I J C T A, 9(11) 2016, pp. 5085-5092
© International Science Press

SECURE AND IMPROVED APPROACH FOR 3-DES ALGORITHM AGAINST CRYPTOGRAPHIC ATTACKS

Abhishek Yadav[*] and Ms. Richa Sharma[**]

Abstract: DES is considered insecure because many different attacks are possible in it. For the encryption of electronic data, we use the Data Encryption Standard which is symmetric-key algorithm [1]. The two basic facts of current day data encryption are authentication and data privacy. As modern society is now becoming more connected day by day, so large amount of information is under threat. Therefore, there is a need for protection which brings data secrecy and data integrity.

This paper discusses about the improvement of DES algorithm to make it more secure. It also points out some disadvantage of DES and 3-DES algorithms. It also discusses about one new algorithm which is an improvement of the 3-DES algorithm. A Comparison has been made between DES, 3-DES and New algorithm. This comparison is conducted on the basis of key size, total rounds, complexity, user effort needed etc.

Key Words: DES, TDES;

1. INTRODUCTION

In cryptography, to make data accessible to the authorized user, it is encoded using encryption techniques. In an encryption technique, the useful information or message, which is referred as plain text, is converted or encrypted using an encryption algorithm. There are many different algorithms which are available and are used to secure information. Some of them are AES, DES, and 3-DES, RC2, RC6, and BLOWFISH.

Still confidential information is unsafe from intruders who easily get access and modify the secret data. Intruders mainly try to steal important data or identities and become deceit person. Some additional improvements are required in already existing algorithms to enhance the security. Data Encryption is a very essential process to provide security. It is necessary to encrypt data before passing it to the network and then at receiver side this data is decrypted to get the original data. However, nowadays most all types of encryption techniques are subject to attack easily. For all cipher text, the most common way of attack is brute force attack in which all possible keys are tried by the intruder to decrypt the data. There are some algorithms in which question is raised for their small key sizes and they dictated a need for a replacement algorithm.

[*] Student, Department of CSE, Lovely Professional University, Phagwara, Punjab-144411. y.abhi180593@gmail.com

[**] Assistant Professor, Department of CSE, Lovely Professional University, Phagwara Punjab-144411 richa20489@gmail.com

As Data encryption standard (DES) is a symmetric-key algorithm, it is used to encrypt the electronic data. But DES is now considered to be more vulnerable for many applications. One of the biggest reasons behind this is the key length (which is 56 bits only) [2]. The brute force attack has the capacity to easily break DES security.

DES is the standard block cipher which takes data or plaintext of fixed length and encrypts it by using a number of complicated operations into some different cipher text. The Key seemingly consists of 64 bits; in which only 56 bits are used by the algorithm. In a similar way there is an algorithm known as Triple Data Encryption Standard (TDES or 3DES) which applies DES 3 times on any particular data or data block. Triple DES generates a very simple method in which size of DES key length increases to protect against different attacks [3]. Triple DES uses 3 different keys to encrypt the data. Triple DES has a key length size of 168 bits because of that three keys, but only 112 bits provide the effectuality security. This is showing that this algorithm is also not much secure.

So there is a need of some improvement in this algorithm so that security of data increases upto some more extent.

2. RELATED WORK

2.1 Evolution of DES

In the field of encryption, DES has undergone many advancements or improvement and served as a base for many different techniques. One of its improvements is Triple DES (3DES or TDES). Triple DES uses 3 keys to encrypt data. So, the total key length size of 3DES is 168 bits. But in reality the effective security provided by it is only 112 bits. As a DES uses 16 rounds to encrypt the data, triple DES uses 48 bits in total to encrypt the data. This technique helps to increase the security up to 3 levels or increase the security, efficiency 3 times more than DES [4]. As 3-DES performs every task 3 times related so its performance also increase 3-times more the DES algorithm. 3-DES uses three keys to encrypt the data.

DES, sometimes used simultaneously with other encryption techniques. Sometimes they are fused to some other encryption algorithms. This type of fusion is used to secure the key generation of the DES. It uses 2 keys to perform initial permutation which is followed by 16 rounds of crossover iterations and finally go through the inverse permutation. It sometimes decreases the brute force chances, but slowed down the process.

Known Attacks on DES

There are many different attacks that are possible on DES in which Brute Force and cryptanalysis techniques are most common. Brute Force is one of the most strongformsof attack on any encryption uptill now. It tries to decrypt the block of encrypted data with all possible keys. So the data we have on the clear text will allow us to accept the right key and stop the search. In average, we will have to try nearly 36'028'797'018'963'968 (36 million of billions) of keys.Modern PC can easily evaluate one to millions keys per seconds. Differential cryptanalysis is a new generic symmetric algorithm. It works by presuming the attacker has some part of original plaintext. The attacker then diminishes the security of the encryption until he or she deciphers the key. The data analysis phase computes the keys by analyzing near about 2^24 chosen plaintext. But mainly, the attacker analysis near about 2^14 chosen plaintext and succeeds with probability of 2^-33.

3. DESCRIPTION ABOUT MODIFIED DES

3.1 Key Generation Process

The code used in this algorithm provides the security to the data more than the security provided by Data Encryption Standard (DES) and 3- DES algorithm. As in this algorithm, encryption of data is taking place more than 3 times, which was fixed in 3-DES algorithm up to 3 times only [6].

In DES and 3- DES algorithm, it was fixed that the user has to enter data and key of size 64 bits only, but in this new algorithm user can enter data and key of any size. One more advantage of this new algorithm over 3-DES algorithm, in 3-DES user has to enter more than one key for encryption, but in this new algorithm only one key is sufficient to encrypt the data in a better way than a 3-DES algorithm.

In this algorithm, if the user enters key of size less than 64 bits, then it by default fill 0's on the end to make it of size 64 bits.Suppose a user enter key (1023456) in hexadecimal form then it covers 28 bits only. So to make this key of size 64 bit it by default fills 09 0'sin the end of key in hexadecimal form. Now, as this new algorithm is encrypting data up to N times it needs N different Keys during the process.

The advantage of this algorithm is that when users enter the first key (K1), it will generate these N no. of keys by own without any effort needed by the user.

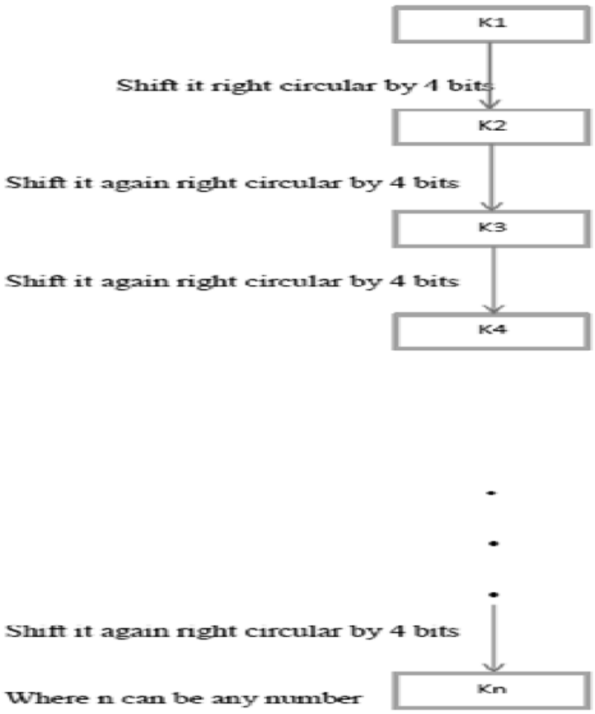
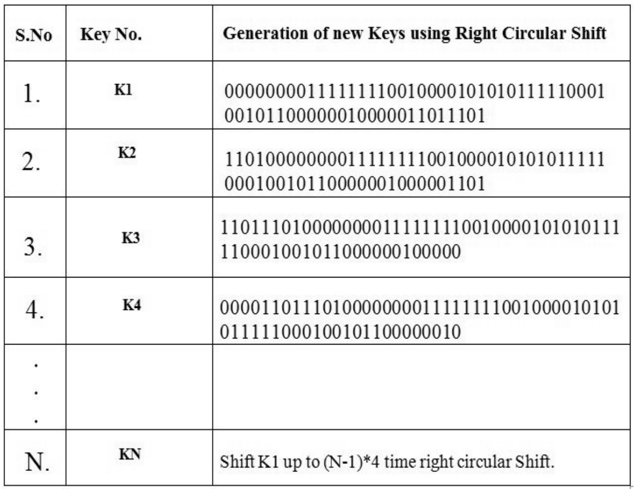

K1
Shift it right circular by 4 bits
K2
Shift it again right circular by 4 bits
K3
Shift it again right circular by 4 bits
K4
Shift it again right circular by 4 bits
Where n can be any number
Kn

Figure 1: Key Generation

Figure 1 shows how different keys are generated by one particular key (K1) in this new algorithm.

Now the next table is showing how actually this right circular shift is taking place in this key generation process.

Table 1
Key Bits Form



S.No	Key No.	Generation of new Keys using Right Circular Shift
1.	K1	00000000111111110010000101010111110001 001011000000010000011011101
2.	K2	11010000000011111111001000010101011111 0001001011000000010000001101
3.	K3	11011101000000000111111110010000101010111 1100010010110000000100000
4.	K4	00001101110100000000011111111001000010101 011111000100101100000010
. . .		
N.	KN	Shift K1 up to (N-1)*4 time right circular Shift.

This table describes how new keys are generated by using only one key (K1) enter by the user. In this process the new key is formed by shifting every previous key 4 bit circular right. This shifting is taking place by shifting every bit4 bits ahead and shift last 4 bits to the starting position.

Plain Text Encryption Process

In this Plain text encryption process, the size of input data can be of any length.In this algorithm,if the user enters data of size less than 64 bits, then it by default fill 0's in the end to make it of size 64 bits.For example, if user enters data (abcde) in hexadecimal form, then it covers 20 bits only.So to make this data of size 64 bit it by default fill 11 0's in the end of key in hexadecimal form.In this encryption process user first enter data and key of any size. Then by adding 0's it is converted up to64 bits. Now these data and key bits go through the DES algorithm and give the output of 64 bits in the encrypted form.

Now the key using in this process will perform a right circular process to generate the next key. This new key will again go through the DES algorithm with the encrypted data comes as an output in the previous process.This process will continue up to the N times where N is the number of times encryption enters by the user.

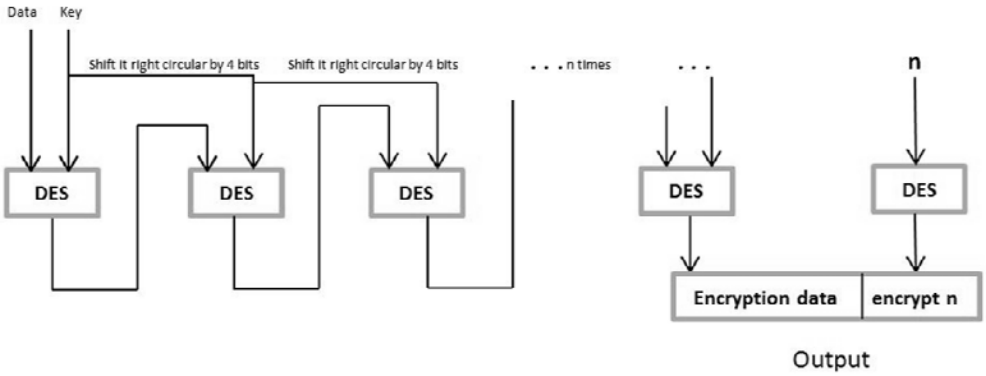
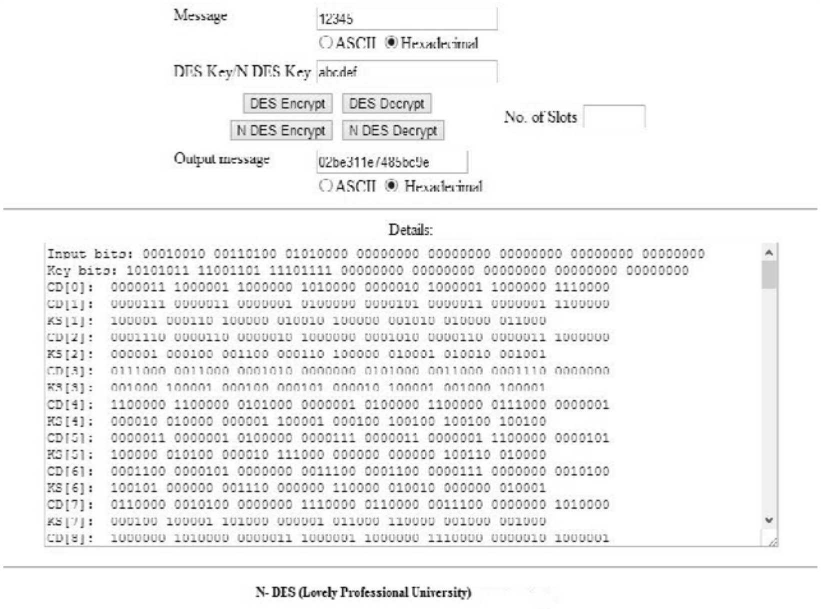


Figure 2: Encryption Algorithm

Figure 2 is showing how one process is related to another process. This diagram is also telling how the outputof the one process will become the input for the next process.

Here N(number of times encryption) can be decided by the user and the value of N is also sent in the encrypted form with the cipher text so that an attacker will not able to get the value of N. The value of N is encrypted using DES and then concatenate with the final cipher text before sending it to destination.

While decryption, firstly encrypted value of N can be decrypted to get number of times encryption (N) then this value is used to decrypt the cipher text to get actual plaintext.



Message 12345

○ ASCII ● Hexadecimal

DES Key/N DES Key abcdef

No. of Slots

Output message 02be311e7485bc9e

○ ASCII ● Hexadecimal

Details:

```
Input bits: 00010010 00110100 01010000 00000000 00000000 00000000 00000000 00000000
Key bits: 10101011 11001101 11101111 00000000 00000000 00000000 00000000 00000000
CD[0]:  0000011 1000001 1000000 1010000 0000010 1000001 1000000 1110000
CD[1]:  0000111 0000011 0000001 0100000 0000101 0000011 0000001 1100000
KS[1]:  100001 000110 100000 010010 100000 001010 010000 011000
CD[2]:  0001110 0000110 0000010 1000000 0001010 0000110 0000011 1000000
KS[2]:  000001 000100 001100 000110 100000 010001 010010 001001
CD[3]:  0111000 0011000 0001010 0000000 0101000 0011000 0001110 0000000
KS[3]:  001000 100001 000100 000101 000010 100001 001000 100001
CD[4]:  1100000 1100000 0101000 0000001 0100000 1100000 0111000 0000001
KS[4]:  000010 010000 000001 100001 000100 100100 100100 100100
CD[5]:  0000011 0000001 0100000 0000111 0000011 0000001 1100000 0000101
KS[5]:  100000 010100 000010 111000 000000 000000 100110 010000
CD[6]:  0001100 0000101 0000000 0011100 0001100 0000111 0000000 0010100
KS[6]:  100101 000000 001110 000000 110000 010010 000000 010001
CD[7]:  0110000 0010100 0000000 1110000 0110000 0011100 0000000 1010000
KS[7]:  000100 100001 101000 000001 011000 110000 001000 001000
CD[8]:  1000000 1010000 0000011 1000001 1000000 1110000 0000010 1000001
```

N- DES (Lovely Professional University)

Figure 3: Interface of The Application

Decryption Process

In DES, encryption and decryption are using the same algorithm. In decryption process the input is the ciphertext and the key processing is always performed in reverse order. The new algorithm is designed like that so that it can decrypt ciphertext to its original form. A very important point during the decryption process, we need to remember about the ciphers is that the round keys (K1 to K16) should be applied in the reverse order. At the encryption site, round 1 uses K1 and round 16 uses K16; of the decryption site, round 1 uses K16 and round 16 uses K1.

In the decryption process user first start with the last key (KN) and the cipher text. This last key is directly calculated by shifting the original key up to (N) *4 time right circular. Here the value of N is calculated by cipher text because its last half part is the encrypted form of the value N. So firstly last half part of this cipher text decrypted by DES to calculate value of N and then by using that value of N we calculate actual plaintext.

Now these cipher data and key bits go through the Decrypt-DES algorithm and give the output of 64 bits.

Now the key using in this process will perform a Left circular process to generate the next key. This new key will again go through the Decrypt-DES algorithm with the data comes as an outpatient the previous process. This process will continue up to the N times where N is number of times encryption enters by the user.

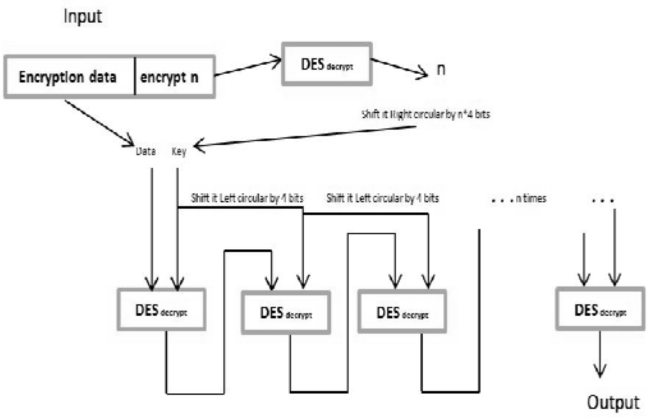


Figure 4: Decryption Algorithm

Figure 4 is showing how one decryption process is related to another process. This diagram is also telling how the decrypted output of the one process will become the input for the next process.

4. COMPARISON BETWEEN DES, 3-DES AND N-DES

There are many points which describe the difference between the previous algorithm(DES and 3-DES)and new algorithm(N-DES). The difference is calculated on the basis of input data size, input key size, etc.. The new algorithm performs filling of 0's at the end, which was notthere in DES and 3-DES.There is also some difference between 3-DES and N-DES on the basis of Decrypt time.

Table 2
Comparison Table

Properties	**DES**	**3-DES**	**N-DES**
Data	Fixed size	Fixed size	Variable size
Key	Fixed size	Fixed size	Variable size
No. of keys needed to insert	1 key	3 keys	1 key
Decryption time	2^52	2^156	2^(N*52)
Rounds	16	48	N*16
User effort	Need more user effort	Need more user effort than DES	Need less user effort than DES

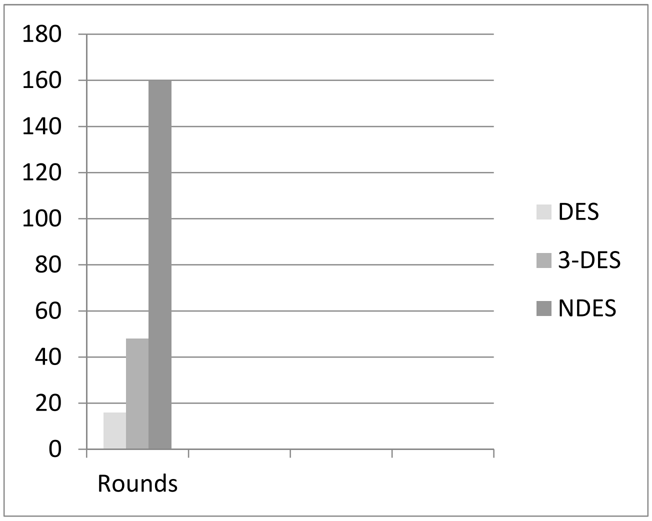


Figure 5: Number of Rounds It Take to Encrypt

This figure is telling the number of rounds it takes in each step to encrypt the data or make it more secure. Here value of N is taken as 10. (Suppose N=10).

5. SUMMARY AND CONCLUSION

This research will help to increase the Security level of data. This code provides the security to the data more than security provided by Data Encryption Standard (DES) and 3- DES algorithm. As in this algorithm encryption of data is take more than 3 times which was in 3-DES algorithm. The interface used here is also very user friendly.

Few best properties of this algorithm are:

- User can enter any size of data which is not in case of DES and 3-DES algorithm.
- User can enter any size of Key which is not in case of DES and 3-DES algorithm.
- Users have to enter only one Key here and it will encrypt data n time by generating n different Keys which is not in case of DES and 3-DES algorithm.

Complexity of algorithm increases much more than 3-DES algorithm.

References

[1] Feistel, H. (1999). Data Encryption Standard (Des).Fips Pub 46-3, 3.

[2] Kelly, S. (2006). 2/22/15 www.ietf .org/rf c/rf c4772.txt.

[3] Paper, W., &Fpgas, S. (2000). Data Encryption using DES / Triple-DES Functionality in Spartan-II FPGAs, 115, 1–14.

[4] Now, D. (2014). Looking for the best ways to protect your company's data, 2–5. Retrieved from http://searchsecurity.techtarget.com/tip/Expert-advice-Encryption-101-Triple-DES-explainedz

[5] Anderson, R., Biham, E., & Knudsen, L. (1998). Serpent : A proposal for the advanced encryption standard. *NIST AES Proposal*, 1–23. Retrieved from https://bitbucket.org/nicholascapo/network-security-project/src/fcbc6e93e555/Literature/serpent.pdf

[6] Bakhtiari, S. (n.d.). Linear Cryptanalysis of DES Cipher Linear Cryptanalysis of DES Cipher.North.

[7] Page, H., Information, F., Policy, S. T., Funds, E., & Policy, S. T. (1987). Computer data authentication, 1–6.

[8] AbdElminaam, D. S., Kader, H. M. A., &Hadhoud, M. M. (2010).Evaluating the performance of symmetric encryption algorithms.*International Journal of Network Security*, *10*(3), 213–219. doi:10.7763/IJCTE.2009.V1.54

[9] Sison, A. M., Tanguilig, B. T., Gerardo, B. D., & Byun, Y. C. (2012). Implementation of improved des algorithm in securing smart card data. Communications in Computer and Information Science, 340 CCIS(c), 252–263. http://doi.org/10.1007/978-3-642-35267-6_33

[10] Tas, P. (2001). The Economic Impacts of NIST's Data Encryption Standard(DES) Program.