# I. DES

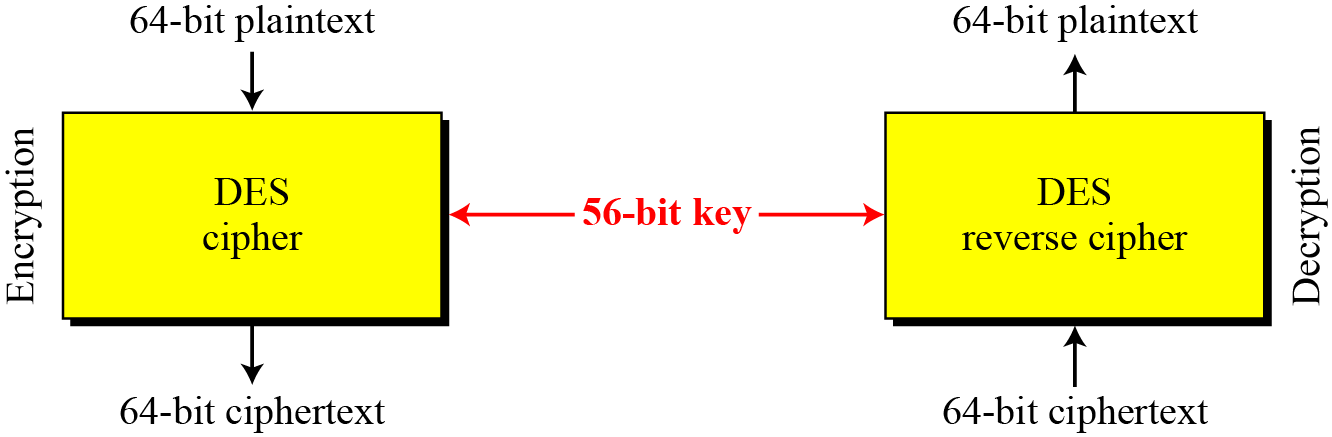
1. **Sơ lược lịch sử về DES**

DES (viết tắt của Data Encryption Standard, hay Tiêu chuẩn Mã hóa Dữ liệu) là một phương pháp mật mã hóa được FIPS (Tiêu chuẩn Xử lý Thông tin Liên bang Hoa Kỳ) chọn làm chuẩn chính thức vào năm 1976.

Hiện nay DES được xem là không đủ an toàn cho nhiều ứng dụng. Nguyên nhân chủ yếu là độ dài 56 bit của khóa là quá nhỏ. Khóa DES đã từng bị phá trong vòng chưa đầy 24 giờ. Đã có rất nhiều kết quả phân tích cho thấy những điểm yếu về mặt lý thuyết của mã hóa có thể dẫn đến phá khóa, tuy chúng không khả thi trong thực tiễn. Thuật toán được tin tưởng là an toàn trong thực tiễn có dạng Triple DES (thực hiện DES ba lần), mặc dù trên lý thuyết phương pháp này vẫn có thể bị phá. Gần đây DES đã được thay thế bằng AES (Advanced Encryption Standard, hay Tiêu chuẩn Mã hóa Tiên tiến).

1. **Tính chất của DES**

DES là một mã khối, mỗi khóa gồm 64 bít, trong đó 56 bít được sử dụng để thực hiện mã hóa/giải mã trong thuât toán. 8 bít còn lại được dùng để kiểm tra/phát hiện lỗi.



Là mã thuộc hệ mã Feistel gồm 16 vòng, ngoài ra DES có thêm một hoán vị khởi tạo trước khi vào vòng 1 và một hoán vị khởi tạo sau vòng 16

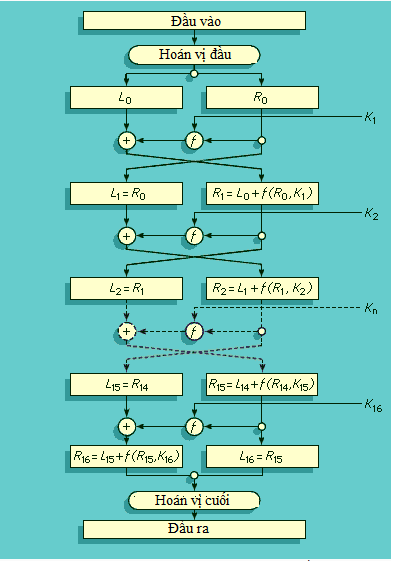
– Kích thước của khối là 64 bít: ví dụ bản tin “meetmeafterthetogaparty” biểu diễn theo mã ASCII thì mã DES sẽ mã hóa làm 3 lần, mỗi lần 8 chữ cái (64 bít): meetmeaf – tertheto – gaparty.

– Kích thước khóa là 56 bít

– Mỗi vòng của DES dùng khóa con có kích thước 48 bít được trích ra từ khóa chính.

– Mã hóa DES gồm ba phần, phần thứ nhất là các hoán vị khởi tạo và hoán vị kết thúc. Phần thứ hai là các vòng Feistel, phần thứ ba là thuật toán sinh khóa con.

1. **Mô tả thuật toán**



Mã hóa DES được thực hiện qua 16 vòng. Thông tin đầu vào là 64 bít, sẽ được chia thành 2 khối (block) trái (L) và phải (R). Sau đó từ khóa (56 bít) người ta tạo ra các khóa con (subkey) 48 bít gọi là Ki. Hàm f ở trên thực chất là 1 hàm hoán vị.

+ Chuỗi đầu vào 64 bit sẽ được đi qua một bảng hoán vị trở thành chuỗi P1. (Việc hoán vị này giống với mã hoán vị cổ điển)

+ Sau khi hoán vị xong, ta chia chuỗi P1 thành 2 phần là L0 và R0. với L0 là 32 bit đầu của chuỗi P1, R0 là 32 bit sau của chuỗi P1.

+ Việc mã hóa tiếp tục được thực hiện bằng cách: dùng chuỗi 32 bit R, kết hợp với khóa K1 thông qua hàm f ra chuỗi R'.(tạo khóa được giải thích bên dưới)

+ Dùng phép toán XOR chuỗi 32 bit L với chuỗi 32 bit R' sinh ra chuỗi L'.

+ Gán chuỗi L1 = R', R1 = L'. Tiếp tục lặp lại quá trình bên trên với khóa K2.

+ Thực hiện việc lặp như vậy 16 lần, ta sẽ có R16, L16. Ghép chuỗi R16 và L16 thành P2.

+ Đưa P2 qua một hoán vị cuối (nghịch đảo của hoán vị đầu) ta sẽ được chuỗi đầu ra 64 bit.

+ Việc giải mã sẽ làm ngược lại toàn bộ quá trình trên.

+ Tạo khóa:

Khóa K ban đầu là một chuỗi 64 bit, tuy nhiên, ta sẽ loại bỏ 8 bit gồm: bit 8, 16, 24, 32, 40, 48, 56, 64 để kiểm tra => sinh ra khóa K' 56 bit.

Tại mỗi bước vòng lặp trên, khóa K' 56 bit sẽ được sử dụng để sinh ra khóa con K\_i 48 bit. Việc tạo khóa con thực hiện như sau:

Chia khóa K' thành 2 phần 28 bit, mỗi phần dịch chuyển n bit theo quy ước (việc dịch giống mã Caesar).

Đẩy 2 phần đã dịch chuyển vào hoán vị nén C - cố định để tạo ra khóa 48 bit đưa vào sử dụng cho vòng mã hóa.

Giữ nguyên 2 phần K' sau khi dịch chuyển, tiếp tục dịch chuyển và đưa qua hoán vị nén để sinh ra khóa K\_2.

Việc tạo khóa lặp lại tương tự cho đến K\_16.

+ Với khóa K\_i 48 bit, ta sẽ đem XOR với thành phần R\_i mở rộng. Với mỗi R\_i 32 bit, sẽ được đưa qua một hoán vị mở rộng, sẽ nhân đôi 16 bit của R\_i tại một số vị trí nhất định để trở thành chuỗi 48 bit R\_i'. Tiếp đó, ta sẽ XOR K\_i và R\_i' => sinh ra R\_ki dài 48 bit. Chia R\_ki thành 8 phần, mỗi phần 6 bit. Đưa từng phần của R\_ki qua 1 hoán vị nén (gọi là S-box, có 8 S-box nên ký hiệu là S\_1, S\_2...). Từng phần 6 bit R\_ki sau khi đi qua hoán vị nén S-box sẽ cho ta các phần 4 bit. Ghép 8 phần lại với nhau, ta sẽ được R' 32 bit.

=>tổng kết:

+ Hàm dịch chuyển theo quy ước, hoán vị nén C để tạo khóa và hoán vị mở rộng R\_i từ 32 bit thành 48 bit là cố định cho tất cả hệ mã DES do đó, các hoán vị này không gọi là khóa.

+ Thành phần khóa của hệ mã DES bao gồm: Khóa K - 64 bit (do hàm dịch và hoán vị nén C là cố định, nên từ K ta có thể dễ dàng tìm ra dãy khóa con K\_i), hoán vị khởi đầu của P1 và các S-box.

1. **Độ an toàn của DES**

+ Điểm yếu

Ký hiệu là phần bù của u (ví dụ 0100101 và 1011010 là bù của nhau) thì DES có tính chất sau:

y = DESz(x) => =DESz ( )

Cho nên nếu biết MÃ y được mã hóa từ TIN x với khóa z thì ta suy ra được mã hóa từ TIN với khóa . Tính chất này chính là một điểm yếu của DES bởi vì nhờ đó kẻ tấn công có thể loại trừ một nửa số khóa cần phải thử khi tiến hành phép thử – giải mã theo kiểu tìm kiếm vét cạn không gian khóa.

+Khóa yếu

Các khóa yếu là các khóa mà theo thuật toán sinh khóa con thì tất cả 16 khóa con đều như nhau Z1 = Z2= Z3= …= Z15= Z16 điều đó khiến cho phép sinh mã và giải mã đối với các khóa yếu này là giống hệt nhau

DESz = DES-1z

Có tất cả 4 khóa yếu như sau:

1) [00000001 00000001 … … 00000001]

2) [11111110 11111110 … … 11111110]

3) [11100000 11100000 11100000 11100000

11110001 11110001 11110001 11110001]

4) [00011111 00011111 00011111 00011111

00001110 00001110 00001110 00001110]

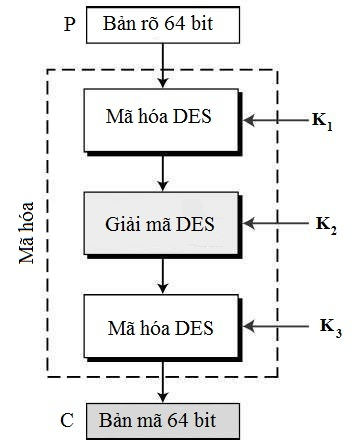
Đồng thời có 10 khóa yếu với thuộc tính là tồn tại Z, Z’ sao cho

DES-1z= DESz’ hay DES-1z’= DES

# II. 3DES

**Thuật toán 3DES**

+ Thuật toán 3DES sử dụng một nhóm khóa bao gồm 03 khóa DES là K1, K2 và K3, mỗi khóa có giá trị 56 bít. Thuật toán mã hóa thực hiện như sau:

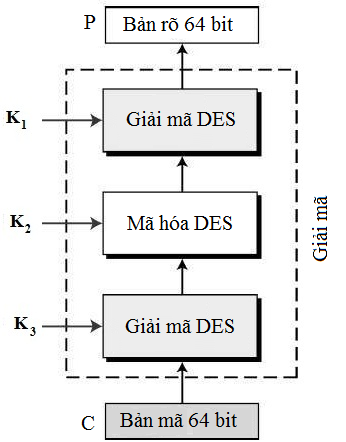


+ Quá trình mã hóa

Bản mã= EK3(DK2(EK1(Bản rõ)))

Trước tiên, thực hiện mã hóa DES với khóa K1, tiếp tục giải mã DES với khóa K2 và cuối cùng mã hóa DES với khóa K3(E – Encryption: quá trình mã hóa; D - Decryption: quá trình giải mã; Bản rõ: Dữ liệu đầu vào của phép mã hóa hoặc dữ liệu đầu ra của phép giải mã; Bản mã: Dữ liệu đầu ra của phép mã hóa hoặc dữ liệu đầu vào của phép giải mã).

+ Quá trình giải mã



Bản rõ = DK1(EK2(DK3(Bản mã))

Quá trình giải mã với việc  giải mã với khóa K3, sau đó mã hóa với khóa K2,và cuối cùng giải mã với khóa K1..

3DES mã hóa một khối dữ liệu có giá trị 64 bít (bản rõ) thành một khối dữ liệu mới có giá trị 64 bít (bản mã). Các tiêu chuẩn chỉ ra phương thức lựa chọn nhóm khóa (K1,K2, K3) như sau:

Lựa chọn 1: K1,K2, K3 là các khóa độc lập

Lựa chọn 2: K1,K2 là hai khóa độc lập và  K3 =K1

Lựa chọn 3: K1=K2=K3

Lựa chọn 1 là phương thức mã hóa mạnh nhất với 168 bít khóa độc lập (168=3x56). Lựa chọn 2 ít bảo mật hơn với 112 bít khóa ( 2x56=112 bít) và lựa chọn 3 chỉ tương đương với việc mã hóa DES 1 lần với 56 bít khóa. Mỗi khóa DES thông thường được lưu trữ và truyền đi trong 8 byte, vì vậy một nhóm khóa yêu cầu 8 hoặc 16, 24 byte cho việc lưu trữ khóa.