Enhanced Data Encryption Standard using Variable Size Key (128N Bits) and 96 Bit Subkey

Awadh Kishor Singh
Computer Science and Engineering
Ghaziabad (UP)
India

Seema Varshney
Computer Science and Engineering
KEC, Ghaziabad (UP).
India

ABSTRACT

In this paper 'EDES (Enhanced Data Encryption Standard) using variable size key (128n bits) and 96bit sub-key', we are providing a solution for an efficient and enhanced encryption for DES (Data Encryption Standard) to send encrypted information or file using more secure key and less time for encryption. Here, we present, design and implementation features of a proposed system EDES to be used for communication with secure information and file in the network.

General Terms

Encryption, Decryption, Substitution, Permutation, Feistel, Plain Text, Cipher Text

Keywords

EDES, EDES3f, MPC-1

1. INTRODUCTION

Today everyone like to send information /file /documents using many types of devices (like Mobile phones, Laptops, fax machine, etc) in form of soft copy or hard copy in the network connected with different types of media (like wireless, Bluetooth, infrared or fixed line connection etc.) want that no anyone can read or misuse the file containing secret information and accept only the right person, so that's why the enhancement on DES requires to make more secure electronic communication on the network using Data Encryption Standard. In this paper, we are providing a solution for an efficient and enhanced encryption for DES (Data Encryption Standard) to send encrypted information or file using more secure key and less time for encryption. Here, we present, design and implementation features of a proposed system EDES (Enhanced DES using variable size key 128xN-bits and sub key of size 96-bit) to be used for communication with secure information and file in the network.

2. PRECIOUS WORK

Many researchers and developers are working on DES [1] & Triple DES [5]. DES is already implemented, and designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS) and [now the National Institute for Standards and Technology (NIST)] in 1977 for commercial and unclassified government applications. DES works with block size 64 bit and key size 56 bits out of 64 bit with 16 sub keys of size each 48 bit. Triple-DES is just three times encryption model using DES. In many research works it was modified in many field of its encryption/ decryption model to

Make better. First Double DES trying to take place by encrypting the same data block (64 bit), two time using two different keys or same key but it have to face the attack of 'meet in the middle attach'. Then DES is improved by using secondary key in New DES implantation approach. Then Triple DES removes its difficulties by encrypting three time the same data block(64 bit) with the three different or same keys. It makes the old DES more secure but it takes time three times more than time taken by old DES encryption/ decryption model. In 2010 the paper 'An Innovative Approach to Enhance the Security of Data Encryption Scheme' published by 'D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati garg' introducing to create unique key for every data block. This approach is feasible only if the blocks are limited because it is difficult to create unique key for each data block if there are huge blocks in numbers.

2.1 Data Encryption Standard

DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks. DES has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations and slow software implementations, although this latter point is becoming less significant today since the speed of computer processors is several orders of magnitude faster today than twenty years ago. IBM also proposed a 112-bit key for DES, which was rejected at the time by the government; the use of 112-bit keys was considered in the 1990s, however, conversion was never seriously considered.

In order to calculate the inputs to the S- and P-box matrix, portions of the data are XORed with portions of the key. One of the 32-bit halves of the 64-bit data and the 56-bit key are used. Because the key is longer than the data half, the 32-bit data half is sent through an expansion permutation which rearranges its bits, repeating certain bits, to form a 48-bit product. Similarly the 56-bit key undergoes a compression permutation which rearranges its bits, discarding certain bits, to form a 48-bit product. The Sand P-box look-ups and the calculations upon the key and data which generate the inputs to these table look-ups constitute a single round of DES.

2.1.1 The function f and key schedule

Round function *f* is calculated by using expansion, substitution and permutation boxes. It takes 32bit data and expands to 48 bit. Then it XORed with 48bit sub-key and result is substituted using eight S boxes to 32 bit data that is permuted using permutation box that takes 32 bit data as input and produce permuted data 32bit as output to give result of function of *f.* Every S table takes a 6-bit chunk and converts it into 4-bit output. At the output of S-block we have 8*4 = 32 bits, which are permuted and outputted for further operation.

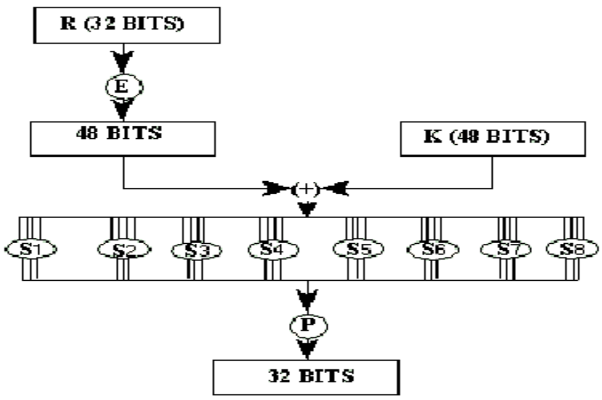

Fig. 1 Round function *f* in encryption

The following equation describes one round operation at encryption:

$$L_{n+1} = R_n$$
$$R_{n+1} = L_n \oplus f(R_n, k_n)$$

Where kn is a permutation of the secret key at time n. Calculation of the round function f is illustrated in fig. 1. Decryption goes in a very similar and symmetric way. The easiest way to explain this is going backwards:

$$R_n = L_{n+1}$$
$$L_n = R_{n+1} \oplus f(L_{n+1}, k_n)$$

3. EDES (ENHANCED DES) USING VARIABLE SIZE KEY (128n bit) AND 96bit SUBKEY

In this paper we are find a better solution that can prevent most of the problems and issues that I have discussed above like bruit force attack, meet in the middle attack, linear and differential cryptanalysis, unique key for limited data blocks, More time taken by 3DES etc.

The first problem of bruit force attack is here resolved by making variable size key that is variable in size it depends on the size of key provided in the form of any text, picture, audio or video. The key is represented as 128n bit key. The provided data for key will be splited into n, 128bit blocks.

Key 128n bit=128bit^1 +128bit^2 +………….128bit^n.

To prevent from linear cryptanalysis and deferential cryptanalysis, the size of sub key 48bit is increase to 96bit, which requires more time and effort to linear and differential cryptanalysis attacker, by concatenating both 48bit and resultant 96 bit is rail fenced(R) then the rail fenced result XORed with next Rail fenced result and so on.

Sub Key 96bit=R ((48bit||48bit), 2) R ((48bit||48bit), 2) ……. R ((48bit||48bit), 2)

After that the size of data block is increase three times to 192bit as a single data block. It requires less cycle to encryption and decryption, and less time for giving throughput. Now the data block size is 64bit so it requires many cycles to encrypt or decrypt data. That's why here the data block size is set to 192bit at a time. This 192bit data is splited into three 64bit internally like (64bit^1+64bit^2+64bit^3), and each round computes as DES round, after finishing each round the complete data is swapped and make different 64 bit like (64bit^3+64bit^1+64bit^2) and so on for every 16 round.

The Complete encryption process of EDES is divided into two parts – EDES Key generation part, and EDES Encryption part.

3.1 EDES key generator

Here all the key bits is divided into N, 128-bit blocks, each 128-bit block permuted by MPC-1 and After applying MPC-1 the 128-bit permuted key input is splitted into two block of size 64-bit each individually, and then both 64-bit parts are used to generate 16 sub-key of size 48-bit as in DES, both 16 sub-keys(48-bits) are merged using "Rail-Fence" (R) technique to generate 16 sub-keys of size 96-bit for each 128-bit Key Block(K). and if next 128-bit block exist the these 16 sub-keys are XORed with new 16 sub-key of size 96-bit generated for next 128-bit key block and so on for all (N) the 128-bit key block. Finally the key generator gives more secure 16 sub-key of size 96-bit for encryption part which execute immediately after finishing the key generation part.

Key 128n bit =128bit1 +128bit2 +………….128bitn

Sub Key 96bit=R ((48bit||48bit), 2) R ((48bit||48bit), 2) ……. R ((48bit||48bit), 2)

4.2 EDES Encryption

EDES Encryption will use 192 bits as a single block for encryption instead 64bit that is used by existing DES. This will split 192 bits into three 64bit blocks and then applied Initial Permutation on each splitted 64 bit block as in DES. Here the 192-bit data is divided into three 64-bit sub-blocks. The right most sub-blocks is encrypted and result is pass to 2nd round as a first sub-block, right 2nd sub-block is encrypted and result is pass to 2nd round as a right most block and the first sub-block XORed with right 2nd encrypted result and passed as a right 2nd sub-block for 2nd round, and so on for all the round.

There are two model described model-1 names EDES Encryption and second and last one is EDES3F Encryption Model. In EDES Encryption model only last two blocks are Encrypting using Feistel Structure to give speedup in encryption/decryption process. But it is little bit less secure then the second model is designed where all the blocks are encrypting using Feistel structure. This, second model is finally applied that takes less time for encryption than DES and needs only single cycle to encrypt 192 bit data block. It makes more secure from the 'bruit force attacks' and needs more time fir linear and deferential cryptanalysis.

Cipher Text = EDES (E, 192 bit Plain Text, 128n bit key)
Plain Text =EDES (D, 192 bit Cipher Text, 128n bit key)
E: Encrypt, D: Decrypt

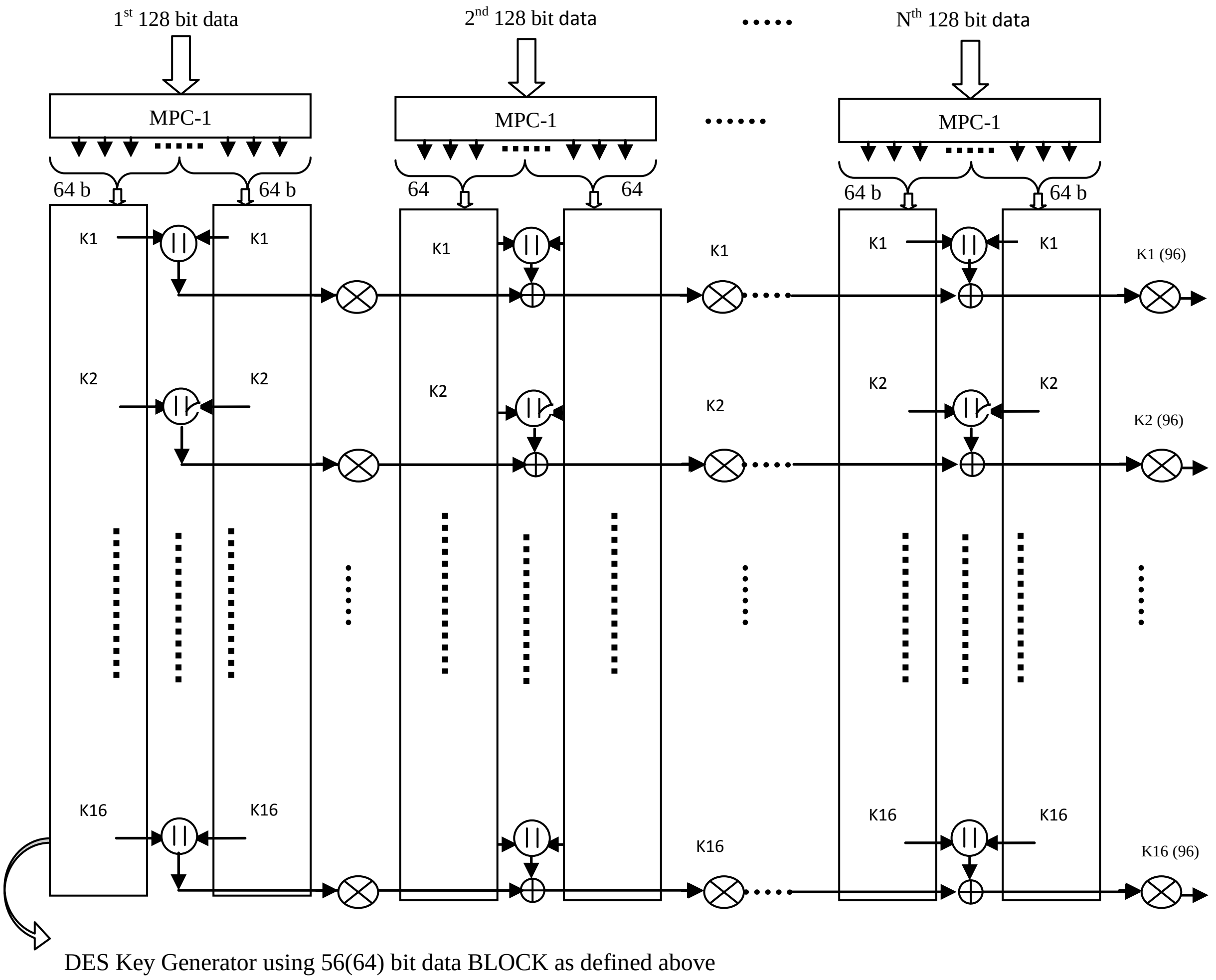

Fig. 2: Block Diagram of Enhanced DES key generator using 128N bit data

4. RESULT AND ANALYSIS

For simulation, text files of different size are taken and passed to both EDES encryption model and Existing DES with the same size key to evaluate the time, taken for encryption by the entire three models, these results are shows as follows in the form of graph fig. 3, 4 and 5. Here DES is Existing Model, EDES is the Model-1 and EDES3f is the Model-2 complete sub block encrypting.

Using 64 bit key for both

data size	1mb	2mb	3mb	4mb	5mb	6mb	7mb	8mb
DES(64b key)	7	15	23	31	38	46	53	61
EDES(128b key)	7	13	19	25	32	38	45	51
EDES3f(128b key)	7	14	22	28	36	42	50	57

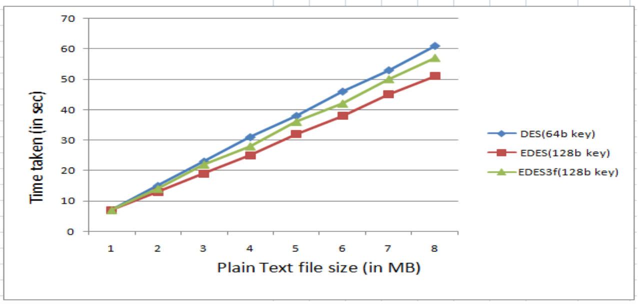

Fig. 3 Encryption time graph with 64-bit key

Using 128x20 bit key for both

Data Size	1mb	2mb	3mb	4mb	5mb	6mb	7mb	8mb
DES(64b key)	7	15	23	31	38	46	53	61
EDES(128x20b key)	7	14	19	26	33	39	45	52
EDES3f(128x20b key)	8	15	24	32	39	47	55	62

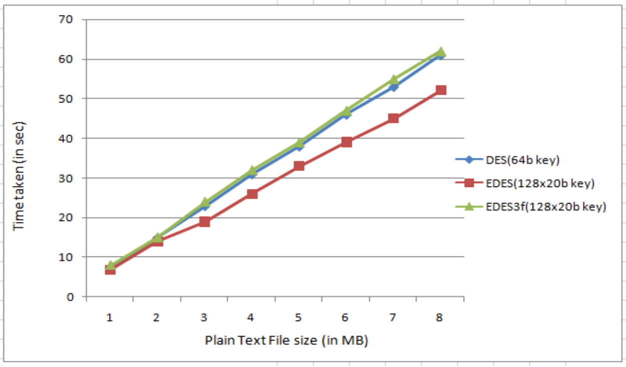

Fig. 4 Encryption time graph with 128x20-bit key

Using 353 KB key for both

Data Size	1mb	2mb	3mb	4mb	5mb	6mb	7mb	8mb
DES(64b key)	7	15	23	31	38	46	53	61
EDES(128x20b key)	9	15	21	28	35	41	47	54
EDES3f(128x20b key)	10	18	25	33	41	48	56	64

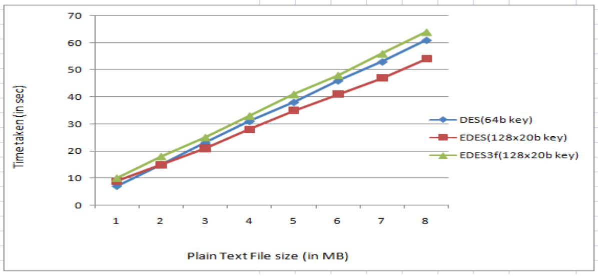

Fig. 5 Encryption time graph with 353-KB key

5. COMPARISION

The following table gives the comparison between Existing DES and our EDES.

Table 1 DES (64/56) VS EDES (192/128n)

	DES	EDES
Block Size	64 bit	192 bit
Key Size	56 bit(64 bit) (Fixed)	128n bit (Variable)
Sub key Size	48 bit	96 bit
Number of Rounds	16	16
Structure	Feistel	Feistel
Key generation Time	Less	More
Encryption/Decryption Time	More	Less
Brute Force Attack takes	Less Time	More Time
Meet in the middle attack	If 2DES	Doesn’t required 2EDES
Linear Crypt analysis	Less effort requires	More effort requires
Differential cryptanalysis	Less effort requires	More effort requires

6. CONCLUSION

After successfully implementation we can encrypt or decrypt any file (text/ picture/ audio/ video) in comparatively less time by using variable size key in the form of any text file, picture, audio or video. And make data more secure that attackers like. Bruit force attack, linear cryptanalysis/ differential crypt analysis etc.

In future the model of key generation can be implemented using parallelism approach that will decrease the time of key evaluation and decrease the overall time requires to encryption/ decryption by our approach.

7. ACKNOWLEDGMENTS

I would like to express my earnest gratitude towards my supervisor Prof. Seema Varshney for her inestimable guidance. Without her innovative ideas and unrelenting support, it would not have been possible for me to successfully complete this thesis. It has been pleasure to work under him.

Lastly, I thank to all friends and my fabulous family for all the wonderful things they have done for me and for standing by me through thick and thin.

8. REFERENCES

[1] "Data Encryption Standard (DES)", Federal Information Processing Standard Publication, FIPS PUB 46-3, National Bureau of Standards, 1977.

[2] P. Kitsos, S. Goudevenos, "VLSI implementations of the triple-DES block cipher”, Electronics, Circuits and Systems, ICECS 2003, Proceedings of the 2003 10th IEEE International Conference, pp 76-79, vol. 1, 2003

[3] T. Schaffer, A. Glaser, “Chip-package Co-implementation of a triple DES Processor”, IEEE Transactions on Advanced Packaging, vol. 27 , pp. 194-202, 2004

[4] S. Praveen, M. Nagesh, “Implementaion of the Triple DES Block Cipher using VHDL”, International Journal of Advances in Engineering & Technology, pp. 117-128, vol 3, issue 1, 2012.

[5] O. Hamdan, B. Zaidan, “New Comparative Study between DES, 3DES and AES within Nine Factors”, Journal of Computing, pp. 152-157, vol 2, issue 3, 2010

[6] R. Shantamurty, “Implementing Triple DES (TCBC) on OpenVMS”, OpenVMS Technical Journal, V15, 2010

[7] Aqib Al Azad, “Efficient VLSI Implementation of DES and Triple DES Algorithm with Cipher Block Chaining concept using Verilog and FPGA”, International Journal of Computer Applications, pp. 6-15, vol 44, No. 16, 2012

[8] V. Kakarla, N.S.Govind, “FPGA Implementation of Hybrid Encryption Algorithm Based on Triple DES and RSA in Bluetooth Communication”, International Journal of Applied Research & Studies, vol. 1, 2012

[9] William C. Barker, Elaine Barker: “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher”, Revised January 2012.

[10] D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati garg: “An Innovative Approach to Enhance the Security of Data Encryption Scheme”, International Journal of Computer Theory and Engineering, Vol. 2, No. 3, June, 2010 1793-8201.

[11] Charles Connell: “An analysis of new DES: A modified version of DES”, july 1990

[12] Arsen Zoksimovski : “IP module for encipher – decipher DES”, ECE993 Security Engineering.

[13] by J. Orlin Grabbe: “The DES Algorithm Illustrated by J. Orlin Grabbe”, This article appeared in ‘Laissez’ Faire City Times, Vol 2, No. 28. Homepage:http://www.aci.net/kalliste/homepage.html