Bài tập 5: DES

Bài tập 1: Một tính chất quan trọng làm cho DES an toàn là các S-box phi tuyến. Trong bài tập này, ta sẽ cùng kiểm tra tính chất này bằng cách tính output của S_1 với một số cặp input/output.

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Hãy chứng minh rằng $S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$, ở đây $\oplus$ ký hiệu phép toán `XOR`, cho các giá trị:

1. $x_1 = 000000,\ x_2 = 000001$
2. $x_1 = 111111,\ x_2 = 100000$
3. $x_1 = 101010,\ x_2 = 010101$

Bài tập 2: Ta muốn kiểm tra liệu $IP(\cdot)$ và $IP^{-1}(\cdot)$ có thực sự là phép toán nghịch của nhau.

IP							
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

IP^{-1}							
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

Ta xét vector gồm 64 bit $x = (x_1,\ x_2,\ \ldots,\ x_{64})$. Hãy chỉ ra rằng $IP^{-1}(IP(x)) = x$ với năm bit đầu tiên của x, tức là với $x_i,\ i = 1, 2, 3, 4, 5$.

Bài tập 3: Output của vòng đầu tiên của thuật toán DES là gì khi bản rõ và khoá toàn bit 0?

Bài tập 4: Output của vòng đầu tiên của thuật toán DES là gì khi bản rõ và khoá toàn là bit 1?