**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 |
| |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | 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 |  |  |  |  |  |  |  |  | |

**Vòng 1:**

R0 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

Ta có E(R0):

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

K = 18574802010055AB



|  |  |
| --- | --- |
| K = 64 bit | K = 56 bit |
| |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | | 1 |  |  |  |  |  |  |  |  | | 2 |  |  |  |  |  |  |  |  | | 3 |  |  |  |  |  |  |  |  | | 4 |  |  |  |  |  |  |  |  | | 5 |  |  |  |  |  |  |  |  | | 6 |  |  |  |  |  |  |  |  | | 7 |  |  |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |  |  | | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | | 1 |  |  |  |  |  |  |  | | 2 |  |  |  |  |  |  |  | | 3 |  |  |  |  |  |  |  | | 4 |  |  |  |  |  |  |  | | 5 |  |  |  |  |  |  |  | | 6 |  |  |  |  |  |  |  | | 7 |  |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |  | |

Cho khóa K = 56 bit đi qua Pc-1 ta có: C0 và D0 Dịch 1 bit ta có C1 và D1:



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

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

Từ C1 và D1 ta cho đi qua Pc-2 ta thu được K1 là:

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

K1 =

Ta lấy E(R0) xor với K1 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R0) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K1 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R0,K1) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 2:**

Ta có F(R0,K1)xor với L0 thu được R1 R1 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L1 = R0 Ta có E(R1):

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

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

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

Dịch 1 bit ta có C2 và D2 là : Từ C2 và D2 ta cho đi qua Pc-2 ta thu được K2 là

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

K2=

Ta lấy E(R1) xor với K2 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R1) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K2 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R1,K2) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 3:**

Ta có F(R1,K2)xor với L1 thu được R2 R2 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L2 = R0 Ta có E(R2):

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

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

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

Dịch 2 bit ta có C3 và D3 là : Từ C3 và D3 ta cho đi qua Pc-2 ta thu được K3 là

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

K3=

Ta lấy E(R2) xor với K3 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R2) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K3 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R2, K3) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 4:**

Ta có F(R2,K3)xor với L2 thu được R3 R3 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L3 = R2 Ta có E(R3):

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

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

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

Dịch 2 bit ta có C4 và D4 là : Từ C4 và D4 ta cho đi qua Pc-2 ta thu được K4 là

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

K4 =

Ta lấy E(R3) xor với K4 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R3) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K4 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R3, K4) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 5:**

Ta có F(R3,K4)xor với L3 thu được R4 R4 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L4 = R3 Ta có E(R4):

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

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

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

Dịch 2 bit ta có C5 và D5 Từ C5 và D5 ta cho đi qua Pc-2 ta thu được K5 là

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

K5 =

Ta lấy E(R4) xor với K5 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R4) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K5 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R4, K5) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 6:**

Ta có F(R4,K5)xor với L4 thu được R5 R5 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L5 = R4 Ta có E(R5):

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

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

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

Dịch 2 bit ta có C6 và D6 Từ C6 và D6 ta cho đi qua Pc-2 ta thu được K6 là

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

K6 =

Ta lấy E(R5) xor với K6 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R5) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K2 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R5, K6) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 7:**

Ta có F(R5, K6) xor với L5 thu được R6 R6 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L6 = R5 Ta có E(R6):

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

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

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

Dịch 2 bit ta có C7 và D7 Từ C7 và D7 ta cho đi qua Pc-2 ta thu được K7 là

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

K7 =

Ta lấy E(R6) xor với K2 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R6) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K7 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R6, K7) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 8:**

Ta có F(R6, K7) xor với L6 thu được R7 R7 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L7 = R6 Ta có E(R7):

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

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

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

Dịch 2 bit ta có C8 và D8 Từ C8 và D8 ta cho đi qua Pc-2 ta thu được K8 là

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

K8 =

Ta lấy E(R7) xor với K8 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R7) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K8 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R7, K8) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 9:**

Ta có F(R7,K8) xor với L7 thu được R8 R8 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L8 = R7 Ta có E(R8):

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

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

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

Dịch 1 bit ta có C9 và D9 Từ C9 và D9 ta cho đi qua Pc-2 ta thu được K9 là

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

K9 =

Ta lấy E(R8) xor với K9 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R8) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K9 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R8, K9) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 10:**

Ta có F(R8,K9) xor với L8 thu được R9 R9 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L9 = R8 Ta có E(R9):

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

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

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

Dịch 2 bit ta có C10 và D10 Từ C10 và D10 ta cho đi qua Pc-2 ta thu được K10 là

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

K10 =

Ta lấy E(R9) xor với K10 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R9) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K10 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R9, K10) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 11:**

Ta có F(R9,K10)xor với L9 thu được R10 R10 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L10 = R9 Ta có E(R10):

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

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

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

Dịch 2 bit ta có C11 và D11 Từ C11 và D11 ta cho đi qua Pc-2 ta thu được K11 là

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

K11 =

Ta lấy E(R10) xor với K11 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R10) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K11 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R10, K11) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 12:**

Ta có F(R10,K11) xor với L10 thu được R11 R11 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L11 = R10 Ta có E(R11):

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

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

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

Dịch 2 bit ta có C12 và D12 Từ C12 và D12 ta cho đi qua Pc-2 ta thu được K12 là

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

K12 =

Ta lấy E(R11) xor với K12 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R11) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K12 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R11, K12) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 13:**

Ta có F(R11,K12) xor với L11 thu được R12 R12 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L12 = R11 Ta có E(R12):

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

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

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

Dịch 2 bit ta có C13 và D13 Từ C13 và D13 ta cho đi qua Pc-2 ta thu được K13 là

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

K13 =

Ta lấy E(R12) xor với K13 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R12) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K13 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R12, K13) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 14:**

Ta có F(R12, K13) xor với L12 thu được R13 R13 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L13 = R12 Ta có E(R13):

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

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

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

Dịch 2 bit ta có C14 và D14 Từ C14 và D14 ta cho đi qua Pc-2 ta thu được K14 là

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

K14 =

Ta lấy E(R13) xor với K14 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R13) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K14 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R13, K14) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 15:**

Ta có F(R13, K14) xor với L13 thu được R14 R14 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L14 = R13 Ta có E(R14):

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

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

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

Dịch 2 bit ta có C15 và D15 Từ C15 và D15 ta cho đi qua Pc-2 ta thu được K15 là

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

K15 =

Ta lấy E(R14) xor với K2 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R14) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K15 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R14, K15) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

**Vòng 16:**

Ta có F(R14, K15) xor với L14 thu được R15 R15 đi qua hàm mở rộng E sẽ thu được bộ hoán vị 48 bit

L15 = R14 Ta có E(R15):

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

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

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

Dịch 1 bit ta có C16 và D16 Từ C16 và D16 ta cho đi qua Pc-2 ta thu được K16 là

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

K16 =

Ta lấy E(R15) xor với K16 ta đc bộ B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   E(R15) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   K16 | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | 5 | 6 | | 1 |  |  |  |  |  |  | | 2 |  |  |  |  |  |  | | 3 |  |  |  |  |  |  | | 4 |  |  |  |  |  |  | | 5 |  |  |  |  |  |  | | 6 |  |  |  |  |  |  | | 7 |  |  |  |  |  |  | | 8 |  |  |  |  |  |  |   Bộ B |

|  |  |
| --- | --- |
| Cho kết quả bộ B đi qua hộp S1 => S8 thu đc Bộ S | Cho bộ S đi qua bộ hoán vị P ta thu được F(R15, K16) |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | 1 | 2 | 3 | 4 | | 1 |  |  |  |  | | 2 |  |  |  |  | | 3 |  |  |  |  | | 4 |  |  |  |  | | 5 |  |  |  |  | | 6 |  |  |  |  | | 7 |  |  |  |  | | 8 |  |  |  |  | |

Ta có F(R15, K16) xor với L15 thu được R16

L16 = R15

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

|  |  |
| --- | --- |
| R16 đổi chỗ cho L16 | 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 R16L16 ta nhận được bản rõ trong dạng thập lục phân sau: