Asian Journal of Applied Science and Technology (AJAST)
Volume 6, Issue 1, Pages 89-98, January-March 2022

Comparative Study on DES and Triple DES Algorithms and Proposal of a New Algorithm Named Ternary DES for Digital Payments

Mounika Jammula

Assistant Professor, Department of Electronics and Communication Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana-500075, India. Email: jmounika ece@cbit.ac.in

DOI: http://doi.org/10.38177/ajast.2022.6111

Article Received: 29 October 2021 *Article Accepted: 31 January 2022* *Article Published: 28 February 2022*

ABSTRACT

Whenever new algorithms are designed intruders try to break the key with the help of attack models. No algorithm is perfect against all attacks. But DES irrespective of its small key size, it has been considered to be strong design cipher till today. Designers of DES guaranteed a security margin of 2 power 56. If any attack which is essentially better than 2 power 56 search then that considered to be attack. To crack DES attackers need to spend $ 220000 so that the key can be revealed in 56 hours. But for digital transactions if the key can expire for less than 5 minutes it's difficult to crack. If this is the case with DES then it will be much more difficult to break Triple DES, which uses 112 bits of key size. The problem with Triple DES is having more rounds, which takes more processing time and space. Not only cryptography, even Light Weight Cryptography needs low processing time and space. Hence a new algorithm named ternary DES is proposed which requires only 56-bit key and 16 rounds. Ternary DES has the advantage of DES with the same key space and number of rounds, and advantage of Triple DES with difficult to break. To propose new algorithms for solving security issues many constraints we need to take into account. With one algorithm we can solve one or a few issues but not all.

Keywords: *DES, S-Box, Triple DES, Ternary DES, Light weight cryptography.*

1. Introduction

Many existing cryptographic algorithms are used to protect digital transactions from threats. Day by day the demands for new innovative products and new IT products are increasing, and digital transactions is not an exception in the competition race. These banking transactions should be secured once algorithm is attacked many things going to be collapsed [1]. Hence before designing one should keep in mind algorithm requirements they are given by it should be well documented. Every step should be specified with mathematical or any other background. The algorithm must be available to all. Only key should be kept secret. We do not need to keep the algorithm secret, we need to keep only key secret.

The proposed algorithm designed in such a way that an opponent who knows the algorithm and has access to one or more cipher texts would be unable to decipher the text. Attacker aim may be destroying the communication between the sensors or stealing the data that is transferred between sensors or nodes. Attacker models will be difficult at different layers. Depending on the policies for various domains we use various security algorithms. Single algorithm doesn't work for all policies. If these policies changes attackers procedures also changes.

Suppose for military applications the data should not be revealed to cyber attackers. In these cases we should able to design a key which changes for every second. In this paper two algorithms DES and Triple DES are compared interms of time complexity [2], and new algorithm named Ternary DES is proposed.

2. DES Algorithm

Data encryption Standard (DES) is a block cipher algorithm proposed by the National Institute of Standards and Technol- ogy (NIST) in 1977 [3]. It follows the Fiestal cipher structure. In DES, plain text (PT) size is 64-bit, the

key size is 64-bit but sub key size is 48-bit, cipher text (CT) is 64-bit, the number of rounds required is 16 and each round requires one sub key which implies the total number of sub keys required is 16 [4].

2.1. Encryption

Fiestal structure consists, multiple rounds of processing plain text. In each round different key is used which is generated by using a key scheduling algorithm. In Fiestal structure if there are 'n' rounds then the same number keys are generated.As shown in fig.1. in this type of structure Ln-1 and Rn-1 blocks are shuffled to produce Rn and Ln blocks respectively with function 'f' and X-OR operation on Ln-1 block. Here L and R represent left and right side blocks with 32-bits each.

(1) Initial Permutation (IP): IP is the first step in DES algorithm which takes 64 bits plain text and modifies the bits shown in Table I.

(2) Inverse of IP (IP^{-1}): It is the last step in DES algorithm and inverse of first step in DES shown in Table II.

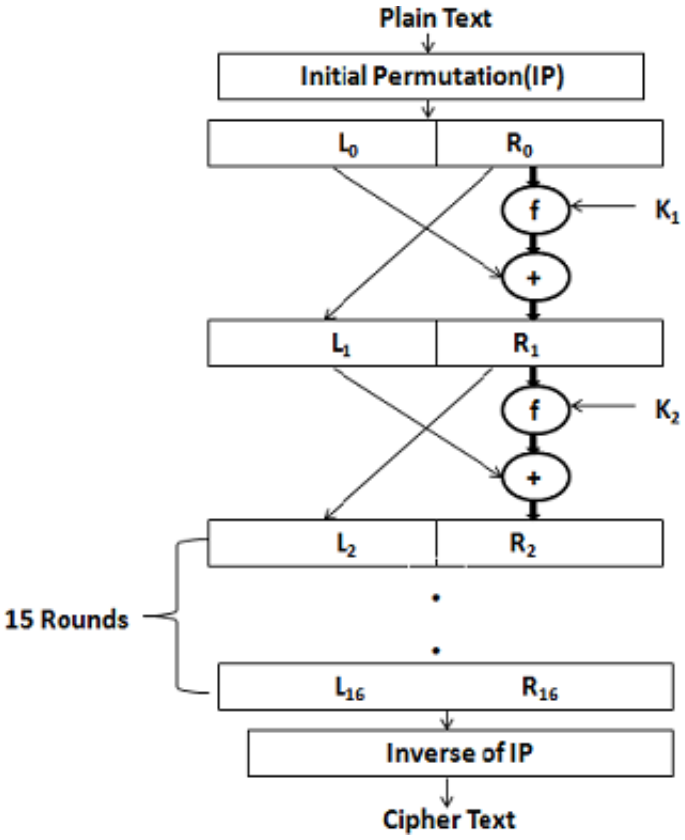

Fig.1. Block Diagram of DES

Table I

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1

59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Table II

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

(3) DES 'f' Function: Function 'f' takes right hand side (RHS) bits and key as inputs and generates 32 bits after permutation (P) as shown in fig.2. Each of B is 8-bits and is given as input to S-Box.

(a) Expansion permutation (E): It is applied on incoming RHS bits to expand from 32 to 48 bits shown in table III.

(b) *Permutation Function (P):* It is the last step in DES 'f' function generates 32 bit output shown in table IV.

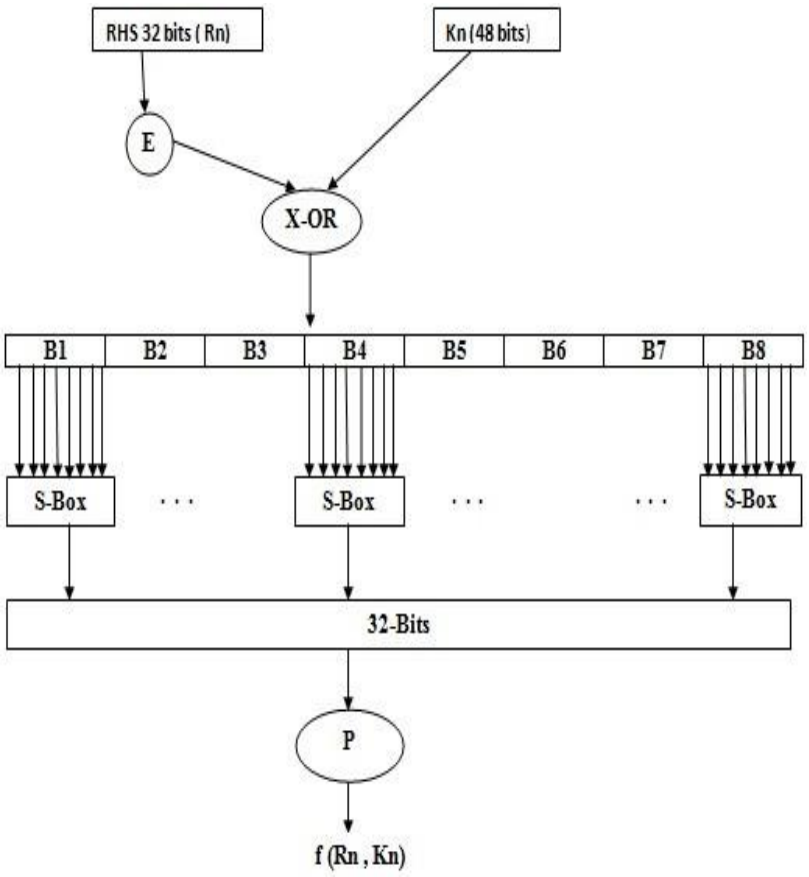

Fig.2. Block Diagram of DES 'f' function

Table III

32	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Table IV

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

(c) S-Box: Security in DES algorithm depends primarily on S-Box. Each S-box takes 6 bit input and produces 4 bit output. All S-Boxes put together produces 32-bit output as shown in fig2. In the fig3 X_0 and X_5 represents row number and X_1, X_2, X_3 and X_4 represents column number. There is no particular explanation how we get S-Boxes. If $X_5\ X_4\ X_3\ X_2\ X_1\ X_0 = (110011)_2$ then row number 3 and column number 9 is selected. If it is input to S_1 box then according to table of S_1, $(1011)_2$ in binary will be produced at the output.

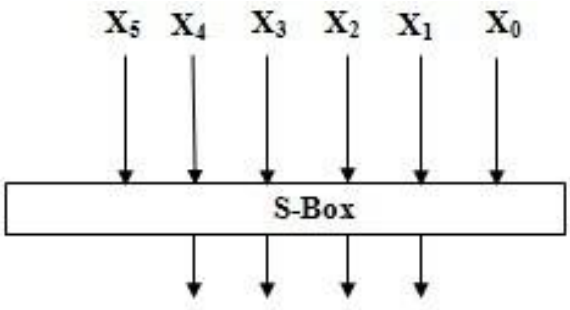

Fig.3. Block Diagram of SBox

Table V - S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Table VI - S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Table VII - S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

Table VIII - S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Table IX - S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Table X - S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

(4) Key Scheduling Algorithm: Normally key is 64-bits but in the generation multiples of 8, bits are not included. These multiples of 8 bits represents parity check bits for error detection hence they can be avoided.

Table XI - S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Table XII - S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

On remaining 56 bits following operations as shown in block diagram are performed which produces 48 bits at the output. Here in 1, 2, 9 and 16 rounds, left circular shift must be by only one bit and in other rounds shift must be by two bits.

2.2. Decryption

In decryption reverse process of encryption is performed.

$L_n = R_{n-1}$ (1)

$R_n = f(R_{n-1}, K_n) \oplus L_{n-1}$ (2)

Hence, in decryption it becomes,

$R_{n-1} = L_n$ (3)

$L_{n-1} = R_n \oplus f(L_n, K_n)$ (4)

In decryption process no need to perform f -1 operation. This is the beauty of Fiestal structure and its reduced burden on computational complexity.

2.3. Problems with DES

(i) Not well documented.

(ii) The values in S-box not mentioned properly.

(iii) Key size of DES is just 56-bits. Hence easily traced by generic attacks.

In laboratories we can break the DES less than a day by using large number of parallel computations using brute force attack. With one machine it is very difficult to break the key and we cannot do exhaustive search with single machine. Breaking the key takes many years. But if it takes one sec for encryption and decryption process,with 2^{32} processors we can break the key in 3 days.

Time complexity = 2^{56} X time required for DES encryption and decryption

But irrespective all these DES is very strong and good design of having security of 2 power 56 key searches.

3. Triple DES

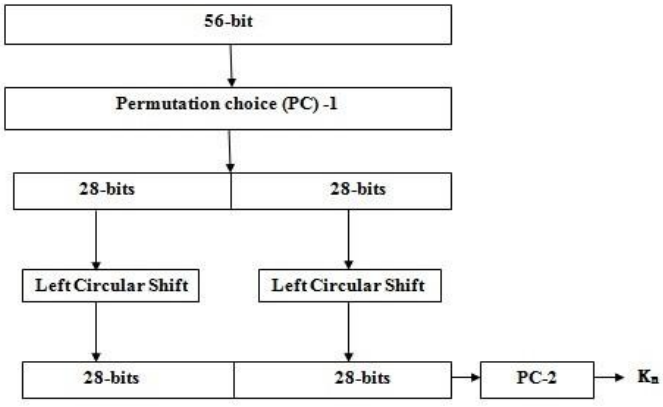

Fig.4. KEY Scheduling Algorithm

DES has broken because of its small key size. Replacement of DES is new block cipher named as triple DES [5]. In this triple DES key size can be 112 bits or 192 bits. If we use 112 bits the first key used for encryption is repeated otherwise not [6].

(1) Encryption: In this we use DES 3 times, Encryption – Decryption – Encryption. Hence the numbers of rounds in triple DES are 48. Plain text(X) is 64 bits, Key size is 112 bits and cipher text (Y) is 64 bits. Here k1 and K2 shown in Fig.5 are of 56 bits [7].

$$Y = EnK1(Dek2(Enk1(X))) \quad (5)$$

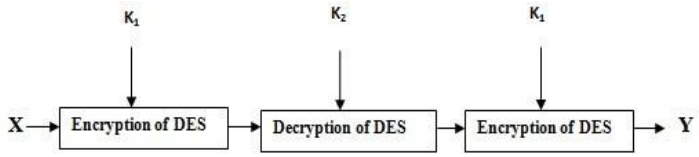

Fig.5. Block diagram of Triple DES encryption

(2) Decryption: As DES is already broken it's easy to mount attacks on triple DES with same kind of attack model on DES but with more time to crack. Decryption process is shown in Fig.6, having decryption - encryption - decryption processes, exactly reverse of encryption.

$$X = Dek1(Enk2(Dek3(Y))) \quad (6)$$

Time complexity = 2^{112} X time required for DES encryption and decryption=5.19 x 10^{33}

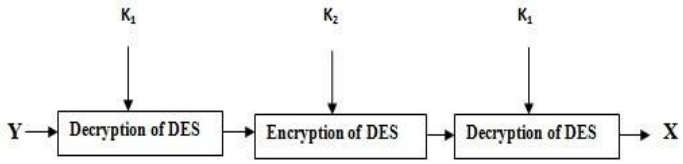

Fig.6. Block diagram of Triple DES decryption

4. Ternary DES

In ternary DES plain text, key and cipher text is of same size as that of DES but there is a change in S-Box size [8]. S-box size going to be 9 X 81. The values in S-Box range from 0 to 81. Hence we can encrypt more number of symbols [9].

Time complexity = 3^{56} X time required for DES encryption and decryption= 5.23 x 10^{26}

Here to crack algorithm it needs a more large number of parallel computations using brute force attack. Hence we can use these algorithms, having key space and number of rounds same as DES and time complexity same as Triple DES.

5. Experimental Results

DES was initially considered a very strong private encryp- tion algorithm, resistant to all known cryptographic attacks at that time it was invented but the key size used to encrypt information is a flaw of the algorithm. Increasing the data structure size and the key length are two recommended measures that ensure the strength of the

encryption algorithm. The running-time is a constraint imposed to the design of the algorithm that restricts its applicability at a moment. During simulation we have consider different size of data blocks ranging from 20 kb to 200 kb. After successful execution, plain text generated, encrypted and decrypted. Results are obtained from simulation environment using different loads. In this paper, the popular secret key algorithms including DES and 3DES were implemented and their performance was compared by encrypting input files of varying contents and sizes, and even AES (Advanced Encryption Standard) also compared. The algorithms were implemented in a uniform language SAGE to compare their performance. DES, Triple DES and Ternary DES are compared in time complexity.

Table XIII - Relationship between Key Length and Number of Rounds in AES

Alogorithm	Key length (Bits)	Number of Rounds
DES	56	16
Triple DES	112	48
Triple DES	168	48
AES	128	10
AES	192	12
AES	256	14
Ternary DES	56	10

Table XIV - Comparative Study In Terms Of Time To Evalute Algorithm

Input Size (kb)	DES	Triple DES	AES
20	2	7	4
50	5	17	8
100	2	7	4
20	12	35	21
150	20	60	30
200	25	74	38

Table XV - Time Complexity

	DES	Triple DES	AES
Time complexity (X time required for DES encryption and decryption)	2^{56}	2^{112}	3^{56}

6. Conclusion and Future Scope

As day by day technology improves cash transactions be- coming more digitalized. To secure these digital transactions cryptographic algorithms are used. In our paper we proposed Triple DES based security technique which shows better result in level of security with respect to the other popular most frequently used algorithms. Although Triple DES is slower than DES in encryption time but according to security level Triple DES is billion times stronger than DES.

In future we will try to implement a new techniques using Ternary logic with high level of security as well as optimizing computational power. The proposed Ternary DES can be implemented in full fledge by defining S-Boxes and other operations involved in DES.

Declarations

Source of Funding

This research did not receive any grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The author declares no competing financial, professional and personal interests.

Consent for publication

Author declares that she consented for the publication of this research work.

References

[1] S. Mitra, B. Jana and J. Poray, "Implementation of a Novel Se- curity Technique Using Triple DES in Cashless Transaction," 2017 International Conference on Computer, Electrical and Communication Engineering (ICCECE), Kolkata, 2017, pp. 1-6.

[2] K. Ali, F. Akhtar, S. A. Memon, A. Shakeel, A. Ali and A. Raheem, "Performance of Cryptographic Algorithms based on Time Complexity," 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 2020, pp. 1-5.

[3] X. Xu and N. Tian, "The Search and Improvement of DES Algorithm for Data Transmission Security in SCADA," 2019 International Con- ference on Intelligent Computing, Automation and Systems (ICICAS), Chongqing, China, 2019, pp. 275-279.

[4] N. Su, Y. Zhang and M. Li, "Research on Data Encryption Standard Based on AES Algorithm in Internet of Things Environment," 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 2019, pp. 2071- 2075, doi: 10.1109/ITNEC.2019.8729488.

[5] R. Pich, S. Chivapreecha and J. Prabnasak, "A single, triple chaotic cryptography using chaos in digital filter and its own comparison to DES and triple DES," 2018 International Workshop on Advanced Image Technology (IWAIT), Chiang Mai, 2018, pp. 1-4.

[6] L. Wang and G. Jiang, "The Design of 3-DES Encryption System Using Optimizing Keys," 2019 China-Qatar International Workshop on Artificial Intelligence and Applications to Intelligent Manufacturing (AIAIM), Doha, Qatar, 2019, pp. 56-58.

[7] I. R. S. Reddy and G. Murali, "A novel triple DES to enhance E- governance security," 2017 International Conference on Energy, Com- munication, Data Analytics and Soft Computing (ICECDS), Chennai, 2017, pp. 2443-2446, doi: 10.1109/ICECDS.2017.8389889.

[8] F.O¨ zkaynak and M. I. Muhamad, "Alternative substitutional box structures for DES," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, 2018, pp. 1-4.

[9] J. Mounika, K. Ramanujam and M. Z. Jahangir, "CMOS based design and simulation of ternary full adder and Ternary coded Decimal (TCD) adder circuit," 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, 2016, pp. 1-5, doi: 10.1109/ICCPCT.2016.7530153.