International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-5, June 2013

A Novel Approach for Data Encryption Standard Algorithm

Prashanti.G, Deepthi.S, Sandhya Rani.K

Abstract—Now a day's providing Security for data is complicated task we have so many security methods that are implemented and deployed but out of them few are using and serving the needs of society. And we can't say that any algorithm is perfect and avoids threats. The main goal of any design of any encryption algorithm must be security against unauthorized attacks. Within the last decade, data in both the private and public sectors are increased which requires Availability, Authentication, Confidentiality, Integrity. In this paper we are considering The DES algorithm that defines the mathematical steps that transform original text (plain text) into a cipher text (secret code) and also transform the cipher text back to the original text. Here introduces a new method to enhance the performance of the Data Encryption Standard (DES) algorithm. This is done by replacing the 8/32 S-Box instead of 6/4 S-Box. The output of each S-Box undergoes AND and XOR operation before going to the permutation P. In this paper we also proposed a new operation Addition modulo instead predefined XOR operation applied during the 16 round of the standard algorithm.

Index Terms— DES, Encryption, Decryption, asymmetric cryptography, symmetric cryptography.

I. INTRODUCTION

Cryptography**:** is usually referred to as the study of secret. It is probably most important aspect of communication security and is becoming increasingly important as a basic building block for computer security[3]. Data that can be read and understood without any special measures is called plaintext. The method of representing plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable form is called cipher-text. The process of reverting cipher-text to its original plaintext is called decryption. There are two techniques used for data encryption and decryption, which are:

Asymmetric Cryptography in this sender and recipient use different keys then it is known as asymmetrical or public key cryptography. The key used for encryption is called the public key and the key used for decryption is called the private key.

Manuscript published on 30 June 2013.
***** Correspondence Author (s)
Prashanti. G*, Computer Science & Engineering Department, Vignan's Lara Institute of Technology and Science, Vadlamudi, Guntur, India.
Deepthi. S, Computer Science & Engineering Department, Vignan's Lara Institute of Technology and Science, Vadlamudi, Guntur, India.
Sandhyarani. K, Computer Science & Engineering Department, Vignan's Lara Institute of Technology and Science, Vadlamudi, Guntur, India.

Symmetric Cryptography If sender and recipient use the same key then it is known as symmetrical or private key cryptography as shown in Fig 1. It is always suitable for long data streams. One of the symmetric block encryption algorithm is DES[9].

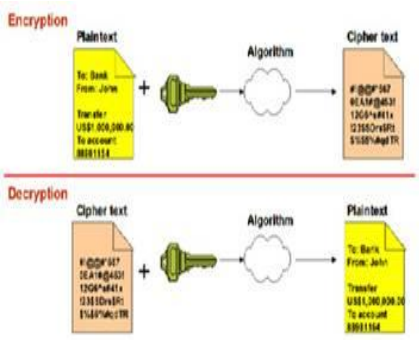

Fig. 1 Symmetric Key Encryption

Cryptography Goals: [2]

1. Confidentiality: 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. Integrity: 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. Availability: Computer system assets are available to authorized parties when needed

II. DATA ENCRYPTION STANDARD

The DES (Data Encryption Standard) algorithm is the most widely used encryption algorithm in the world [15]. For many years, and among many people, "secret code making" and DES have been synonymous. 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)[1]. The Data Encryption Standard (DES), as specified in FIPS Publication 46-3, is a block cipher operating on 64-bit data blocks as shown in Fig 2

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.[14] 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 *L*0 and *R*0). 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.

1. Expansion (*E*): The 32-bit input word is first expanded to 48 bits by duplicating and reordering half of the bits.[7]
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 R Block is then XORED with LBlock and the resultant fed to the next RBlock 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.

Pseudo Code: Data Encryption Standard:

INPUT: plaintext p1 . . . p64; 64-bit key 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.
   Note: Where k=64 bits out of which 8 parity bits are discarded outcome is 56 bits, after Left circular shift and PC2 which results 48 bit key.

2. (L0, R0) ←IP(p1, p2,. . .p64) (Use IP Table to permute bits; split the result into left and right 32-bit halves L0=p58p50 . . . p8,R0=p57p49 . . . p7)
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 XOR *f* (R i-1, Ki)

where *f*(Ri-1, Ki) = P(S(E(Ri-1) XOR Ki)), computed as follows:

(a) Expand Ri-1 = r32r1r2 . . . r32 r1 from 32 to 48 bits, M ←E(Ri-1).
(b) M' , ←M XOR Ki. Represent M ' as eight 6-bit character strings: M'= (B1 . . . B8)
(c) M " ← (S1(B1), S2(B2), . . . S8(B8)). Here Si(Bi) maps to the 4-bit entry in row r and column c of Si
(d) M"' ←P (M"). (Use P per table to permute the 32 bits of M"=m1m2 . . . m32, yielding m16m7 . . . m25)

4. b1b2 . . . b64 ← (R16, L16). (Exchange final blocks L16, R16.)
5. C ←IP^{-1} (b1b2 . . . b64).
6. End.

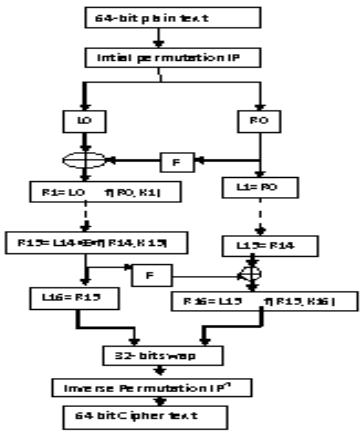

Fig. 2 DES Algorithm

III. PROPOSED DES ALGORITHM

In this paper we proposed a new improvement to the DES algorithm which makes the use of the new operation known as addition modulo (+).it takes two inputs and performs Addition and resulting output assume like x. later perform x mod 2^w Where w is the number of bits that depends on given input.

Example: x and y are the Inputs

X=1100 1000
Y=1000 1111
$X^{'1}$ is obtained by performing x+y
X^1= 1 0101 0111

Carry can be thrown off (or) perform modulo 2^8
X^1 is converted to decimal number
X^1= 343 mod 2^8 = 87
Binary equivalent of x^1 is 0101 0111
To find original x value perform following operation
$X=x^1+(-y)$
To obtain (-y) = 2^8-y =>256-143=113
Perform X^1+ (-y) which results
Original x

0111 0001
0101 0111

1100 1000 ⟵ original x value

The graphical representation of the proposed Des as shown in Fig.3

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

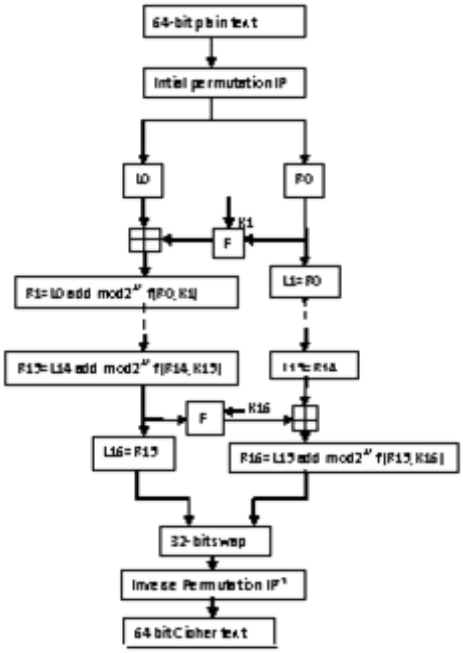

Fig. 3 Proposed DES Algorithm.

A. Algorithm of modified data encryption standard with addition modulo operation

INPUT: plaintext p1 . . . p64; 64-bit key 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.

Note: Where k=64 bits out of which 8 parity bits are discarded outcome is 56 bits, after Left circular shift and PC which results 48 bit key.

2. (L0, R0) ←IP (p1, p2,. . .p64) (Use IP Table to permute bits; split the result into left and right 32-bit halves L0=p58p50 . . . p8,R0=p57p49 . . . p7)
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 additionmodulo2^{32} f (R i-1, Ki)

where f(Ri-1, Ki) = P(S(E(Ri-1) XOR Ki)), computed as follows:
(a)Expand Ri-1 = r32r1r2 . . . r32 r1 from 32 to 48 bits, M←E(Ri-1).
(b)M' ←M XOR Ki. Represent M ' as eight 6-bit character strings: M'= (B1 . . . B8)
(c)M " ← F' where function F'= ((((s1Λs2) XOR s3) Λ s4)XOR s5) Λ s6). Here si(Bi) maps to the 8/32 S-Box that consist of 256 entries.
(d)M"' ←P (M"). (Use P per table to permute the 32 bits of M"=m1m2 . . . m32, yielding m16m7 . . . m25)
4. b1b2 . . . b64 ← (R16, L16). (Exchange final blocks L16, R16.)
5. C ←IP^{-1} (b1b2 . . . b64).
6. End.

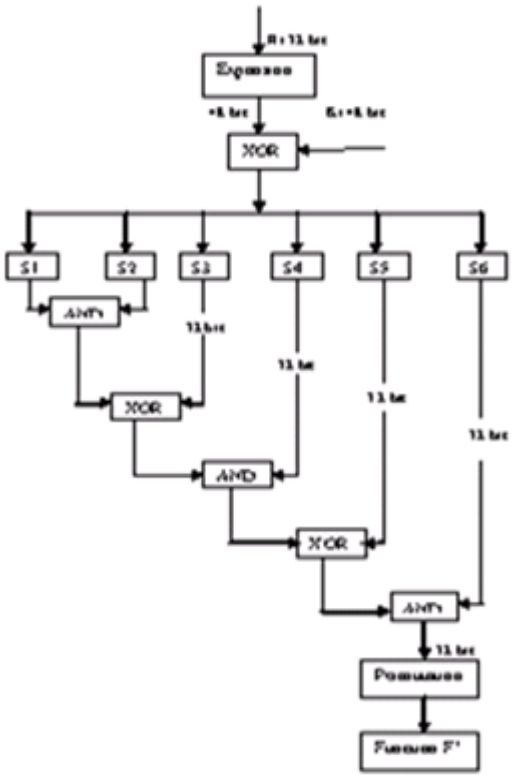

Fig. 4 Function F Design for proposed Algorithm

Here, using this proposed algorithm solve example. Our Input Message is 0123456789ABCDEF which is our plain text is converting into cipher text using this proposed algorithm. Here, the modified DES encrypts 64-bit blocks with a 56 bit key K. after an initial permutation of the bits, a plaintext block goes through 16 iterations (rounds) of a complex function and then passes through a final permutation that yields the cipher text block.
During each round i, the right half of the block is expanded to 48 bits and XORed with a 48 bit internal key Ki derived from K. the result then passes through 6 s-boxes which are nonlinear substitutions results 32 output bits from 8 input bits.
The 32 bit result undergoes AND, XOR operations and is then permuted and performs addition modulo2^{32} with left half of the block. As shown in Fig.4 Finally the two halves of the block are swapped before going through the next round.
After completing 16 rounds the result will be undergone for IP^{-1} and finally we will get cipher text of 64 bits length. For the input given above the following TABLE.I shows 16 rounds and resulting output.
Input: 0123456789ABCDEF
Output: E46037E66BA9FEB8

TABLE I: Result of proposed DES 16 Rounds

Round	Sub Key(Ki)	Left Bits(Li)	Right Bits(Ri)
IP		CC00CCFF	F0AAF0AA
1	1B02EFFC7072	F0AAF0AA	CE620D18

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

2	79AEB9DBC9EF	CE620D18	22D1F6C2
3	55FC8A426F99	22D1F6C2	DE6B4E29
4	72ADD6DB351D	DE6B4E29	AB5BFB24
5	7CEC07EB53AE	AB5BFB24	E4977040
6	63A53E507B2F	E4977040	2BB88B30
7	EC84B7F618BC	2BB88B30	2531F060
8	F78A3AC13BFB	2531F060	D0B8BCB2
9	E0DBEBEDE781	D0B8BCB2	7436155C
10	B1F347BA464F	7436155C	56FFC0E2
11	215FD3DED386	56FFC0E2	D66AAA00
12	7571F59467E9	D66AAA00	587FC4EA
13	97C4D1FABA41	587FC4EA	A6FFD004
14	5F43B7F2E73A	A6FFD004	FAA3CA30
15	BF918D3D3F0A	FAA3CA30	E9FFF05C
16	EB3D8B0E17F5S	E9FFF05C	5BC44D34

B. Avalanche Effect

A change in one bit of the plain text or one bit of the key should produce a change in many bits of the cipher text this is referred to as the Avalanche Effect.

The following example shows the result when the first bit of the plain text is changed that results more changes in the resulting bits of the cipher text.

Plain text: **1**123456789ABCDEF

↑

Altered Bit

TABLE II: Result of avalanche effect for proposed DES 1stRound

Round	Input	Left Bits(Li)	Right Bits(Ri)	δ
IP	0123456789ABCDEF1123456789ABCDEF	CC00CCFF CC01CCFF	F0AAF0AA F1AAF0AA	2
1	CC00CCFFF0AAF0AACC01CCFFF1AAF0AA	F0AAF0AA F1AAF0AA	CE620D18 CE1CCE19	6

IV. CONCLUSION

As we towards a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism. 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 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. This new algorithm gives avalanche effect than the original DES algorithm and also solves cryptanalysis attack

ACKNOWLEDGMENT

We take this opportunity to acknowledge those who have been great support and inspiration through the research work. Our sincere thanks to Mrs. B.Renuka Devi, head of the department of CSE to her diligence and motivation. Special thanks to Vignan's Lara Institute of Science and Technology, for giving us such a nice opportunity to work in the great environment and for providing the necessary facilities during the research and encouragement from time to time. Thanks to our colleagues who have been a source of inspiration and motivation that helped to us and to all other people who directly or indirectly supported and help us to fulfill our task. Finally, we heartily appreciate our family members for their motivation, love and support in our goal.

REFERENCES

[1] New Approach of Data Encryption Standard Algorithm Shah Kruti R., Bhavika Gambhava.
[2] J.Orlin Grabbe ―The DES Algorithm Illustrated‖
[3] W. Stallings, Cryptography and Network Security: Principles and Practices, 5th ed., Prentice Hall, 1999.
[4] The CAST-128 Encryption Algorithm. C. Adams, Entrust Technologies, May 1997. http://tools.ietf.org/pdf/rfc2144.pdf
[5] Cryptography And Network Security By Atul Kahate
[6] a simplified idea algorithm nick Hoffman http://www.nku.edu/~christensen/simplified%20IDEA%20algorithm.pdf
[7] Network security and cryptography by bernard menezes
[8] National Bureau of Standards – Data Encryption Standard, Fips Publication 46,1977.
[9] O.P. Verma, Ritu Agarwal, Dhiraj Dafouti,Shobha Tyagi ― Performance Analysis Of Data Encryption Algorithms ― , 2011.
[10] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha ― Performance Evaluation of Symmetric Cryptography Algorithms, IJECT, 2011.
[11] Diaa Salama, Abdul Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhound ― Performance Evaluation of Symmetric Encryption Algorithm ―, IJCSNS, 2008.
[12] Dr. Mohammed M. Alani ― Improved DES Security‖, International Multi-Conference On System, Signals and Devices, 2010.
[13] 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
[14] B.Scheier, Applied Cryptography: Protocols, Algorithms and Source Code in C,2nd ed.., John Wiley & Sons,1995.
[15] The DES 15 years of public scrutiny. dorothy e denning. http://faculty.nps.edu/dedennin/publications/DES-15Years.pdf

Prashanti.G is Assistant Professor at Department of Computer Science and Engineering, Vignan's Lara Institute of Technology and Science, Vadlamudi, Guntur, Andhra Pradesh, India. She has received her M.Tech degree from Vignan Engineering College, Vadlamudi,, Guntur, Andhra Pradesh, India

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Deepthi.S is Assistant Professor at Department of Computer Science and Engineering, Vignan's Lara Institute of Technology and Science, Vadlamudi, Guntur, Andhra Pradesh, India. She has received her B.Tech degree from K.L College of Engineering, Guntur, Andhra Pradesh, India in 2008. She has received her M.Tech degree from Nalanda Institute of Engineering and Technology, Guntur, Andhra Pradesh, India

Sandhya Rani.K is Assistant Professor at Department of Computer Science and Engineering, Vignan's Lara Institute of Technology and Science, Vadlamudi, Guntur, Andhra Pradesh, India. She has received her M.Tech degree from Vignan Engineering College, Vadlamudi,, Guntur, Andhra Pradesh, India

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)