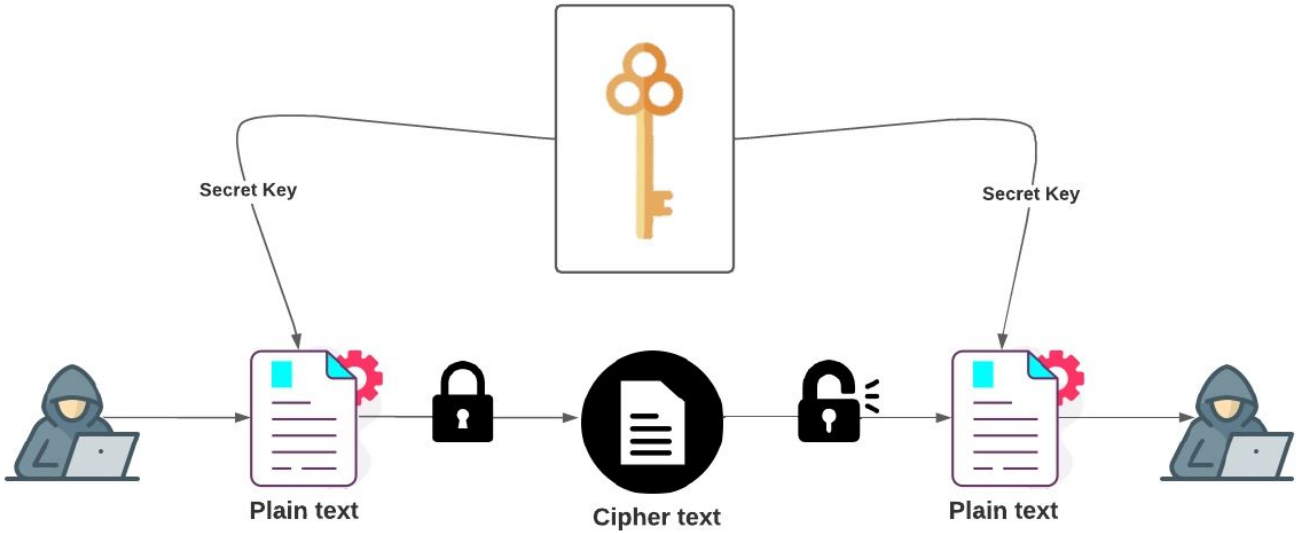
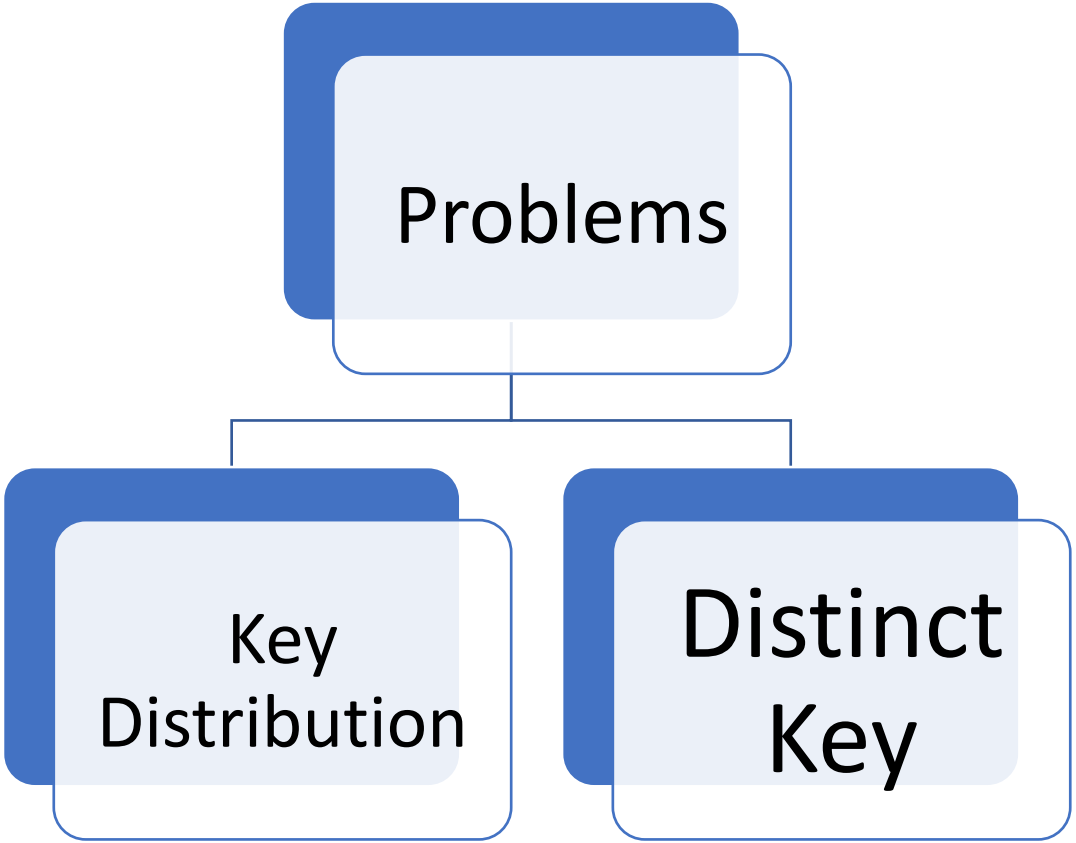
Unit 2 Cryptography



Cryptography & Network Security

- Cryptography
- Cryptography & Cryptanalysis
- Encryption Techniques
- Types of Cryptography
- Symmetric Encryption Algorithms

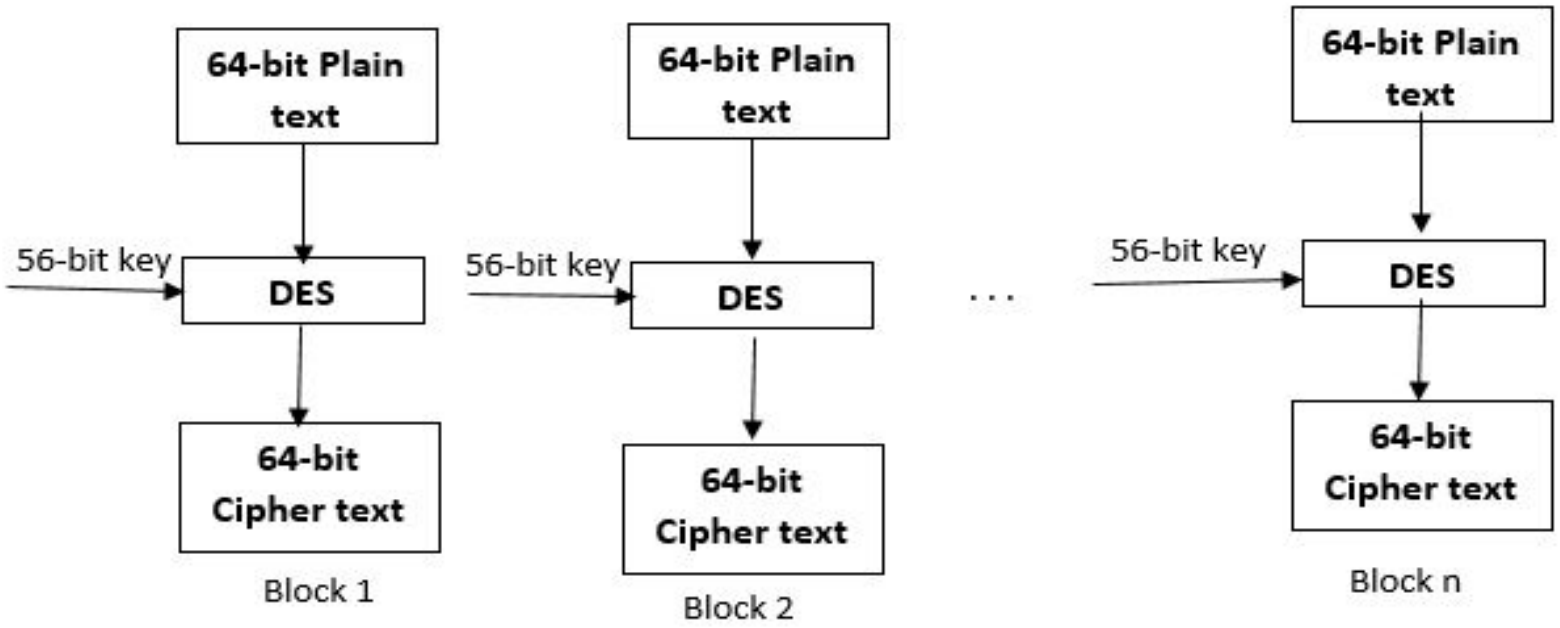
Symmetric Key Cryptography



DES (Data Encryption Standard) History

- IBM developed Lucifer cipher by team led by Feistel
- used 64-bit data blocks with 128-bit key
- then redeveloped as a commercial cipher with input from National Security Agency (NSA) and others
- in 1973 National Bureau of Standards (NBS) issued request for proposals for a national cipher standard
- IBM submitted their revised Lucifer which was eventually accepted as the DES

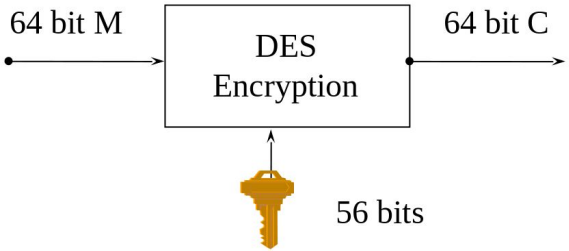
Conceptual Working of DES



(Figure: Conceptual working of DES)

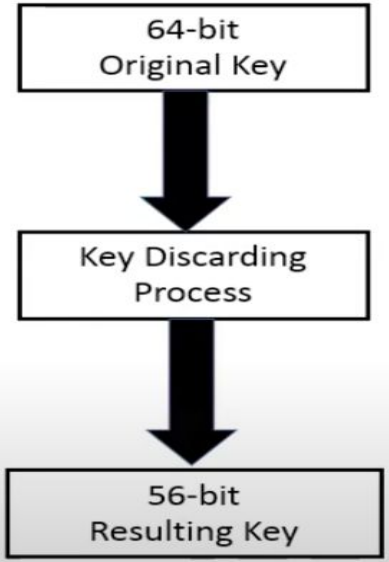
DES (Data Encryption Standard)

- Published in 1977, standardized in 1979.
- Key: 64 bit quantity=8-bit parity+56-bit key
- Every **8th** bit is a parity bit.
- 64 bit input, 64 bit output.



DES (Data Encryption Standard)

- **Key discarding process**



Every 8th Bit of Original Key is Discarded

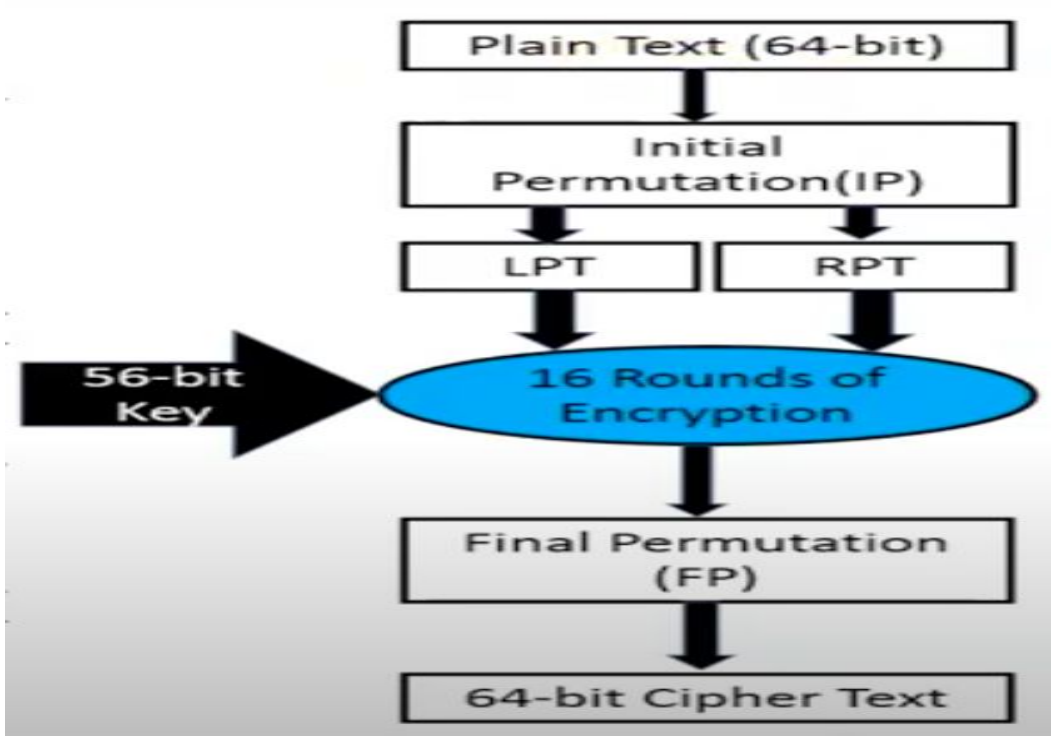
1	2	21	38	58	15	37	26
22	55	44	3	53	27	11	60
49	28	14	42	61	48	63	41
18	39	56	10	64	16	62	8
45	40	20	54	4	33	34	52
7	30	47	59	32	5	35	25
29	12	13	6	24	46	57	36
17	23	50	31	43	51	9	19

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

Steps of DES

Step 1	• 64 bit plain text block is handed over to an initial Permutation (IP) function.
Step 2	• IP performed on 64-bit plain text block.
Step 3	• IP produces two halves of the permuted block known as Left Plain Text (LPT) and Right Plain Text (RPT).
Step 4	• Each LPT and RPT to go through 16 rounds of encryption process.
Step 5	• LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
Step 6	• 64-bit Cipher text block is generated.

Broad level steps of DES



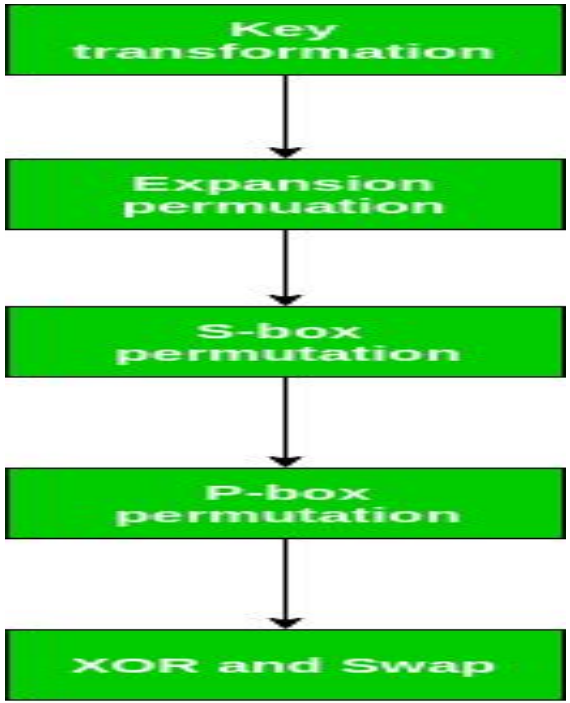
Initial Permutation (IP)

- the Initial permutation (IP) happens **only once and it happens before the first round.**
- For example, the IP replaces the 1st bit of the original plain text block with the 58th bit of the original plain text,
- the 2nd bit with the 50th bit of the original plain text block and so on.
- This is nothing but jugglery of bit positions of the original plain text block.
-

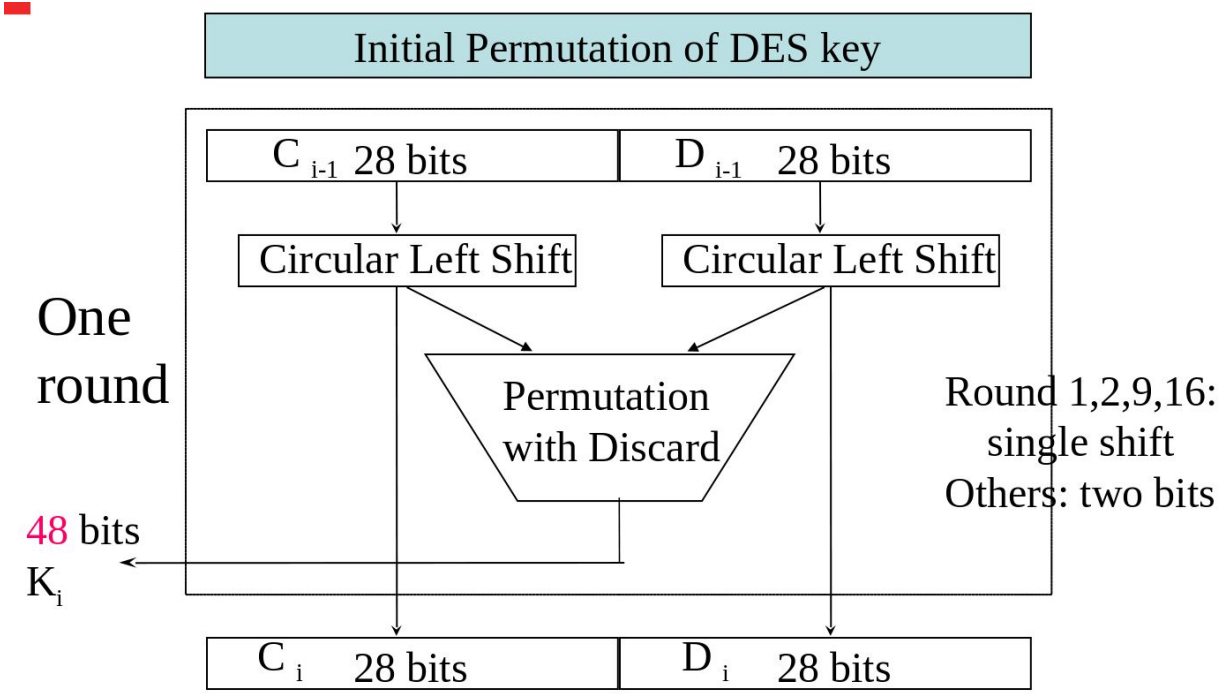
58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	33	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Figure - Initial permutation table

Details of DES Round



Per-Round Key Generation



Per-Round Key Generation

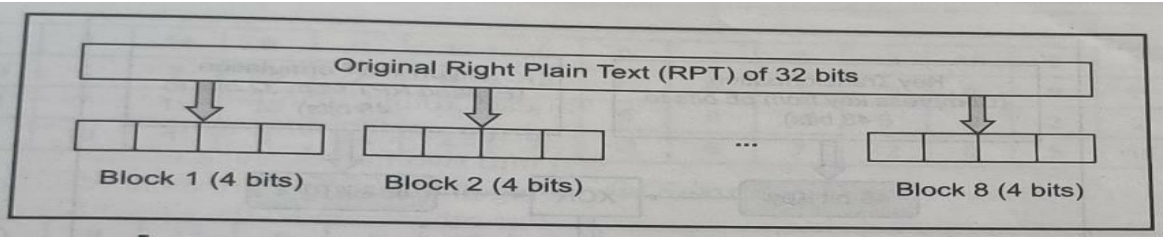


Fig. 3.27 *Division of 32-bit RPT into eight 4-bit blocks*

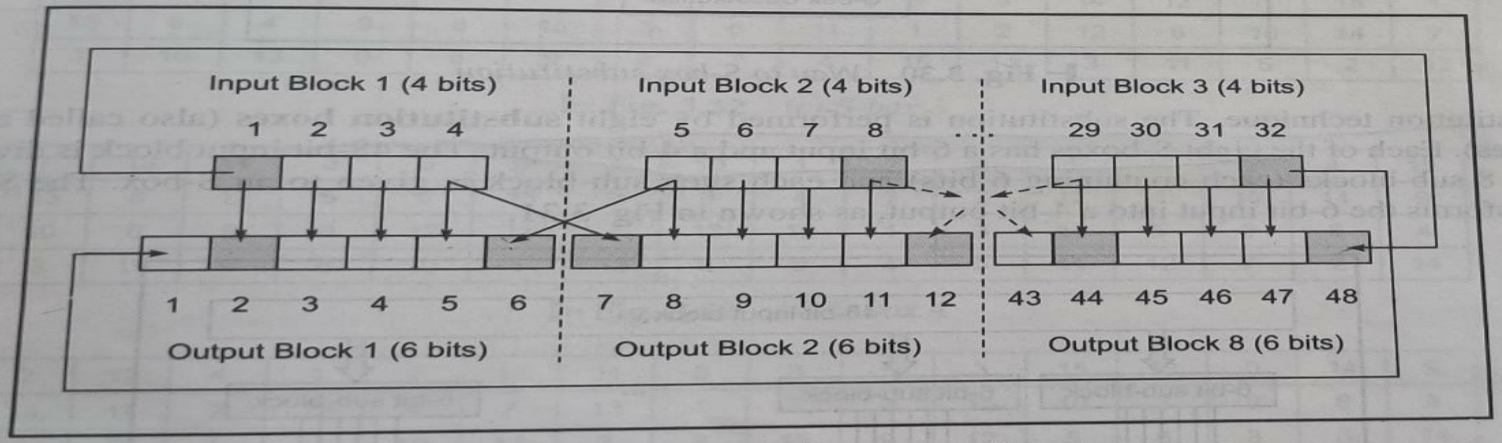


Fig. 3.28 *RPT expansion permutation process*

Key Transformation

- The initial 64-bit key is transformed into a 56-bit key by discarding every 8th bit of the initial key.
- From this 56-bit key, a different **48-bit Sub Key** is generated during each round using a process called **as key transformation**.
- For this the 56 bit key is divided into two halves, each of 28 bits.
- These halves are circularly shifted left by one or two positions, depending on the round.
- If the round number is **1, 2, 9 or 16** the shift is done by **only 1 position**
- For other rounds, the circular shift is done by 2 positions, The number of key bits shifted per round is show in figure.

Key Transformation

- After an appropriate shift, 48 of the 56 bit are selected.
- For selecting 48 of the 56 bits, shift is applied, for instance, after the shift, bit number 14 moves on the 1st position, bit number 17 moves on the 2nd position and so on.
- Shift is done based on the table, it contains only 48 bit positions. Bit number 18 is discarded, same with 7 others.
- Since the key transformation process involves permutation as well as selection of a 48-bit sub set of the original 56-bit key it is called **Compression Permutation**.

14	17	11	24	1	5	3	28	15	6	21	10
[illegible]										
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Figure - compression permutation

Expansion Permutation

- After initial permutation, we had two 32-bit plain text areas called as Left Plain Text(LPT) and Right Plain Text(RPT).
- During the expansion permutation, **the RPT is expanded from 32 bits to 48** bits. Bits are permuted as well hence called as expansion permutation.
- The 32 bit RPT is divided into 8 blocks, with each block consisting of 4 bits.
- Then, each 4 bit block of the previous step is then expanded to a 6 bit block, i.e., per 4 bit block, 2 more bits are added.

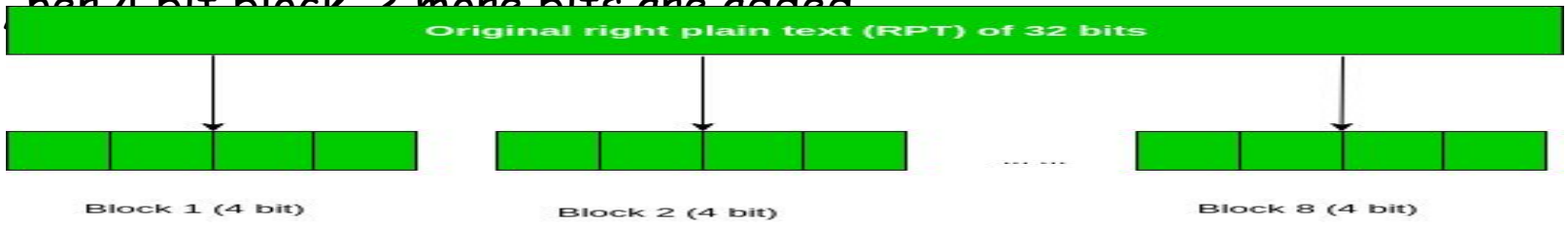


Figure - division of 32 bit RPT into 8 bit blocks

Expansion Permutation

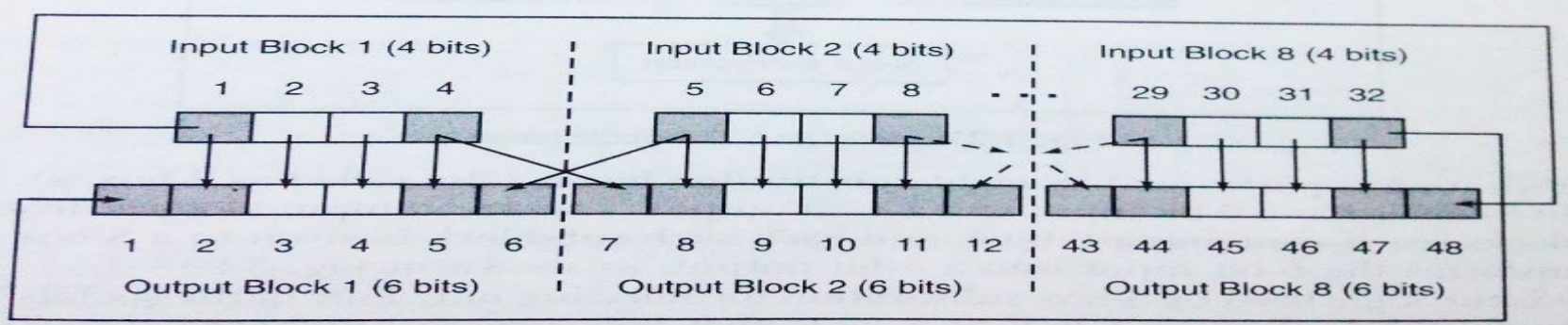
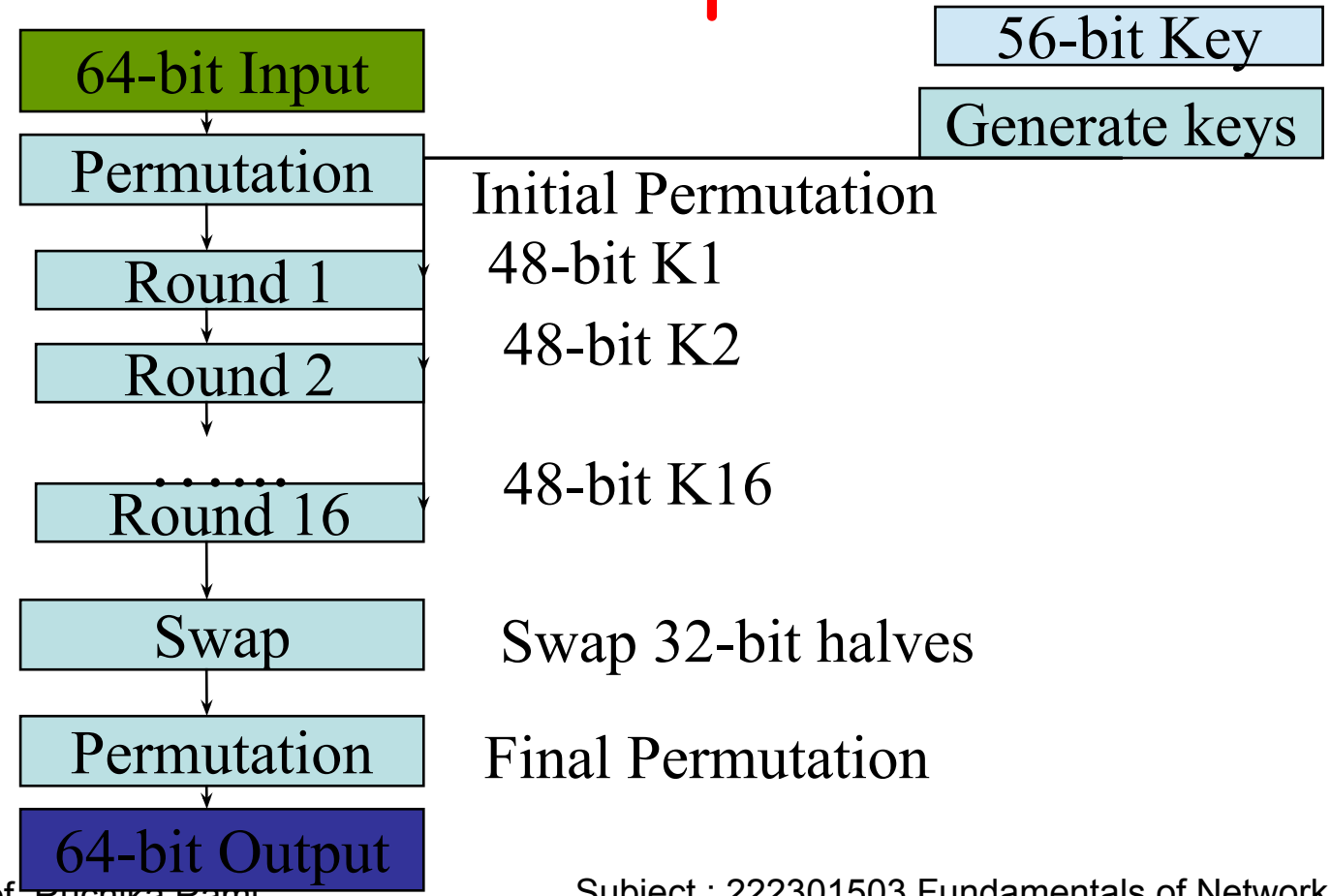


Fig. 3.25 *RPT expansion permutation process*

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

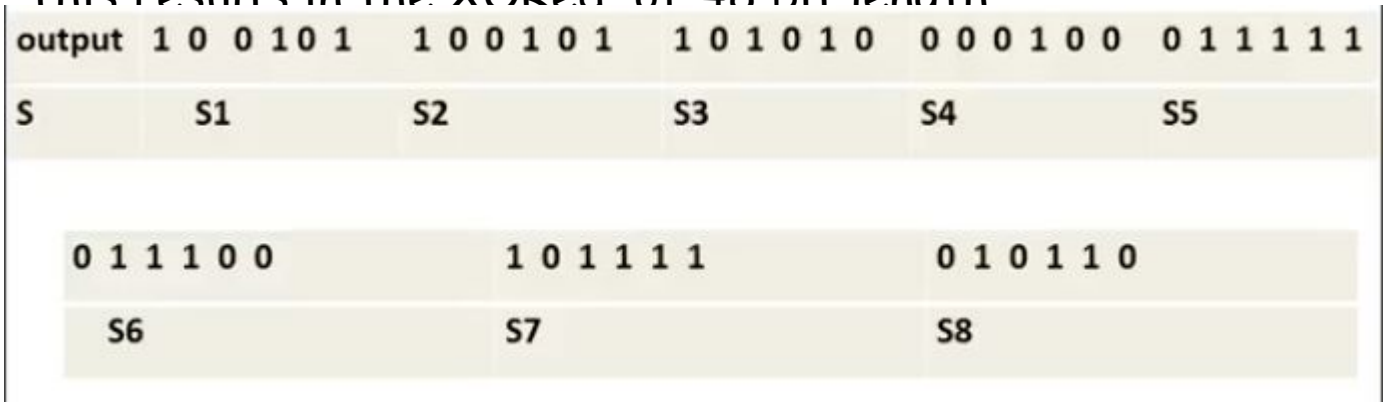
Fig. 3.26 *RPT expansion permutation table*

DES Top View


64-bit Input
Permutation
Round 1
Round 2
.....
Round 16
Swap
Permutation
64-bit Output
56-bit Key
Generate keys
Initial Permutation
48-bit K1
48-bit K2
48-bit K16
Swap 32-bit halves
Final Permutation

XOR

- This step involves the bitwise XOR operation
- Expanded RPT of 48 bit length XOR Compressed Key of 48 bit length.
- This results in the XORed of 48 bit length



S Box Substitution

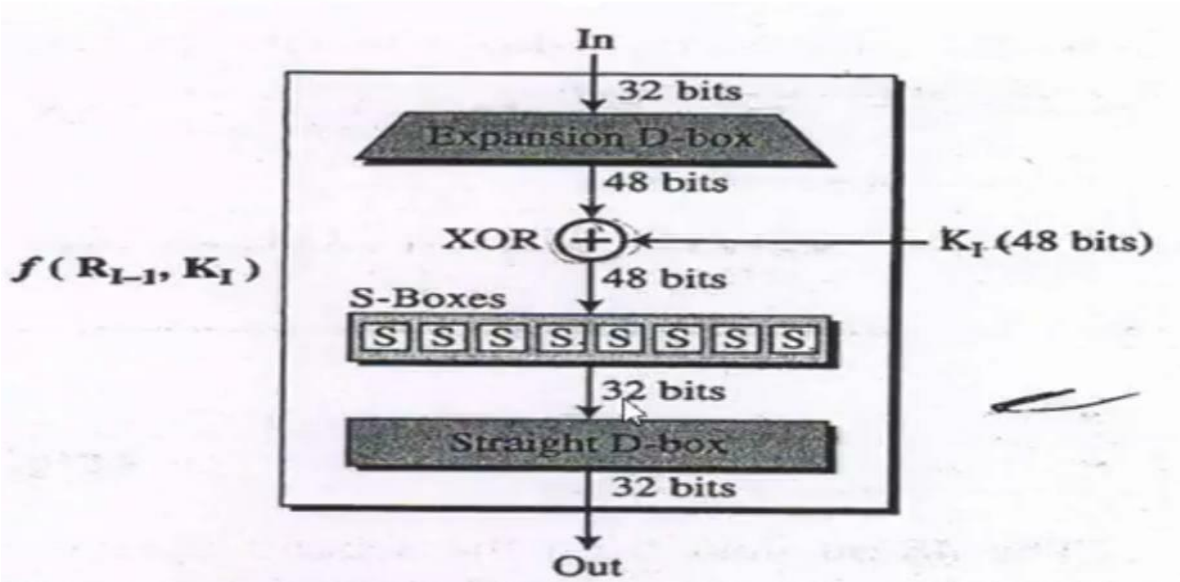
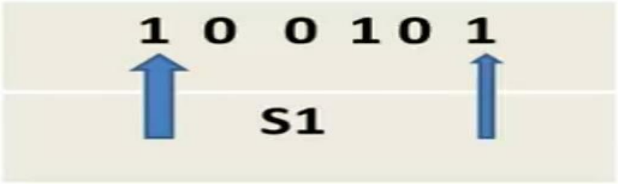


Fig. 6.5 *DES function*

S Box Substitution

- The XORed RPT is fed into the S Box Substitution step.
- the XORed RPT is again divided into 8 blocks of 6 bit each.
- For each block, there is a separate S Box table which gives 4 bit output.
- There are 8 S Box tables corresponding to 8 blocks.
- For example, Block 1 will be fed to S Box 1, Block 2 to S Box 2 and so on.
- S Box tables consist of 4 rows and 16 columns. Each row contains 0 to 15 numbers in haphazard manner.
- These 0 to 15 numbers can be represented with 4 bits.
- Each block contains 6 bits, these 6 bits tell us the row number and the column number of the S Box table corresponding to that block.
- The 1st bit and the 6th bit determines the row number whereas 2nd, 3rd, 4th and 5th bits determine the column number.

S Box Substitution



11 = 3

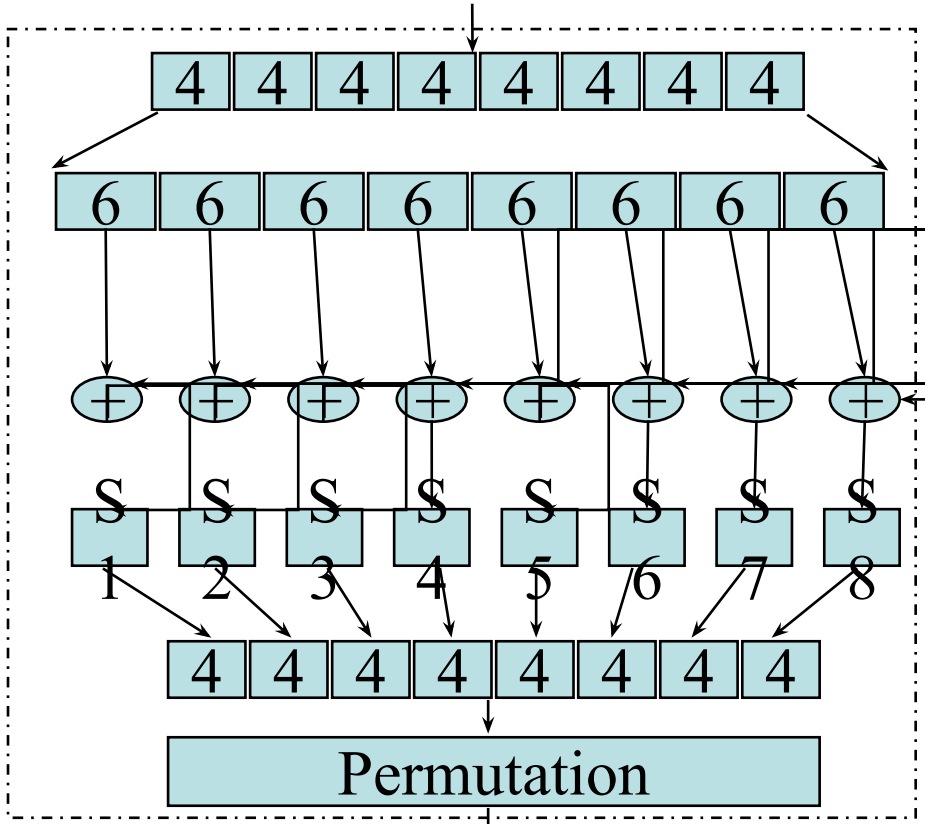
0010 = 2

mw	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	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	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S1	S2	S3	S4	S5	S6	S7	S8
1 0 0 0	1 0 1 0	1 1 1 1	1 1 1 0	0 1 1 0	0 1 0 1	0 1 1 1	1 1 1 0
1,2,3,4	5,6,7,8,	9,10,11,12	13,14,15,16	17,18,19,20	21,22,23,24	25,26,27,28,	29,30,31,32

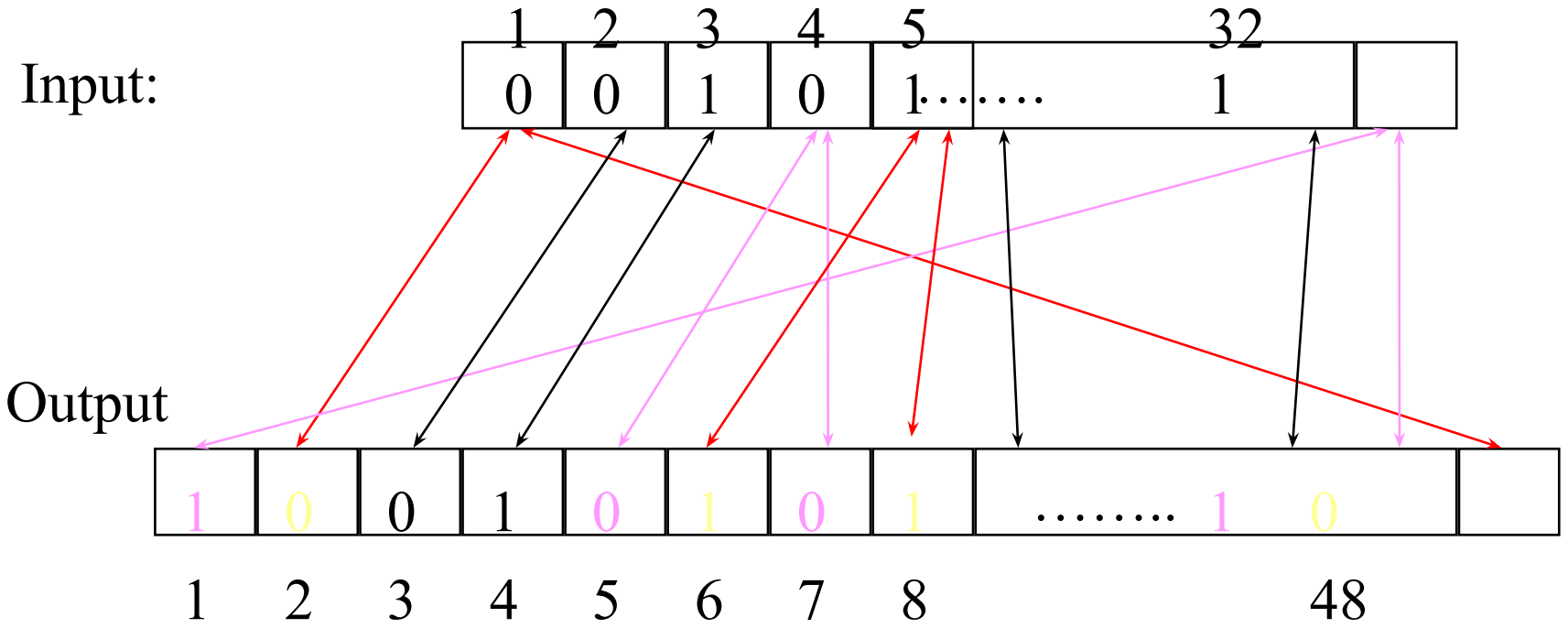
S Box Substitution

Mangler Function



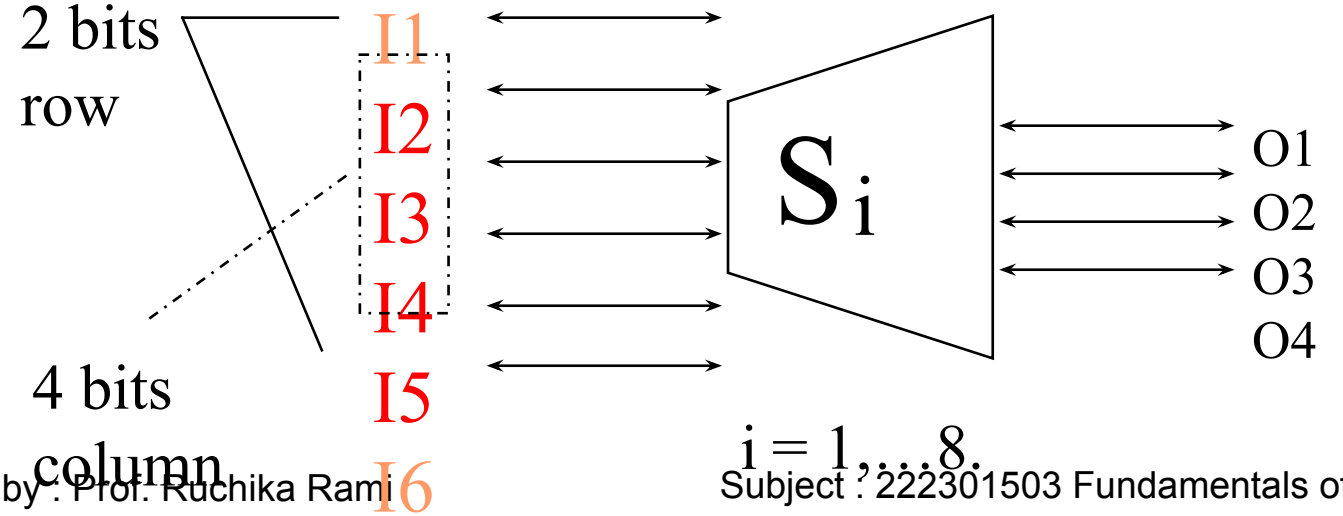
The permutation produces "spread" among the chunks/S-boxes!

Bits Expansion (1-to-m)



S-Box (Substitute and Shrink)

- 48 bits ==> 32 bits. (8*6 ==> 8*4)
- 2 bits used to select amongst 4 substitutions for the rest of the 4-bit quantity



S-Box Example (S-Box 1)

Each row and column contain different numbers.

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

Example: input: 100110 output: ???

P Box Permutation

- S Box RPT will be permuted according to the P Box table giving rise to P Box RPT.

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

Fig. 3.32 *P-box permutation*

XOR and SWAP

- All the operations till now have been performed on 32 bit RPT.
- Now XOR LPT with the outcome of P Box permutation.
- The result of this XOR is new RPT.
- Swap the old RPT and make it new LPT.
- At the end of the 16 rounds, the Final Permutation is done on the combined LPT and RPT giving rise to 64 bit first Cipher Text block.
- It is c

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

Fig. 3.34 Final Permutation

A DES Round

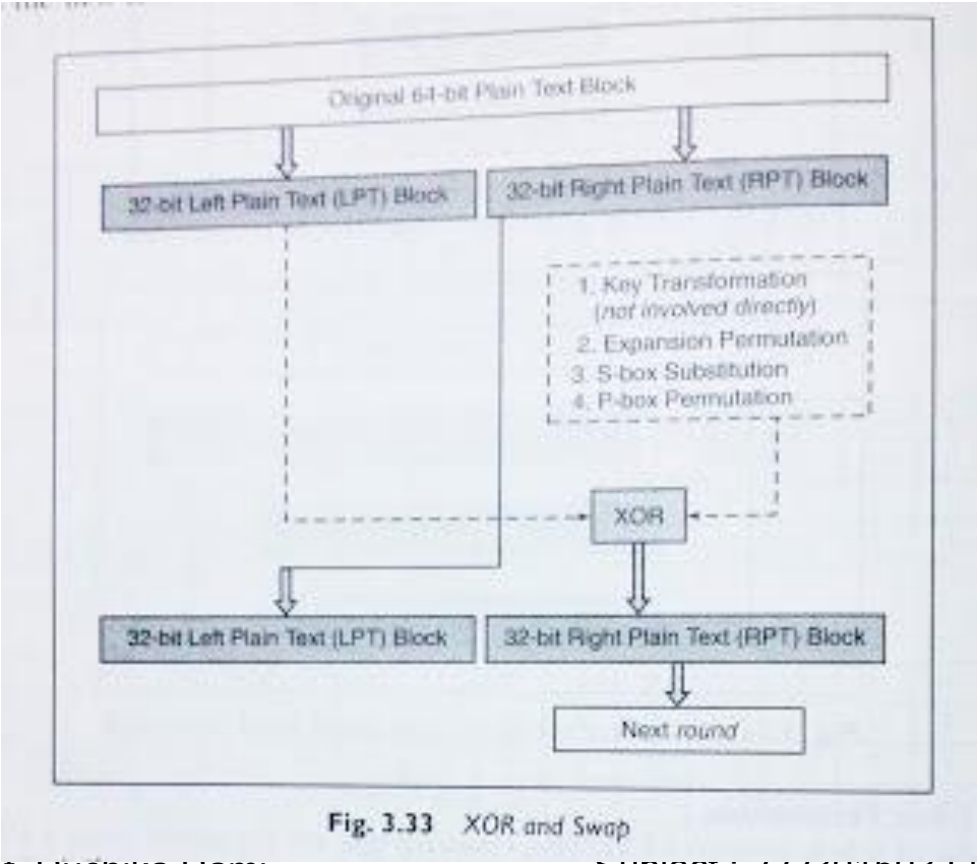
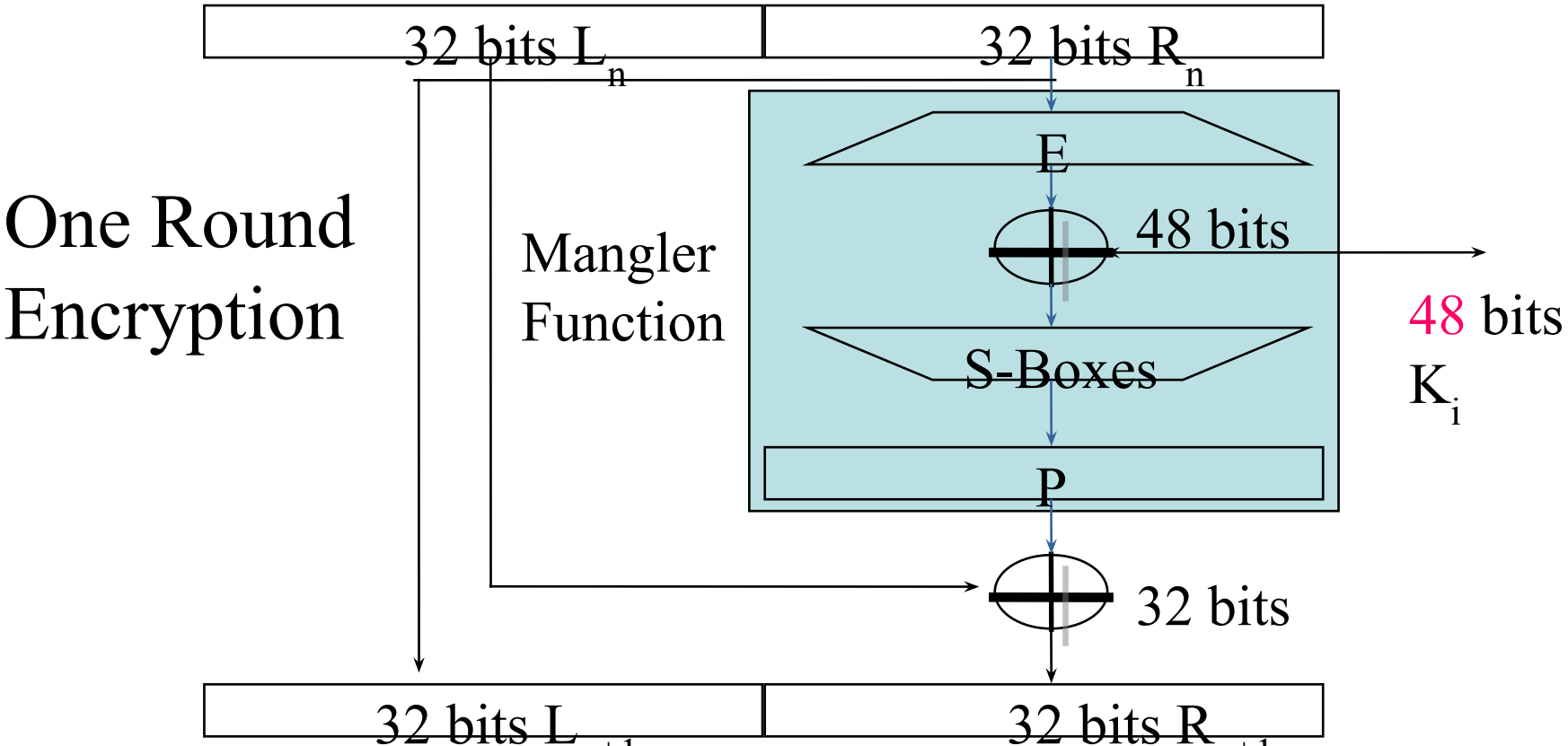


Fig. 3.33 *XOR and Swap*

A DES Round


One Round Encryption
Mangler Function
32 bits L_n
32 bits R_n
E
48 bits
S-Boxes
P
48 bits K_i
32 bits
32 bits L_{n+1}
32 bits R_{n+1}

DES Standard

- Cipher Iterative Action :
  - Input: 64 bits
  - Key: 48 bits
  - Output: 64 bits
- Key Generation Box :
  - Input: 56 bits
  - Output: 48 bits

One round (Total 16 rounds)

Strength of DES – Key Size

- 56-bit keys have $2^{56} = 7.2 \times 10^{16}$ values
- Brute force search looks hard
- Recent advances have shown is possible

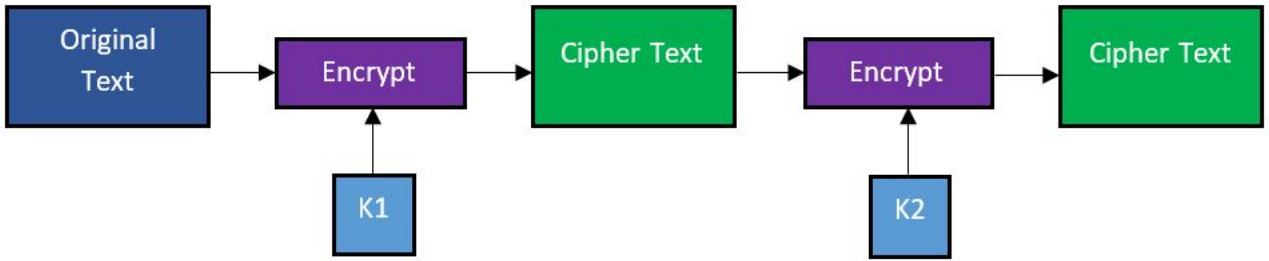
– in 1997 on a huge cluster of computers over the Internet in a few months

– in 1998 on dedicated hardware called "DES cracker" by EFF in a few days ($220,000)

– in 1999 above combined in 22hrs!

DES Replacement

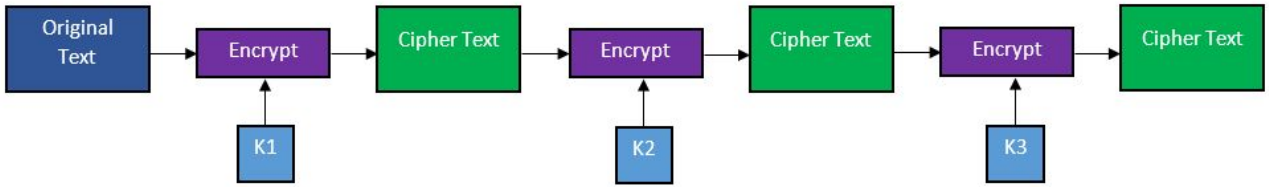
- Double-DES (2DES)



Double DES

DES Replacement

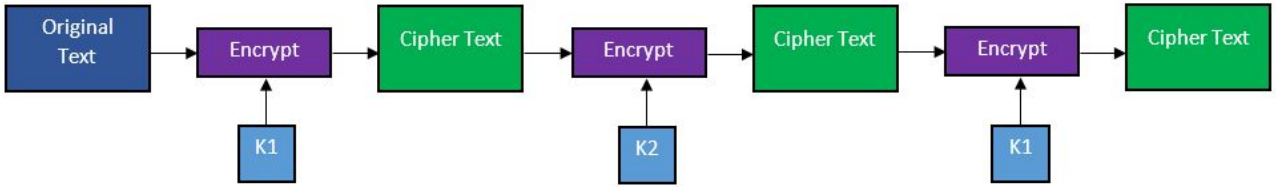
- Triple-DES (3DES)



Triple DES with 3 keys

DES Replacement

- Triple-DES (3DES)



Triple DES with 2 keys

Advanced Encryption Standard (AES)

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- It is based on 'substitution-permutation network'.
- Computations performed on bytes. Hence, AES treats the 128 bits of a plaintext block as 16 bytes.

AES

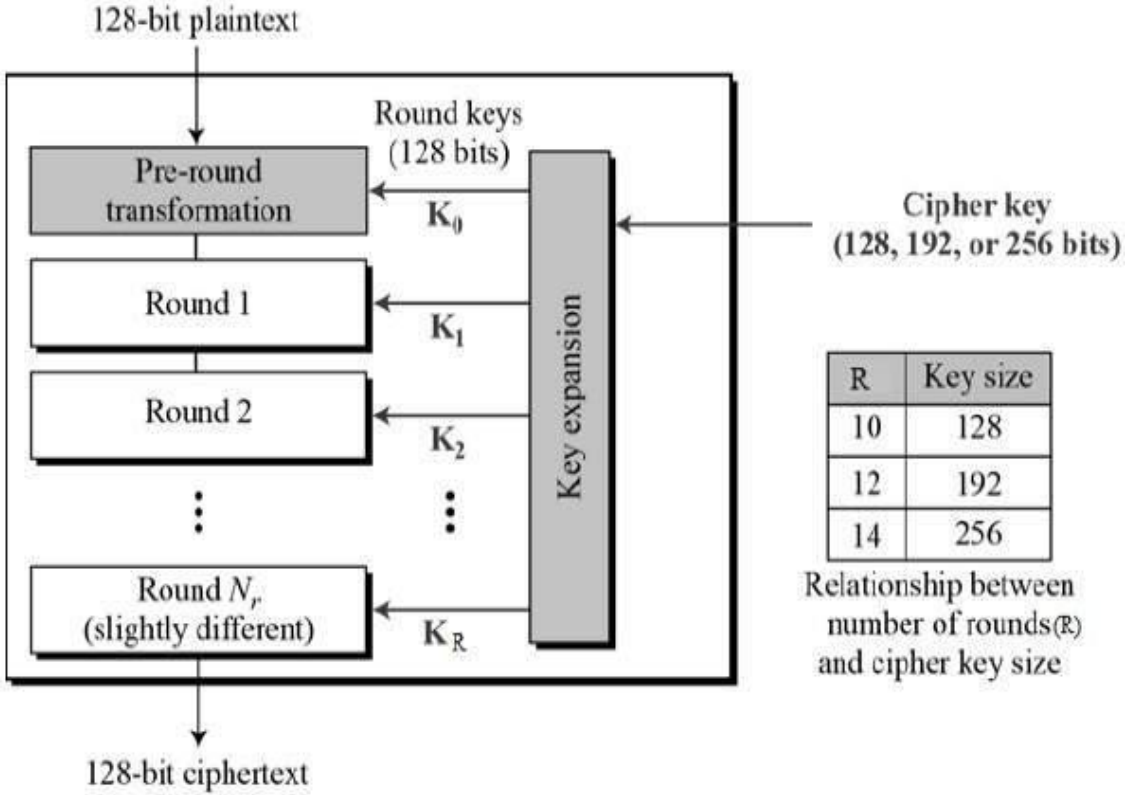
- These 16 bytes are arranged in 4 columns and 4 rows for processing as a matrix –
- No. of rounds in AES is variable and depends on the length of the key.
- AES uses

–10 rounds for 128-bit keys,

–12 rounds for 192-bit keys

–14 rounds for 256-bit keys.

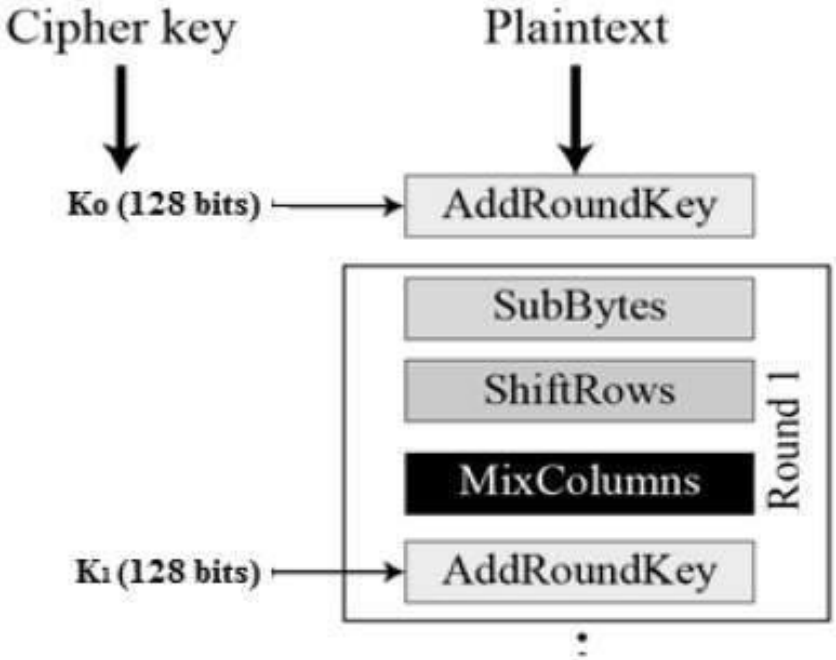
Schematic of AES



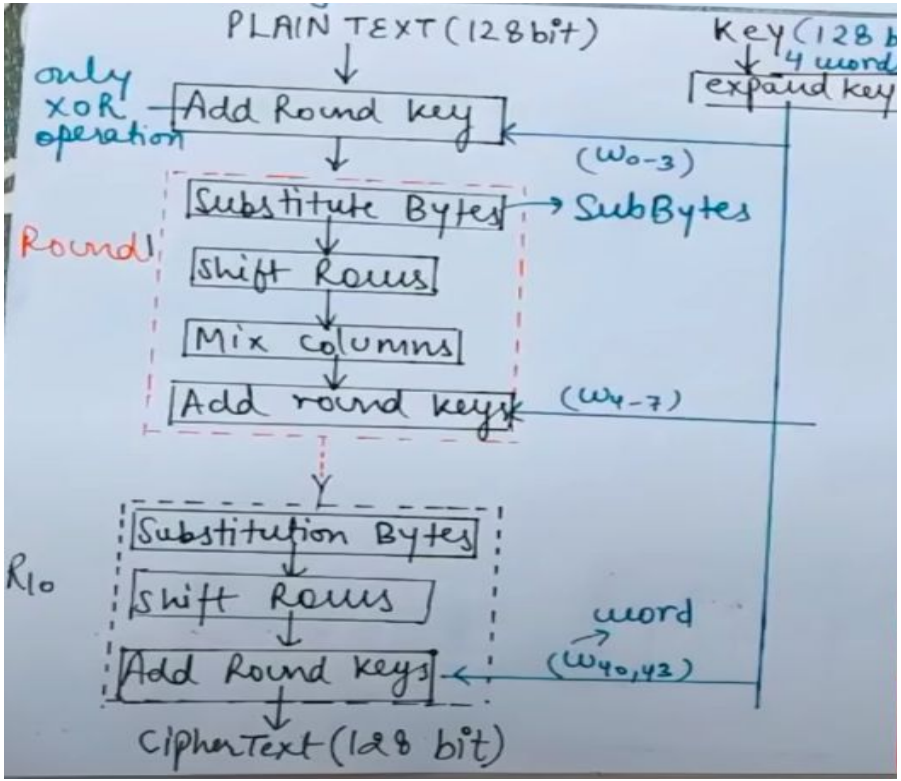
R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

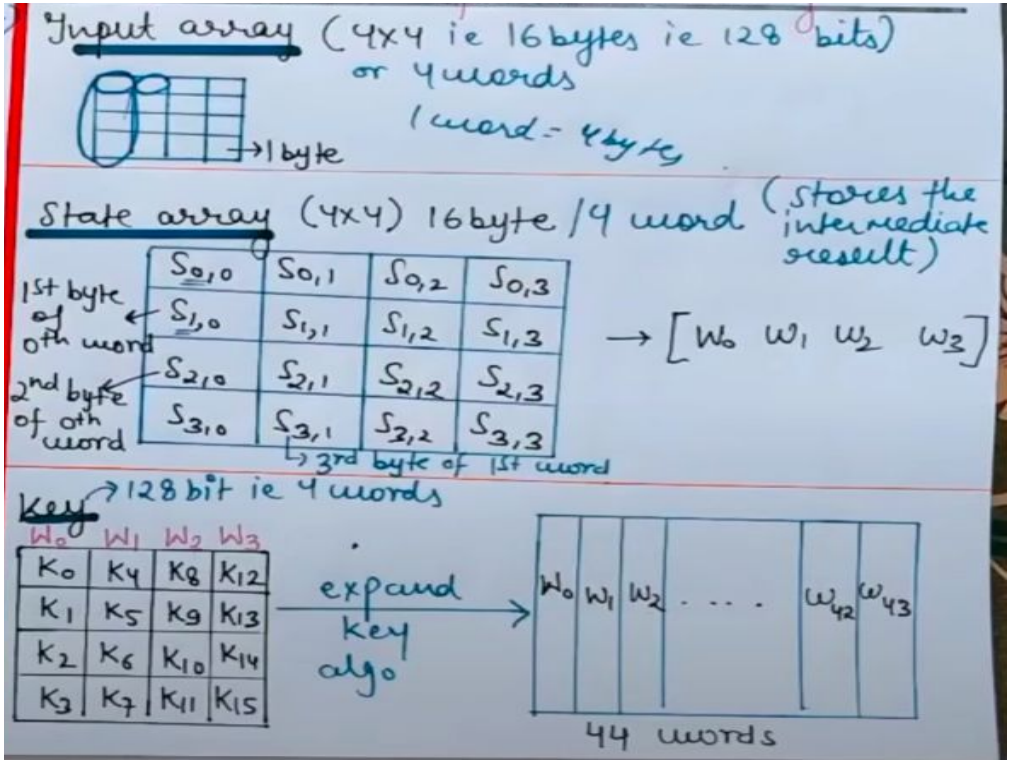
Encryption Process of AES



Encryption Process of AES

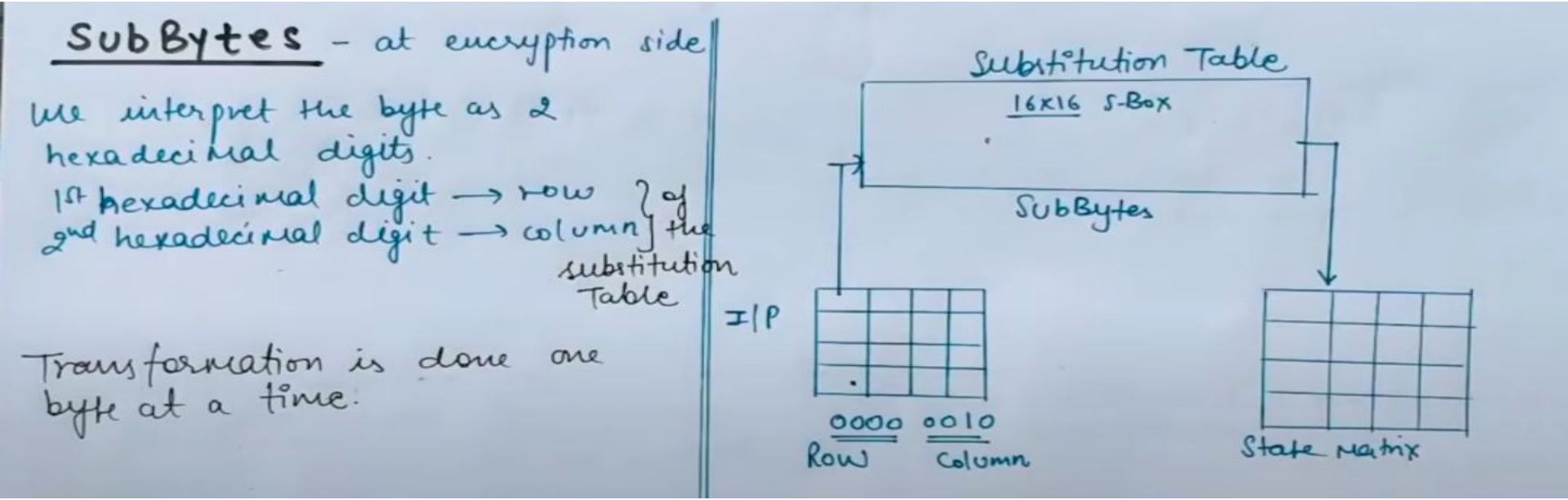


Sub Processes



Sub Processes

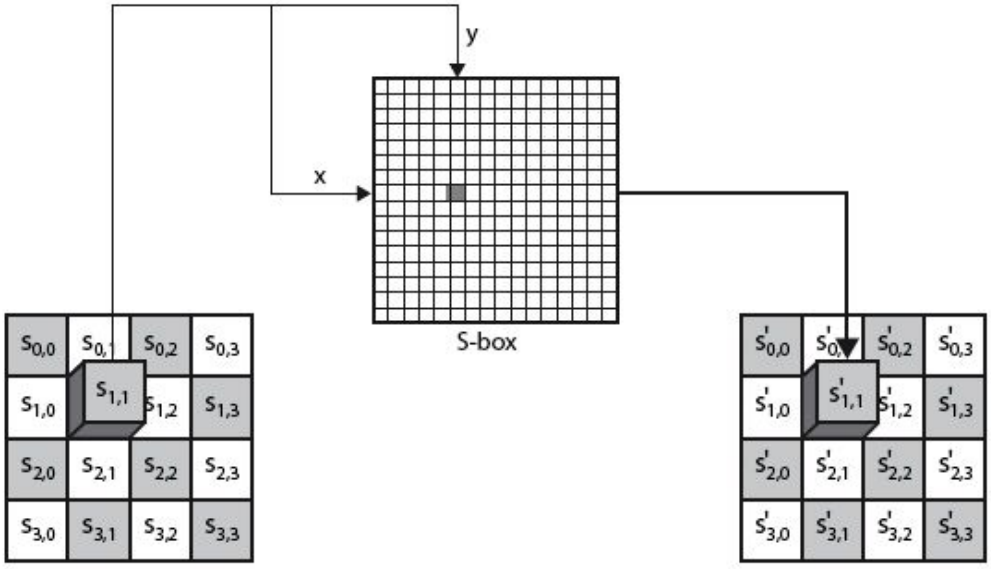
Byte Substitution (SubBytes)



Sub Processes

Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box). The result is in a matrix of 4 rows and 4 columns.



Sub Processes

Shift rows

Each of the 4 rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

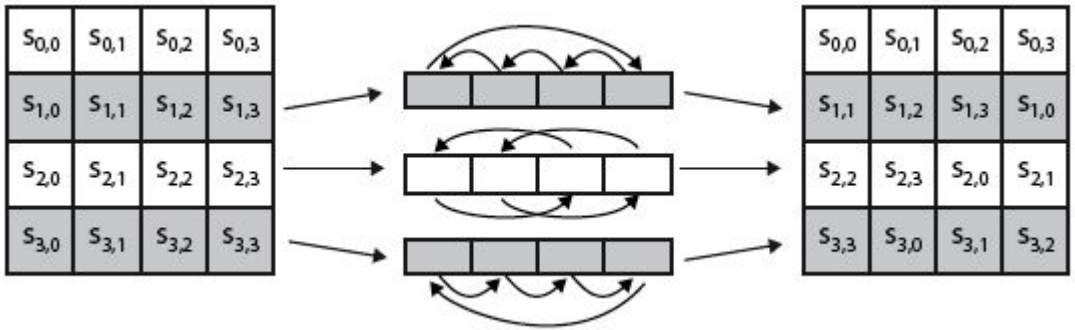
First row is not shifted.

Second row is shifted one (byte) position to the left.

Third row is shifted two positions to the left.

Fourth row is shifted three positions to the left.

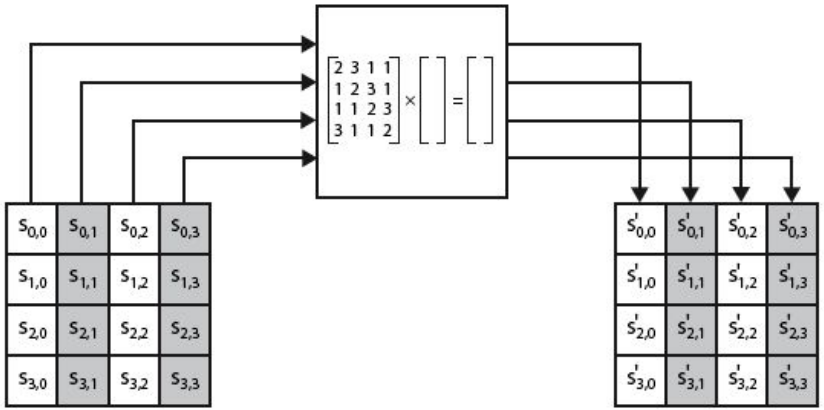
The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.



Sub Processes

Mix Columns

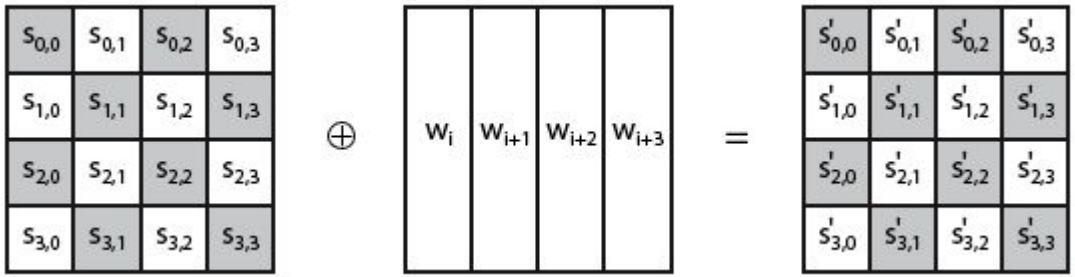
- Each column of 4 bytes is now transformed using a special mathematical function.
- This function takes as input the 4 bytes of 1 column and outputs 4 completely new bytes, which replace the original column.
- The result is another new matrix consisting of 16 new bytes.
- This step is not performed in the last round.



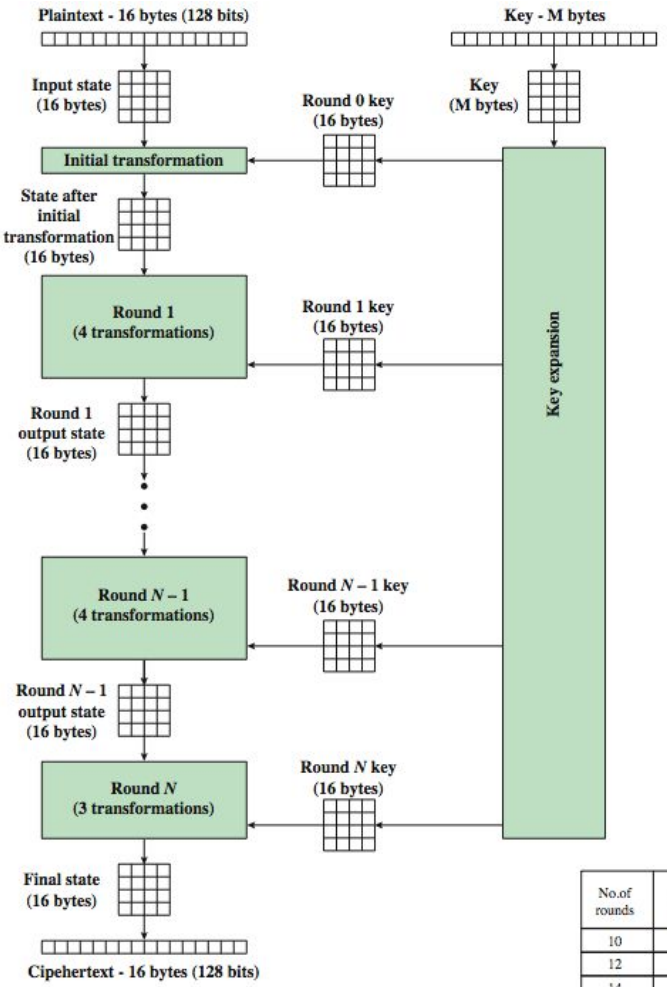
Sub Processes

Add round key

- The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key.
- If this is the last round then the output is the ciphertext.
- Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.



AES View



No.of rounds	Key Length (bytes)
10	16
12	24
14	32

THANK YOU