PESU ISFCR

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES UNIVERSITY

Welcome to

PES University

Ring Road Campus, Bengaluru

10 June 2020

PESU Center for
Information Security,
Forensics and
Cyber Resilience

APPLIED CRYPTOGRAPHY

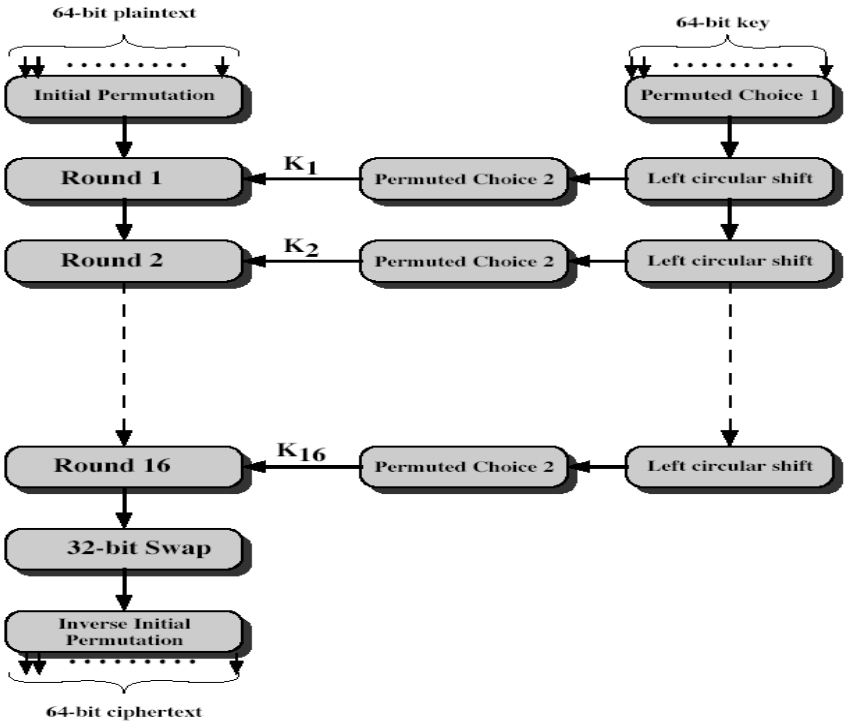
Private key Systems

Lecture 5

Initial and Final permutations

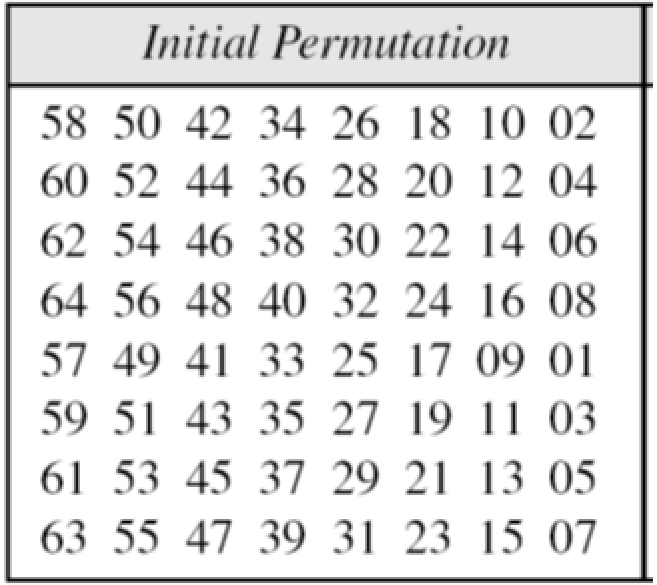
Change in bit position changes a lot in output

Initial permutation



- Initial permutation IP which shuffles the 64 bit input block
- A final permutation being inverse of Initial permutation

Initial permutation tables

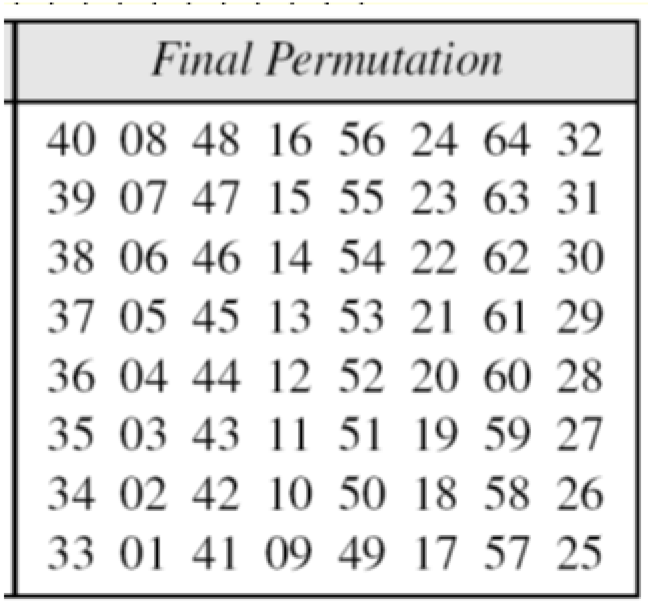


Initial Permutation

58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

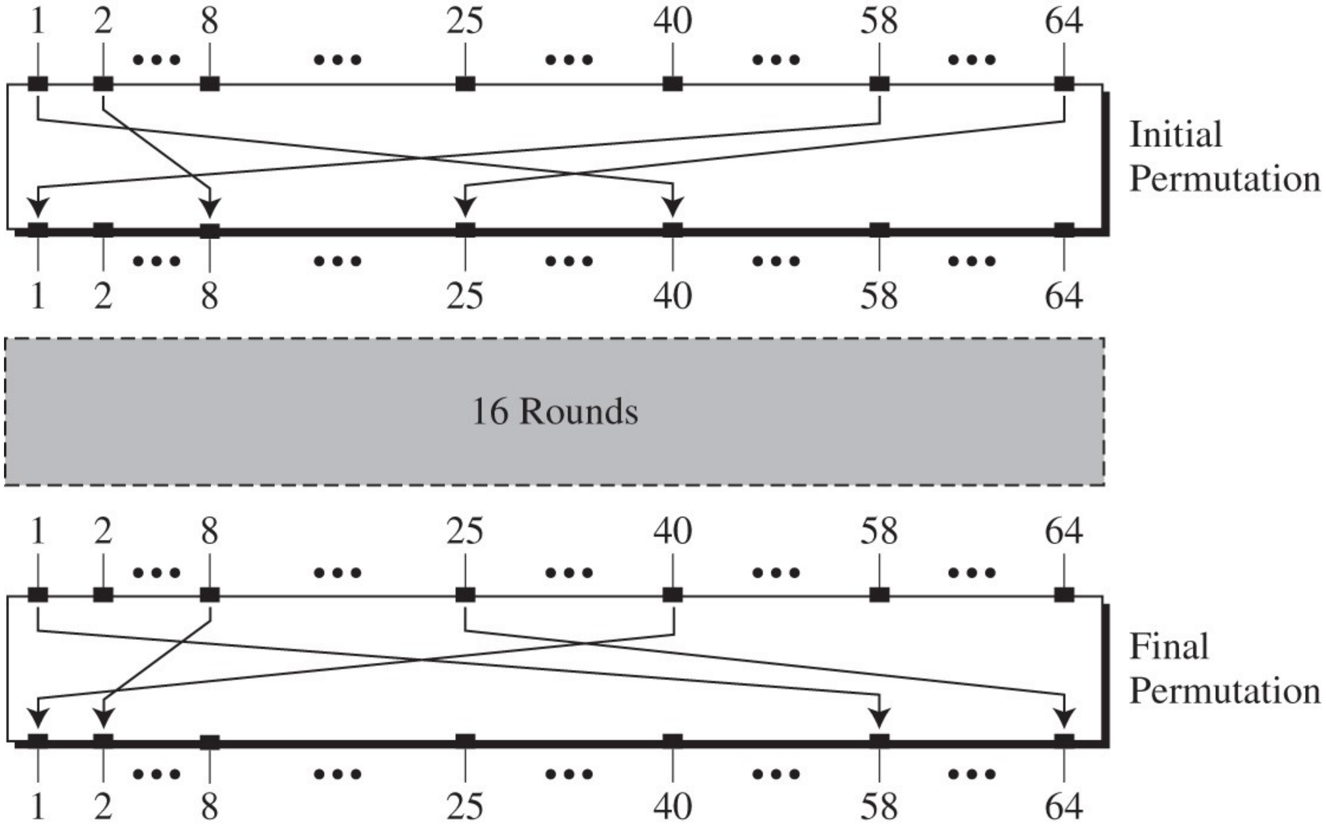
- Means a value which is present a 1 bit at input of p-box (0 or 1) should be moved to 58 bit in output of p-box.

Final *permutation tables*

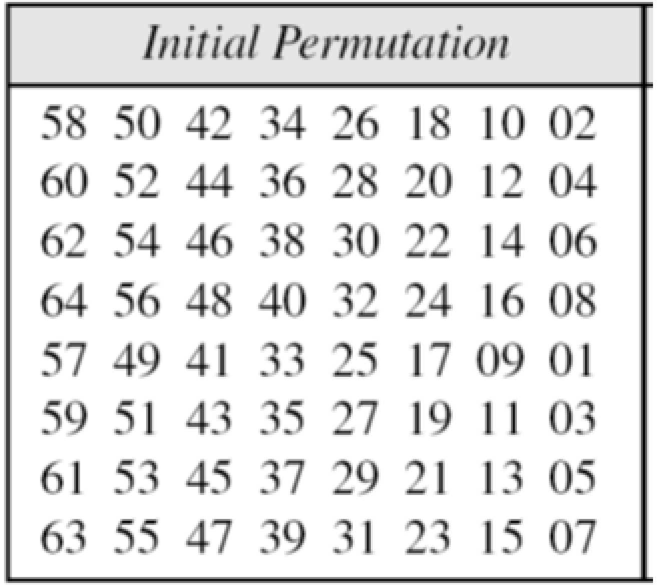


Final Permutation							
40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25

- Inverses the initial permutation values
- Observe that a value at 58 position will be moved to 1 position which is nothing but reverse of initial permutation.


1
2
8
25
40
58
64
Initial Permutation
16 Rounds
Final Permutation

Find the output of the initial permutation box when the input is 0x0000 0080 0000 0002



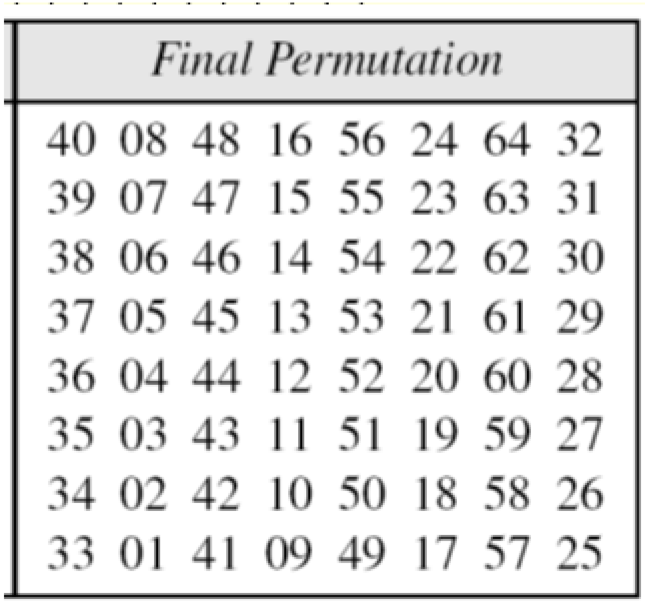
Initial Permutation							
58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

- Input is in hexadecimal number
- Convert it into binary format
- Place the bit values according to initial permutation table
- Convert back the result to hexadecimal number

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
0				0				0				0				Data
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Binary
58	50	42	34	26	18	10	02	60	52	44	36	28	20	12	04	IP
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	IP o/p
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	
0				0				8				0				
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	
62	54	46	38	30	22	14	06	64	56	48	40	32	24	16	08	
0	0	0	0	0	00	0	0	0	0	0	0	0	0	0	0	
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	
0				0				0				0				
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
57	49	41	33	25	17	09	01	59	51	43	35	27	19	11	03	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	
0				0				0				2				
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	
61	53	45	37	29	21	13	05	63	55	47	39	31	23	15	07	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	

when the input is 0x0000 0080 0000 0002
Output is   0x0002 0000 0000 0001

Prove that the initial and final permutations are the inverse of each other (Assignment for Learners)



Final Permutation							
40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25

- From the previous slide input for final permutation is

  0x0002 0000 0000 0001

When bit value changes according to final permutation table the result is

  0x0000 0080 0000 0002

Which is same as input to initial permutation

- Therefore initial and final permutation are inverse of each other

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU ISFCR

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PESU IoT

PESU Center for
Internet
of Things