IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

A Novel Way to Understand DES

Gurline Kaur[1], Manjit Kaur[2]

Assistant Professor, P.G. Dept. Of Comp. Science & Applications, Kanya Maha Vidyalaya, Jalandhar, Punjab[1]

Student, M.Sc. IANS (Information & Network Security) Sem. IV, P.G. Dept of Comp. Science & Applications, Kanya Maha Vidyalaya, Jalandhar, Punjab[2]

Abstract: We are living in a world where there is a danger every fraction of second. With the world becoming a global village, we live in an e-society where everyone is vulnerable to numerous possible cyber attacks. But there is also a way to pay hide to such unforeseen situations. Cryptography is one field which was developed with a sole aim to secure every entity. There are various types of techniques and algorithms available. This paper is aimed at explaining DES in an innovative way. DES algorithm or symmetric block cipher consists of 16rounds. There are various other algorithms which are based on DES's Fiestel structure. Hence, there is always a need to explain the actual working of DES. Therefore, through his papers the authors have tried to solve round 1 of DES, thereby explaining in detail how the round 1 key and cipher text is obtained with the help of an example and various tables. This paper will help not only in understanding the DES algorithm, but also the various other following algorithms. Also the cyber attacks and their corresponding counter measures can be understood more clearly if the working of DES is clear.

Keywords: Cryptography, Fiestel structure, Block cipher, permutation, substitution, left circular shift.

I. INTRODUCTION

Cryptography is termed as the study of secret. It is most important aspect of communication security and is becoming increasingly important as a basic building block of computer security. Cryptography can be defined as a technique of coding the message and then sending it in the network, so that no one in the network could read the message. Cryptography makes the use of keys to code and decode the message. The message is coded at the sender side with the key and then the message is decoded at the receiver side with the key so that it becomes readable. The key can be same or different at the sender and receiver side depending on the type of cryptography technique. There are two techniques used for message coding and decoding, which are: Asymmetric or public key cryptography and Symmetric or private key cryptography. One of the symmetric block encryption algorithms is DES.

DES or Data Encryption Standard is the most popular type of private key cryptography. DES stands for Data Encryption Standard adopted by the National Bureau of Standards (NIST) in 1977. Its purpose is to provide a standard method for protecting sensitive commercial data. The algorithm is known as the Data Encryption Algorithm (DEA). DES works on the principle of block ciphers. DES processes a block of 64 bits at a time and the key of 56 bit is used. It has consists of sixteen rounds. DES follows the Feistel Structure (Feistel Structure: decrypt cipher text is very similar to encrypt plaintext).

In DES the same operations are carried out 16 times and then the final cipher text is produced. DES encryption was broken in 1999 by EFF i.e., Electronics Frontiers Foundation. This resulted in NIST issuing a new directive that required organizations to use Triple DES which means, three consecutive applications of DES.

II. LITERATURE SURVEY

In [1] Kenekayoro Patrick T has discussed that DES was formally institutionalized in 1976 turning into the principal encryption framework to meet the National Bureau of Standards (NBS) criteria for an encryption framework (Schneier, 1996), and the initially institutionalized encryption framework. After thirty four years, development in cryptography has been enormous and beneficial changes have been made.

In [2] Yashpal Mote, ParitoshNehete, Shekhar Gaikwad have suggested that DES was officially established in 1974. From this very period, certain techniques were documented that distorted its security. 3DES introduced an updated version of DES. In order to increment the encryption level this mechanism is performed three times but on other hand it is same as the real DES. Alternatively of all this, as compared to other cryptograph techniques this method has low speed.

In [3] Prashanti.G, Deepthi.S and Sandhya Rani.K have described the DES (Data Encryption Standard) algorithm has a wide scope due to its functionality. Many people think "secret code making" and DES have been synonymous. DES was considered to be as unsystematized facts being used by an algorithm. So contemporary enhancement has been recommended to the DES algorithm that uses an operation termed as modulo (+).

In [4] D. Coppersmith proved that the Data Encryption Standard (DES) came into existence in 1974 which was introduced by IBM and formulated as a national standard in 1977.Many experts in this field tried to fragment this system from that very period of time. Security measures has been demonstrated by us for the this built in system which depicts that in order to be successful you need more than 10-15 bytes of the specified plaintext.

Copyright to IJARCCE

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

In [5] Divya Sukhija have presented that Data Encryption Standard (DES) a symmetric algorithm is an essential benchmark for the encryption of data. This system has been swapped by Advanced Encryption Standard (AES) which would be discussed further. DES has the capacity to encrypt data 64 bits at a time as compared to a stream cipher which encrypts data one bit at a time. In 1960's International Business Machines (IBM) Corporation organized a project as a result of which DES came into existence and a cipher was introduced called LUCIFER.

In [6] Amit Dhir has shown the features of DES block as nonspecific, inconsistent and its dependency on bit and plaintext. To standardize this dependability it involves minimum of five series of DES. Therefore, key and cipher text are integrated together to serve the "mixing" function. Thus, DES has the usage more of than 72 quadrillion (72 x 1015) possible encryption keys.

In [7] Mandeep Singh Narula and Simarpreet Singh, present that due to the fact of its security and speed the DES algorithm is considered widely and highly recognizable. Hence, as DES is only a 64-bit (eight characters) block cipher, including 255 steps on average which can redeem the encryption key where it is not viable to penetrate DES. The algorithm stated as outdated due to the small key size, swift development in electronic circuitry blended with equivalency of Feistel ciphers.

III. WORKING OF DES

- DES takes 64 bits of plaintext as input and then applies an initial permutation on it.
- Then the output which comes is moved to the Round 1 and in this way, processing takes place for 16 times.
- The output which is generated after the 16th round is swapped.
- On this, inverse initial permutation is applied.
- After applying reverse initial permutation is applied.
- After applying inverse initial permutation, the cipher text which we get is the actual cipher text.

The whole procedure of DES is as explained in the diagram, which clearly depicts the flow of DES in 16 rounds.

In DES, the key is of 64 bit but the PC1 or Permuted Choice 1 (simple permutation) is applied and it is converted to 56 bit. Again the left circular shift is applied and permuted choice two is applied.
So the 48 bit key is applied in each round.

- DES takes 64 bits of plaintext as input and then applies an initial permutation on it.

A. DES Example
This paper will be explaining DES in an innovative way with the help of an example, solving it in each steps thereby getting the required correct cipher text. For this the following key and Plain text will be input:

Key :- 5,8,1,F,B,C,9,4,D,3,A,4,5,2,E,A
Plaintext :- 3,5,7,0,E,2,F,1,B,A,4,6,8,2,C,7

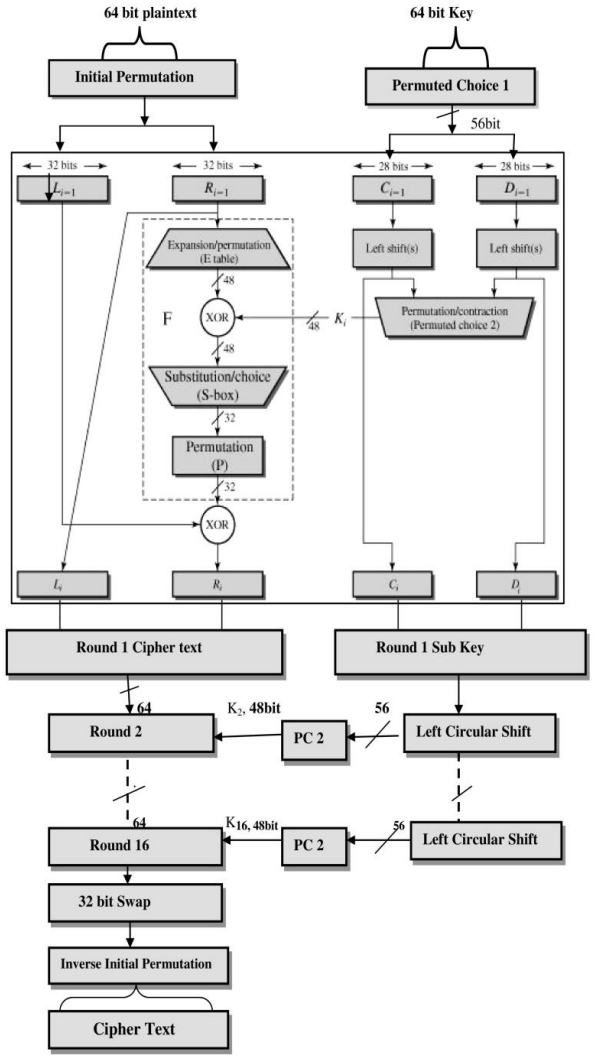

Fig1. Diagram showing DES procedure in 16 rounds

The initial step is to get the binary equivalents of all the input. For this TABLE I will be helpful which a simple decimal to hexadecimal equivalent is:

TABLE I Hexa Table

Number	Bit 4	Bit 3	Bit 2	Bit 1	Hexa Equiv
0	0	0	0	0	0
1	0	0	0	1	1
2	0	0	1	0	2
3	0	0	1	1	3
4	0	1	0	0	4
5	0	1	0	1	5
6	0	1	1	0	6
7	0	1	1	1	7
8	1	0	0	0	8
9	1	0	0	1	9
10	1	0	1	0	A
11	1	0	0	1	B
12	1	1	0	0	C
13	1	1	0	1	D
14	1	1	1	0	E
15	1	1	1	1	F

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2016.54140

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

B. KEY Conversion

The diagram clearly states that initially 64 bit key is converted to 56 bit key. Converting the given key 5,8,1,F,B,C,9,4,D,3,A,4,5,2,E,A in binary we get the TABLE II from TABLE I.

5 = 0101 8 = 1000 and so on.

TABLE II Key to Binary (8*8=64)

0	1	0	1	1	0	0	0
0	0	0	1	1	1	1	1
1	0	1	1	1	1	0	0
1	0	0	1	0	0	1	1
1	1	0	1	0	0	1	1
1	0	1	0	0	1	0	0
0	1	0	1	0	0	1	0
1	1	1	0	1	0	1	0

Now applying following PC 1 (8*7=56) matrix to TABLE II.

TABLE III Permuted Choice 1 (8*7=56)

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

This will convert TABLE II key or 64 bit key to TABLE IV or 56 bit key. TABLE IV is applied with a simple logic of permutations. This 6 bit key is intentionally shown as Co and Do because left shift has to be applied to Co.

TABLE IV (8*7=56) BIT KEY Co

1	0	1	1	1	1	0
0	1	1	0	1	0	0
0	1	1	0	1	0	0
1	0	0	0	1	0	1

TABLE IV (8*7=56) BIT KEY Do

1	1	0	1	0	0	1
0	0	0	1	0	1	1
1	0	1	0	0	0	0
1	1	1	1	1	1	1

Now Co is taken and left shift is applied to Co and Do of TABLE IV as a whole or by shifting its bit positions to left by 1, resulting in TABLE V or C1 and D1.

TABLE V (8*7=56 bits) Left shift on Co = C1

0	1	1	1	1	0	0
1	1	0	1	0	0	0
1	1	0	1	0	0	1
0	0	0	1	0	1	1

Apply left shift on Do = D1

1	0	1	0	0	1	0
0	0	1	0	1	1	1
0	1	0	0	0	0	1
1	1	1	1	1	1	1

TABLE 5 is result of 56 bit key which will now be converted to (8*6=48 bit Key) with the help of PC 2 or TABLE VI as follows.

TABLE VI Permuted Choice 2 (8*6=48)

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

TABLE VII Applying PC2 (Permuted Choice Two) on TABLE V (8*6=48 bit Key)

0	0	1	0	0	1
1	1	1	0	1	0
0	0	0	1	0	1
1	0	1	0	0	1
1	1	1	0	0	1
0	1	1	0	0	0
1	1	0	1	1	1
0	1	1	0	1	0

This is the first round sub key of 16 rounds Fiestel structure of DES.

C. Plain Text Conversion

Converting the given plain text 3,5,7,0,E,2,F,1,B,A,4,6,8, 2, C,7 in binary we get the TABLE VIII from TABLE I.

TABLE VIII Plain Text to Binary (8*8=64 bits)

0	0	1	1	0	1	0	1
0	1	1	1	0	0	0	0
1	1	1	0	0	0	1	0
1	1	1	1	0	0	0	1
1	0	1	1	1	0	1	0
0	1	0	0	0	1	1	0
1	0	0	0	0	0	1	0
1	1	0	0	0	1	1	1

Now applying TABLE IX or Initial Permutation to TABLE VIII, we get TABLE X (8*8=64 bit plain text).

TABLE IX Initial Permutation (8*8=64 bits)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2016.54140

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

TABLE X Applying initial permutation (IP) to plain text 8*8=64 bit

1	0	1	0	1	1	1	0
0	0	0	1	1	0	1	1
1	0	1	0	0	0	0	1
1	0	0	0	1	0	0	1
1	1	0	1	1	1	0	0
0	0	0	1	1	1	1	1
0	0	0	1	0	0	0	0
1	1	1	1	0	1	0	0

Again from the diagram Fig. 1, it is clear that after this step, DES will work on only the right part of the plain text, so dividing TABLE X and Lo and Ro.

TABLE X Lo (4*8=32)

1	0	1	0	1	1	1	0
0	0	0	1	1	0	1	1
1	0	1	0	0	0	0	1
1	0	0	0	1	0	0	1

TABLE X Ro (4*8=32)

1	1	0	1	1	1	0	0
0	0	0	1	1	1	1	1
0	0	0	1	0	0	0	0
1	1	1	1	0	1	0	0

Now applying TABLE XI or Expansion Permutation (E) (8*6=48) on Ro, results in TABLE XII (8*6=48 bit plain text).

TABLE XI Expansion Permutation or E (8*6=48 bits)

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	11
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

TABLE XII Applying Expansion Permutation or E to Ro (8*6=48 bits)

0	1	1	0	1	1
1	1	1	0	0	0
0	0	0	0	1	1
1	1	1	1	1	0
1	0	0	0	1	0
1	0	0	0	0	1
0	1	1	1	1	0
1	0	1	0	0	1

Now we apply round 1 sub key or TABLE VII (8*6=48 bit) to TABLE XII (Plain Text (8*6=48 bit)) and XOR them to get TABLE XIII.

TABLE XIII 48 bit Plain Text after XOR with key (8*6=48)

0	1	0	0	1	0
0	0	1	0	1	0
0	0	0	1	1	0
0	1	0	1	1	1
0	1	1	0	1	1
1	1	1	0	0	1
1	0	1	1	0	1
1	1	0	0	1	1

At this step they boxes are applied to TABLE XIII thereby converting it from 48 bits to (8*4=32 bits).

Row No. = Decimal Equivalent of 1st and Last Bit
Column No.= Decimal Equivalent 2nd, 3rd, 4th and 5th bits

Taking Row 1 of TABLE XIII 010010
Row R1= 00 = 0
Column C1 = 1001 = 9
Hence, number at Row 0 and Column 9 of SBOX 1 = 10 = 1010

Taking Row 2 of TABLE XIII 000010
Row R2= 00 = 0
Column C2 = 0001 =1
Hence, number at Row 0 and Column 1 of SBOX 2 = 1 = 0001

Taking Row 3 of TABLE XIII 000110
Row R3= 00 = 0
Column C3 = 0011 = 3
Hence, number at Row 0 and Column 3 of SBOX 3 = 14 = 1110

Taking Row 4 of TABLE XIII 010111
Row R4= 01 = 1
Column C4 = 1011 = 11
Hence, number at Row 1 and Column 11 of SBOX 4 = 12 = 1100

Taking Row 5 of TABLE XIII 011011
Row R5= 00 = 0
Column C5 = 1001 = 9
Hence, number at Row 0 and Column 9 of SBOX 5 = 10 = 1010

Taking Row 6 of TABLE XIII 111001
Row R6= 11 = 3
Column C6 = 1100 = 12
Hence, number at Row 3 and Column 12 of SBOX 6 = 0110 = 6

Taking Row 7 of TABLE XIII 101001
Row R7= 11 = 2
Column C7 = 0100 = 4
Hence, number at Row 2 and Column 4 of SBOX 8 = 1 = 0001

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2016.54140

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Taking Row 8 of TABLE XIII 110011
Row R8= 11 = 3
Column C8 = 1001 = 9
Hence, number at Row 3 and Column 9 of SBOX 8 = 12 = 1100

TABLE XIV Matrix After Applying S-Boxes (8*4=32 bit) or R0

1	0	1	0
0	0	0	1
1	1	1	0
1	1	0	0
1	0	0	1
0	1	1	0
0	0	0	1
1	1	0	0

Applying Permutation TABLE XV (8*4=32) on R0 OR TABLE XIV, we get TABLE XVI.

TABLE XV Permutation P (8*4=32)

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

TABLE XVI Ro after applying Permutation P (8*4=32 bits)

0	0	1	0
1	0	1	1
1	0	1	0
0	0	0	1
0	1	0	1
0	0	1	1
0	1	1	0
1	1	0	0

Now, Lo or TABLE X is XO Red with TABLE XVI to get TABLE XVII.

TABLE XVII

1	0	0	0
0	1	0	1
1	0	1	1
1	0	1	0
1	1	1	1
0	0	1	0
1	1	1	0
0	1	0	1

As per diagram Ro becomes left, hence combining TABLE XVII and TABLE X, to get final cipher etxt TABLE XVIII.

TABLE XVIII Cipher Text (8*8=64)

1	1	0	1	1	1	0	0
0	0	0	1	1	1	1	1
0	0	0	1	0	0	0	0
1	1	1	1	0	1	0	0
1	0	0	0	0	1	0	1
1	0	1	1	1	0	1	0
1	1	1	1	0	0	1	0
1	1	1	0	0	1	0	1

Applying TABLE I or Hexa TABLE to TABLE XVIII, we will get cipher text of round 1 as:
1101 = D 1100 = C 0001 =1

Cipher Text = D,C,1,F,1,0,F,4,8,5,B,A,F,2,E

IV. CONCLUSION

This paper is aimed at explaining the basic working of DES algorithm. Although it is a symmetric cryptography based algorithm, but there is always a need to understand how DES works, in order to get the detailed knowledge of all the other algorithms. This working is based on only Round 1 of algorithm. The same procedure can be applied to the remaining 15 rounds to get the final cipher text of complete DES.

REFERENCES

[1] Kyoro Patrick T, The Data Encryption Standard Thirty Four Years later: An Overview, African Journal of Mathematics and Computer Science Research Vol. 3(10), pp. 267-269, October 2010.
[2] Pal Mote, Paritosh Nehete and Shekhar Gaikwad, Superior Security Data Encryption Algorithm (NTRU), ISSN: 2229-6913 Issue July 2012, Vol. 6.
[3] Shanti.G, Deepthi.S and Sandhya Rani.K, A Novel Approach for Data Encryption Standard Algorithm, IJEAT Volume-2, Issue-5, June 2013.
[4] D. Coppersmith, The Data by D. Coppersmith Encryption Standard (DES) and its strength against attacks, VOL. 38 NO. 3 MAY 1994.
[5] Divya sukhija, A Review Paper on AES and DES Cryptographic Algorithms, IJECSE, Volume 3, Number 4.
[6] Amit Dhir, Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs, WP115 (v1.0) March 9, 2000.
[7] Mandeep Singh Narula and Simarpreet Singh, Implementation of Triple Data Encryption Standard using Verilog, Volume 4, Issue 1, January 2014.

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2016.54140