International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 7, Issue 10 (July 2013), PP. 11-20

Performance Analysis of Data Encryption Standard Algorithm & Proposed Data Encryption Standard Algorithm

Shah Kruti Rakeshkumar.[1]
[1]Babariya Institute of Technology, Assistant Professor

Abstract:- The principal goal guiding the design of any encryption algorithm must be security against unauthorized attacks. Within the last decade, there has been a vast increase in the accumulation and communication of digital computer data in both the private and public sectors. Much of this information has a significant value, either directly or indirectly, which requires protection. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. Performance and security level is the main characteristics that differentiate one encryption algorithm from another. Here introduces a new method to enhance the performance of the Data Encryption Standard (DES) algorithm is introduced here. 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.

Keywords:- DES, Encryption,Decryption,SAC

I. INTRODUCTION

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 process of converting plain text "unhidded" to a cryptic text "hidded" to secure it against data thieves. This process has another part where cryptic text needs to be decrypted on the other end to be understood in figure 1.

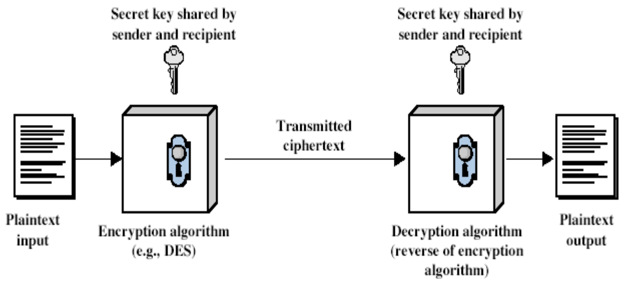

Fig. 1: Encryption/Decryption

Cryptography Goals :[2]

1. CONFIDENTIALLY : Information in computer transmitted information is accessible only for reading by authorized parties.
2. AUTHENTICATION- Origin of message is correctly identified with an assurance that identity is not false.
3. INTERGRITY- Only authorized parties are able to modify transmitted or stored information.
4. NON REPUDIATION- Requires that neither the sender, nor the receiver of message be able to deny the transmission.
5. ACCESS CONTROL- Requires access may be controlled by or for the target system.
6. AVAILIBILITY- Computer system assets are available to authorized parties when needed.

II. DATA ENCRYPTION STANDARD

Without doubt the first and the most significant modern symmetric encryption algorithm is that contained in the Data Encryption Standard (DES).The DES was published by the United States' National Bureau of Standards in January 1977 as an algorithm to be used for unclassified data (information not concerned with national security). The Data Encryption Standard (DES), as specified in FIPS Publication 46-3, is a block cipher operating on 64-bit data blocks. The encryption transformation depends on a 56-bit secret key and consists of sixteen Feistel iterations surrounded by two permutation layers: an initial bit permutation *IP* at the input, and its inverse IP^{-1} at the output. The structure of the cipher is depicted in Figure 2. The decryption process is the same as the encryption, except for the order of the round keys used in the Feistel iterations.[12]

The 16-round Feistel network, which constitutes the cryptographic core of DES, splits the 64- bit data blocks into two 32-bit words, LBlock and RBlock (denoted by $L0$ and $R0$). In each iteration (or round), the second word Ri is fed to a function ***f*** and the result is added to the first word Li. Then both words are swapped and the algorithm proceeds to the next iteration. The function f of DES algorithm is key dependent and consists of 4 stages.

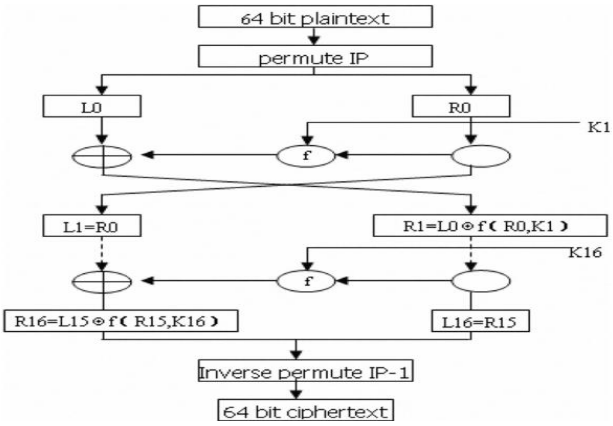

Fig. 2:DES Algorithm

1. Expansion (*E*):The 32-bit input word is first expanded to 48 bits by duplicating and reordering half of the bits.[11]
2. Key mixing : The expanded word is XORed with a round key constructed by selecting 48 bits from the 56-bit secret key, a different selection is used in each round.
3. Substitution. The 48-bit result is split into eight 6-bit words which are substituted in eight parallel 6×4-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 RBlock is then XORED with LBlock and the resultant fed to the next RBlock register.The unmodified RBlock is fed to the next LBlock register. With another 56 bit derivative of the 64 bit key, the same process is repeated.

III. IMPROVED 4-STATES OPERATION

To increase the security and key space, that makes the encryption algorithms more robustness to the intruders, a new manipulation bits process has been added in by using different truth table for manipulation bits process work on 4- states (0,1,2,3) , while the traditional binary process (XOR) work on (0, 1) bits only. The symbol # has been used to refer to the operator that execute this process use truth tables that shown in figure 3.[7]

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.

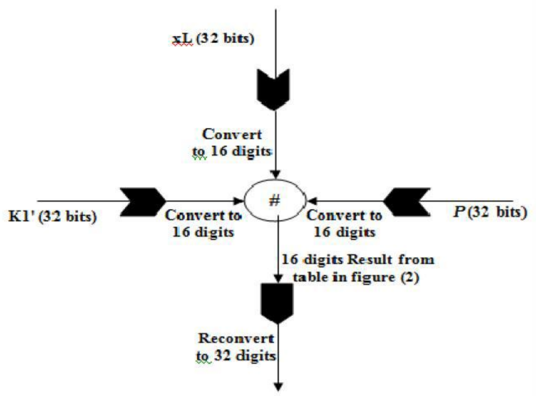

Fig. 3: Design of Modified DES Algorithm

Here, example for # operation, this operation need 3 inputs, first one specify the table number that should be used to calculate the result among the four truth tables as shown in Table 1, the other 2 inputs define the row and column number in the specified table where the cross point of them gives the result this result is in 16 digits.

Input in 32 bit binary format 10010111010100101010011110100010 01 which is converted into the number
2 1 1 3 1 1 0 2 2 2 1 3 2 2 0 2 1

Input 1: 0 1 3 0 1 2 2 3 1
Input 2: 3 2 2 1 0 1 2 1 1
Input 3: 1 0 0 2 1 3 2 1 2
Result : 3 0 2 3 1 2 2 2 2

#0	0	1	2	3	#1	0	1	2	3
0	3	2	1	0	0	0	1	2	3
1	2	3	0	1	1	1	0	3	2
2	1	0	3	2	2	2	3	0	1
3	0	1	2	3	3	3	2	1	0

#2	0	1	2	3	#3	0	1	2	3
0	2	3	0	1	0	1	0	3	2
1	3	2	1	0	1	0	1	2	3
2	0	1	2	3	2	3	2	1	0
3	1	0	3	2	3	2	3	0	1

Table: Truth Table

IV. PROPOSED ALGORITHM OF DES

This research proposed a new improvement to the DES algorithm. The proposed improvement makes use of the new operation defined in the previous section, operation (#) applied during each round in the original DES algorithm, where another key is needed to apply this operation, this key may come in binary form and convert to a 4-states key. Here, originally DES algorithm linear cryptanalysis and differential cryptanalysis attacks are heavily depends on the S-box design.

Consequently, multiple keys will be used in each round of the original DES, the first key Ki will be used with the ***f*** function. The second key will be the first input to the # operation, the second input will be the output of the ***f*** function, and the third input to the # operation will be the value Li, Algorithm shows the three 32-bits input to the # operation ,and the 32-bits output, with places needed to convert these 32- bits to 16-digits. These three inputs to the # operation should be firstly converted from 32 bits to a 16 digits each may be one of four states (0,1,2, 3), i.e., each two bits converted to its equivalent decimal digits.
Algorithm of modified data encryption standard with 4 state operation :

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

OUTPUT:- 64-bit ciphertext block C=c1 . . .c64.
1. (key schedule) Compute sixteen 48-bit round keys Ki, from K.
2. (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 right32-bit halves L0=m58m50 . . . m8,R0=m57m49 . . . 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* (R i-1, Ki) where *f*(Ri-1, Ki) = P(S(E(Ri-1) Å Ki)), computed as follows:
(a) Expand Ri-1 = r1r2 . . . r32 from 32 to 48 bitsT_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
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 inrow r and column c of Si
(d)T"' _P(T"). (Use P per table to permute the 32 bits of T"=t1t2 . . . t32,

yielding t16t7 . . . t25.)
and the operation # in Ri = Li-1 # *f* (R i-1, Ki) is computed as follows:
(a) convert the 32 bits resulted from *f* (R i-1, Ki) into 4-states 16 digits call it***f '***
(b) convert the 32 bits of Li-1 to 4-states 16 digits call it Li-1'
(c) convert the 32 bits of Ki' to 4-states 16 digits call it Ki"
(d) compute Ri by applying the # operation on *f* ', Li-1', and Ki" according to truth tables shown in figure
4. b1b2 . . . b64 _ (R16, L16). (Exchange final blocks L16, R16.)
5. C _ IP-1 (b1b2 . . . b64). (Transpose using IP-1 C = b40b8 . . . b25.)
6. End.

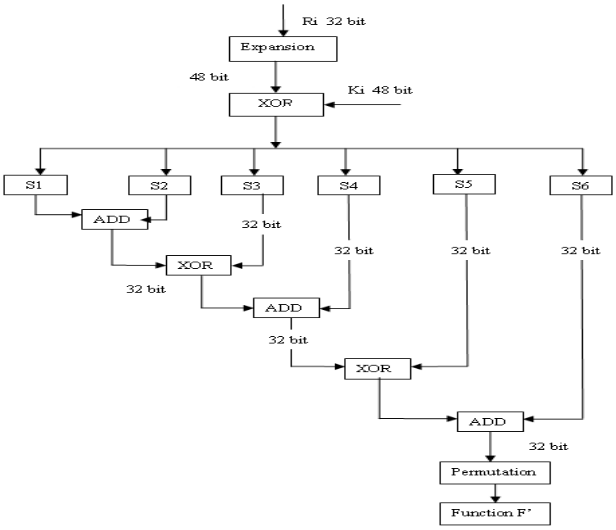

Fig. 4: Function F Design

V. TEST RESULTS.

In order to study the performance, the algorithm has been tested on an Intel based machine running Microsoft Windows 7 with a 2.50 GHz Intel Core 2 i5 processor and 4 GB of main memory. The algorithm is developed on JAVA with Net Beans 6.9 software. The proposed algorithm has been extensively tested for avalanche effect and SAC. Both the criterion tested on proposed algorithm and is compared with original algorithm. The following subsections show the experimental results.

Test Results of Avalanche Effects

SR NO.	Original Secret Key	Modified Secret Key	DES Algorithm	Proposed DES Algorithm
1	05771BBAA FCDE9F3	15771BBAAF CDE9F3	480	487
2	56AD1230E FAD1790	46AD1230EF AD1790	470	483
3	109ADE987 211ADFB	109ADC9872 11ADFB	490	498
4	23ACB259A BD56890	03ACB259A BD56890	485	500
5	09ADFB553 3129FFD	29ADFB5533 129FFD	461	490
6	AADDFF33 221290AB	AADDFF332 21290A3	446	498
7	BADF09135 789225A	2ADF091357 89225A	447	467
8	AB1298DA 3968235A	8B1298DA39 68235A	463	472
9	1159023AD	5159023ADE	486	497

	EAF2215D	AF2215D		
10	23AD5A9D 3B68F0D12	03AD5A9D3 B68F0D12	470	492
11	198012876A DFBDEAB	398012876A DFBDEAB	450	475
12	01929687A BADB1098	03929687AB ADB1098	462	492
13	0578AABC DFF4311E	4578AABCD FF4311E	482	499
14	FF0795AB1 CD54296	FF0795AB1C D54292	462	483
15	0379ACEFF BB0D152	0379ACEFFB B0D142	475	524
16	5912ADE98 70ABF98	5912ADEB87 0ABF98	470	503
17	ABD198254 0FEAD01	ABD1982540 FEAF01	439	468
18	24680ADF1 3579ADE	04680ADF13 579ADE	456	477
19	A13DE0981 358319A	213DE098135 8319A	445	509
20	DFCA19093 5ADF013	5FCA190935 ADF013	480	522
21	01ADF2987 65ABCDE	01ADF298F6 5ABCDE	456	504
	Average		467.92	492.04

Table 1 :One bit change in key

SR NO.	Original Secret Key	Modified Secret Key	DES Algorithm	Proposed DES Algorithm
1	13345779 9BBCDFF 1	133457799 BBCDFF2	484	493
2	11345766 89ACCBE E	2134576689 ACCBEE	446	495
3	1453699A AFF00DC 2	1453699AA FF00DC7	479	485
4	7564133A EFF0BCD 1	F564133AE FF0BCD3	458	469
5	05771BB AAFCDE 9F3	25771BBA AFCDE9F1	459	469
6	56AD123 0EFAD17 90	77AD1230E FAD1790	485	499
7	109ADE9 87211AD FB	909ADC987 211ADFB	479	492
8	23ACB25 9ABD568 90	73ACB259 ABD56890	465	489
9	09ADFB5 533129FF	69ADFB55 33129FFD	450	475

	D			
10	AADDFF 33221290 AB	ABDDFF33 221290A3	446	498
11	BADF091 35789225 A	BADF0919 5789225A	459	472
12	AB1298D A3968235 A	9B1298DA3 968235A	467	505
13	1159023A DEAF221 5D	115902FAD EAF2215D	492	506
14	23AD5A9 D3B68F0 D12	23AD5C9D 3B68F0D12	485	490
15	19801287 6ADFBD EAB	198012876 ADF8DEA B	454	489
16	01929687 ABADB1 098	01929687F BADB1098	460	482
17	0578AAB CDFF431 1E	0578AA94 DFF4311E	458	490
18	FF0795A B1CD542 96	FF0795AB0 4D54296	474	499
19	0379ACE FFBB0D1 52	0379ACEFF 3B0D142	488	499
20	5912ADE 9870ABF 98	5912ADEB 870ABF90	468	497
21	ABD1982 540FEAD 01	2BD198254 0FEAF03	478	511
	Average		468.56	492.52

Table 2 : Two bit change in key

SR NO.	Original Secret Key	Modified Secret Key	DES Algorithm	Proposed DES Algorithm
1	13345779 9BBCDFF 1	033457799 BBCDFF2	483	521
2	11345766 89ACCBE E	0134576689 ACCBE8	482	492
3	1453699A AFF00DC 2	D453699A AFF00DC3	481	490
4	7564133A EFF0BCD 1	6764133AE FF0BCD3	455	482
5	05771BB AAFCDE	20771BBA AFCDE9F3	486	492

	9F3			
6	56AD1230EFAD1790	56881230EFAD1790	481	502
7	109ADE987211ADFB	609ADE987211ADFB	487	500
8	23ACB259ABD56890	03ACB259A8D56890	488	497
9	09ADFB5533129FFD	29ADFA553B129FFD	480	490
10	AADDFF33221290AB	AADDF833221290A3	472	498
11	BADF09135789225A	BADF09F35789225A	487	498
12	AB1298DA3968235A	AB1248DA3968235A	481	506
13	1159023ADEAF2215D	11590D3ADEAF2215D	464	481
14	23AD5A9D3B68F0D12	23AD5A9D3FE9F0D12	479	496
15	198012876ADFBDEAB	F98012876ADFBDEAB	485	500
16	01929687ABADB1098	01929687AB2F31098	460	507
17	0578AABCDFF4311E	0570FABCDFF4311E	466	500
18	FF0795AB1CD54296	FF0795AB1C414296	469	489
19	0379ACEFFBB0D152	0379ACE7EAB0D152	477	487
20	5912ADE9870ABF98	1912ADED870ABF9C	466	488
21	ABD1982540FEAD01	ABD19825C8BEAD01	476	500
22	24680ADF13579ADE	24680AD792579ADE	486	501
23	A13DE0981358319A	A13DE09F1358319A	474	503
24	DFCA190935ADF013	DFCA190935ADF152	469	500

25	01ADF29 8765ABC DE	01A9F2987 64AB4DE	490	504
	Average		476.9 6	496.96

Table 3 : Three bit change in key

Now another criterion for testing on proposed DES algorithm is SAC which states that any output bit *j* of an S-box should change with probability ½ when any single input bit *i* is inverted for all *i, j*. The SAC is one of the design criterions for function f. Such S-Boxes exhibit which is generally referred to as Good Avalanche Effect, where inverting any input bit i causes approximately half of the output bits to be inverted, this is equivalent to good Diffusion.

Here, In SAC when we given 48 bits input to the function F and perform all operation in function F after that we got 32 bits output. In those 32 bits output data numbers of bits are change when we change 1 or more bits change in input data.

Now, we saw when we change one bit in input data at that time number of bits are change. The following Table shows the SAC results when change one bit in input data.

SR No	**DES**	**Proposed DES**	**DES Results(%)**	**Proposed DES Results (%)**
1	2	17	6.25	53.125
2	2	16	6.25	50
3	2	20	6.25	62.5
4	3	15	9.375	46.875
5	4	17	12.5	53.125
6	2	17	6.25	53.125
7	3	20	9.375	62.5
8	2	16	6.25	50
9	2	16	6.25	50
10	2	16	6.25	50
11	3	18	9.375	56.25
12	2	18	6.25	56.25
13	4	17	12.5	53.125
14	2	16	6.25	50
15	3	16	9.375	50
16	2	18	6.25	56.25
17	2	17	6.25	53.125
18	2	17	6.25	53.125
Average	2.444	17.055	7.639	53.298
Difference	14.611		45.659	

Table 4 : SAC 1 bit change in input data to function F

SR No	**DES**	**Proposed DES**	**DES Results(%)**	**Proposed DES Results(%)**
1	2	19	6.25	59.375
2	2	20	6.25	62.5
3	5	23	15.625	71.875
4	2	18	6.25	56.25
5	1	15	3.125	46.875
6	3	21	9.375	65.625

7	2	19	6.25	59.375
8	2	17	6.25	53.125
9	2	15	6.25	46.875
10	2	17	6.25	53.125
11	5	18	15.625	56.25
12	2	17	6.25	53.125
13	1	18	3.125	56.25
14	1	15	3.125	46.875
15	3	19	9.375	59.375
16	1	20	3.125	62.5
17	2	18	6.25	56.25
18	2	15	6.25	46.875
Average	2.222	18	6.94	56.25
Difference	15.777		49.30	

Table 5 : SAC 2 bits change in input data to function F

When we change one bit in an input at that time number of output bits are change in original DES 7.638% ratio and modified DES 53.2986% ratio. So, finally difference between original DES and proposed DES is 45.69%

When we change two bits in an input at that time number of output bits are change in original DES 6.94% ratio and modified DES 56.25% ratio. So, finally difference between original DES and proposed DES is 49.305%.

VI. CONCLUSION

As we toward a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique. DES is now considered to be insecure for some applications like banking system. there are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable. By adding additional key, modified S-Box design, modifies function implementation and replacing the old XOR by a new operation as proposed by this thesis to give more robustness to DES algorithm and make it stronger against any kind of intruding. DES Encryption with two keys instead of one key already will increase the efficiency of cryptography.

ACKNOWLEDGMENT

I take this opportunity to acknowledge those who have been great support and inspiration through the research work. My sincere thanks to Prof. Bhavika Gambhava for her diligence, guidance, encouragement and help throughout the period of research, which have enabled me to complete the research work in time. I express my deep sense of gratitude to Prof. C. K. Bhensdadia, Professor and Head of Computer Engineering Department of Dharmsinh Desai University, Nadiad, Gujarat for providing the necessary facilities during the research and encouragement from time to time. I also thank him for the time that he spread for me, from his extreme busy schedule. Special thanks to the institute, Dharmsinh Desai University, for giving me such a nice opportunity to work in the great environment. Thanks to my friend and colleague who have been a source of inspiration and motivation that helped to me during my dissertation period. And to all other people who directly or indirectly supported and help me to fulfill my task. Finally, I heartily appreciate my family members for their motivation, love and support in my goal.

REFERENCES

[1] National Bureau of Standards – Data Encryption Standard, Fips Publication 46,1977.

[2] O.P. Verma, Ritu Agarwal, Dhiraj Dafouti,Shobha Tyagi " Performance Analysis Of Data Encryption Algorithms " , 2011

[3] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha " Performance Evaluation of Symmetric Cryptography Algorithms, IJECT, 2011.

[4] Diaa Salama, Abdul Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhound " Performance Evaluation of Symmetric Encryption Algorithm ", IJCSNS, 2008

[5] Dr. Mohammed M. Alani " Improved DES Security" ,International Multi-Conference On System, Signals and Devices, 2010

[6] Tingyuan Nie, Teng Zhang " A Study of DES and Blowfish Encryption Algorithm",TENCON, 2009

[7] Afaf M. Ali Al- Neaimi, Rehab F. Hassan " New Approach for Modified Blowfish Algorithm Using 4 – States Keys" , The 5th International Conference On Information Technology,2011

[8] J.Orlin Grabbe "The DES Algorithm Illustrated"

[9] Dhanraj, C.Nandini, and Mohd Tajuddin " An Enhanced Approch for Secret Key Algorithm based on Data Encryption Standard", International Journal of Research And Review in Computer Science, August 2011

[10] Gurjeevan Singh, Ashwani Kumar, K.S. Sandha "A Study of New Trends in Blowfish Algorithm ", International Journal of Engineering Research and Application,2011

[11] W. Stallings, Cryptography and Network Security: Principles and Practices, 5th ed., Prentice Hall, 1999.

[12] B.Scheier, Applied Cryptography : Protocols, Algorithms and Source Code in C,2nd ed.., John Wiley & Sons, 19995.