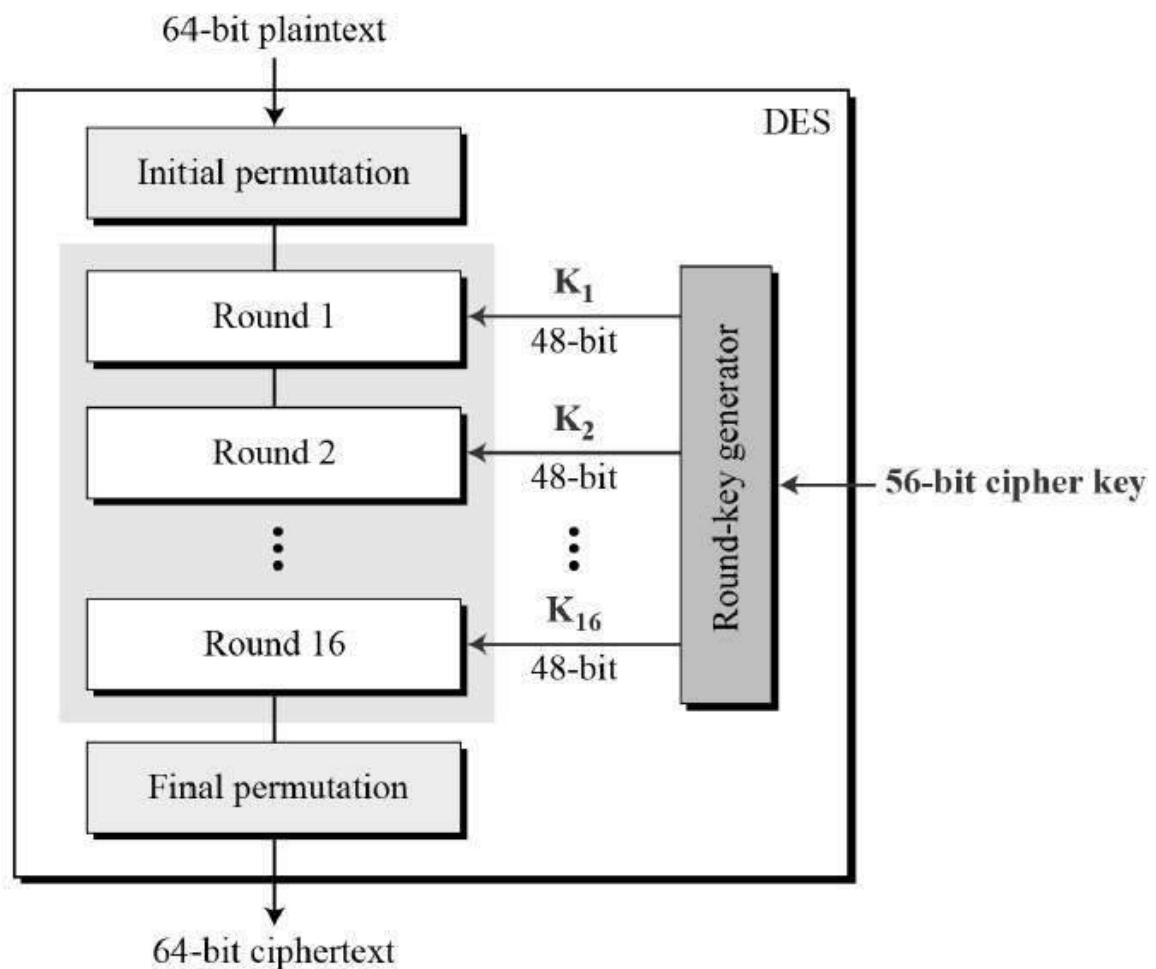


Data Encryption Standard (DES) là gì?

Data Encryption Standard (DES) hay còn được gọi là Tiêu chuẩn mã hóa dữ liệu bằng phương pháp khóa đối xứng. Vào đầu những năm 1970 DES được nghiên cứu và công bố bởi các nhà nghiên cứu của IBM.

Năm 1977 nó chính thức được Viện tiêu chuẩn và công nghệ quốc gia Hoa Kỳ (NIST) thông qua để bảo vệ những **dữ liệu** mật cho chính phủ. Thế nhưng sau vài thập niên khả năng phát triển của DES không khả quan và nó đã chính thức ngừng hoạt động vào năm 2005.

Nguyên lý hoạt động của DES

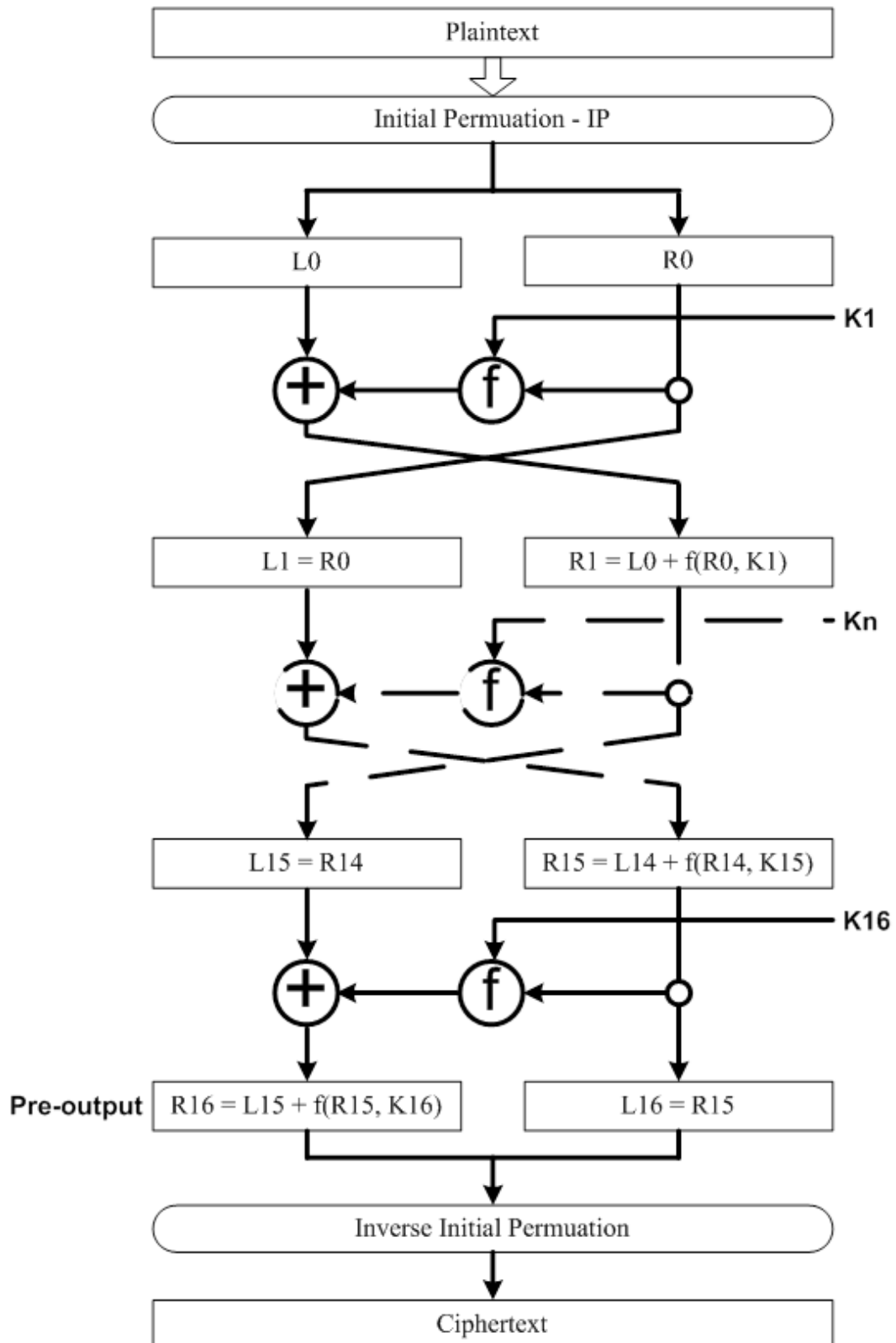


Để thực hiện thao tác mã hóa và giải mã tin nhắn DES sử dụng cùng một key riêng tư. Và tất nhiên key này cả người nhận và người gửi đều nhận biết và sử dụng được.


Thuật toán mã hóa dữ liệu DES – Encipher

1. Lưu đồ thuật toán mã hóa

Thuật toán DES được sử dụng để mã hóa và giải mã các block (khối) dữ liệu 64 bit dựa trên một key (khóa mã) 64 bit. Chú ý, các block được đánh số thứ tự bit từ trái sang phải và bắt đầu từ 1, bit đầu tiên bên trái là bit số 1 và bit cuối cùng bên phải là bit số 64. Quá trình giải mã và mã hóa sử dụng cùng một key nhưng thứ tự phân phối các giá trị các bit key của quá trình giải mã ngược với quá trình mã hóa.



2.Hoán vị khởi tạo - IP

Hoán vị khởi tạo