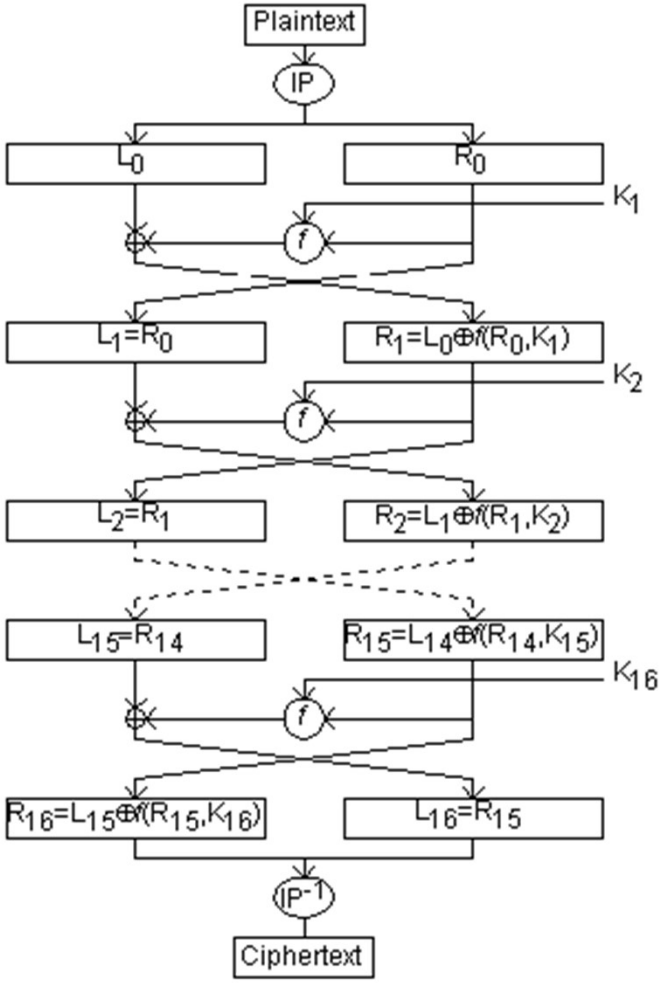
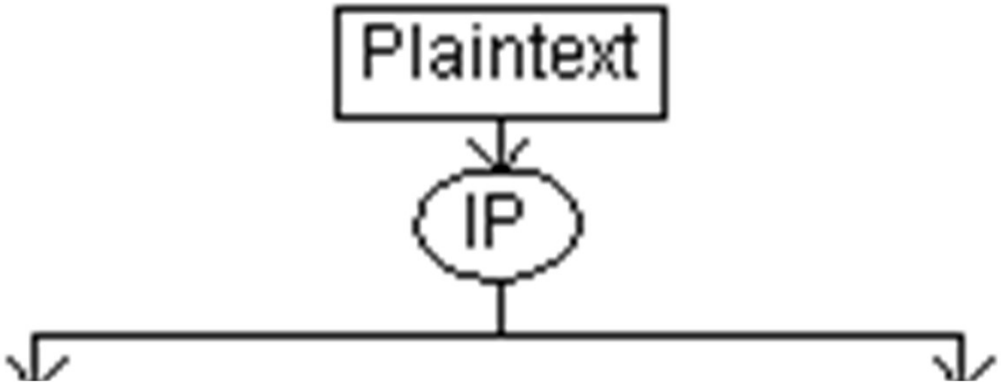
Advanced Cryptography

IT3RA 2558 :D

Paranat K.


Plaintext
IP
L0
R0
K1
f
L1=R0
R1=L0⊕f(R0,K1)
K2
f
L2=R1
R2=L1⊕f(R1,K2)
L15=R14
R15=L14⊕f(R14,K15)
K16
f
R16=L15⊕f(R15,K16)
L16=R15
IP-1
Ciphertext


Plaintext
IP

Intitial and Inverse Permutation in DES

ถ้ามี Plain Text แปลงเป็น เลขฐาน 16 ก่อน

Message : 0123456789ABCDEF

แปลงเป็นฐาน 2

0000 0001 0010 0011 0100 0101 0110 0111

1000 1001 1010 1011 1100 1101 1110 1111

Intitial and Inverse Permutation in DES (Con't)

0000 0001 0010 0011 0100 0101 0110 0111
1000 1001 1010 1011 1100 1101 1110 1111

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

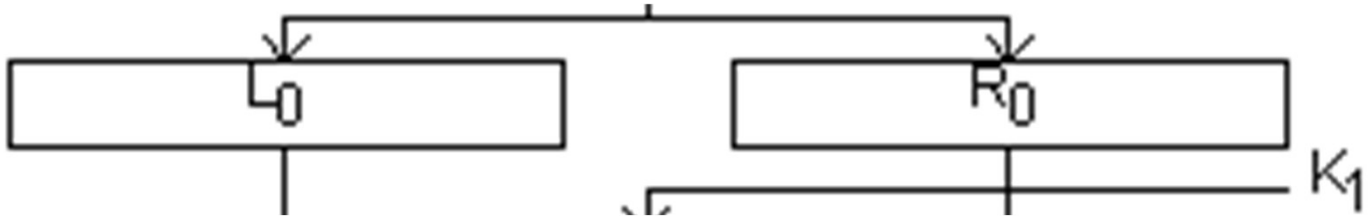
The Initial Permutation: IP

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

เอา Bit มาเขียนใหม่ตามตาราง Intitial Permutation : IP

เช่น ตารางฝั่งขวาเลขแรกแถวแรกคือ 58 เราก้มาดูตารางฝั่งซ้ายที่เป็นเลข 58 มันเท่ากับ 1 เราก็เขียน 1

IP : 1100 1100 0000 0000 1100 1100 1111 1111 1111 0000 10101010 1111 0000 1010 1010


0
R0
K1

Devide to Left And Right

IP : 1100 1100 0000 0000 1100 1100 1111 1111

1111 0000 10101010 1111 0000 1010 1010

เอา ค่า IP 64 Bit มาตัดออกแบ่งข้างละ 32 bit

Left : 1100 1100 0000 0000 1100 1100 1111 1111

Right : 1100 1100 0000 0000 1100 1100 1111 1111

Generate Key IN DES

โจทย์กำหนด K = 133457799BBCDFF1

แปลงเป็นเลขฐาน 16 ก่อน

00010011 00110100 01010111 01111001

10011011 10111100 11011111 1110001

Generate Key IN DES (Cont)

K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 1110001

pc-1						
49	42	35	28	21	14	7
0	50	43	36	29	22	15
8	1	51	44	37	30	23
16	9	2	52	45	38	31
55	48	41	34	27	20	13
6	54	47	40	33	26	19
12	5	53	46	39	32	25
18	11	4	24	17	10	3

เอาค่าในตารางฝั่งขวาไปเขียนเทียบตารางฝั่งซ้าย
ทำให้ได้การลดทอนจาก 64 Bit เหลือ 32 Bit จะทำให้เราได้ค่า K+

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

K+ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

Generate Key IN DES (Cont)

K+ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

พอเราได้ค่า K+ มาแล้ว เอามาแบ่งซ้ายขวาดังภาพ

แทยซ้ายด้วย C0 : 1111000 0110011 0010101 0101111
แทนขวาด้วย D0 : 0101010 1011001 1001111 0001111

โดยมีกฎดังต่อไปนี้

	Rounds (รอบ)	Shifts (ซิบไปทางซ้ายกี่บิต)
1. ถ้า	**1,2,9,16**	**One bits**
2. ถ้า	**Others**	**Two Bits**

Generate Key IN DES (Cont)

รอบที่ 0
ค่าที่ได้จากสไลด์ที่แล้ว

แทยซ้ายด้วย C0 : 1111000 0110011 0010101 0101111
แทนขวาด้วย D0 : 0101010 1011001 1001111 0001111

รอบที่ 1
เริ่มทำตามกฎจากสไลด์ที่แล้ว

แทยซ้ายด้วย C1 : 1110000 1100110 0101010 1011111
แทนขวาด้วย D2 : 1010101 0110011 0011110 0011110

เริ่มเข้ากฎ Shiftbit ข้อ 1

รอบที่ 2
เริ่มทำตามกฎจากสไลด์ที่แล้ว

แทยซ้ายด้วย C1 :
แทนขวาด้วย D2 :

เริ่มเข้ากฎ Shiftbit ข้อ 1

Generate Key IN DES (Cont)

รอบที่ 3
ค่าที่ได้จากสไลด์ที่แล้ว

แทยซ้ายด้วย C0 :
แทนขวาด้วย D0 :

รอบที่ 4
เริ่มทำตามกฎจากสไลด์ที่แล้ว

แทยซ้ายด้วย C1 :
แทนขวาด้วย D2 :

รอบที่ 5
เริ่มทำตามกฎจากสไลด์ที่แล้ว

แทยซ้ายด้วย C1 :
แทนขวาด้วย D2 :

Generate Key IN DES (Cont)

รอบที่ 6

ค่าที่ได้จากสไลด์ที่แล้ว

แทยซ้ายด้วย C0 :

แทนขวาด้วย D0 :

รอบที่ 7

เริ่มทำตามกฎจากสไลด์ที่แล้ว

แทยซ้ายด้วย C1 :

แทนขวาด้วย D2 :

รอบที่ 8

เริ่มทำตามกฎจากสไลด์ที่แล้ว

แทยซ้ายด้วย C1 :

แทนขวาด้วย D2 :

Generate Key IN DES (Cont)

รอบที่ 9

ค่าที่ได้จากสไลด์ที่แล้ว

แทยซ้ายด้วย C0 :

แทนขวาด้วย D0 :

รอบที่ 10

เริ่มทำตามกฎจากสไลด์ที่แล้ว

แทยซ้ายด้วย C1 :

แทนขวาด้วย D2 :

รอบที่ 11

เริ่มทำตามกฎจากสไลด์ที่แล้ว

แทยซ้ายด้วย C1 :

แทนขวาด้วย D2 :

Generate Key IN DES (Cont)

รอบที่ 12

ค่าที่ได้จากสไลด์ที่แล้ว

แทยซ้ายด้วย C0 :

แทนขวาด้วย D0 :

รอบที่ 13

เริ่มทำตามกฎจากสไลด์ที่แล้ว

แทยซ้ายด้วย C1 :

แทนขวาด้วย D2 :

รอบที่ 14

เริ่มทำตามกฎจากสไลด์ที่แล้ว

แทยซ้ายด้วย C1 :

แทนขวาด้วย D2 :

Generate Key IN DES (Cont)

รอบที่ 15

ค่าที่ได้จากสไลด์ที่แล้ว

แทยซ้ายด้วย C0 :

แทนขวาด้วย D0 :

รอบที่ 16

เริ่มทำตามกฎจากสไลด์ที่แล้ว

แทยซ้ายด้วย C1 :

แทนขวาด้วย D2 :

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ

รอบที่1

แทยซ้ายด้วย C0 : 1110000 1100110 0101010 1011111
แทนขวาด้วย D0 : 1010101 0110011 0011110 0011110

เอา C,D จาก KEY มาใส่ตารางและแปลงไปเป็น K1

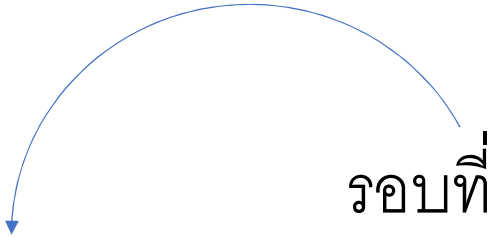
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	1	0	0	0	0	1	1	0	0	1	1	0
15	16	17	18	19	20	21	22	23	24	25	26	27	28
0	1	0	1	0	1	0	1	0	1	1	1	1	1
29	30	31	32	33	34	35	36	37	38	39	40	41	42
1	0	1	0	1	0	1	0	1	1	0	0	1	1
43	44	45	46	47	48	49	50	51	52	53	54	55	56
0	0	1	1	1	1	0	0	0	1	1	1	1	0

$PC-2$							
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

K1 = 000110 110000 001011 101111 111111 00011 000001 110010

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ



แทยซ้ายด้วย C_1 :
แทนขวาด้วย D_1 :

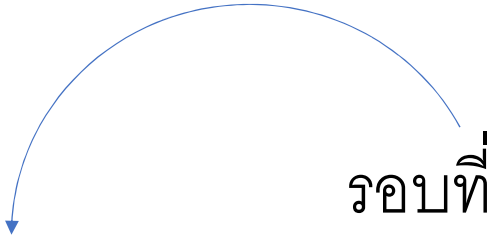
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K2 =.....

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ



รอบที่ 3

แทยซ้ายด้วย C_2 :
แทนขวาด้วย D_2 :

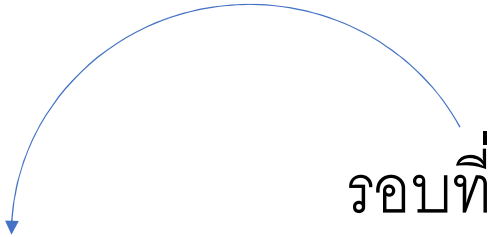
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K3 =.....

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 **bit** เหลือ 48 **bit** เอาค่าจาก **Key** มาทำทุกรอบ ให้ครบ 16 รอบ



รอบที่ 4

แทยซ้ายด้วย C_3 :
แทนขวาด้วย D_3 :

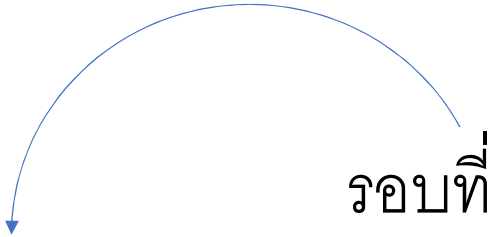
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K2 =.....

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ



แทยซ้ายด้วย C_1 :
แทนขวาด้วย D_1 :

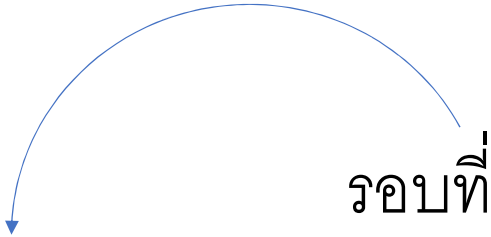
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K2 =.....

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ



แทยซ้ายด้วย C_1 :
แทนขวาด้วย D_1 :

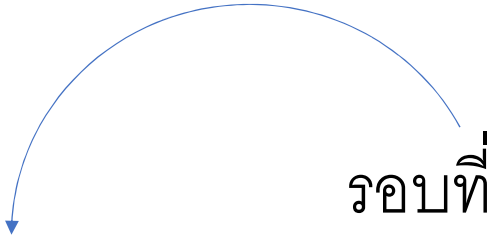
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K2 =.....

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ



แทยซ้ายด้วย C_1 :
แทนขวาด้วย D_1 :

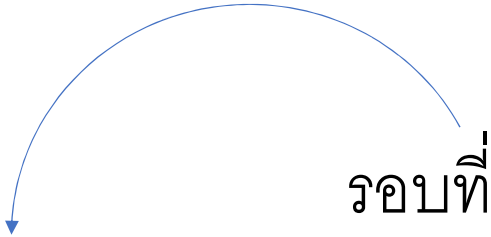
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K2 =.....

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ



แทยซ้ายด้วย C_1 :
แทนขวาด้วย D_1 :

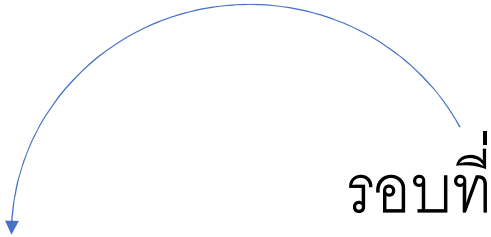
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K2 =.....

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ



แทยซ้ายด้วย C_1 :
แทนขวาด้วย D_1 :

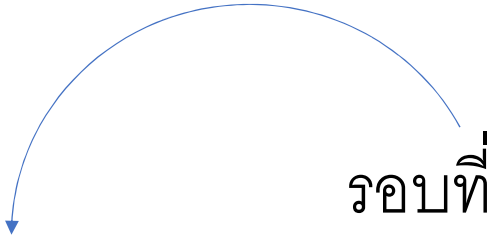
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K2 =.....

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ



แทยซ้ายด้วย C_1 :
แทนขวาด้วย D_1 :

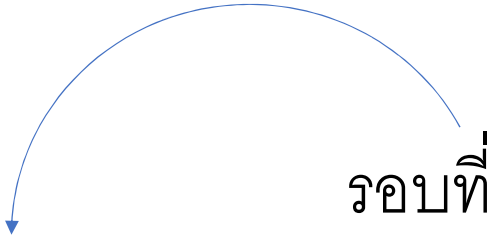
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K2 =.....

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ



แทยซ้ายด้วย C_1 :
แทนขวาด้วย D_1 :

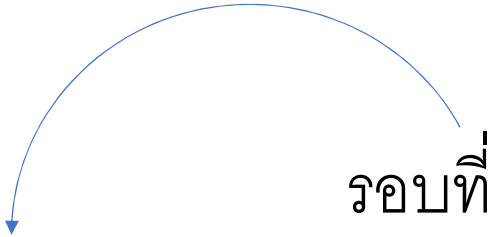
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K2 =.....

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ



แทยซ้ายด้วย C_1 :
แทนขวาด้วย D_1 :

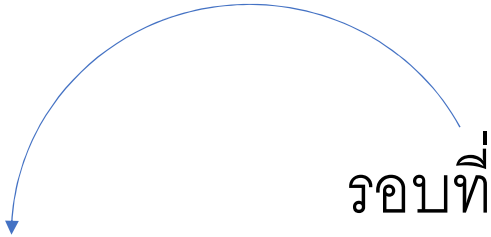
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K2 =.....

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ



แทยซ้ายด้วย C_1 :
แทนขวาด้วย D_1 :

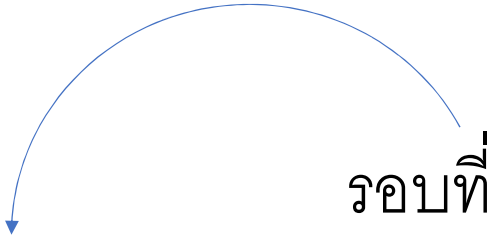
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K2 =.....

Compression p-Box

ทำหน้าที่สลับตำแหน่งและลดจำนวนบิตของอินพุทจาก 56 bit เหลือ 48 bit เอาค่าจาก Key มาทำทุกรอบ ให้ครบ 16 รอบ



แทยซ้ายด้วย C_1 :
แทนขวาด้วย D_1 :

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	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56

$PC-2$							
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

K2 =.....