Khoa Khoa học & Kỹ thuật máy tính
Trường ĐH Bách Khoa TP.HCM

Cryptography and Network Security
Lab 1

Nguyen Nhat Nam

Ngày 16 tháng 2 năm 2016

Part 1. Tìm hiểu phiên bản đơn giản của giải thuật mã hóa DES (Simplified DES) và các mô hình mã hóa khối.

a. Giải thuật DES đơn giản hóa (S-DES) được phát triển bởi GS. Edwward Schaefer tại Đại học Santa Clara vào năm 1996.

+ **Mã hóa**: dùng khối 8-bit (plaintext) và khóa 10 bit, sinh ra khối 8-bit (ciphertext).

+ **Giải mã**: dùng khối 8-bit (ciphertext) và khóa 10-bit, sinh ra khối 8-bit (plaintext).

Tham khảo: File Simplified+DES_v3.pdf

b. Mã khối (như mã SDES) được áp dụng để mã hóa một khối dữ liệu có kích thước xác định. Để mã hóa một bản tin dài, bản tin được chia ra thành nhiều khối và áp dụng mã khối cho từng khối một. Có nhiều mô hình áp dụng mã khối là ECB, CBC, CTR, OFB và CFB. Trong bài lab này sinh viên cần tìm hiểu các mô hình mã hóa trên và ứng dụng vào bài lab.

Bài tập:

1. Sử dụng S-DES để giải mã chuỗi 10100010 với key 0111111101, ghi lại các kết quả trung gian như IP, F_K, SW, IP^{-1}.

2. Phân tích ngắn gọn các ưu điểm và nhược điểm của các mô hình mã hóa ECB, CBC, CTR, OFB.

Part 2. Lập trình thuật toán mã hóa và giải mã S-DES.

Các yêu cầu:

- Chương trình mã hóa một file văn bản dùng thuật toán mã hóa S-DES. Dữ liệu đầu vào được cho trong file "**plaintext.txt**", kết quả được lưu vào file "**result_ciphertext.txt**".
- Chương trình giải mã một file văn bản dùng thuật toán mã hóa S-DES. Dữ liệu đầu vào được cho trong file "**result_ciphertext.txt**", kết quả được lưu vào file "**plaintext.txt**".
- Áp dụng các mô hình mã hóa như ECB, CBC kết hợp với giải thuật S-DES để mã hóa và giải mã bản tin dài (khuyến khích sử dụng mô hình CBC).
- Ngôn ngữ sử dụng: sinh viên có thể dùng bất kì ngôn ngữ nào để hiện thực giải thuật đáp ứng yêu cầu bài toán.
  Một số ngôn ngữ gợi ý: Java, PHP, C#, Scala, Go Programming, Python,...
- Sinh viên **không được phép** sử dụng các thư viện mã hóa có sẵn.

Quy định nộp bài:

- **Mã nguồn**: Mã nguồn và file thực thi.
- **Báo cáo**: Ngôn ngữ sử dụng, mô tả các hàm/phương thức sử dụng trong chương trình, mô hình mã hóa được chọn, hướng dẫn cài đặt và chạy chương trình. Báo cáo không quá 3 trang, định dạng PDF. Lưu ý sinh viên cần ghi rõ mã số sinh viên và lớp học để thuận tiện cho việc chấm bài.
- **Hình thức nộp bài**: Nộp bài qua SAKAI, không nhận bài qua email. Deadline vào 17h ngày 26/02/2016.

Lưu ý cho Lab 1:
Sinh viên vắng mặt buổi lab, Sinh viên không nộp bài đúng hạn hoặc chương trình **không chạy được** sẽ nhận điểm 0 cho cột điểm bài tập.

HẾT