(1), 111-117.

[16] Faragallah, O. S., Afifi, A., El-Shafai, W., El-Sayed, H. S., Alzain, M. A., Al-Amri, J. F., & Abd El-Samie, F. E. (2020). Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications. *IEEE Access*, *8*, 103200-103218.

Author Biography

[1]Ahmed Abd Ali, Master of Education, College of Education, Al-Mustansiriya University
[2]Dina Nader MA Iraq College of Education Department of Computer Science / Iraqi Computer Authority
[3]Arkan Muhammad, master's degree from Iraq / Department of Computers, College of Education / Al-Mustansiriya University