Nhập môn mã hóa mật mã
Bài tập nhóm 2

Ngày 19 tháng 12 năm 2022

1 Lý thuyết

Trong mật mã học, thám mã đóng vai trò quan trọng trong quá trình phát triển chung của ngành, với mục tiêu là tìm những điểm yếu hoặc không an toàn trong các giao thức chỉ với những dữ liệu công khai. Trong bài tập này, các bạn sinh viên được yêu cầu đọc bài báo "Cryptanalysis of Block Ciphers" (đã đăng trên trang môn học) về các phương thức thám mã cơ bản trên mật mã khối và viết báo cáo về những gì tìm hiểu được.

Yêu cầu

1. Chọn 1 trong 5 đề tài sau: (Nội dung có trong bài báo, 1 đề tài được chọn bởi tối đa 2 nhóm)
   - Linear cryptanalysis.
   - Differential cryptanalysis.
   - Square saturation - integral - multiset attacks.
   - Slide attacks - secret s-box cryptanalysis.
   - Complementation property attacks and weak keys.

   Phần tìm hiểu phải chỉ ra được các phương pháp trên thực hiện việc tấn công như thế nào, trong điều kiện gì, độ phức tạp trên lý thuyết của thuật toán, và thuật toán dựa trên các định lý nào.
2. Đưa ra ví dụ cụ thể mô tả cách tấn công đã tìm hiểu.

2 Thực hành

Trong bài tập 1, các nhóm đã hoàn thành việc sinh khóa, trong phần này, các bạn sinh viên được yêu cầu thực hiện mã hóa/giải mã một tập tin lưu trữ văn bản thuần túy (.txt).

Yêu cầu

1. Cài đặt: *Sử dụng ngôn ngữ C/C++, không dùng thư viện hỗ trợ lưu trữ/tính toán số nguyên lớn*, được sử dụng lại toàn bộ nội dung bài tập 1.
   - Viết chương trình gồm các chức năng cơ bản sau:
     - Sinh khóa hoặc nhập khóa RSA cá nhân: Người dùng được chọn 1 trong 2 lựa chọn, hoặc để chương trình sinh cặp khóa RSA, hoặc nhập vào khóa bí mật cá nhân.
     - Mã hóa tập tin: Nhận vào đường dẫn đến tập tin văn bản cần mã hóa (`.txt`) (P, ví dụ: P: `/home/usr/data/plaintext.txt`), khóa công khai của người nhận (rPK) và đường dẫn đến tập tin mã hóa (C, ví dụ: C: `/home/usr/data/ciphertext.txt`). Chương trình sẽ tiến hành mã hóa tập tin P bằng khóa công khai rPK và lưu vào tập tin C.

  - Giải mã tập tin: Nhận vào đường dẫn đến tập tin văn bản cần giải mã (`.txt`) (C, ví dụ: C: `/home/usr/data/ciphertext.txt`) và đường dẫn đến tập tin giải mã (P, ví dụ: P: `/home/usr/data/plaintext.txt`). Chương trình sẽ tiến hành giải mã tập tin C bằng khóa cá nhân đã được tạo cho người dùng ở chức năng tạo khóa và lưu vào tập tin P.
- Cài đặt ví dụ đã nêu ở phần lý thuyết.

2. Báo cáo:
   - Đánh giá ưu/nhược điểm của hệ thống mã hóa tập tin ở trên:
     - Giả sử có kẻ tấn công E đứng giữa, bắt được các tập tin đã mã hóa, E có thể làm gì với tập tin đó và gây tác hại gì đến hệ thống? Người bị tấn công có thể phát hiện được không?
     - Đưa ra các biện pháp phát hiện/phòng tránh cho các trường hợp tấn công của E đã nêu ở trên. Cộng điểm nếu có cài đặt.
   - Báo cáo chi tiết về chương trình , bao gồm:
     - Cách chạy chương trình
     - Thời gian thực hiện, ưu/nhược điểm của chương trình đã cài đặt.

3 Các quy định nộp bài

3.1 Các quy định chung

1. Sinh viên cần nộp đầy đủ các thành phần sau:
   - File báo cáo đồ án: report.pdf
   - Thư mục chứa mã nguồn chương trình: source
   - Trong thư mục source, cần có file README.TXT hướng dẫn chi tiết cách chạy chương trình.
2. Phần cài đặt được thực hiện trong 2 tuần.
3. **Phần báo cáo lý thuyết được thực hiện trong 1 tuần**.
4. Đồ án làm theo nhóm đã đăng ký.
5. Phần nộp bài (do trưởng nhóm đại diện nộp) sẽ gồm có 2 phần là mã nguồn (lưu trong thư mục Source) và báo cáo (lưu trong thư mục Report), được nén thành 1 file bằng định dạng ZIP có tên dạng như sau: MSSV01_MSSV02_MSSV03_MSSV04_MSSV05.zip (với nhóm có 5 thành viên).

3.2 Mã nguồn

1. Mã nguồn không thể biên dịch (báo lỗi biên dịch như sai cú pháp) hoặc không thể chạy được (báo các lỗi như lỗi runtime, sai logic chương trình) sẽ không được tính điểm.
2. Các hành vi gian lận liên quan đến mã nguồn (sao chép mã nguồn giữa các nhóm, sao chép mã nguồn trên Internet, ...) sẽ bị 0 điểm cả bài tập.

3.3 Báo cáo

Phần báo cáo tối thiểu cần có các câu trả lời cho những yêu cầu đã nêu trong đề bài. Các hành vi sao chép giữa các nhóm, sao chép nội dung trên mạng hoặc sao chép nội dung tiếng Anh rồi dịch sang tiếng Việt đều không được phép, trừ những nội dung lý thuyết như mã giả thuật toán được yêu cầu tìm hiểu, định lý, hệ quả liên quan.

Hết