IAS (IT352) Lab Program-1(a)

Use any one of the following programming languages Python/Java/C++/C to implement round key generation algorithm of Data Encryption Standard (DES). Your program should take run-time input (alphanumeric) then it should convert into binary then it should generate all sixteen round keys. Print all round keys on terminal and also store them on text file (.txt). **Do not use any library directly on your program.**

Permutation Choice-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

PC-1

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
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

IAS (IT352) Lab Program-1(b)

Use any one of the following programming languages Python/Java/C++/C to show initial and final permutation of Data Encryption Standard (DES) are inverse of each other. Your program should take run-time input (alphanumeric) then it should convert into binary then show the output step by step. Print all results (initial binary values, output of initial permutation table, output of final permutation. **Do not use any library directly on your program.**

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

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

IAS (IT352) Lab Program-1 (c)

Use any one of the following programming languages Python/Java/C++/C to implement Expansion permutation box of Data Encryption Standard (DES). Your program should take run-time input (alphanumeric) then it should convert into binary then show the output step by step. Print all results (initial binary values block-by-block of 64 bits). Divide 64 bit block into two sub-blocks of 32 bits and apply expansion permutation on right block of 32 bit block. Print all intermediate values and also store them on text file (.txt). **Do not use any library directly on your program.**
