International Journal of Emerging Trends in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 2, Issue 5 (Sep-Oct 2015), PP.08-15

An Approach to Enhance the DES Algorithm for Encryption System

Ravindra Jogekar[1], Pranay Meshram [2,] Ashish Mohod [3]
[1 3](Department of Computer Science & Engg, Priyadarshini J L College of Engg, Nagpur/ RTMNU, India)
[2](Department of Information Technology, Priyadarshini J L College of Engg, Nagpur/ RTMNU, India)

Abstract :- The main goal for designing any encryption algorithm is to provide security against unauthorized access or attacks. Data Encryption Standard algorithm is a symmetric key algorithm and it is used to secure the data. The Enhanced DES algorithm works on increasing the length of key or increased the number of states in which the information is to be represented or complex S-BOX design or combination of above criteria. By increasing the key length, the number of combinations for key will increase which is hard for the intruder to do the brute force attack. As the S-BOX design will become the complex there will be a good avalanche effect. As the number of states increases in which the information is represented, it is hard for the intruder to crack the actual information. Proposed algorithm work on new operation called “Hash function” depends on using two keys in place of the predefined XOR operation applied during the 16 round of the standard algorithm. One key used in “F” function and another key consists of a combination of 16 states (0, 1, 2…13, 14, and 15) instead of the ordinary 2 state key (0, 1). By doing this replacement it will add a new level of protection, strength and more robustness against cracking the code.

Keywords: - DES, Encryption, Decryption

I. INTRODUCTION

The Cryptography is usually referred to as - the study of secret, while now a days is most attached to the definition of encryption. Encryption is the conversion of data into a form, called cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. It is the easiest and most practical method of protecting data stored or transmitted electronically and is particularly essential with sensitive data. Encryption uses a mathematical algorithm to scramble readable text that cannot be read unless the reader has the key to "unlock," or convert, the information back to its readable form. This means that your sensitive data cannot be accessed without you providing a password. Even a single failure to encrypt a sensitive data whether through an e-mail, via a stolen flash drive or laptop, can result in a security breach with criminal or civil liabilities and irreparable harm to finances and the reputation of the university.

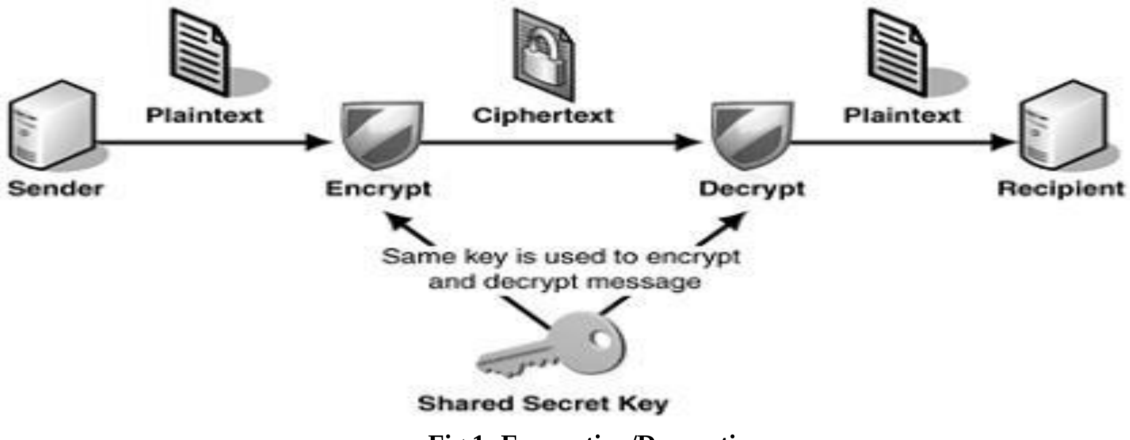

Fig 1: Encryption/Decryption

II. DATA ENCRYPTION STANDARD

Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations. Although this is considered "strong" encryption, many companies use "triple DES", which applies three keys in succession. DES originated at IBM in 1977 and was adopted by the U.S. Department of Defense. It is specified in the ANSI X3.92 and X3.106 standards and in the Federal FIPS 46 and 81 standards. The algorithm is best suited to implementation in hardware, probably to discourage implementations in software, which tend to be slow by comparison.

However, modern computers are so fast that satisfactory software implementations are readily available. DES is the most widely used symmetric algorithm in the world, despite claims that the key length is too short. Ever since DES was first announced, controversy has raged about whether 56 bits is long enough to guarantee security.

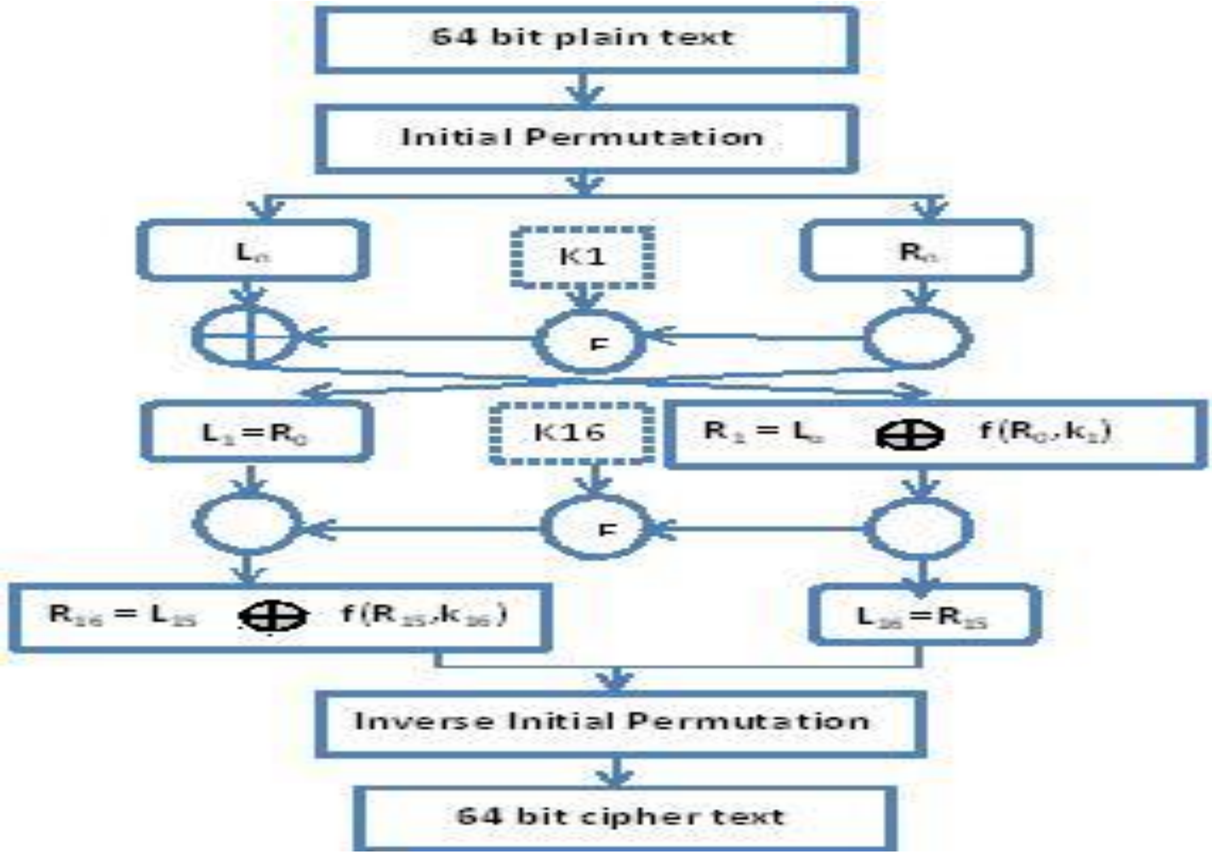

Fig 2: DES Algorithm

1. **Expansion (*E*):** The 32-bit input word is first expanded to 48 bits by duplicating and reordering half of the bits.[2]
2. **Key mixing:** The expanded word is XORed with a round key constructed by selecting 48 bits from the 56-bit secret key, different selection is used in each round.

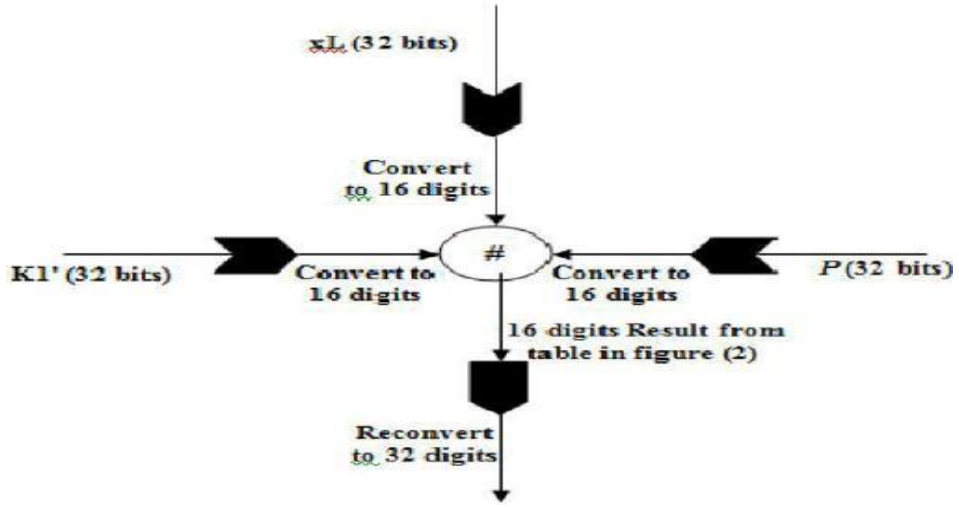

Fig 3: Modified DES Algorithm

3. **Substitution:** The 48-bit result is split into eight 6-bit words which are substituted in eight parallel 6x4-bit S-boxes. All eight S-boxes are different but have the same special structure.
4. **Permutation (P):** The resulting 32 bits are reordered according to a fixed permutation before being sent to the output.

The modified R Block is then XORED with L Block and the resultant fed to the next R Block register. The unmodified R Block is fed to the next L Block register. With another 56 bit derivative of the 64 bit key, the same process is repeated. [6]

1. The plaintext block is subject to an Initial Permutation to shift the bits around.
2. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
3. The plaintext and key are processed in 16 rounds consisting of:
   - 3.1. The key is split into two 28-bit halves.
   - 3.2. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
   - 3.3. The halves are recombined and subject to a Compression Permutation to reduce the key from 56 bits to 48 bits. This Compressed Key is used to encrypt this round's plaintext block.
   - 3.4. The rotated key halves from step 2 are used in next round.
   - 3.5. The data block is split into two 32-bit halves.
   - 3.6. One half is subject to an Expansion Permutation to increase its size to 48 bits.
   - 3.7. Output of step 6 is exclusive-OR with the 48-bit compressed key from step 3.
   - 3.8. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
   - 3.9. Output of step 8 is subject to a P-box to permute (scramble) the bits.
   - 3.10. The output from the P-box is exclusive-OR with the other half of the data block.
   - 3.11. The two data halves are swapped and become the next round's input.

III. DATA ENCRYPTION SYSTEM

A new method to enhance the performance of the Data Encryption Standard (DES) algorithm. This is done by replacing the predefined XOR operation applied during the 16 round of the standard algorithm by a new operation depends on using two keys, each key consists of a combination of 4 states (0, 1, 2, 3) instead of the ordinary 2 state key (0, 1). This replacement adds a new level of protection strength and more robustness against breaking methods.

The new operation needs 3 inputs, the first one specify the table number that should be used to calculate the result among the 4 tables, the other 2 inputs define the row and column number in the specified table where the cross point of them gives the result.[1]

IV. ENHANCED DES ALGORITHM

A new method to enhance the performance of the Data Encryption Standard (DES) algorithm. This is done by replacing the predefined XOR operation applied during the 16 round of the standard algorithm by a new operation depends on using two keys, each key consists of a combination of 4 states (0, 1, 2, 3) instead of the ordinary 2 state key (0, 1). This replacement adds a new level of protection strength and more robustness against breaking methods.

The new operation needs 3 inputs, the first one specify the table number that should be used to calculate the result among the 4 tables, the other 2 inputs define the row and column number in the specified table where the cross point of them gives the result.[1]

V. PROPOSED DES ALGORITHM

This research proposed a new improvement to the DES algorithm. The 64 bit data of the plain text message is input to the initial Permutation Function (IP). The initial permutation is rearranging the bits. Output of IP is divided into two halves. One is left half ‘L’ and another is right half ‘R’. Each half is consisting of 32 bits. Right half is input to the Expansion Function. R input is first expanded to 48 bits by using a table that defines a permutation plus an expression that involves duplication of 16 of the R bits. The resulting 48 bits are XORed with Ki, which consist of 48 bit.

Initially Ki is 64 bit key from which each 8th parity bit of each byte is discarded, which is the Permuted Choice-1 function. And key will become of 56 bits. 56 bit key is divided into two halves. Left half which is Ci and Right half is Di. At each round Ci and Di are separately subjected to a circular left shift, rotation, of 1 or 2 bits. Shifted values serve as input to the next round. Now shifted Ci and shifted Di will be the input to the Permuted Choice-2 function. Output of Permuted Choice -2 function is 48 bit, which is the input to the XOR function.

The output of XORed is 48 bits which the input to the Substitution Function. Output of this function is 32 bit. The substitution function is consists of 6 S-BOX. Each S-BOX has 8 bit of input and 32 bit of output. Perform the XOR operation between the first and second S-BOX output. Output of XOR operation is XORed with the output of the 3rd S-BOX. And output of XOR operation is XORed with the output of 4th S-BOX. Output of this XOR operation is XORed with the output of the 5th S-BOX. Output of the XOR operation is XORed with the 6th S-BOX output.

From the input to the Expansion to the output of last ADD operation is worked as “F” Function.

Algorithm of modified data encryption standard with 16 state operations is given below. [7]

INPUT: plaintext m1…m64; 64-bit two keys K=k1…. k64 and K'=k1'….k64' (includes 8 parity bits).

OUTPUT: 64-bit cipher text block C=c1…c64.

1. (Key schedule) Compute sixteen 48-bit round keys Ki, from K.
   1.1. (key schedule) compute sixteen 32-bit round keys KI', from K'
2. (L0, R0) ← IP (m1, m2, … m64)
   (Use IP Table to permute bits; split the result into left and right 32-bit halves L0=m58, m50… m8,R0=m57,m49… m7)
3. (16 rounds) for i from 1 to 16, compute Li and Ri as follows:
   3.1. Li=Ri-1
   3.2. Ri = Li-1 # f (Ri-1, Ki)
   Where, f(Ri-1, Ki) = P(S(E(Ri-1) Å Ki)), computed as follows:
   a. Expand Ri-1 = r1r2 . 32 from 32 to 48 bits. T ← E(Ri-1).(Thus T= r32r1r2.. r32r1.)
   b. T' ← T XOR Ki . represent T' as eight 6-bit character strings: T' = (B1 . . . B8)
   c. T" ← F where Function F = (((((((S1+S2) mod 2 ^ 32) XOR S3) + S4) mod 2^32) XOR S5) +S6)mod 2^32 Here, Si(Bi) maps to the 8 bit entry in row r and column c of Si
   d. T"' ← P(T"). (Use P per table to permute the 32 bits of T"=t1, t2 …t32, yielding t16t7 . t25.) and the operation # in Ri = Li-1 # f (Ri-1, Ki) is computed as follows:

      I. Convert the 32 bits resulted from f (R i-1, Ki) into 16-states 8 digits call it 'f'.
      II. Convert the 32 bits of Li-1 to 16-states 8 digits call it Li-1'
      III. Convert the 32 bits of Ki' to 16-states 8 digits call it Ki"
      IV. Compute Ri by applying the # operation on f ', Li-1', and Ki" according to truth tables shown in Table.

4. b1b2 . . . b64 ← (R8, L8). (Exchange final blocks L8, R8.)
5. C ← IP-1 (b1b2 . . . b64). (Transpose using IP-1 C = b40b8 . . . b25.)
6. End.

Proposed model of Enhanced Multi State DES Algorithm is shown below.

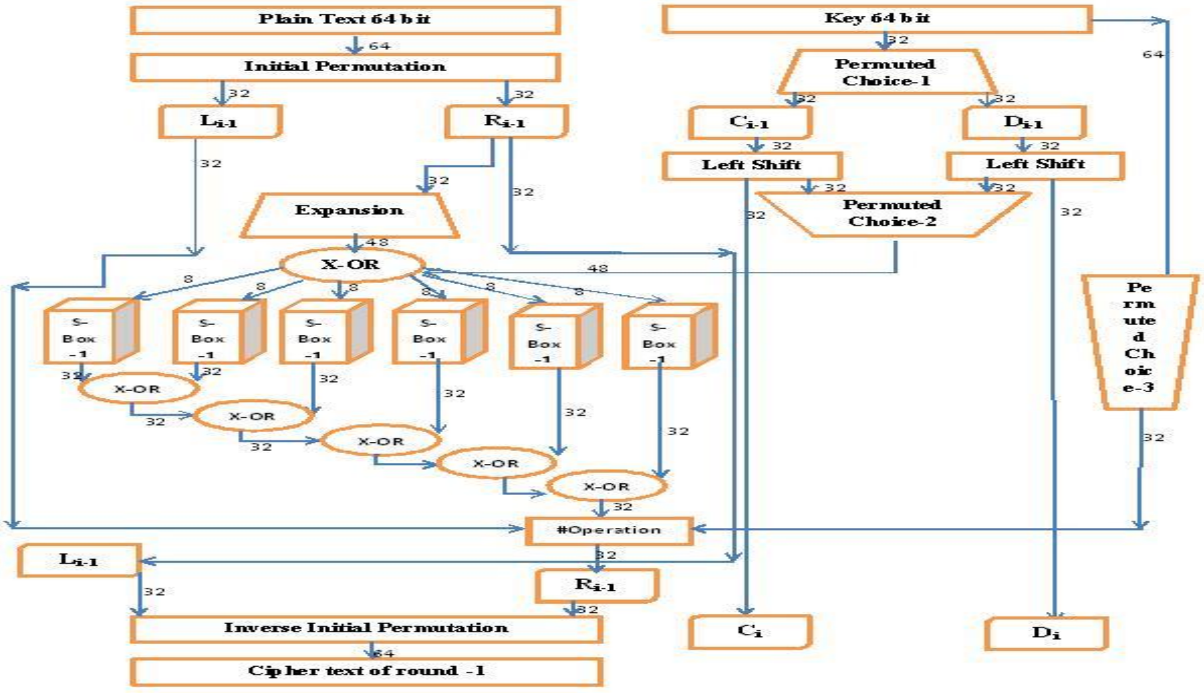

Fig 4: Proposed Model

Let’s take one example using proposed algorithm. Our Input Message is 41427A36313E5254 which is our plain text is converting into cipher text using this proposed algorithm. Here, there are 16 rounds for convert plain text to cipher text. In each round it contain two keys. First we convert plain text into binary format also we have to convert key into binary format which is also in hex format. Now, performing all operation of this proposed algorithm and get the cipher text.

The substitution function is consists of 6 S-BOX. Each S-BOX has 8 bit of input and 32 bit of output. Perform the XOR operation between the first and second S-BOX output. Output of XOR operation is XORed with the output of the 3rd S-BOX. And output of XOR operation is XORed with the output of 4th S-BOX. Output of this XOR operation is XORed with the output of the 5th S-BOX. Output of the XOR operation is XORed with the 6th S-BOX output.

```
Step 1. keys: K = 4135235951463231 Data: P =41427A36313E5254
Step 2. Initial Permutation of Message which is given by User.
Step 3. for i =1 to 16 round Ln = Rn-1
            Rn = Ln-1 # f(Rn-1,Kn)
Step 4. After complete one round we got F1 = R1 = EA67369D
            L1 = 11A8FCC7
At the end of 16th round, Inverse Permutation is
```

```
10000011      00010011      01011011      01101000
11001001      01101000      00001111      01101010
```

So, finally we got our cipher text 41CA793E91BE7074.

VI. RESULTS AND COMPARISION

Compare proposed enhanced multi state DES algorithm with original des algorithm, we got good avalanche effect and also solve cryptanalysis attack.

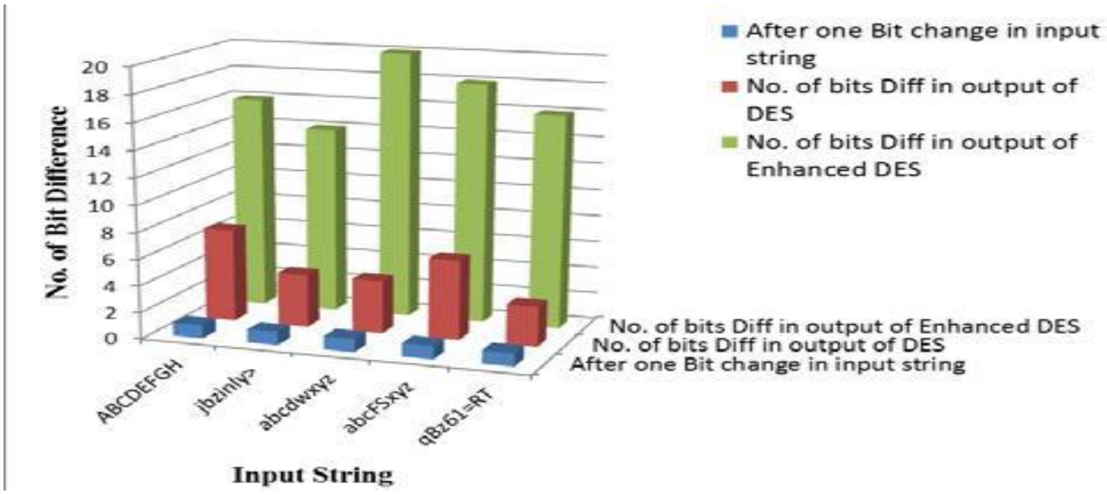

Fig 5: Avalanche effect of 64 bit of input Data for DES and Enhanced DES with multi state logic

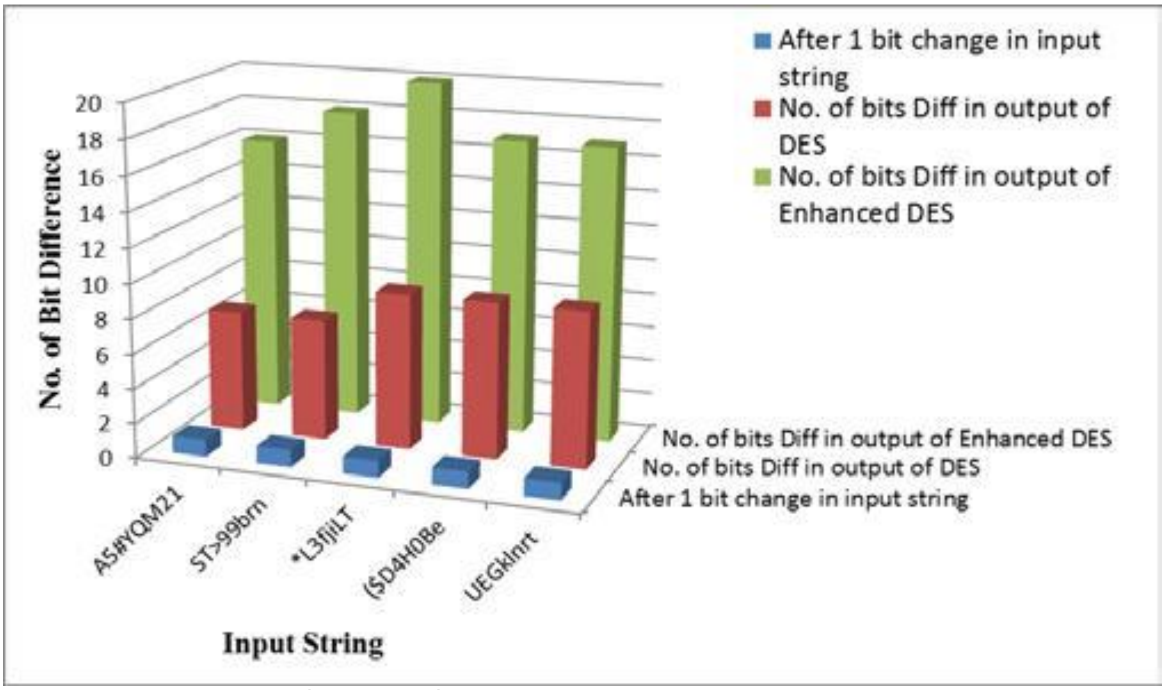

Fig 6: 64 bit of input key for DES and Enhanced DES with multi state logic

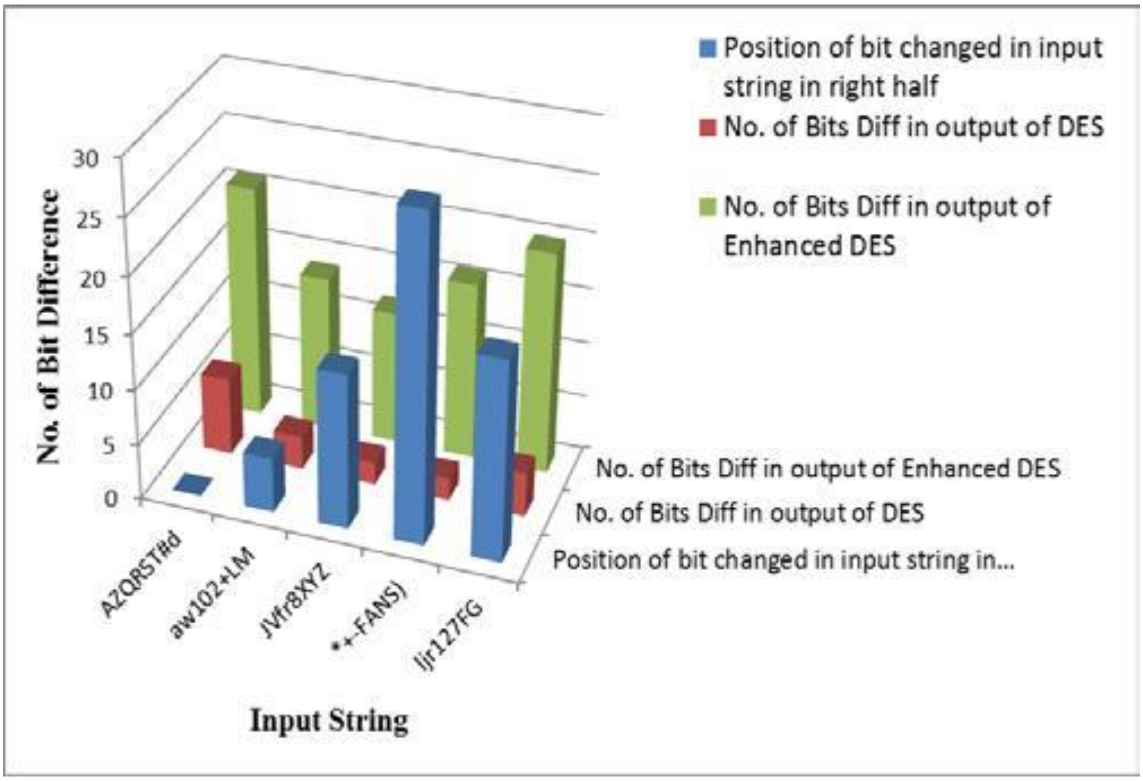

Fig 7: SAC of 'F' Function for DES and Enhanced DES with multi state logic

VII. CONCLUSION

The volume of information exchanged by electronic means such as internet, wireless phones, Fax, etc. is increasing very rapidly. It is very serious that information through internet, an enormous computer network, is vulnerable to hackers and that privacy of wireless phones without security can be invaded. We should develop improved cryptosystems to provide greater security.

Proposed algorithm in this paper has been designed the DES-like cryptosystem called the Enhanced Multi State DES. It extends the DES algorithm so that the iterative number of the f function during the full 16 round of each sub-block is different, in order to decrease the probability of the full 16 round characteristic against the differential cryptanalysis. Summary of Enhanced algorithm are:

i. Creating the S-BOX design as complex as possible so it will create the good avalanche effect. Because in S-Box design there is a 8 bit of input and 32 bit of output.(Extra 24 bits)

ii. Number of combination of key 256 * 232 to decipher plaintext. It hard to do brute force attack.

iii. Increasing the number of states for presenting the information, will increasing the number of combination of the information so it will be the hard for the intruder to detect the actual information.

Value extracted from hash table is depends on the plaintext message, not any particular pattern.

REFERENCES

[1] K. Anchugam and M. Tamilselvi, “New Data Encryption Standard Algorithm”, IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.4, April 2013.

[2] Prashanti G., Dipti S, Sandhya Rani K., “A Novel Approach for Data Encryption Standard Algorithm”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013.

[3] Devendra Kumar Malakar, Prof. Dineshchandra Jain, CSE Department, Shri Vaishnav Institute of Technology and Science, Indore, Madhya Pradesh, India, “The Problem Analysis on Encryption Techniques in Cryptography”, International Journal of Societal Applications of Computer Science Vol 2, Issue 5 May 2013, ISSN 2319 – 8443.

[4] M. A. Al Zain and E. Pardede, “Using Multi Shares for Ensuring Privacy in Database-as-a-Service”, 44th Hawaii, International Conference on System Sciences (HICSS), 2011, pp 1-9. doi:10.1109/HICSS.2011.478

[5] Dr. Mohammed M. Alani College of Computer Engineering and Sciences, Gulf University, Kingdom of Bahrain, “DES96 - Improved DES Security”, 7th International Multi-Conference on Systems, Signals and Devices, IEEE 2010.

[6] Akhil Kaushik Assistant Professor, Computers Department, Manoj Bamela Assistant Professor, Electronics Department, AnantKumar B.Tech Pre-final, Computers Engineering from T.I.T&S College Bhiwani, Haryana, India, “Block Encryption Standard for Transfer of Data”, International Conference on Networking and Information Technology, IEEE 2010.

[7] W. Stallings, “Cryptography and Network Security: Principles and Practices, 4th ed., Prentice Hall”.

[8] https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf