Data Encryption Standard
For IT 7th Sem Students

Developed and Presented By:

Dileep Kumar Yadav
Assistant professor
Dept. of CSE
V.B.S PU,Jaunpur
Mb. No.8726943272
Email-dileep1482@gmail.com

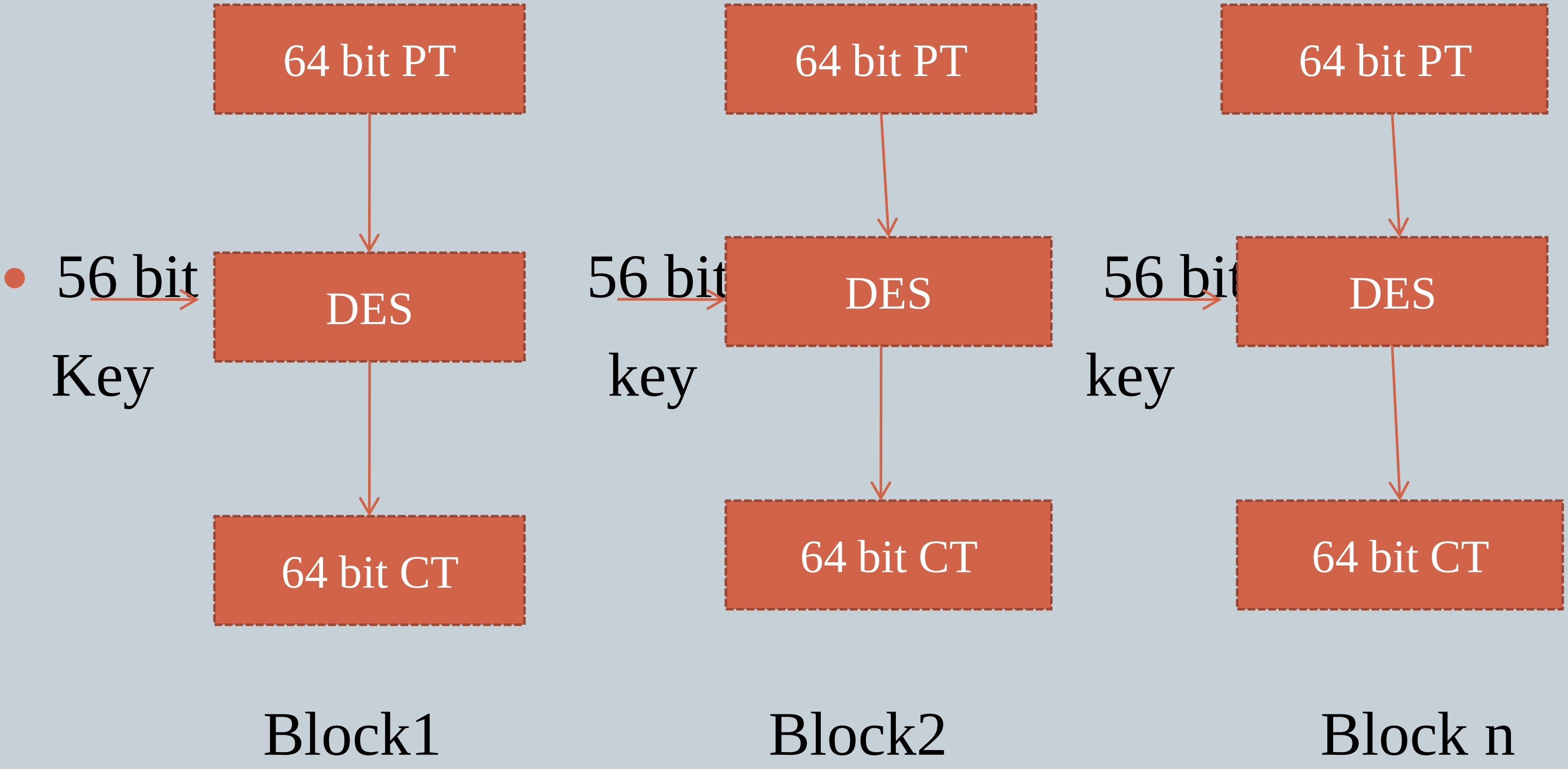
Data Encryption Standard(DES)

- DES also called DEA i.e. Data Encryption Algorithm.
- Most widely used block cipher in the world.
- Origin of DES was 1972, when the US the national bureau of standards (NBS) now it is called NIST.
- In 1976 US federal govt. decided to adopt this algorithm and give name i.e. DES.
- DES encrypt 64 bit plain text data using 56 bit key.

How DES Works

- **Conceptual view of DES:**
- DES is a block cipher. It encrypts data in blocks of size 64 bits each.
- 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text.
- The same algorithm and key are used for encryption and decryption.
- The key size is 56 bit key.
- We have mentioned that DES uses a 56 bit key, actually the initial key consists of 64 bit however before the DES process even starts every eighth bit of the key is discarded to produce a 56 bit key.
- That discarded bits are 8,16,24,32,40,48,56,64.

Cont…



- 56 bit Key

64 bit PT

DES

64 bit CT

Block1

56 bit key

64 bit PT

DES

64 bit CT

Block2

56 bit key

64 bit PT

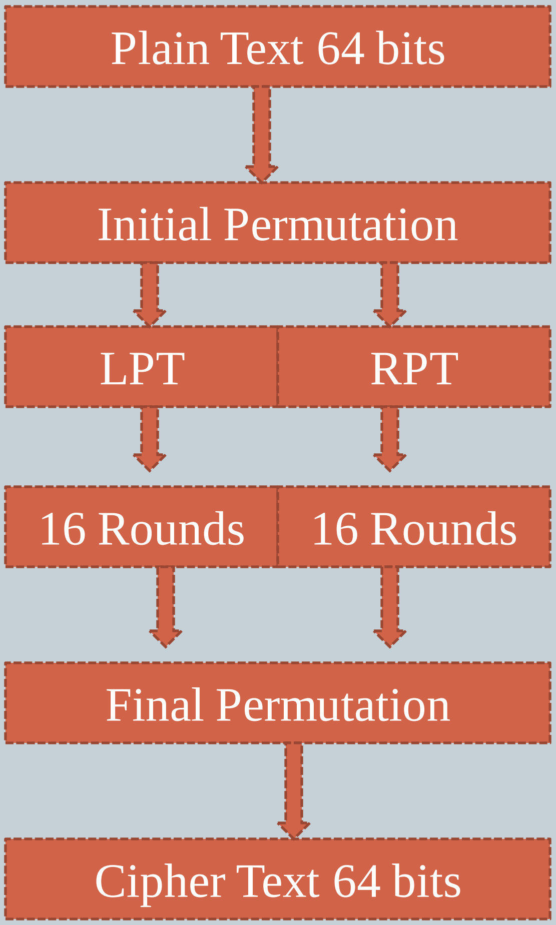
DES

64 bit CT

Block n

Broad Level Steps in DES

- Step 1
- Step 2
- Step 3
- Step 4
- Step 5
-
- step 6



Plain Text 64 bits

Initial Permutation

LPT

RPT

16 Rounds

16 Rounds

Final Permutation

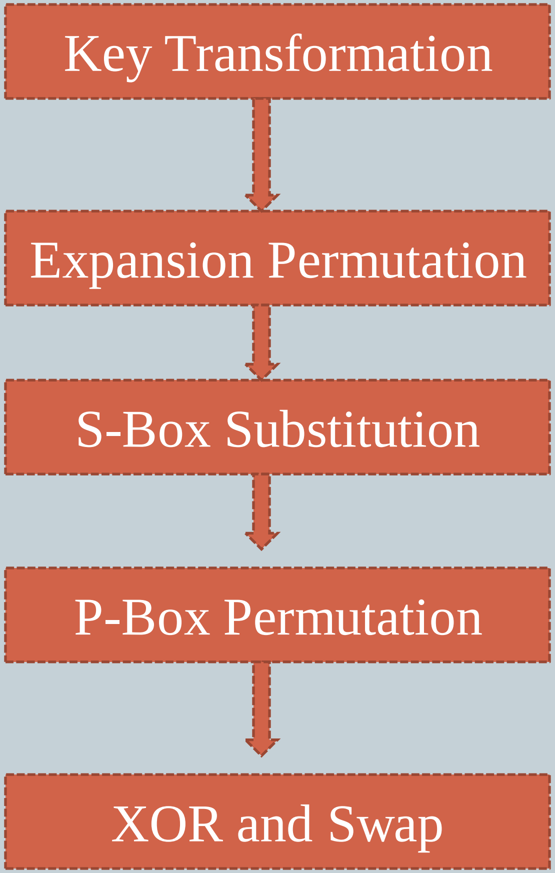
Cipher Text 64 bits

Initial Permutation(IP)

- It is happens only once and it happens before the 1st round.
- It says that IP replaces the 1st bit of the original plain text block with the 58th bit of the original plain text block , the 2nd bit with 50th bit and so on..
- After IP is done the resulting 64 bit permuted text block is divided into two half blocks that is LPT and RPT each of 32 bits
- Now 16 rounds are performed on these two blocks.

Details of One Rounds in DES

- Step 1
- Step 2
- Step 3
- Step 4
- Step 5



Key Transformation

Expansion Permutation

S-Box Substitution

P-Box Permutation

XOR and Swap

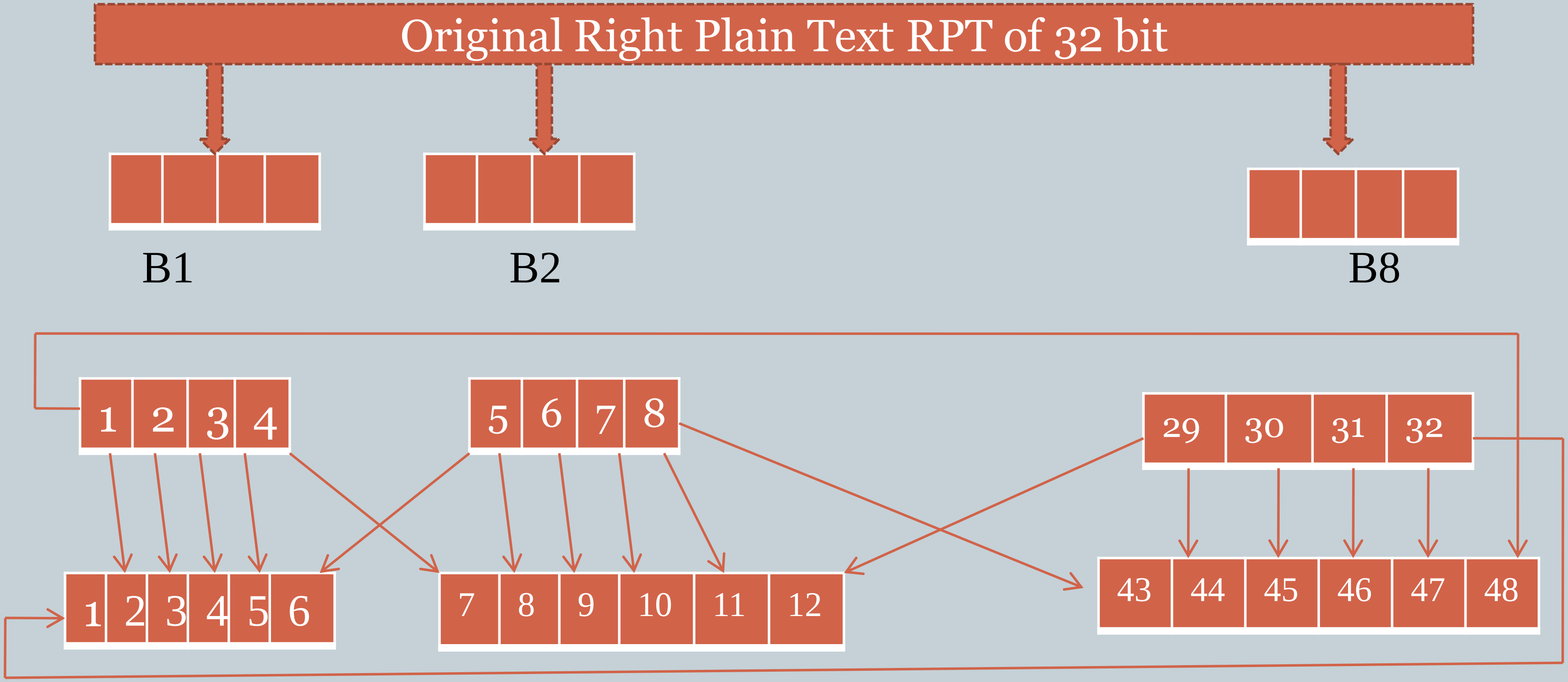
Step 1-Key Transformation

- We have noted that the initial 64 bit key is transformed into a 56 bit key by discarding every 8th bit of the initial key. Thus for each round a 56 bit key is available.
- From this 56 bit key ,a different 48 bit sub key is generated during each round using a process called key transformation.
- For this the 56 bit key is divided into two half each of 28 bit
- These half are circularly shifted left by one or two positions depending on the round.
- After an appropriate shift 48 of the 56 bits are selected .

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
No. of key be shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Step 2- Expansion Permutation

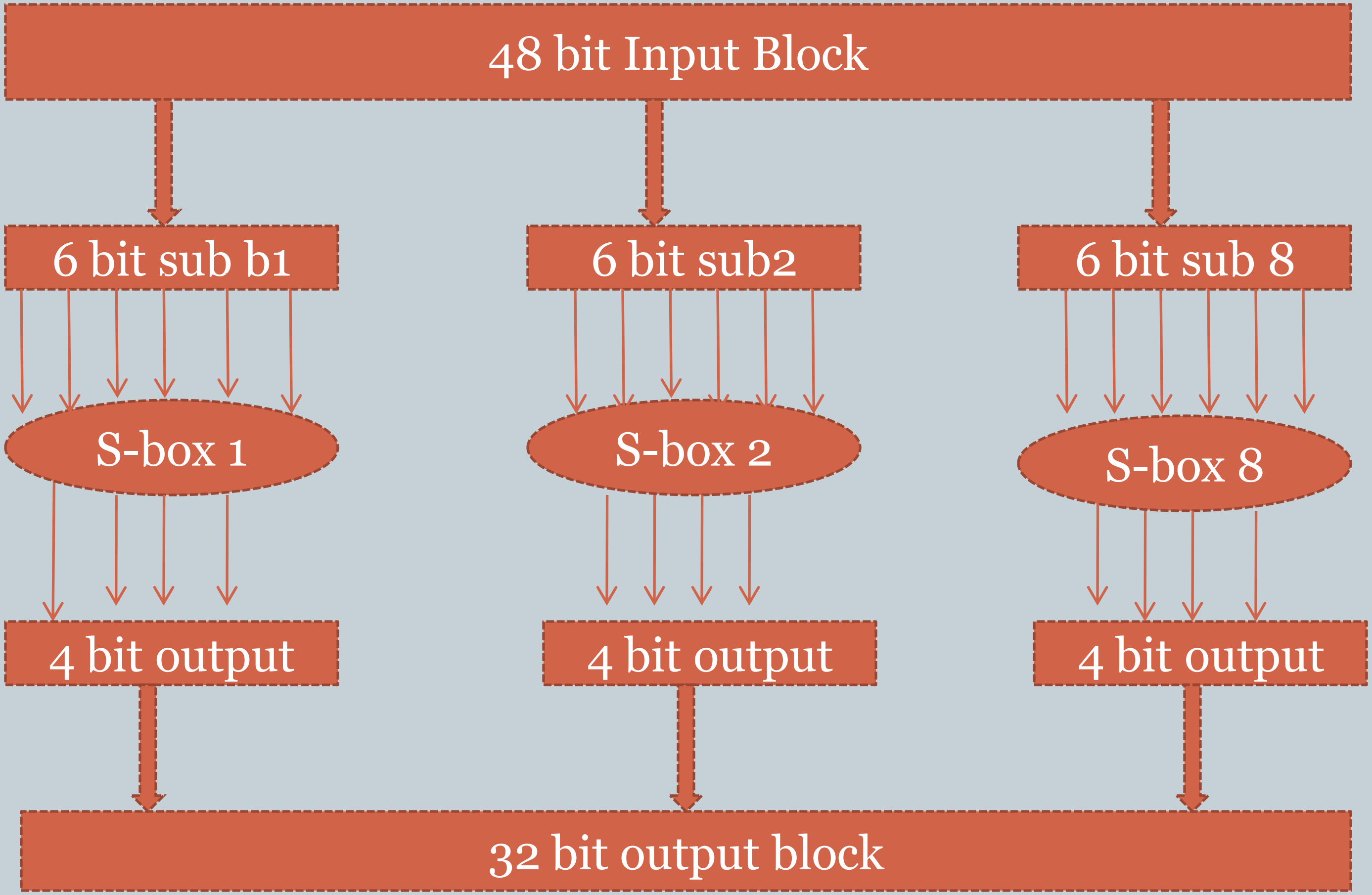
- During expansion permutation the RPT is expanded from 32 bit to 48 bit.
- The 32 bit RPT is divided into 8 blocks with each block consist of 4 bit. Each 4 bit block expanded to corresponding 6 bit block.



Step 3-S-Box Substitution

- Now 1stly the key transformation process compresses the 56 bit key to 48 bit then expansion permutation process expands 32 bit RPT to 48 bit.
- Now the 48 bit key is XORed with the 48 bit RPT and the resulting output is given to next step which is the S-box Substitution.
- It is a process that accepts the 48 bit input from the XOR operation involving the compressed key and expanded RPT and produces a 32 bit output using the substitution technique.
- The substitution is performed by 8 substitution boxes i.e. called S-Box.
- Each of the 8 s-boxes has 6 bit input and 4 bit output.

Cont…



48 bit Input Block

6 bit sub b1

6 bit sub2

6 bit sub 8

S-box 1

S-box 2

S-box 8

4 bit output

4 bit output

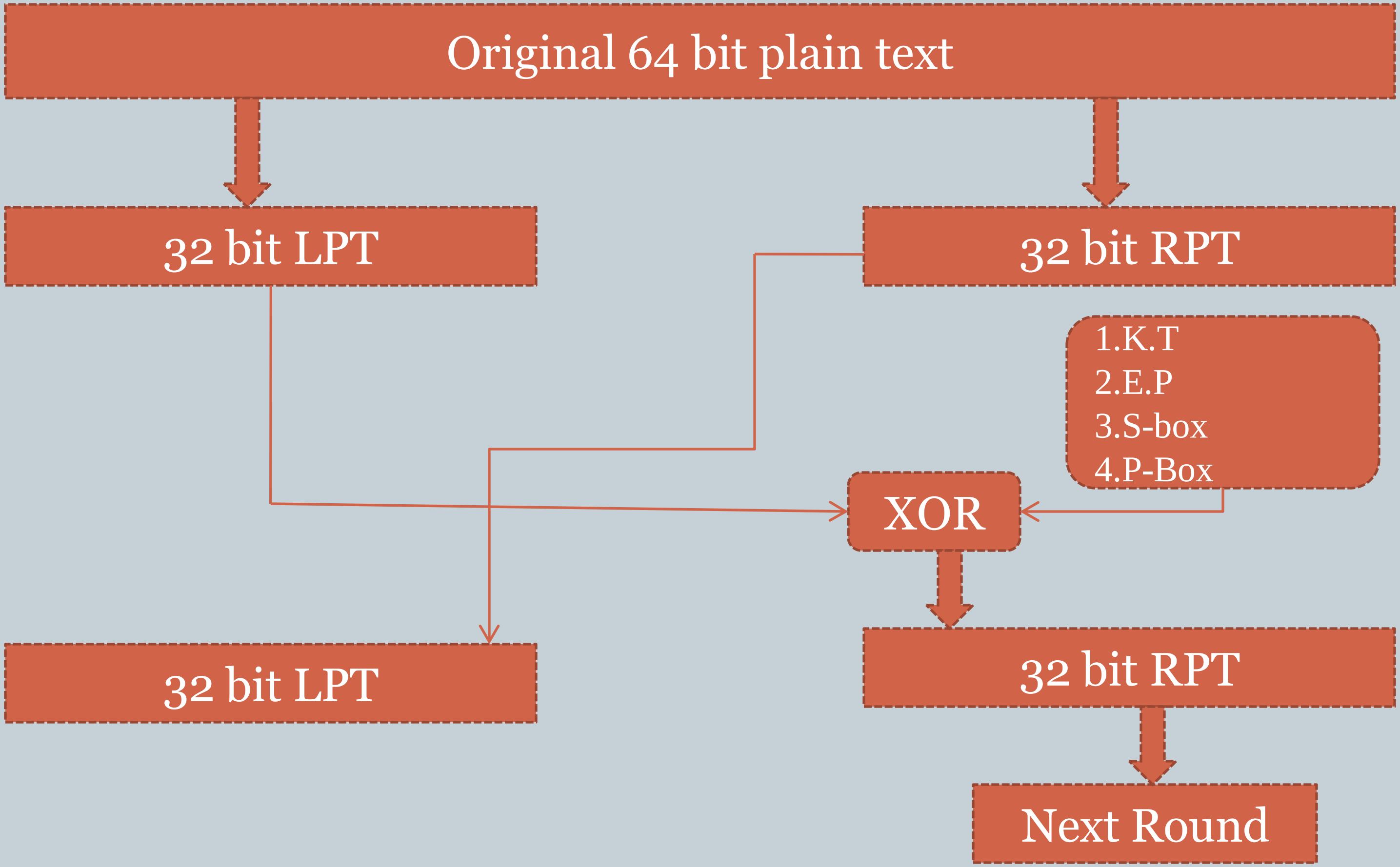
4 bit output

32 bit output block

Step 4-P-Box Permutation

- The output of S-box consist of 32 bit. These 32 bit is permuted using a P-box.
- This technique is simple permutation mechanism i.e. replacement of each bit with another bit is stored in the specified P box table without any expansion or compression this is called P-box Permutation.

Step 5-XOR and Swap



Final Permutation

- At the end of rounds the final permutation is performed.
- This is simple transposition the 40th input bit takes the 1st output position and 8th input bit takes the 2nd output position and so on…

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

Problem of DES

- Key agreement or key distribution.
- Same key is used for encryption or decryption one key per communicating parties is required.
- So if there are so many communicating parties then there are so many keys are required.

Strength of DES

- Key size i.e.56 bit key

  i.e. 2^56 possible keys

  =7.2*10^16 keys

- Nature of the algorithms

✓ S-box Substitution

✓ P-box Permutation

✓ Timing Attack

Reference

- Cryptography and network security “Atul Kahate” 3e,Mc Graw hill education.