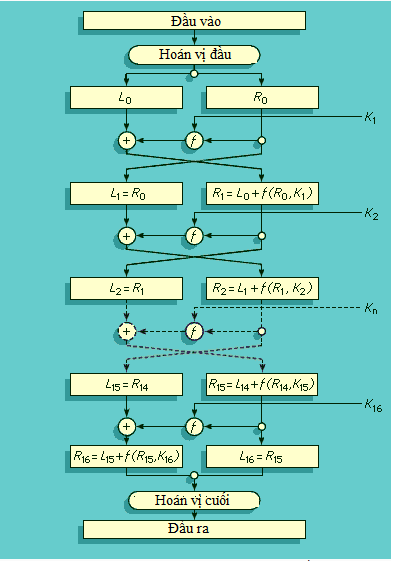
CÁC THUẬT TOÁN MÃ HÓA THƯỜNG SỬ DỤNG TRONG NGÂN HÀNG HIỆN NAY

1. DES và 3DES
2. Giới thiệu tổng quản

* Thuật toán mã khối DES (Data Encryption Standard) là một thuật toán mã khối với kích thước khối 64 bít và kích thước khóa 56 bít, được công bố chính thức bởi Tổ chức Tiêu chuẩn xử lý thông tin liên bang Hoa Kỳ (FIPS) vào tháng 11/1976 và được xuất bản trong tài liệu FIPS PUB 46 (01/1977). Thuật toán DES đã trải quả nhiều lần cập nhật: năm 1988 (FIPS-46-1), 1993 (FIPS-46-2), 1998 (FIPS-46-3). Tiền thân của thuật toán DES là thuật toán Lucifer, một thuật toán do IBM phát triển. Cuối năm 1976, DES được chọn làm chuẩn mã hóa dữ liệu của Hoa Kỳ, sau đó được sử dụng rộng rãi trên toàn thế giới trong lĩnh vực an toàn, bảo mật thông tin trên môi trường số.

**2. Một số đặc điểm kỹ thuật**

* Thuật toán DES được thiết kế để mã hóa và giải mã các khối dữ liệu 64 bít với một khóa có độ dài 64 bít. Việc giải mã phải được thực hiện bởi một khóa tương ứng như trong quá trình mã hóa, 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.
* Qúa trình mã hóa của DES 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.
* Trong quá trình mã hóa, dữ liệu đầu vào phải thực hiện quá trình hoán vị đầu (initial permutation) và hoán vị cuối (final permutation) sau vòng thứ 16. Việc thực hiện hoán vị phục vụ cho quá trình đưa thông tin vào và lấy thông tin ra từ các khối phần cứng, tạo điều kiện cho việc cài đặt phần cứng. Hàm cơ sở f cho phép đảm bảo tính bảo mật trong thuật toán DES này.



Việc thực hiện nhiều lần các bước lặp với tác dụng của f là nhằm tăng cường tính phi tuyến và tính khuếch tán đã có trong hàm f.

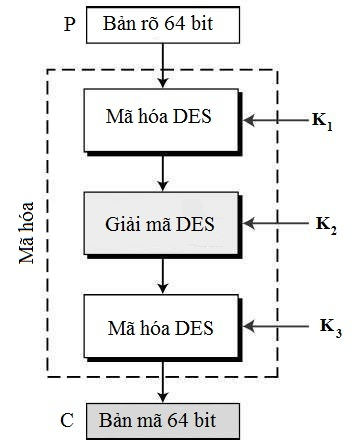
Cấu trúc của vòng lặp DES thực hiện theo công thức sau:

(Li,Ri) = (Ri-1, Li-1 XOR f (Ri-1,Ki))

Trong đó (Li,Ri) là nửa trái và nửa phải lấy được của phép biến đổi vòng lặp thứ i. Chi tiết về hàm hoán vị f, bạn đọc có thể tham khảo thêm tại Tiêu chuẩn TCVN 11367-3:2016.

**Thuật toán 3DES**

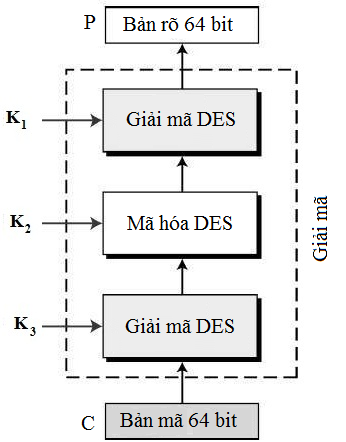
Thuật toán 3DES sử dụng một nhóm khóa bao gồm 03 khóa DES là K1, K2 và K3, mỗi khóa có giá trị 56 bít. Thuật toán mã hóa thực hiện như sau:



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).



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.