Hướng dẫn thực hành bài lab AES kết hợp LSB

trên nền tảng Ubuntu

1. Mục đích

● Hiểu nguyên lý mã hóa đối xứng sử dụng thuật toán AES (Advanced Encryption Standard)
● Nắm được kỹ thuật giấu tin trong ảnh bằng phương pháp LSB (Least Significant Bit)
● Thực hành mã hóa và giấu tin vào ảnh, sau đó giải mã và trích xuất lại thông tin
● Làm quen với các công cụ mã hóa và steganography dòng lệnh trên Ubuntu

2. Lý thuyết thuật toán

● **AES (Advanced Encryption Standard)**: Thuật toán mã hóa đối xứng, sử dụng khóa bí mật để mã hóa/giải mã dữ liệu
● **Giấu tin LSB**: Thay bit ít quan trọng nhất của từng pixel trong ảnh bằng dữ liệu cần giấu (thường là ảnh BMP hoặc JPG)
● **Các bước chính**:

1. Mã hóa thông tin bằng AES
2. Nhúng ciphertext vào ảnh sử dụng LSB
3. Trích xuất dữ liệu từ ảnh và giải mã lại thông điệp gốc

3. Nội dung thực hành

3.1 Khởi động bài lab

Truy cập đường dẫn: https://github.com/vuongnguyen168/lsb_aes_tool.git tải bài lab về và lưu trong thư mục labtainer/trunk/labs

Cài đặt lab: rebuild -b lsb_aes_tool

Khởi động bài lab: labtainer -r lsb_aes_tool

Cài đặt các công cụ cần thiết:

sudo apt update
sudo apt install steghide openssl

3.2 Chuẩn bị dữ liệu cần giấu

● Tạo một file văn bản chứa thông tin cần bảo mật:

echo "This is a secret message" > secret.txt

3.3 Mã hóa nội dung bằng AES

● Dùng `openssl` để mã hóa nội dung:

openssl enc -aes-256-cbc -salt -in secret.txt -out secret.enc -pass pass:yourpassword

● Kiểm tra file `secret.enc` đã được tạo:

ls

3.4 Giấu dữ liệu vào ảnh bằng LSB

● Chuẩn bị ảnh gốc định dạng `.jpg` hoặc `.bmp` (ví dụ `cover.jpg`)
● Dùng `steghide` để giấu file mã hóa vào ảnh:

steghide embed -cf cover.jpg -ef secret.enc(Enter passphrase)

→ Nhập passphrase để bảo vệ dữ liệu khi được yêu cầu

3.5 Giải mã và khôi phục dữ liệu

● Trích xuất dữ liệu từ ảnh:

steghide extract -sf cover.jpg(overwrite)

→ Nhập passphrase đúng để giải nén file `secret.enc`

● Giải mã nội dung:

openssl enc -d -aes-256-cbc -in secret.enc -out decrypted.txt -pass pass:yourpassword

● Xem nội dung thông điệp đã được giải mã:

cat decrypted.txt

● Kiểm tra dung lượng ảnh đã giấu tin:

ls -lh cover.jpg

=> So sánh với dung lượng ảnh gốc ban đầu (nếu có), bạn có thể thấy sự chênh lệch nhỏ do dữ liệu nhúng vào.

4. Kết quả

● Hoàn thành toàn bộ các bước: mã hóa → giấu tin → trích xuất → giải mã thành công
● Kiểm tra dữ liệu khôi phục đúng như ban đầu
● Rút ra nhận xét về sự thay đổi kích thước ảnh và tính bảo mật của kỹ thuật kết hợp này