### Hệ mật DES (Data Encryption Standard) : Tiêu chuẩn mã hoá dữ liệu

###### https://lilthawg29.files.wordpress.com/2021/08/image-32.png?w=1024

#### Giới thiệu

##### Tồng quan

DES (Data Encryption Standard) là chuẩn mã hóa dữ liệu đầu tiên trên thế giới, do Cơ quan an ninh Quốc gia Hoa Kỳ (NSA) đề xuất trên cơ sở cải tiến thuật toán Lucifer do hãng IBM công bố năm 1964. DES đã được sử dụng rộng rãi ở Hoa Kỳ và nhiều quốc gia khác trong các thập kỷ 70, 80, 90 cho đến khi được thay thế bởi Tiêu chuẩn mã hóa dữ liệu tiên tiến AES (Advanced Encryption Standard) vào năm 2002.

##### Lịch sử hình thành và phát triển:

###### 1972:

###### 1974:

###### ­1976:

##### Sử dụng cấu trúc mạng Feistel Network để mã hóa và giải mã dữ liệu (phân chia dữ liệu thành hai nửa và thực hiện một loạt các hoạt động, bao gồm hoán vị (permutation), thay thế (substitution), và phép XOR, trước khi kết hợp nửa dữ liệu lại với nhau.)

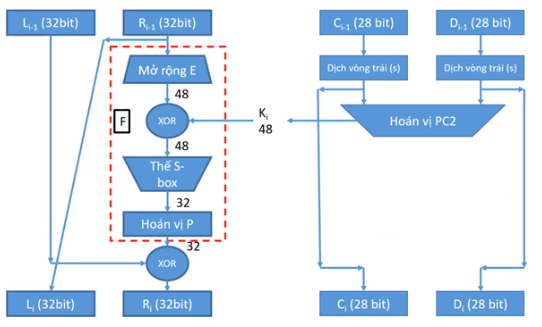
#### Thuật toán DES

##### Sơ đồ hoàn chỉnh:

###### 

##### Chi tiết thuật toán: Gồm 16 vòng

###### Chi tiết 1 vòng:



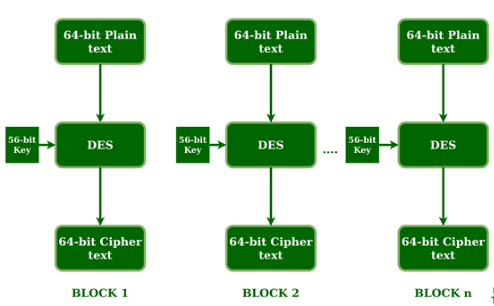
###### Thuật toán mã:

Chuẩn bị đầu vào (input)

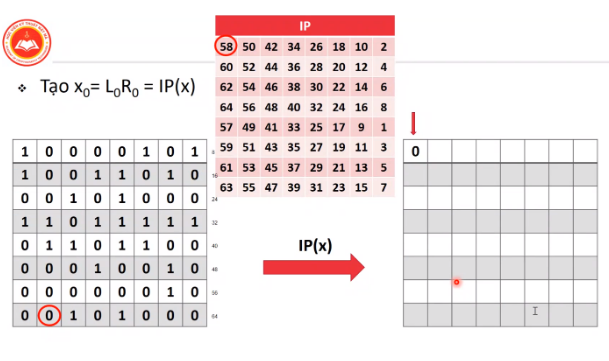
Chọn thông điệp

Chuyển sang nhị phân

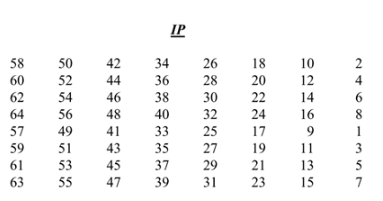
Chia thành các Block 64 bit (padding(đệm) nếu cần )



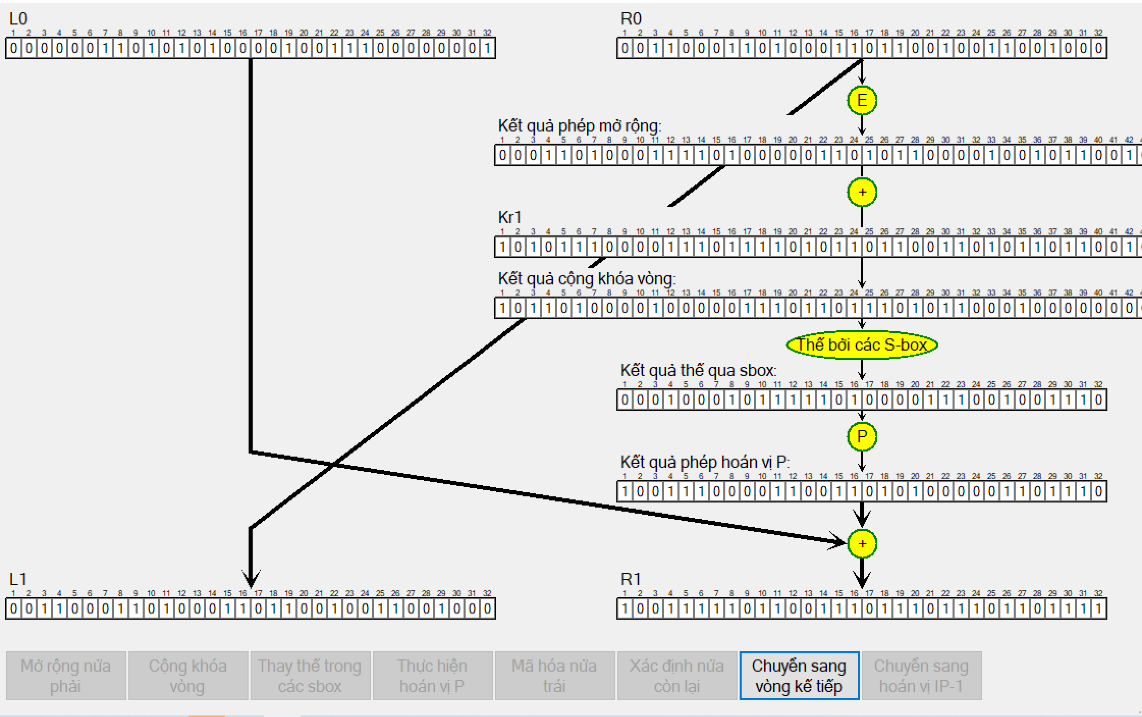
Hoán vị IP



Ghi lại x ----(viết lại từ dưới lên thứ tự cột 2, 4, 6, 8, 1, 3, 5, 7)---> IP(x)

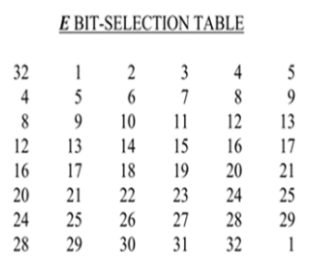


Hàm F (Feistel):

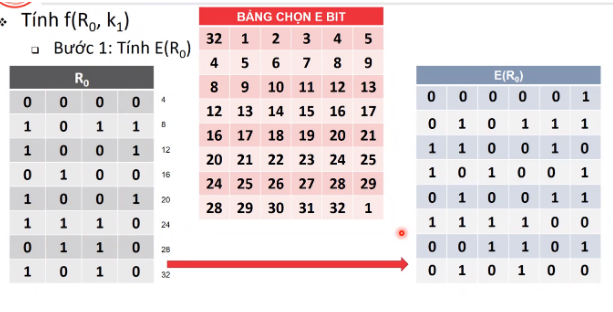


**E (Mở rộng R)**

Đưa phần R0 qua hoán vị mở rộng E ( mục đích của hoán vị mở rộng này là mở rộng R0 lên 48 bits để tý XOR với K1 cũng 48 bits).

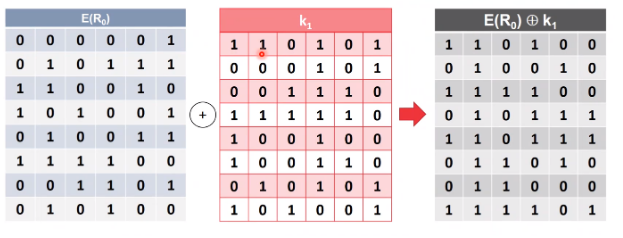


Hoán vị mở rộng E nhìn chung là việc lặp lại 2 bit cuối của hàng trước và viết tiếp bit của hàng sau.

Vd: 

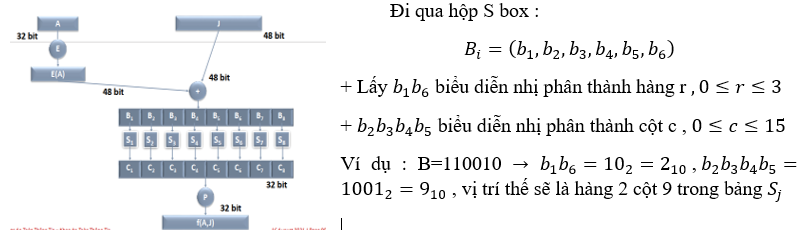
**XOR**

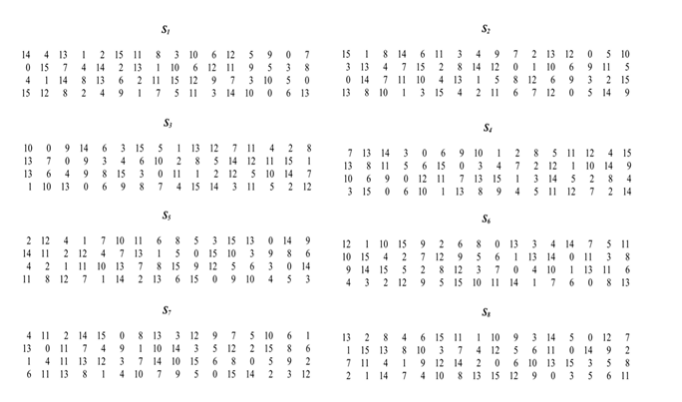
Ri(48) XOR Ki(48)

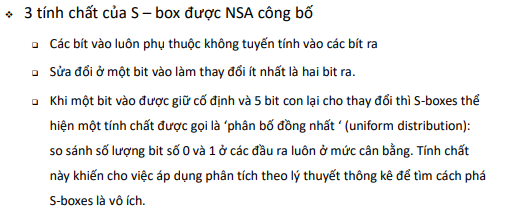
Vd: 

**S (S-boxes)**

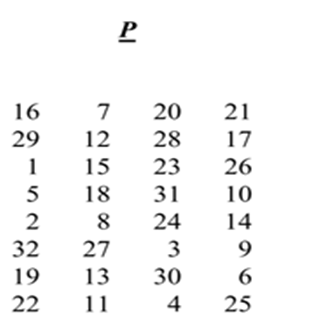
Chia 48 bits thành 8 khối, mỗi khối 6 bits (mỗi hàng 1 khối)







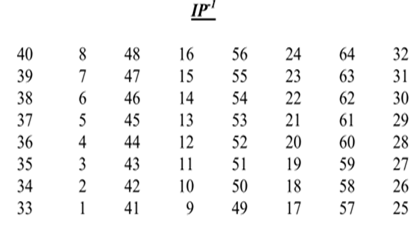
**P (Hoán vị P)**



Sau đó lấy L0 XOR với kết quả vừa tìm được ta được R1,L1 được gán = R0 ban đầu.

Hoán vị IP-1

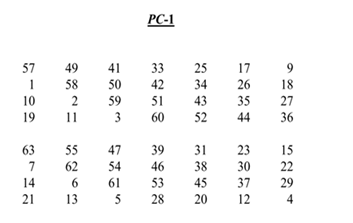
Khi hết 16 vòng thì cho qua hoán vị IP-1



###### Thuật toán sinh khoá key

Hoán vị PC-1

Khoá 64 bits từ ban đầu qua hoán vị PC-1(Permuted Choice – 1) loại bỏ 8 bits chia hết cho 8 : 8,16,24,32,40,48,56,64.



C0= 28 bits đầu, D0 = 28 bits cuối.

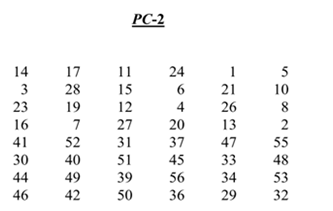
Thuật toán dịnh trái bit (…)

dịch vòng trái C0và D0

Dịch vòng trái ở các vòng khác nhau, chỉ có vòng 1,2,9,16 là dịch 1 trái 1 bit, còn lại là 2 bit.

Hoán vị PC-2

PC-2 hoạt động tương tự PC-1 chỉ khác ở sự hoán vị, các bit 9,18,22,25,35,38,43,54 bị lược bỏ.



Đầu ra lúc này là K1 = 48 bits.

Lưu lại kết quả của C0và D0 sau khi dịch vòng trái và gán vào C1 và D1 để chuẩn bị cho vòng 2.

#### Tính chất DES

###### 

###### 

###### 

#### Các biến thể của DES

##### DES bội hai

###### 

##### DES bội ba

###### 