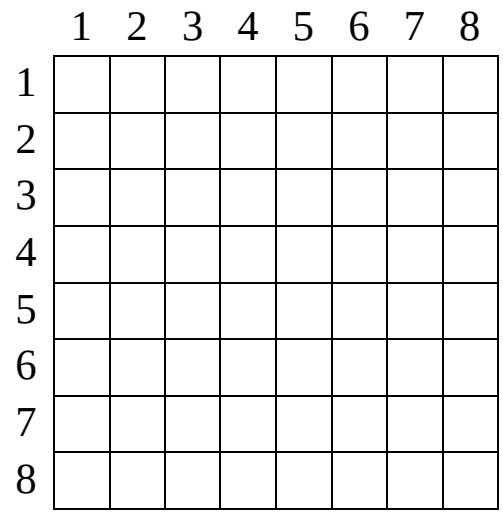
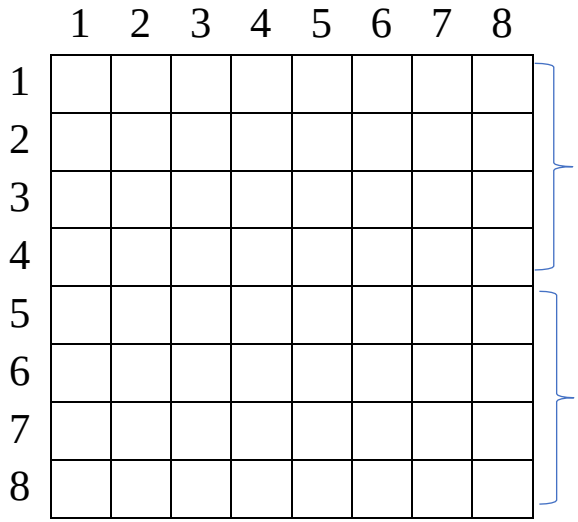
Họ và tên: Hà Huy Sơn

Mssv: 18574802010055

hahuyson➔ P = hahuyson

0110 1000 0110 0001 0110 1000 0111 0101 0111 1001 0111 0011 0110 1111 0110 1110

P	Bộ hoán vị IP
	

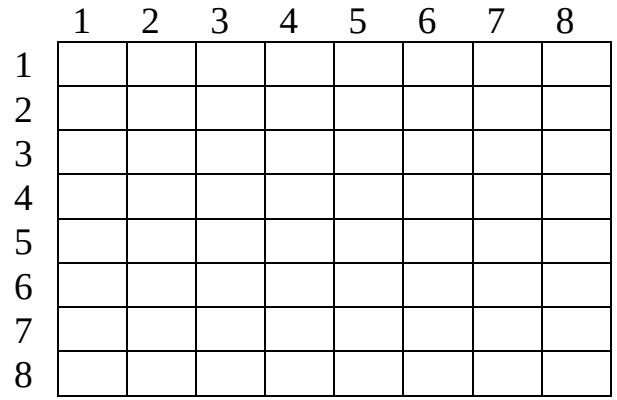
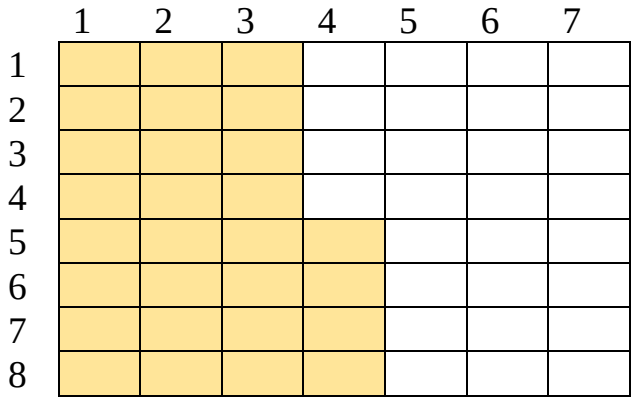
Vòng 1:

R_0 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có $E(R_0)$:

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K = 18574802010055AB

K = 64 bit	K = 56 bit
	

Cho khóa K = 56 bit đi qua Pc-1 ta có: C_0 và D_0

	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

Dịch 1 bit ta có C_1 và D_1:

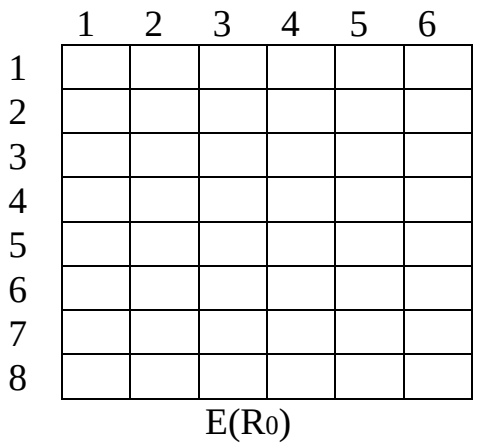
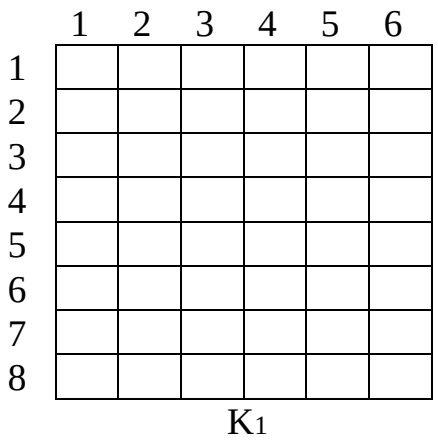
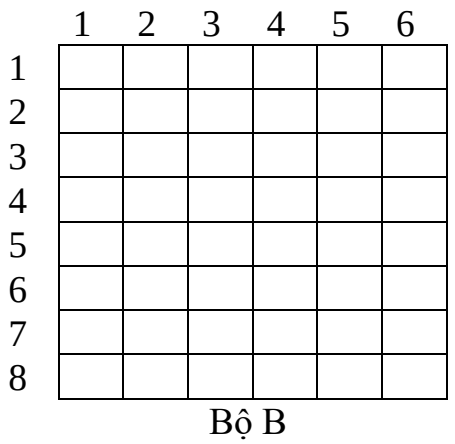
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

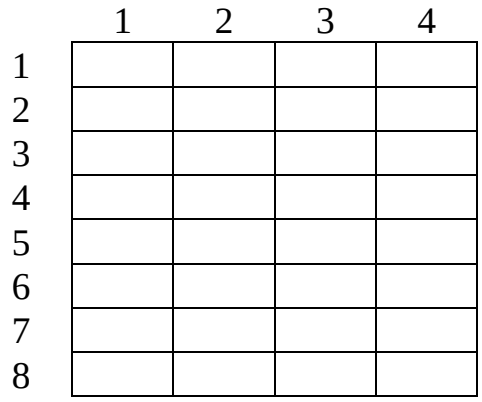
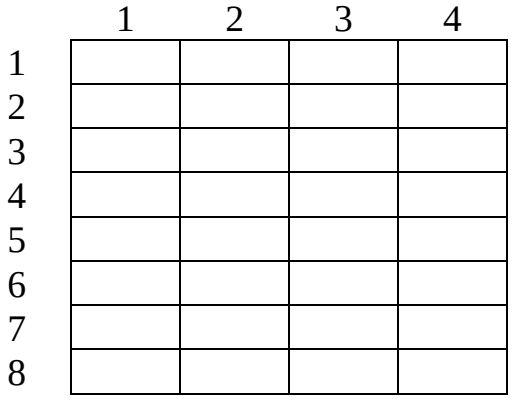
Từ C_1 và D_1 ta cho đi qua Pc-2 ta thu được K_1 là:

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_1 =

Ta lấy E(R_0) xor với K_1 ta đc bộ B

 E(R_0)	 K_1	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được F(R_0,K_1)
	

Vòng 2:

Ta có $F(R_0,K_1)$xor với L_0 thu được R_1

$L_1 = R_0$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_1 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có $E(R_1)$:

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 1 bit ta có C_2 và D_2 là :

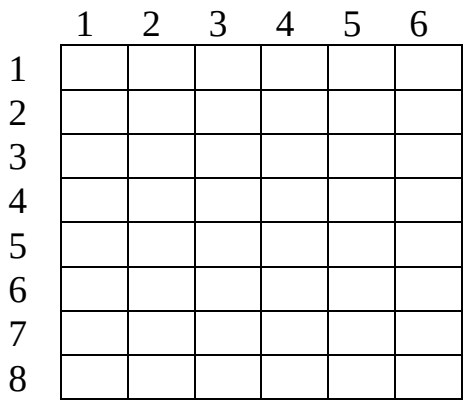
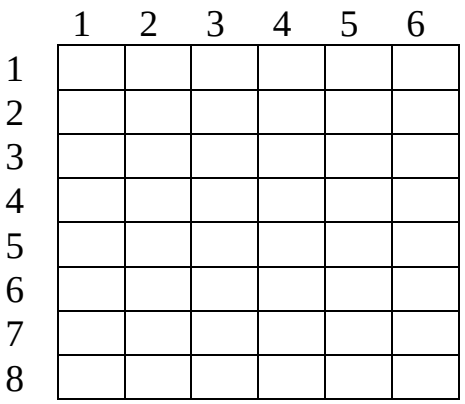
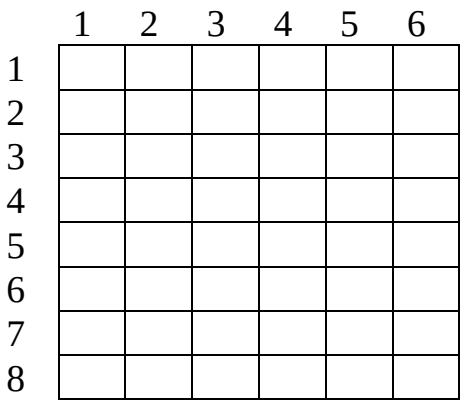
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

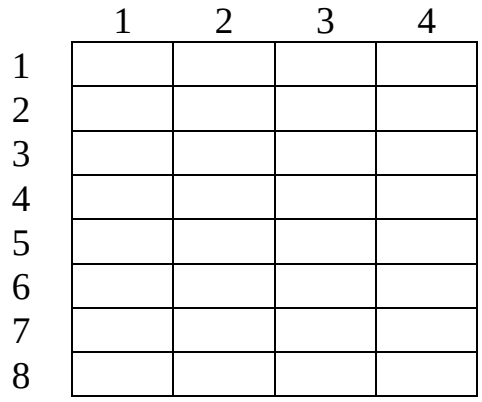
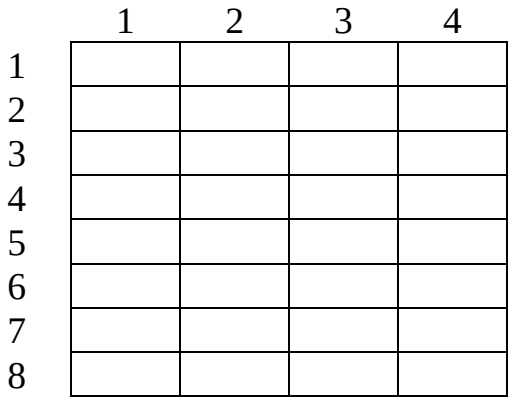
Từ C_2 và D_2 ta cho đi qua Pc-2 ta thu được K_2 là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_2=

Ta lấy E(R_1) xor với K_2 ta đc bộ B

E(R_1)	K_2	Bộ B
		

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được F(R_1,K_2)
	

Vòng 3:

Ta có F(R_1,K_2)xor với L_1 thu được R_2

$L_2 = R_0$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_2 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có E(R_2):

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 2 bit ta có C_3 và D_3 là :

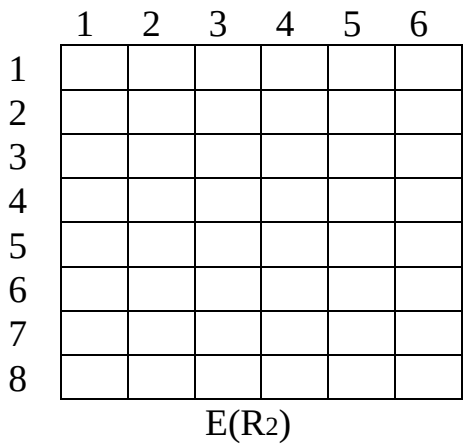
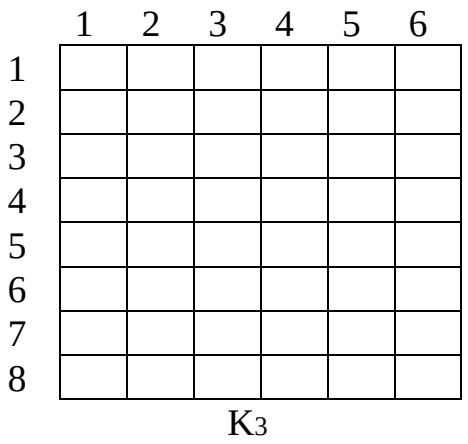
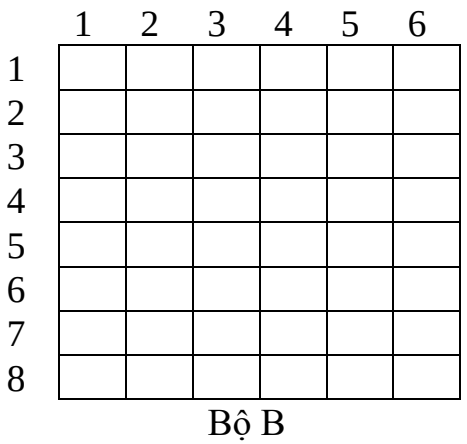
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

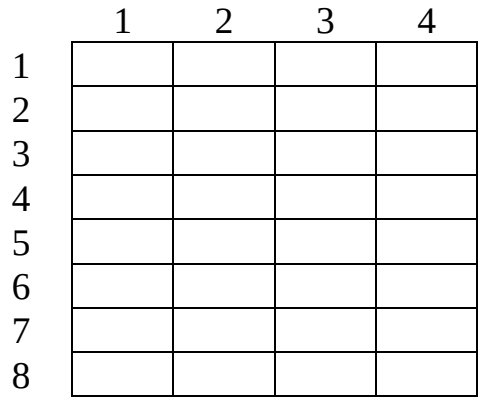
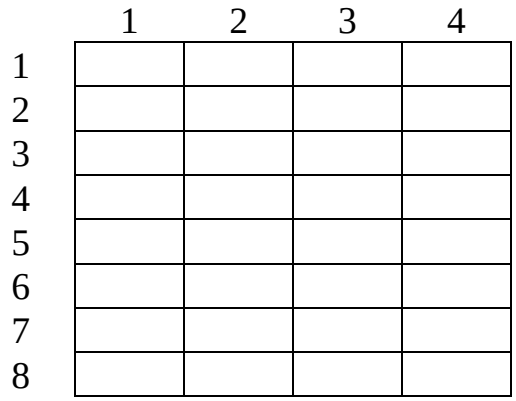
Từ C_3 và D_3 ta cho đi qua Pc-2 ta thu được K_3 là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_3=

Ta lấy E(R_2) xor với K_3 ta đc bộ B

 E(R_2)	 K_3	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được F(R_2, K_3)
	

Vòng 4:

Ta có $F(R_2,K_3)$xor với L_2 thu được R_3

$L_3 = R_2$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_3 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có $E(R_3)$:

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 2 bit ta có C_4 và D_4 là :

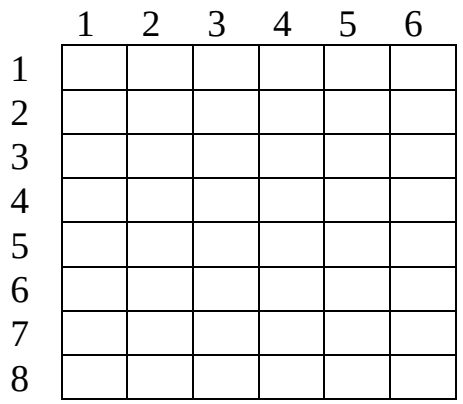
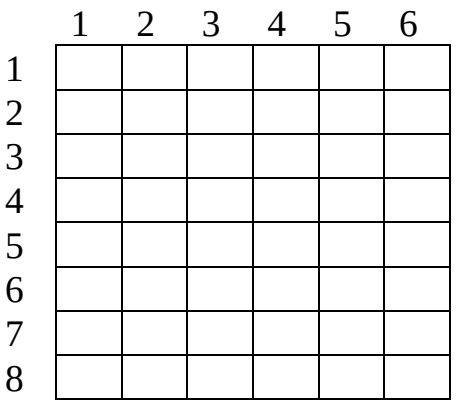
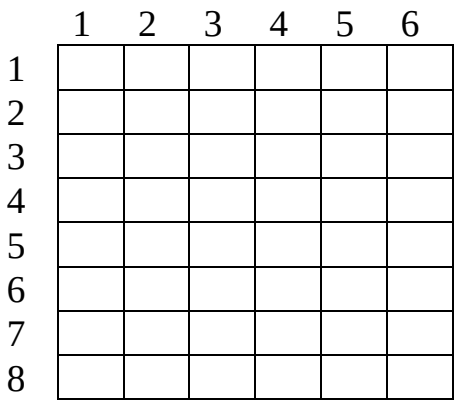
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

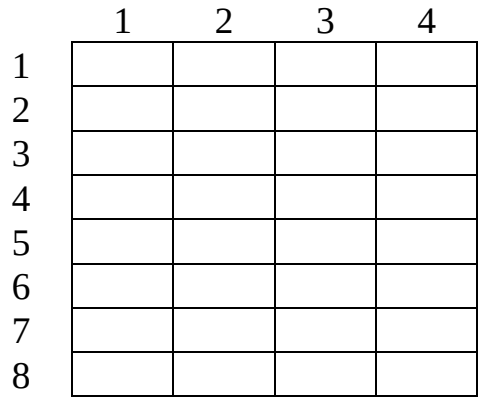
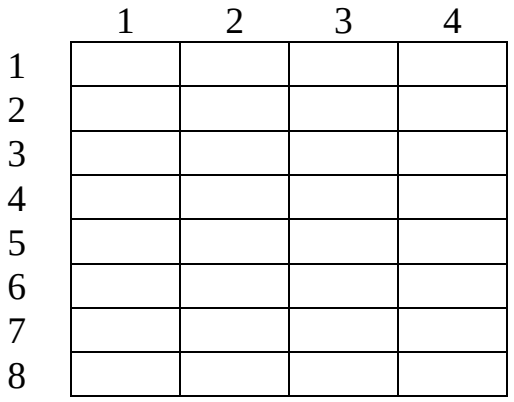
Từ C_4 và D_4 ta cho đi qua Pc-2 ta thu được K_4 là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_4 =

Ta lấy $E(R_3)$ xor với K_4 ta đc bộ B

 $E(R_3)$	 K_4	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được $F(R_3, K_4)$
	

Vòng 5:

Ta có F(R_3,K_4)xor với L_3 thu được R_4

$L_4 = R_3$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_4 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có E(R_4):

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 2 bit ta có C_5 và D_5

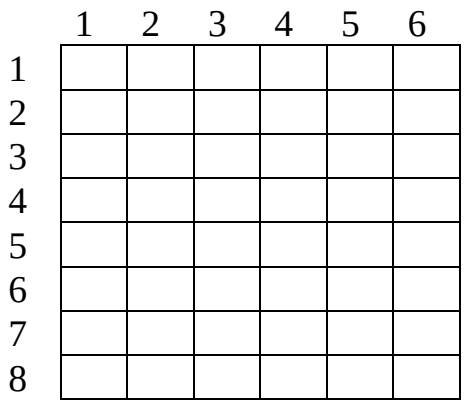
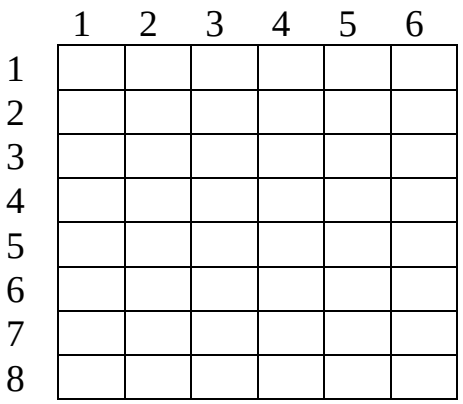
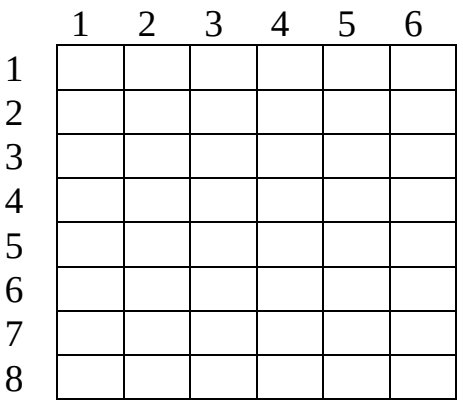
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

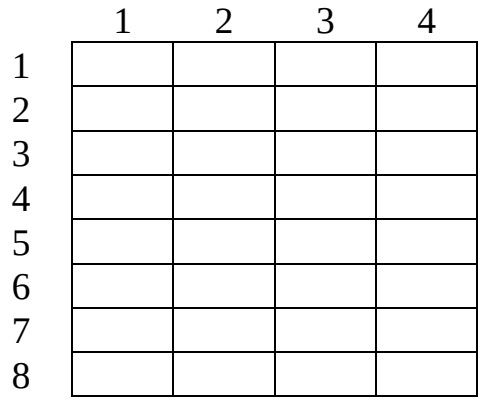
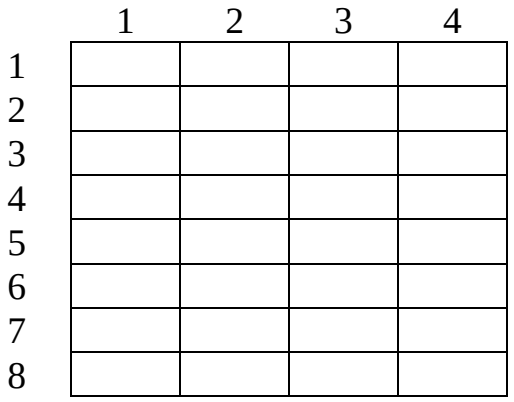
Từ C_5 và D_5 ta cho đi qua Pc-2 ta thu được K_5 là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_5 =

Ta lấy E(R_4) xor với K_5 ta đc bộ B

 E(R_4)	 K_5	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được F(R_4, K_5)
	

Vòng 6:

Ta có F(R_4,K_5)xor với L_4 thu được R_5

$L_5 = R_4$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_5 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có E(R_5):

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 2 bit ta có C_6 và D_6

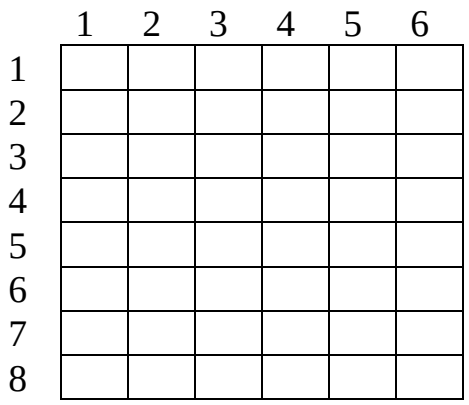
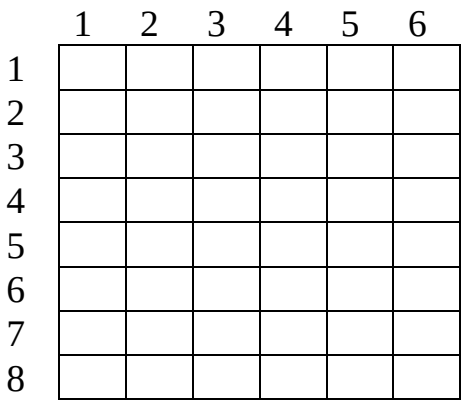
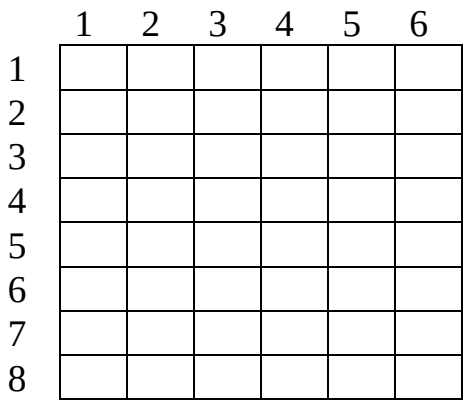
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

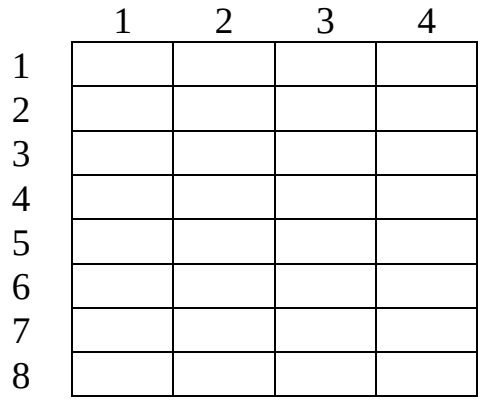
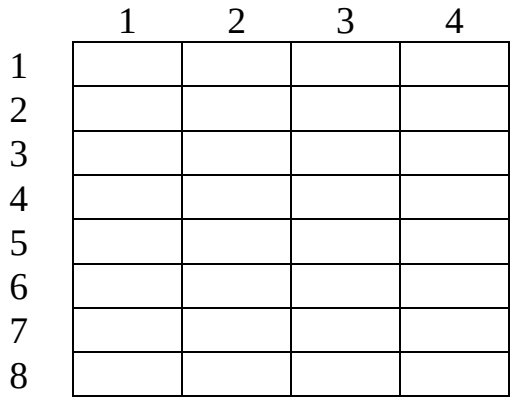
Từ C_6 và D_6 ta cho đi qua Pc-2 ta thu được K_6 là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_6 =

Ta lấy E(R_5) xor với K_6 ta đc bộ B

 E(R_5)	 K_2	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được F(R_5, K_6)
	

Vòng 7:

Ta có $F(R_5, K_6)$ xor với L_5 thu được R_6

$L_6 = R_5$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_6 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có $E(R_6)$:

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 2 bit ta có C_7 và D_7

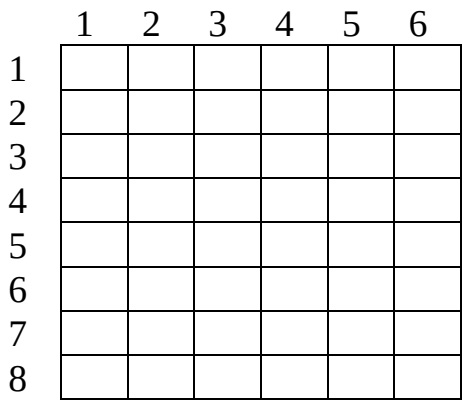
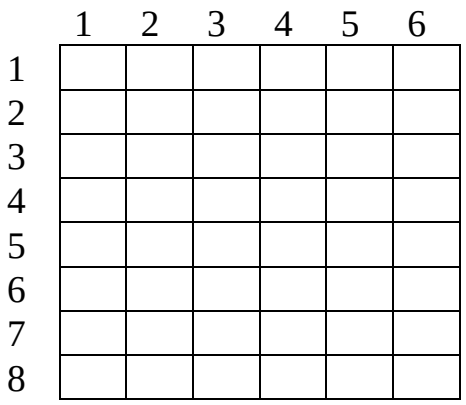
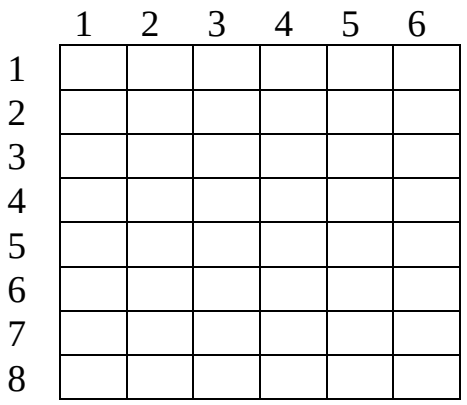
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

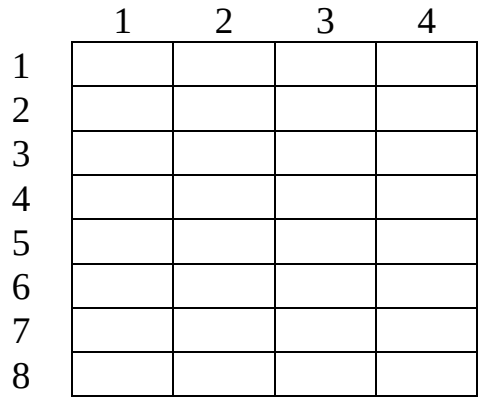
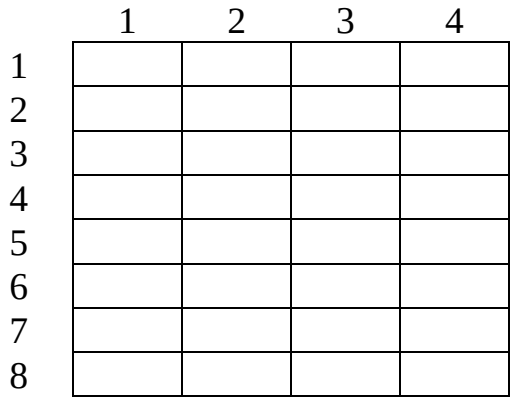
Từ C_7 và D_7 ta cho đi qua Pc-2 ta thu được K_7 là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_7 =

Ta lấy E(R_6) xor với K_2 ta đc bộ B

 E(R_6)	 K_7	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được F(R_6, K_7)
	

Vòng 8:

Ta có F(R_6, K_7) xor với L_6 thu được R_7

$L_7 = R_6$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_7 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có E(R_7):

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 2 bit ta có C_8 và D_8

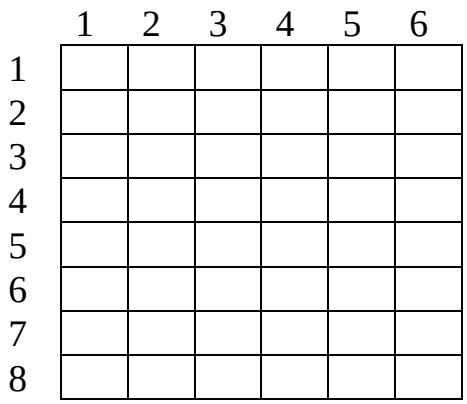
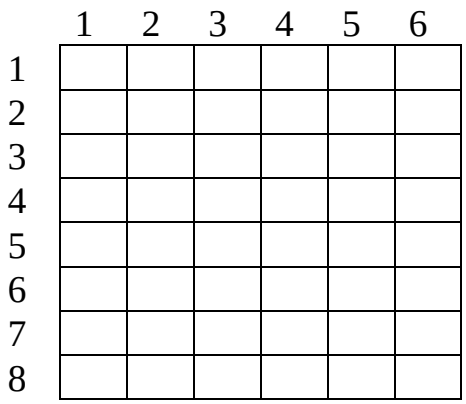
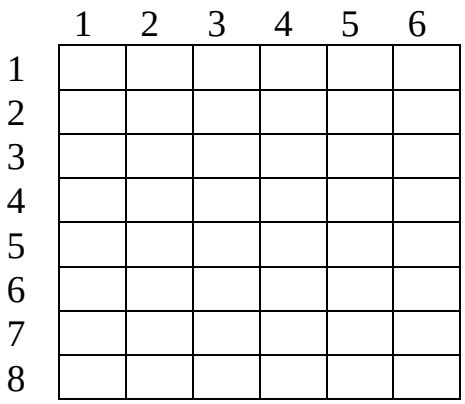
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

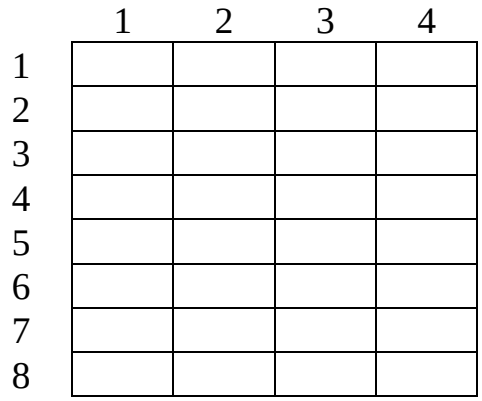
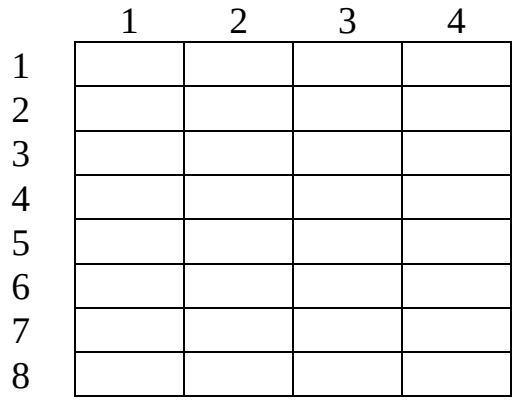
Từ C_8 và D_8 ta cho đi qua Pc-2 ta thu được K_8 là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_8 =

Ta lấy E(R_7) xor với K_8 ta đc bộ B

 E(R_7)	 K_8	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được F(R_7, K_8)
	

Vòng 9:

Ta có $F(R_7,K_8)$ xor với L_7 thu được R_8

$L_8 = R_7$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_8 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có $E(R_8)$:

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 1 bit ta có C_9 và D_9

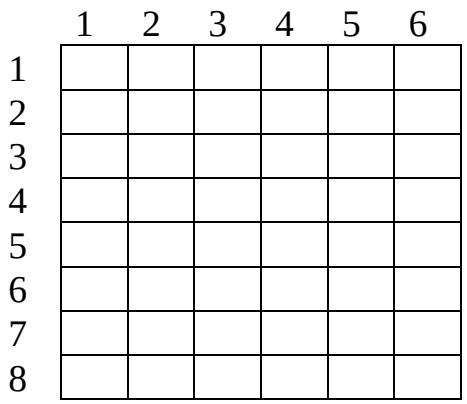
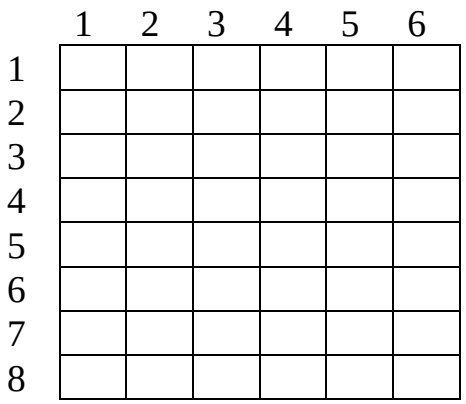
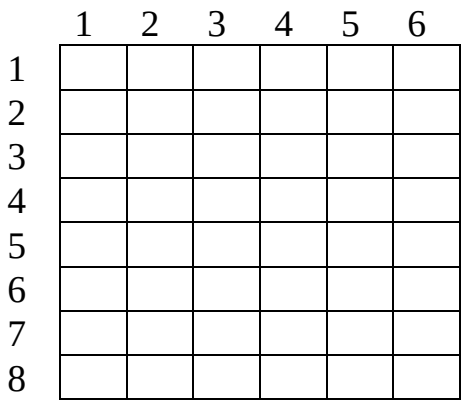
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

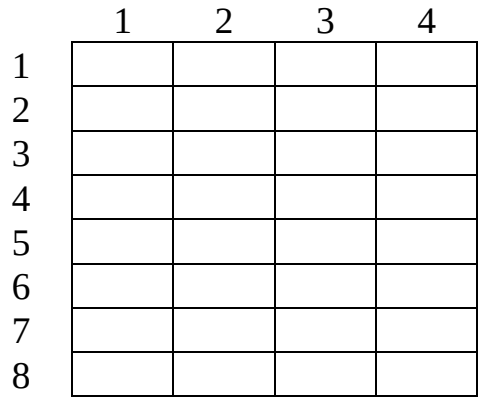
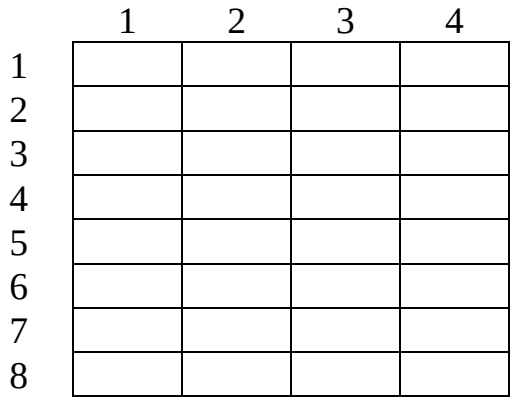
Từ C_9 và D_9 ta cho đi qua Pc-2 ta thu được K_9 là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_9 =

Ta lấy $E(R_8)$ xor với K_9 ta đc bộ B

 $E(R_8)$	 K_9	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được $F(R_8, K_9)$
	

Vòng 10:

Ta có $F(R_8,K_9)$ xor với L_8 thu được R_9

$L_9 = R_8$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_9 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có $E(R_9)$:

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 2 bit ta có C_{10} và D_{10}

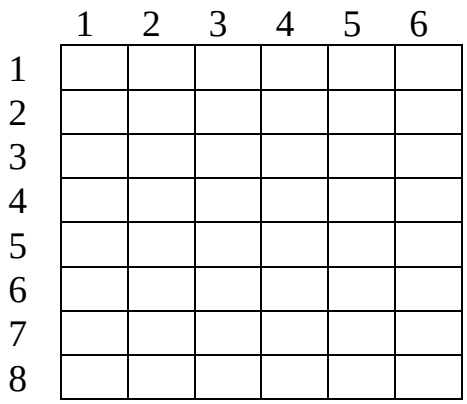
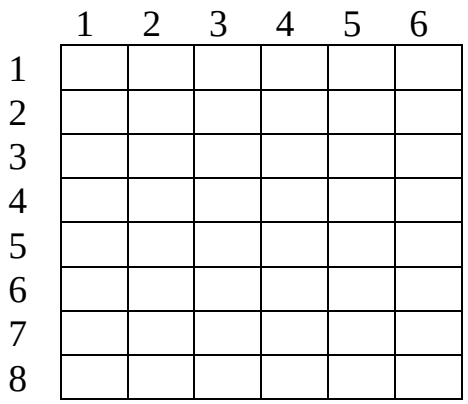
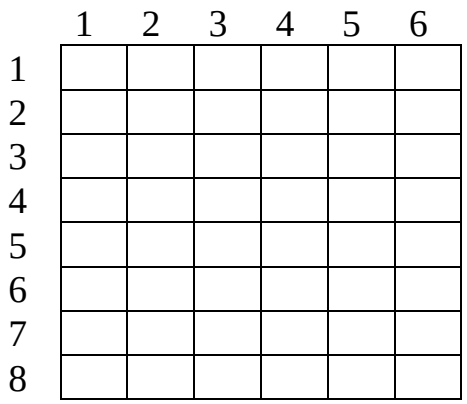
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

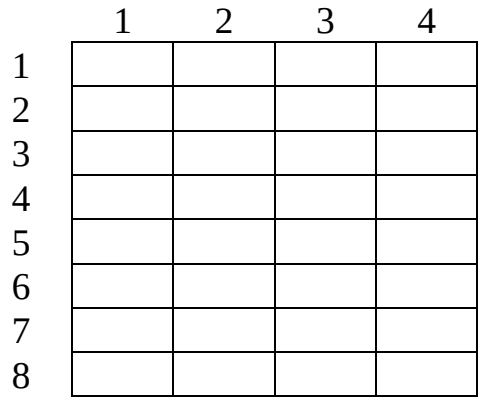
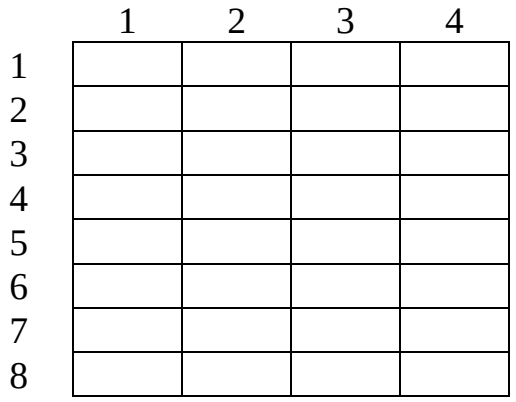
Từ C_{10} và D_{10} ta cho đi qua Pc-2 ta thu được K_{10} là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_{10} =

Ta lấy E(R_9) xor với K_{10} ta đc bộ B

 E(R_9)	 K_{10}	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được F(R_9, K_{10})
	

Vòng 11:

Ta có F(R_9,K_{10})xor với L_9 thu được R_{10}

$L_{10} = R_9$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_{10} đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có E(R_{10}):

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 2 bit ta có C_{11} và D_{11}

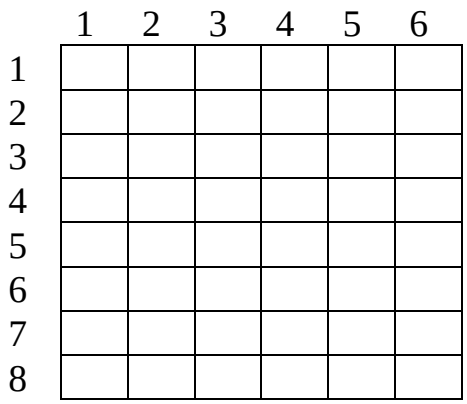
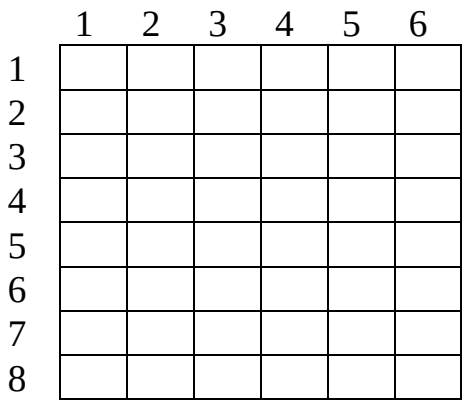
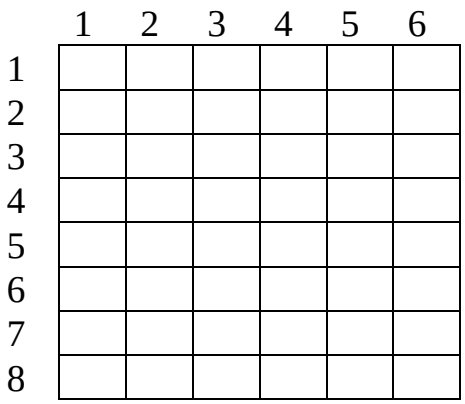
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

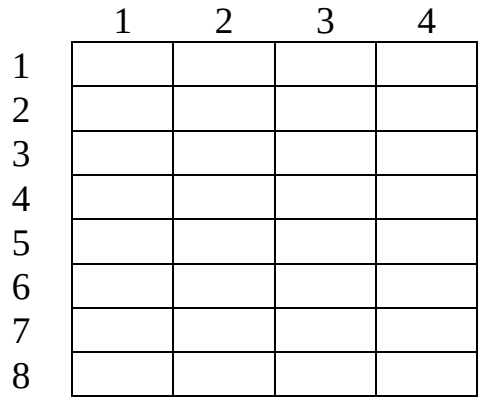
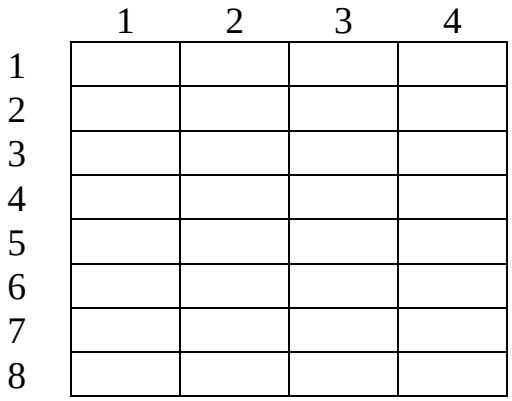
Từ C_{11} và D_{11} ta cho đi qua Pc-2 ta thu được K_{11} là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_{11} =

Ta lấy $E(R_{10})$ xor với K_{11} ta đc bộ B

 $E(R_{10})$	 K_{11}	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được $F(R_{10}, K_{11})$
	

Vòng 12:

Ta có F(R_{10},K_{11}) xor với L_{10} thu được R_{11}

$L_{11} = R_{10}$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_{11} đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có E(R_{11}):

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 2 bit ta có C_{12} và D_{12}

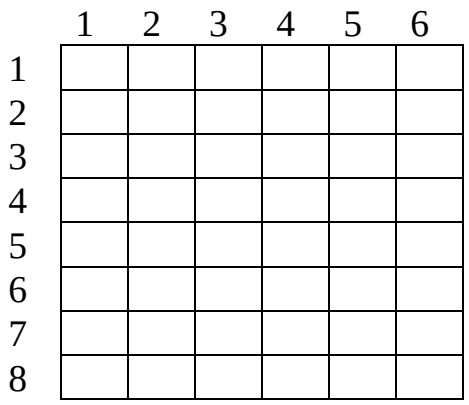
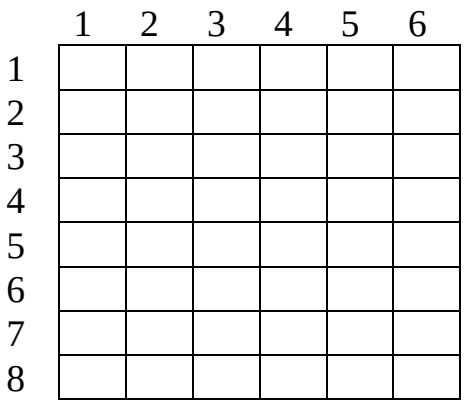
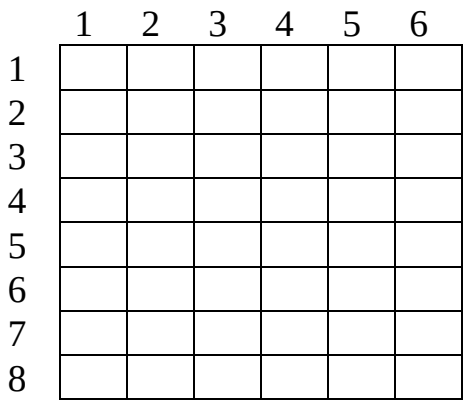
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

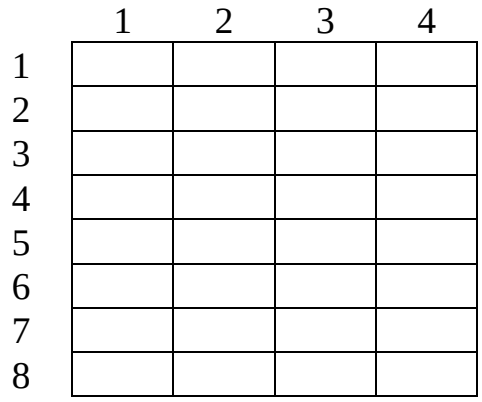
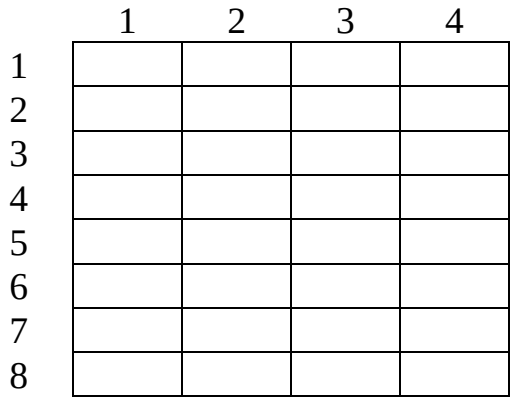
Từ C_{12} và D_{12} ta cho đi qua Pc-2 ta thu được K_{12} là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_{12} =

Ta lấy E(R_{11}) xor với K_{12} ta đc bộ B

 E(R_{11})	 K_{12}	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được F(R_{11}, K_{12})
	

Vòng 13:

Ta có $F(R_{11},K_{12})$ xor với L_{11} thu được R_{12}

$L_{12} = R_{11}$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_{12} đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có $E(R_{12})$:

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 2 bit ta có C_{13} và D_{13}

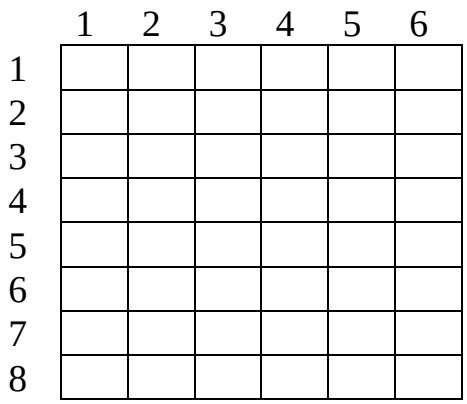
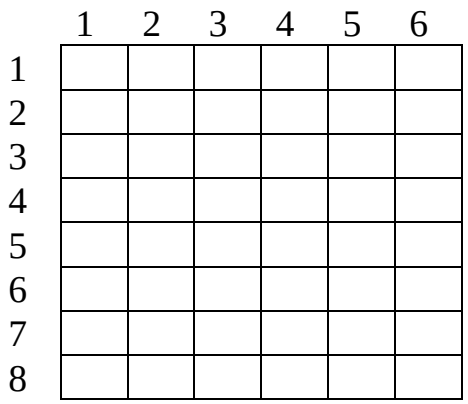
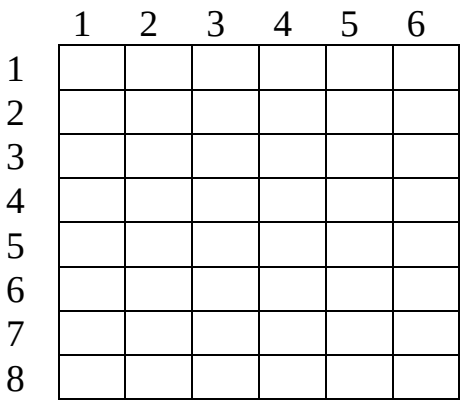
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

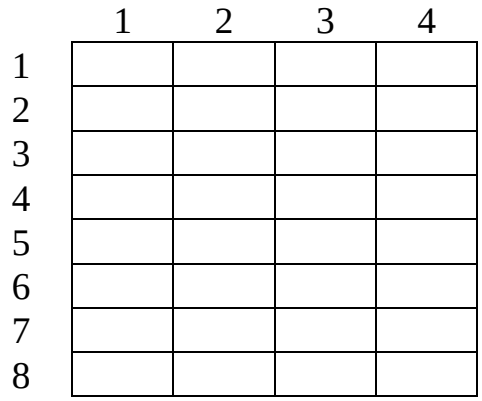
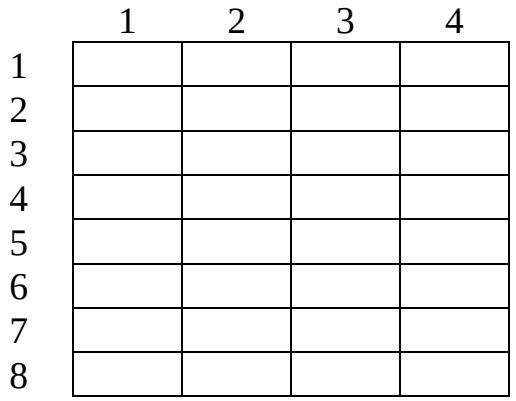
Từ C_{13} và D_{13} ta cho đi qua Pc-2 ta thu được K_{13} là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_{13} =

Ta lấy $E(R_{12})$ xor với K_{13} ta đc bộ B

 $E(R_{12})$	 K_{13}	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được $F(R_{12}, K_{13})$
	

Vòng 14:

Ta có F(R_{12}, K_{13}) xor với L_{12} thu được R_{13}

$L_{13} = R_{12}$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_{13} đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có E(R_{13}):

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 2 bit ta có C_{14} và D_{14}

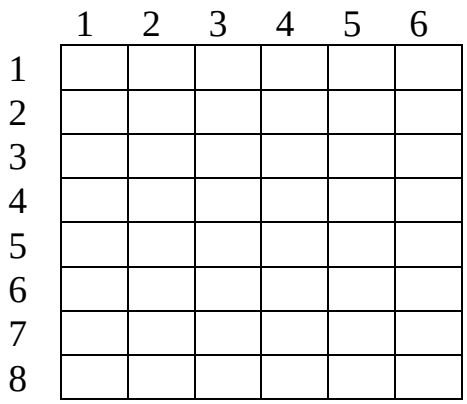
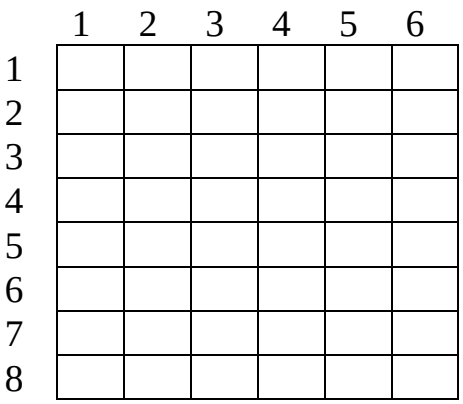
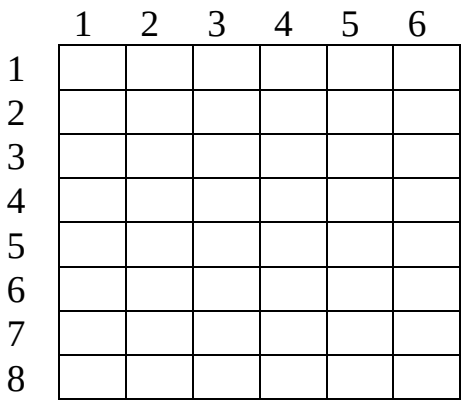
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

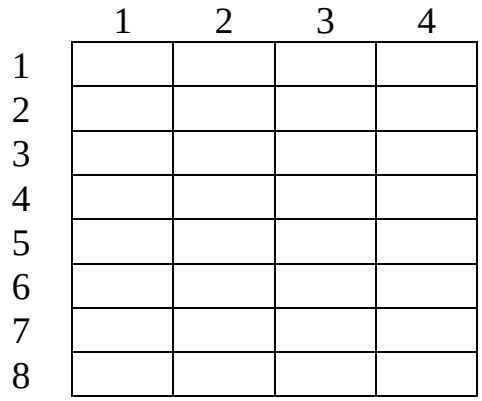
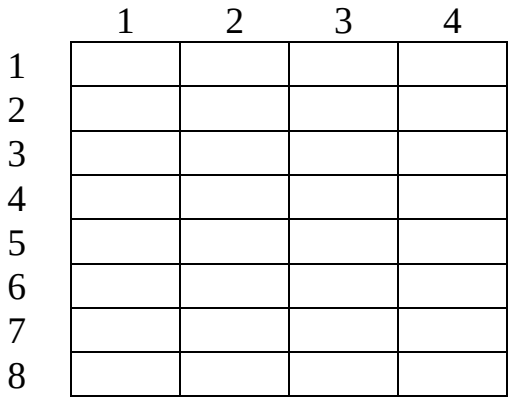
Từ C_{14} và D_{14} ta cho đi qua Pc-2 ta thu được K_{14} là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_{14} =

Ta lấy E(R_{13}) xor với K_{14} ta đc bộ B

 E(R_{13})	 K_{14}	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được F(R_{13}, K_{14})
	

Vòng 15:

Ta có F(R_{13}, K_{14}) xor với L_{13} thu được R_{14}

$L_{14} = R_{13}$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_{14} đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có E(R_{14}):

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 2 bit ta có C_{15} và D_{15}

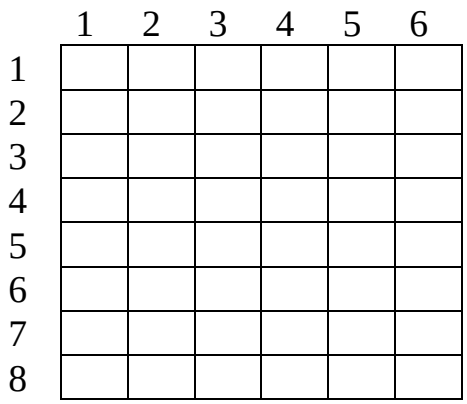
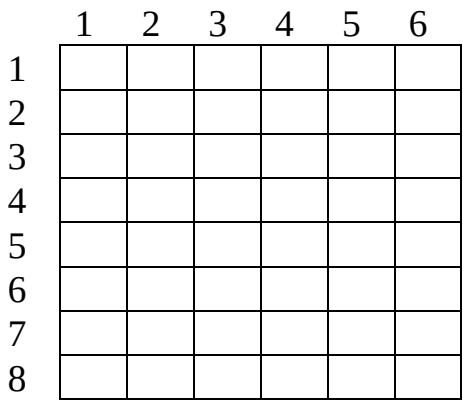
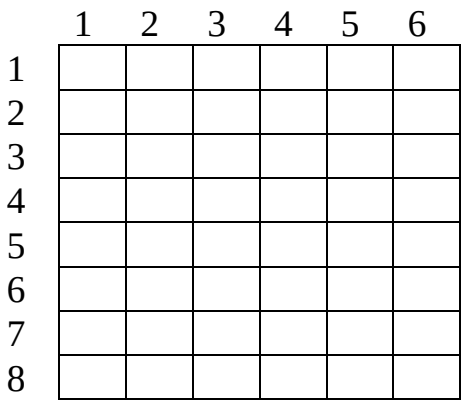
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

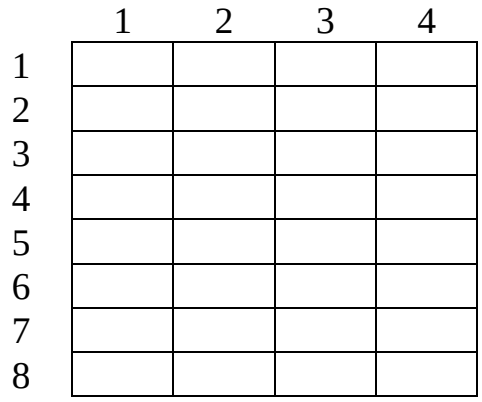
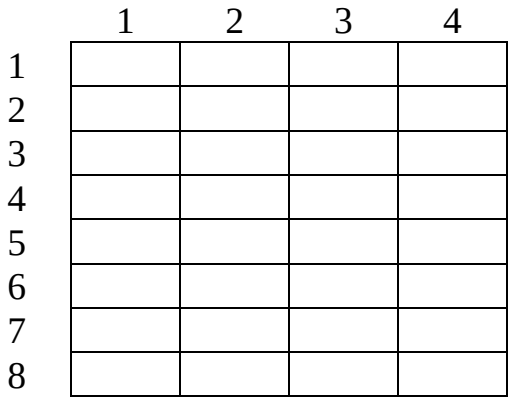
Từ C_{15} và D_{15} ta cho đi qua Pc-2 ta thu được K_{15} là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_{15} =

Ta lấy $E(R_{14})$ xor với K_2 ta đc bộ B

 $E(R_{14})$	 K_{15}	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được $F(R_{14}, K_{15})$
	

Vòng 16:

Ta có F(R_{14}, K_{15}) xor với L_{14} thu được R_{15}

$L_{15} = R_{14}$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_{15} đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có E(R_{15}):

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

Dịch 1 bit ta có C_{16} và D_{16}

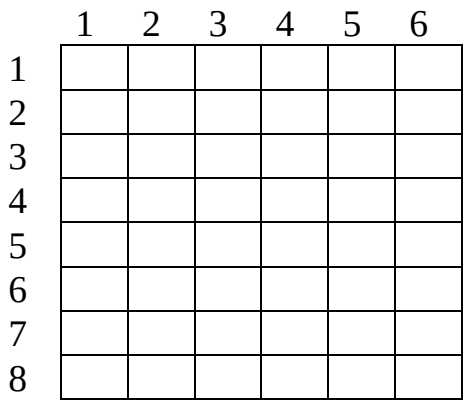
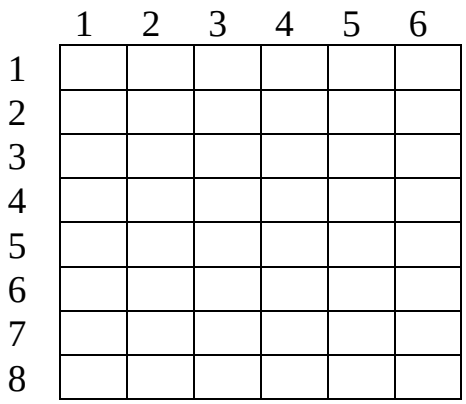
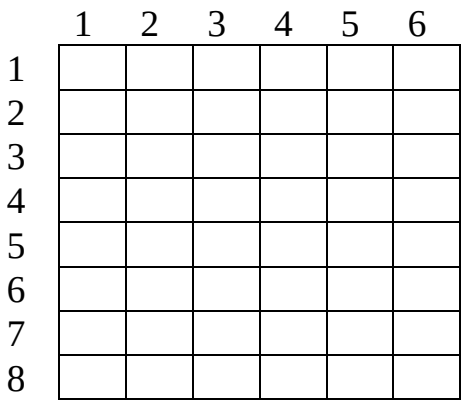
	1	2	3	4	5	6	7
1							
2							
3							
4							
5							
6							
7							
8							

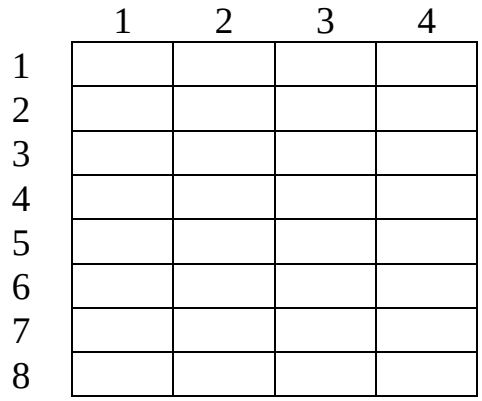
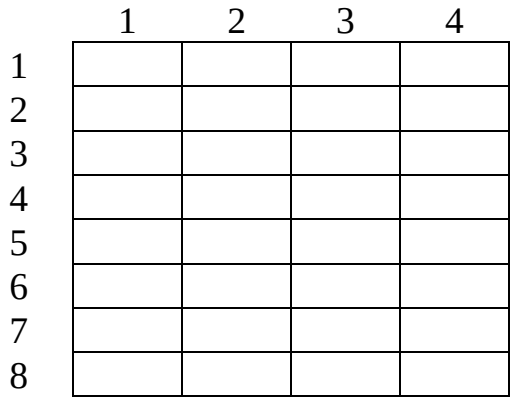
Từ C_{16} và D_{16} ta cho đi qua Pc-2 ta thu được K_{16} là

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						
7						
8						

K_{16} =

Ta lấy $E(R_{15})$ xor với K_{16} ta đc bộ B

 $E(R_{15})$	 K_{16}	 Bộ B

Cho kết quả bộ B đi qua hộp S_1 => S8 thu đc Bộ S	Cho bộ S đi qua bộ hoán vị P ta thu được $F(R_{15}, K_{16})$
	

Ta có F(R_{15}, K_{16}) xor với L_{15} thu được R_{16}

$L_{16} = R_{15}$

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

R_{16} đổi chỗ cho L_{16}	Đi qua hoán vị IP^{-1} thu được

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

Kết luận: Cuối cùng áp dụng IP^{-1} cho $R_{16}L_{16}$ ta nhận được bản rõ trong dạng thập lục phân sau: