Bài thực hành: Cài đặt giải thuật tấn công 2DES bằng phương pháp Meet-in-the-middle

1. **Mục đích**
   - Giúp hiểu được phương pháp mã hóa DES và kĩ thuật tấn công Meet-in-the-Middle lên 2DES.
2. **Yêu cầu đối với sinh viên**
   - Có kiến thức về mã hóa DES, hiểu cơ bản ngôn ngữ lập trình python
3. **Nội dung bài thực hành**

Khởi động bài lab:

imodule https://github.com/baprang186/labtainer/raw/main/imodule_cryp-attk-2des-mitm.tar

Vào terminal, gõ:

labtainer cryp-attk-2des_mitm

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong, màn hình sẽ xuất hiện 1 terminal với người dùng **student**. Khởi động môi trường ảo để thực hiện bài lab, thực hiện lệnh:

source venv/bin/activate

a) Nhiệm vụ 1: Tấn công DES với chương trình mitm.py

Trước tiên, thực hiện mã hóa DES bằng chương trình des.py

python3 des.py

Bài thực hành cho sẵn một chương trình tấn công là mitm.py, sử dụng các cặp khóa dự đoán trước để tiến hành tấn công. Để tấn công lên DES, ta cần 1 danh sách khóa k1 và dùng nó làm đầu vào cho tấn công DES dùng chương trình mitm.py

python3 mitm.py

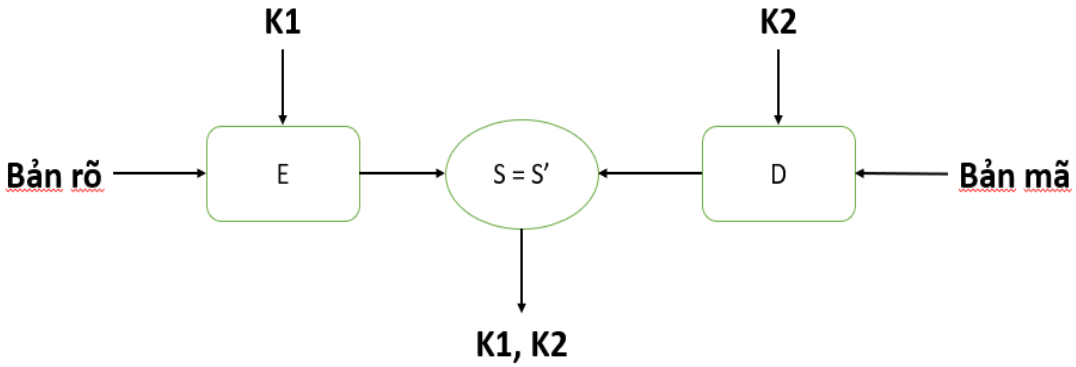
Kết quả sẽ tìm được khóa đúng từ danh sách khóa key1 cho trước.

b) Nhiệm vụ 2: Tấn công 2DES với Meet-in-the-middle

Phương pháp Meet-in-the-Middle (MitM) là một kỹ thuật tấn công mật mã hiệu quả để giảm đáng kể số lượng hoán vị cần thiết để giải mã văn bản đã được mã hóa bằng nhiều khóa.

Kẻ tấn công sẽ cố gắng mã hóa văn bản thuần với các khóa khác nhau để tạo văn bản mật mã trung gian, đồng thời giải mã văn bản mật mã với các khóa khác

nhau. Nếu tìm thấy sự trùng khớp, các khóa này có khả năng chính là hai khóa mã hóa được sử dụng trong hệ thống.



Tiếp tục bài lab với mã hóa 2DES, sử dụng code 2des.py để sinh bản mã và bản rõ cho đầu vào:

python3 2des.py

Để tấn công 2DES, ta cần danh sách 2 khóa K1, K2 đã được liệt kê và dự đoán từ trước. Sử dụng danh sách 2 khóa từ keys1.txt và keys2.txt làm đầu vào và tấn công bằng mitm.py:

python3 mitm.py

Kết quả của chương trình là tìm được 2 khóa K1, K2 dùng để mã hóa ở trên.

Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab cryp-attk-2des_mitm

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

startlab –r cryp-attk-2des_mitm