Final paper

Q#:Solve the given paper step by step mathematically and explain one line sentence in detail and encrypt it using DES algorithm in this paper

Abstract:

Modern Technology like wireless network helps us to con-nect instantly with people anywhere and at any time. Se-curity of Wireless network is the main challenge faced by todays world. It is where cryptography play a vital role to provide security to the wireless network. Numerous encryp-tion calculations are accessible to secure the information. This paper deals with ordinarily utilized symmetric encryp-tion calculation which is DES Algorithm. Test results are given to illustrate the execution of this calculation.

AMS Subject Classification

Key Words and Phrases: DES, Feistel function, Per-mutation, Key schedule

1 INTRODUCTION

Cryptography is an art of conveying messages in coded form which is understood only by the intended recipient. The recipient in turn decodes to read the message. The transfer of data through public network with security issues can be protected with cryptography. There are several standard symmetric and asymmetric algorithms which are highly secured and time tested.

TYPES OF CRYPTOGRAPHY

Cryptography is mainly divided into two types.

Symmetric algorithm

Asymmetric algorithm

1. Symmetric Algorithm.

   In this type a single key which is kept secret among the sender and the recipient is used so that no unauthorized person can use the data, which is to be transferred.

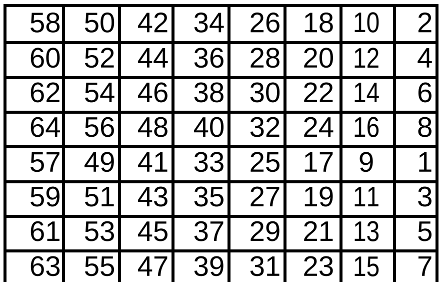
2. Asymmetric Algorithm.

   In this type a public key and private key are used where public is known to everyone whereas the private key is only known to the recipient of the message. This encryption is considered more secure when compared with symmetric algorithm. When speed is compared symmetric algorithm works faster.

3. Initial Permutation:

64 bit - (8*8)

1 2 3 4 5 6 7 8 ----64



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
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

First we apply the initial permutation. We must follow the initial permutation (IP). The transposition order, in which the 58th bit will be the first position, and the 50-bit one will be in the 2nd position, and the 2nd, 3rd position and similarly 7-bit will be in the last position.

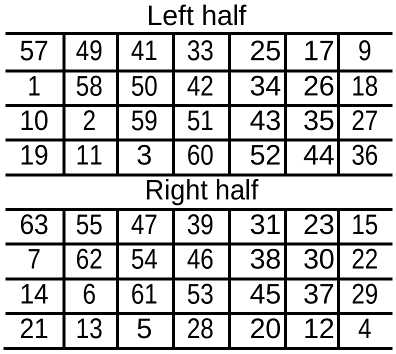
Therefore, we must follow this transposition order in the DES algorithm.

This will be the order of transposition of the bit position in plain text: 58 bits will be the first position, 50 bits will be the second position. So now we will rearrange the order according to the rearrangement. We are going to start the 1st round.

4. Permutation Key PC-1 :

Input for Pc-1 is 64

And output is 56



Left half

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36

Right half

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

5. Permutation Expansion:

The first thing we should divide the simple text into 3 halves. Half left and half right.

The right half is assigned to the rearrangement of the decomposition. Swapping extensions means we have to spend a few bits.

So here, the input for PE is 32-bit and the output is 48-bit. Thus, 16 bits will be added to the decomposition P. So this is the transpose order to follow for the decomposition of the permutation.

So position 1 ... 32, and 16 bits on the side will be added.

For example:

32	01	02	03	04	04
04	05	06	07	08	09
08	09	10	11	16	13
12	13	14	15	20	17
16	17	18	19	24	21
20	21	22	23	28	25
24	25	26	27	32	29
28	29	31	31	32	01

When this 16 bit will be added the complete length of E permutation will become 48 bit. So, input is 32 bits and output is 48 bits.

After applying the permutation extension, we must XOR the result of the permutation extension with Pc-2, so for PC-2 we need to generate a sub key.

In the flowchart, the key size is 64 bits. We will use 64 bits as input for PC-1.

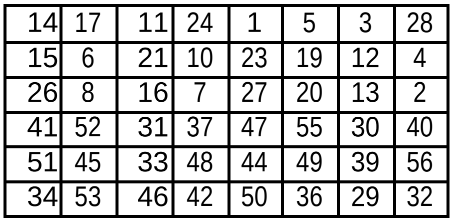
6. Binary Shifting:

No. of Cycle	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Amount of bits	1	1	2	2	2	2	2	2	1	2	2	2	2	2	1	16

Depend upon Rounds number how many bits we will shift. So, in Round 1 to Round 16 We have to perform 1 bit Circular shift.

So, in all these rounds we have to shift 1 bit and in rest of the Rounds numbers we have to shift 2 bits.

7. Permutation Key PC-2:



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

After applying the left circular shift, we will output the PC-2. Therefore having 56 key bits will be reduced to 48 bits.

PC-2, then, at this bit position will be reduced to 48 bits after applying PC-2 according to this bit position, we will rearrange the bits. The PC-2 output is 48 bits and the input is 56.

The output of PC-2 is XOR with expansion permutation where we got 32 bits to 48 bits. then the output is 48. This 48 bit will be applied to S-frames. Again, 48 bits will be reduced to 32 bits..

8. S-Blocks:

8 - S boxes

Input=48 bits

Output=32 bits

Each S box will get 6 bit input and will reduce 2 bits and output will be 4 bits

6→S1→ 4

6→S2→4

6→S3 →4

6→S4→4

6→S5→4

6→S6→4

6→S7→4

6→S8→4

If we consider 6 bits 100110

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

The first bit and the last bit considered as Row number

S box is table of values i.e rows and columns

4 rows in S box and 16 columns

Rows=0123

Columns=0, 1, 2……..15

1 0 – Row 2}

0 0 1 1 – Column 4} →8→1000 so this is the output of S box 1

9. Permutation P:

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

After receiving the output of block S, we apply the permutation to obtain the output. We will again follow the transpose order. The length in bits will not change; the format of the bits will change. We will change the position of the bit in accordance with the given transpose order.

The number of bits will not be reduced or added.

Input is 32

Output is also 32.

Only will rearrange.

So here 16 bit will be at 1st position

7 bit will be 2nd

20 in 3rd position

After applying P the output of is 32 bit which is XOR with left half.

So, in initial stage we divide in to two half left and right. This left half is XOR with output for permutation. Right half will be shifted to left half.

10. Final Permutation:

We will follow the same function 16 times

After completing 16 rounds, we will apply a 32-bit swap, which means that the left half will be saved in the right half, and the right half will be saved in the left half, so a 32-bit swap will be performed.

After applying a 32-bit swap, 64-bit ones will be assigned for reverse initial permutation

We will apply the reverse initial permutation, where we must change the order of the bits

So the input will be 64

The output will be 64

Bits will not be added or deleted.

Any number that we give the reverse initial permutation will have the same exit number

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

So the reverse initial permutation will be cipher text

Like this DES algorithm, it applies to 16 rounds, and in each round we will generate sub keys in parallel

Each sub key will be used in each round.

According to the round, the number of bits should not be shifted

In round # 1, 2 ... .16 on the left, 1 circular shift will be applied

And in the remaining rounds we will make 2 bits applied to the left circle.