Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Study of DES Standard, its Modes, Attacks and Variants

Anju[*]
SES, BPSMV,HARYANA
Haryana, India

Rajani Bala
SES, BPSMV,HARYANA
Haryana, India

Mrs. Sonal Beniwal
SES,BPSMV,HARYANA
Haryana, India

Abstract-Due to increases in technologies , Digital transmission become available. Multimedia data transmission increases day by day.Many application facilities and trasaction are done over internet . There should be some secret information that need security during transmission. Digital data are easy to copy and distribute. Due to this reason some standard algorithm introduced . In these America govt. for financial Applications and today widely used in various applications.Financial Company now replace DES by its Variant 3-DES.

Index Keyword:Cryptography, DES, 3-DES, Ciphertext, Plaintext, encryption, Decryption, Key.

I. Introduction

Cryptography is the study of various techniques for sending the data in distinct form so that only the intended receiver can recover the original data and read the data. Cryptography is the most important basic building block of data security.The requirements of security was arises due to two factor: first , the increased use of shared system like time sharing system and second, introduction of distributed system and network communication. Cryptography main goal is to keep sensitive data secure from unauthorized user.Cryptography need two basic element for encryption and decryption i.e encryption/decryption algorithm and key.On the basis of key two types of encryption is done.If the single key is used for both encryption and decryption then it is symmetric cipher(private key cryptography).On other side ,if pair of keys(public and private keys) is used, the private key used for encryption and public key used for decryption ,then it is asymmetric cipher(public key cryptography).In symmetric cipher a secure communication channel is used for transferring of secret key. But in asymmetric cipher,public key is known by everyone and private key is secret.So,there is no need for secure communication channel.On the basis of how data processed in algorithm, there is two different cipher. First, stream cipher:data processed as one byte at a time only.Second, block cipher: data processed as a collections of byte(block) at a time. In this paper,we review the DES(Data Encryption Standard).DES is a symmetric block cipher and most widely used encryption scheme on which various encryption standard is based.

II. Block Cipher

Block cipher operates on fixed length groups of bytes called block. During encryption, block cipher might take any size block(4,16 bytes etc) as input and produce corresponding same size output(4,16 bytes etc).Decryption is also same; the input and output block size is same as encryption.Block cipher is slow in process than stream cipher and memory requirement is also more.But keys are reusable and it is more effective for preknown data. For improving the effect of encryption algorithm, four “modes of operation” have been defined.Section 4 describe these modes.

III. DES

The NBS(National Bureau of Standard) today known as NIST(National Institute of Standard and Technology) proposed a project for standard encryption algorithm in 1972.The main focus of the project was to provide effective security to sensitive data during transmission over network.The director of ICST(Institute for Computer and Science Technology) R.M. Davis together with NSA(National security agency) evaluate the security of various cryptographic algorithm that would be accept as Federal Standard. In 1974, IBM submitted the result of WalterTuchman and Carl Meyer project with 64-bits block and key size 56-bits long and known as LUCIFER DES algorithm.NBS held two public workshops on LUCIFER DES algorithm mathematical and technical criterias.The output of that workshops was DES.

On 23 November,1977 NBS proposed the DES as FIPS-46(Federal Information Processing Standard).In 1981, DES was adopted by ANSI(American National Standard).DES algorithm take 64-bit block as plain text input and apply 56-bit key on input block , at the end produced 64-bit block cipher text.In decryption input is 64-bit cipher block and apply same 56-bit key to produced 64-bit plain text. DES is based on both Substitution and Transposition.

IV. Modes Of DES

In FIPS 81, define four modes of DES:
1.Electronic Codebook (ECB) mode
2.Cipher Block Chaining (CBC) mode
3.Cipher Feedback (CFB) mode
4.Output Feedback (OFB) mode.

5.Counter (CTR)Mode

NIST Publication 800-38A define this mode. These modes can be used with both DES and Triple DES.

ECB Mode : Each 64-bit plaintext block is encrypted and decrypted using same key.It is secure for smaller size data only(Figure1).Padding is also allowed in this mode.Each block is independent so no error propagation.

$$C1=E(K,P1)\ ,\ P1=D(K,C1).$$

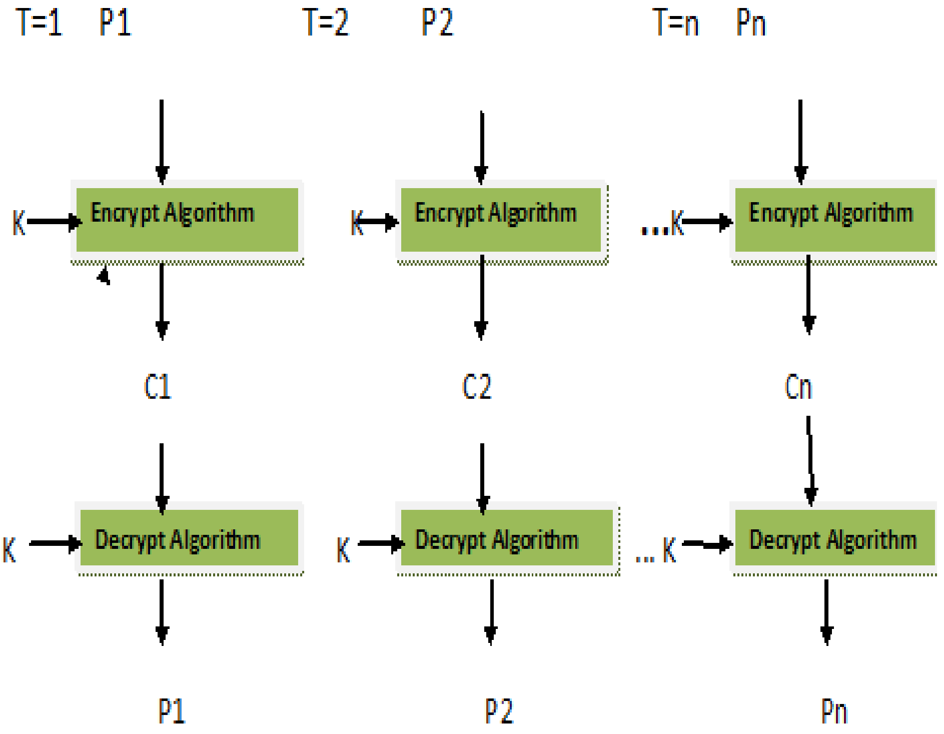


Figure1 Electronic Codebook Mode

CBC Mode: Each input plaintext block XORed with preceding ciphertext block and encrypted using same key.For decryption ,each cipher block decrypted using same key and then output is XORed with preceding cipher block(Figure2).IV(Initialization Vector) is used. IV is a random 64-bit block and keep secret.CBC use chaining so error propagation.

$$C1=E(K,\ IV \oplus P1) \qquad P1= IV \quad \oplus(K,\ C1)$$

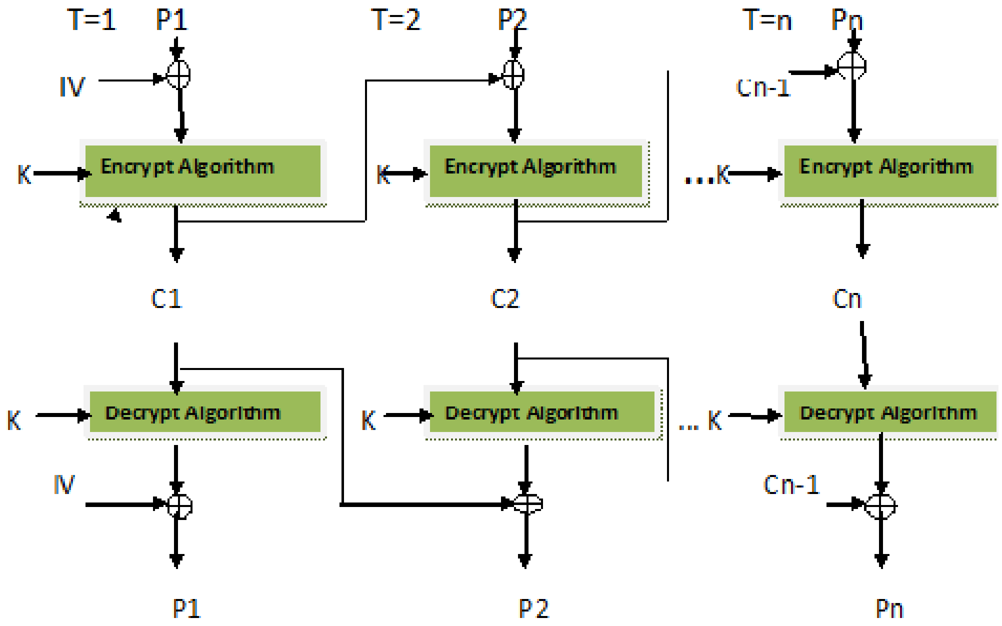


Figure2 Cipher Block Chaining Mode

CFB Mode : It convert the block cipher into stream cipher and encrypt plaintext by dividing it into segment of size s=8 bits.This provide bit or byte-level encryption and same key use.CFB mode also uses a random IV, and preceding ciphertext block XORed with plaintext block.(Figure3) Error propagation.

$$C1= P1 \oplus Ss[E(K,IV)] \quad , P1= C1 \oplus Ss[E(K,IV)]$$

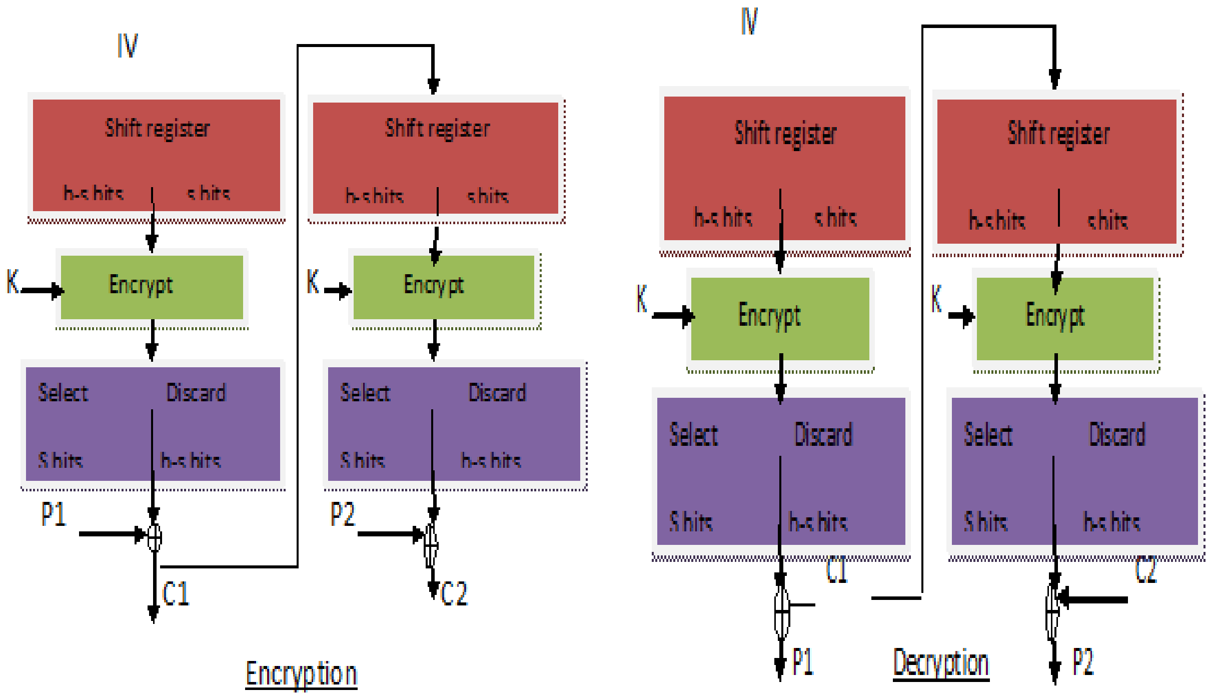


Figure3. Cipher Feedback Mode

OFB Mode : As CFB mode, OFB also convert block cipher into strem cipher and use random IV .IV is divided into segment and encrypted using same key which is XORed with the plaintext during each step.(Figure4).No error propagation.

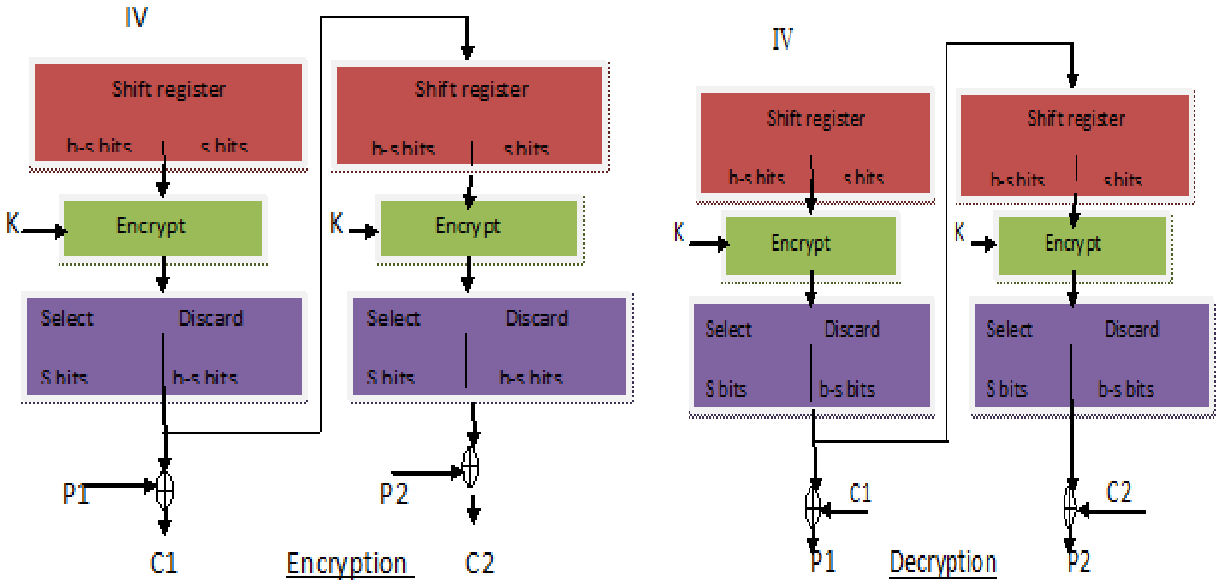


Figure4 :Output Feedback Mode

CTR Mode: It is also stream cipher like CFB and OFB mode,difference is use of Counter .Every time counter value is increased by one The counter can be use random values and counter value is encrypted using same key.Then output is XORed with input plaintext block(Figure5)No error propagation.

$$C1=P1 \oplus E(K,Counter) \, , P1= C1 \oplus D(K, Counter).$$

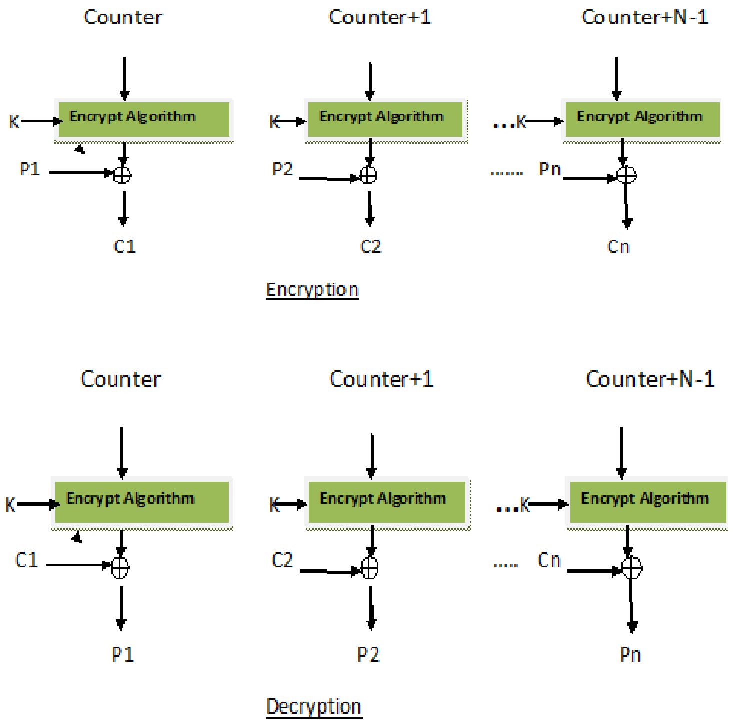


Figure 5. Counter Mode

V. DES ALGORITHM DESCRIPTION

DES encryption algorithm take 64-bit block plaintext and 64-bit key . Every eight bit of key is either used for parity check or ignored .Left 56-bit is used for encryption purpose.DES algorithm use the 16 round consisting same function.

DES Encryption: The encryption scheme is shown in Figure 6.There are two input to algorithm :Plaintext and Key. Steps of encryption are:

1. Firstly ,the plaintext to be encrypted is divided into fixed size 64-bit block.
2. Every eight bit of 64-bit key is ignored and 56-bit key is input to algorithm.
3. On the block of plaintext(64-bit) initial permutation(IP) is performed and divided into two halves Li ,Ri(each of 32-bit). On the key(56-bit) permuted choice1(PC1) is performedand it is also divided into two halves Ci, Di (each of 28-bit) .
4. After permutation, Data is processed in 16 rounds of same function f.
5. During each round, permuted key halves shifted left circular by 1 or more depend on implementation and then apply permuted choice 2(PC2)(48-bit key as output).
6. In each round data is encrypted using 48-bit key and output of first round become input of second round .
7. After 16th round ,32-bit halves output is swapped and produced Preoutput.
8. At last inverse initial permutation(IP^) is performed on preoutput and finally get the 64-bit ciphertext.

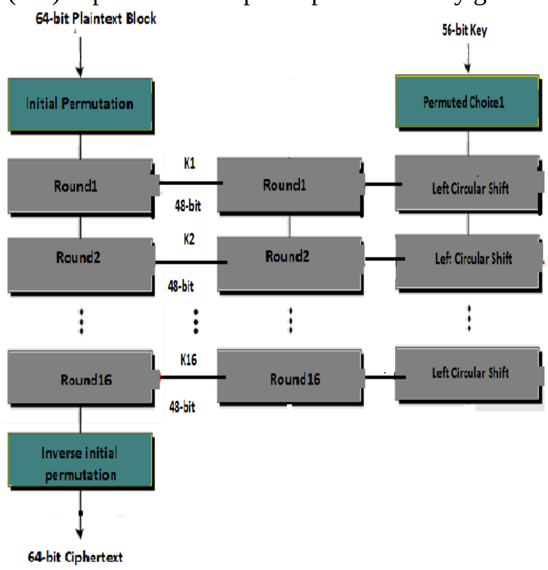


Figure 6:DES Encryption Scheme

Initial and Inverse Initial Permutation: These both are defined by tables and 64-bit input is numbered as1-64(entry of number in table define there position). (Table 1) .

TABLE 1

INITIAL and INVERSE PERMUTATION

Initial Permutation								Inverse Initial Permutation							
58	50	42	34	26	18	10	2	40	8	48	16	56	24	64	32
60	52	44	36	28	20	12	4	39	7	47	15	54	23	63	31
62	54	46	38	30	22	14	6	38	6	46	14	53	22	62	30
64	56	48	40	32	24	16	8	37	5	45	13	52	21	61	29
57	49	41	33	25	17	9	1	36	4	44	12	51	20	60	28
59	51	43	35	27	19	11	3	35	3	43	11	50	19	59	27
61	53	45	37	29	21	13	5	34	2	42	10	49	18	58	26
63	55	47	39	31	23	15	7	33	1	41	9	48	17	57	27

Round Detail and Function f : Input to each round is Li, Ri, Ci and Di. In each round Li is the preceding Ri(Li=Ri-1). Ri is calculated from preceding Ri by applying function f and output of f is XORed with preceding Li. (Figure7).

$[R_i=L_{i-1} \oplus f\,(R_{i-1},K_i)$

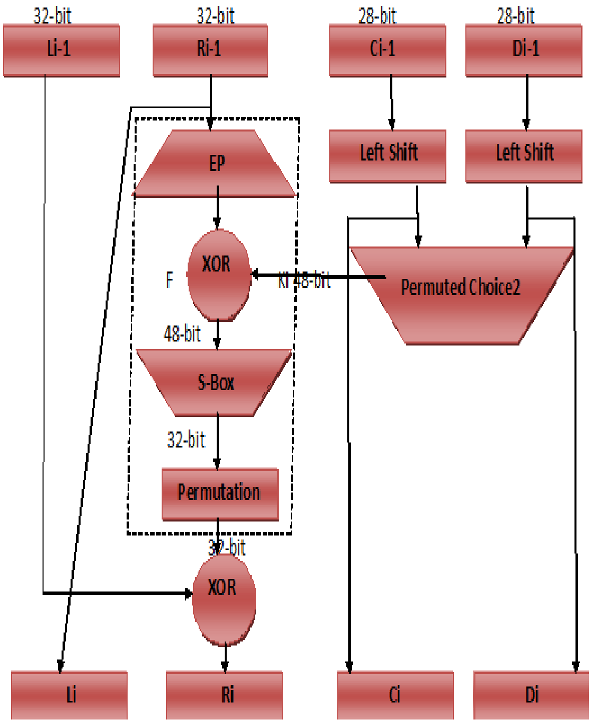


Figure 7.Round Scheme

The function f consists four steps:

1) *Expansion Permutation(EP):* The input to f is 32-bit block but key size is 48-bit after permuted choice 1.So there is need to expand input data block to 48-bit.(Table2)
2) *XORing*: Key after PC2 is XORed with output of EP.
3) *Substitution:* The s-boxes are used for substitution purpose. The input is 48-bit and ouput is 32-bit.
4) *Permutation:* 32-bit is then permuted.This is the output of function f(Table2).

TABLE 2

EP and PERMUTATION FUNCTION

Expansion Permutation					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Permutation Function							
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

*S-Box:*The substitution consist of eight s-boxes. Each s-box accept 6-bit input and produced 4-bit output.In 6-bit .first and last bit indicate row(0-3) and middle four bit define column entry(0-15).S-box implementation should be keep secret.

VI. KEY DESCRIPTION

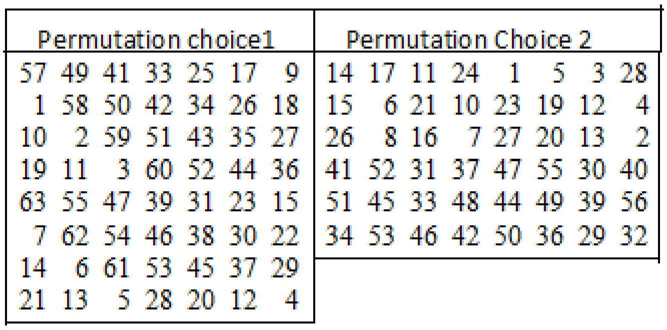
In DES, 64-bit key is provide and each 8th bit is ignore to produced 56-bit key. DES algorithm apply following step on key :

1. Firstly, apply PC1 on 56-bit key.(Figure 6).It simple rearrange the position of bits(Table3).
2. After PC1, in each round, key is divided into two halves Ci, Di (each of 28-bit) then shift each part in left by one or more places depending on implementation.(Figure7).
3. PC2 is apply and 48-bit key is produced.(Table3) This key XORed with 48-bit data(Figure 7).

*Permutation Choice1 (PC1) and Choice2 (PC2):*After discard the every 8th bit of key(64-bit),56-bit key is produced. In PC1, position of every bit of key(56-bit) is rearranged. After this, left circular shift is performed and then apply PC2. In PC2, some bit is again discard and rearranged bit to produced 48-bit key i.e XORed with data.(Table3)

TABLE 3

PC1 and PC2



Permutation choice1							Permutation Choice 2							
57	49	41	33	25	17	9	14	17	11	24	1	5	3	28
1	58	50	42	34	26	18	15	6	21	10	23	19	12	4
10	2	59	51	43	35	27	26	8	16	7	27	20	13	2
19	11	3	60	52	44	36	41	52	31	37	47	55	30	40
63	55	47	39	31	23	15	51	45	33	48	44	49	39	56
7	62	54	46	38	30	22	34	53	46	42	50	36	29	32
14	6	61	53	45	37	29								
21	13	5	28	20	12	4								

VII. AVALANCHE EFFECT in DES

It is most important property. In this ,if one bit is change either in plain text or in key , result is the half of the ciphertext bit is change,so it is not easy to perform analysis of ciphertext.

VIII. 2-DES and 3-DES

DES has strength 2^{56}, meaning that the most efficient way , to attack DES in practice one has to try each and every possible key until the correct encryption key is identified, this takes average $2^{56}/2 = 2^{55}$.steps.Problem with DES

1. Key size is very small.
2. S-box implementation kept secret.

Double-DES, uses 2 keys and two encryption/decryption algorithm. Ciphertext is generated as C= E(K2,E(K1,P)) and plain text is generated as P=D(K1,D(K2,C)) Now key size is 112-bit.Triple-DES can't overcome the problem of Man-In-Middle attack absolute .It use two keys with three stages of encryption. The plaintext message first encrypted with one key, decrypt, the result with a second key and finally encrypt this last result with the first key again. figure-8

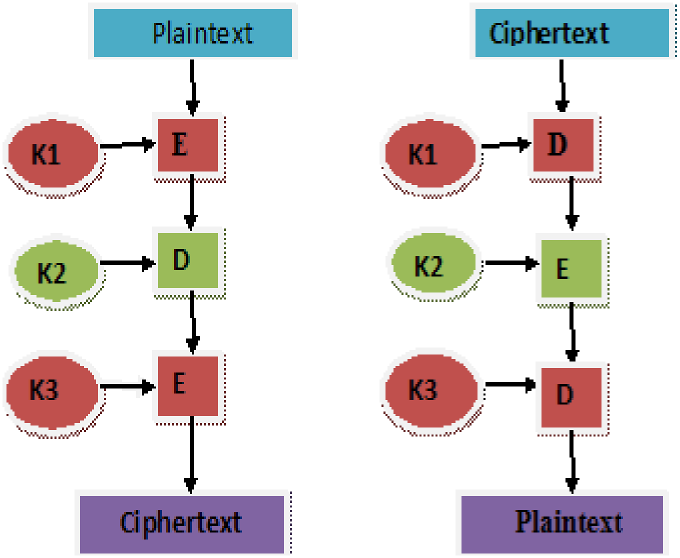


Figure 8. 3-DES Encryption/ decryption

IX. KEY ATTACKS in DES

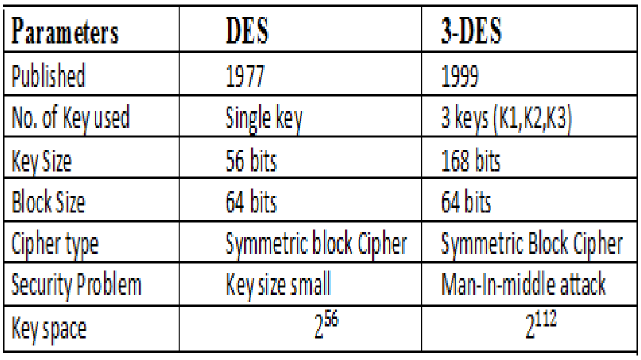
In single DES the key space is only 2^{56} which is very small. Due to this Double-DES introduce with Two Keys(total size112-bits).but there is another problems of Man-In-Middle attack and numbers of Known-plaintext attack.To cryptanalysis 2-DES 2^{56}Chosen-Plaintext to decrypted the message. But in triple DES , Known-plaintext attacks to 2^{112} which is not easy for practical.

X. COMPARATIVE ANALYSIS

In table a comparative analysis between DES and 3-DES is shown comparision is made on various factor.(table 4)

TABLE 4

COMPARISION b/w DES and 3-DES



Parameters	DES	3-DES
Published	1977	1999
No. of Key used	Single key	3 keys (K1,K2,K3)
Key Size	56 bits	168 bits
Block Size	64 bits	64 bits
Cipher type	Symmetric block Cipher	Symmetric Block Cipher
Security Problem	Key size small	Man-In-middle attack
Key space	2^{56}	2^{112}

XI. CONCLUSION

Cryptography is important element to protect informationIn this paper,we discussed symmetric block cipher standard-DES.DES provide the security to the data during transaction. financial services industry depends almost entirely on the DES to encrypt financial transactions .. Before 1970, cryptographic standard is not considered secure and DES replaced by 3DES everywhere encryption is done due the security issues we discussed above.DES is also support various modes to improve its security efficiency. DES also have two variants-2DES and 3DES .DES have the Man-In-Middle attack problem still. A comparative analysis defined that 3-DES provide more security but memory usage of DES is less than 3-DES.

Acknowledgment

We would like to express our sincere gratitude to Mrs. Sonal Beniwal for her continuous encouragement and guidance over the paper.

References

[1] National Institute of Standards and Technology, “Data Encryption Standard(DES)”, FIPS 46-2, 1993

[2] National Institute of Standards and Technology, “ Data Encryption Standard (DES)”, FIPS PUB 46-3, Gaithersburg, MD, 1999.

[3] National Institute of Standards and Technology, “Data Encryption Standard (DES)”. http://csrc.nist.gov/publications/fips/fips46- 3/fips46-3.pdf,(2001).

[4] A.Nadeem, “A performance comparison of data encryption algorithms”, IEEE information and communication technologies, pp.84-89, 2006.

[5] Arjen K. Lenstra and Eric R. Verheul, “Selecting Cryptographic Key Sizes” ,October 1999.

[6] E. Biham and A. Shamir, “Differential Cryptanalysis of the Full 16-round DES”, “ Advances in Cryptology - CRYPTO’92”, “ Lecture Notes in Computer Science”, Vol. 740, pp. 487–496, Springer-Verlag, 1993.

[6] FIPS 197. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[7] http://www.copacobana.org.

[8] http://en.wikipedia.org/wiki/DES.

[9] http://www.cl.cam.ac.uk/~rnc1/descrack/DEScracker.html

[10] ANSI X9.52-1998. URL: http://webstore.ansi.org/ansidocstore/product.asp?sku=ANSI+X9.52-1998.

[11] FIPS 81. URL: http://csrc.nist.gov/publications/fips/fips81/fips81.html.

[12] NIST SP 800-38a. URL: http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

[13] Subbarao V. Wunnava, “Data Encryption Performance and Evaluation Schemes” Proceedings IEEE Southeastcon 2002, pp 234-238 .