Từ “hello” khóa K1..

Bước 1: Tạo khóa con K1

- Đầu tiên, khóa DES gốc (56 bit) được mở rộng thành một khóa mở rộng (64 bit) bằng cách thêm một số bit kiểm tra. Sau đó, khóa này được chia thành hai nửa: left key (28 bit) và right key (28 bit).

- Sau đó, cả hai nửa khóa này được xoay vòng sang trái một số bước dựa trên một lịch trình đã cố định để tạo ra khóa con K1 (48 bit).

Bước 2: Mã hóa DES với khóa con K1 và dữ liệu đầu vào "hello"

- Bây giờ, chúng ta sử dụng khóa con K1 để mã hóa dữ liệu đầu vào "hello".

- Dữ liệu đầu vào "hello" (đã được chuyển đổi thành dạng nhị phân và mở rộng để có đủ 64 bit) được đưa qua một hoán đổi ban đầu (initial permutation) để chuyển đổi nó theo một thứ tự cố định.

- Sau đó, dữ liệu được chia thành hai nửa: left half (L0) và right half (R0).

- Nửa phải R0 được truyền qua hàm con mã hóa F (function), sử dụng khóa con K1 để tạo ra một kết quả.

- Kết quả từ hàm F sau đó được XOR với nửa trái L0.

- Nửa trái L0 trở thành nửa phải của vòng lặp tiếp theo, và nửa phải R0 trở thành kết quả của vòng lặp này.

Bước 3: Lặp lại vòng lặp

- Quy trình từ Bước 2 được lặp lại một số lần (thường là 16 lần) để tạo ra dữ liệu đã mã hóa cuối cùng.

Bước 4: Hoán đổi cuối cùng (final permutation)

- Cuối cùng, kết quả từ vòng lặp cuối cùng được đưa qua hoán đổi cuối cùng để tạo ra dữ liệu đã mã hóa (ciphertext).