HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA: CÔNG NGHỆ THÔNG TIN 2

Học phần: Mật mã học cơ sở

Trình độ đào tạo: **Đại học**

Hình thức đào tạo: **Chính qui**

THÔNG TIN ĐỀ TÀI DỰ ÁN

ĐỀ TÀI SỐ 5

1. Tên đề tài: Minh hoạ phương pháp thám mã tấn công với số mũ công khai nhỏ

2. Số lượng sinh viên yêu cầu: 3-5 sinh viên.

3. Mô tả đề tài

Đề tài tập trung vào việc nghiên cứu, mô phỏng và minh họa một trong những lỗ hổng của hệ mật mã RSA khi sử dụng số mũ công khai nhỏ (như e=3). Đây là một phương pháp tấn công phân tích mật mã học nổi tiếng, dựa trên việc lợi dụng đặc điểm toán học của RSA khi bản rõ có kích thước nhỏ hoặc được gửi tới nhiều người dùng với cùng giá trị e. Mục tiêu của đề tài là giúp sinh viên hiểu rõ rủi ro khi thiết kế hệ thống mật mã không đảm bảo đầy đủ các điều kiện an toàn.

Các yêu cầu chính của đề tài:

- Nghiên cứu lý thuyết:
    - Tìm hiểu thuật toán RSA: cách sinh khóa, mã hóa và giải mã.
    - Tìm hiểu về vai trò của số mũ công khai e, đặc biệt là khi chọn giá trị nhỏ như 3 hoặc 5.
    - Tìm hiểu các kiểu tấn công:
        - Tấn công khi $m^e < n$
        - Tấn công Håstad (khi cùng bản rõ gửi tới nhiều người)
        - Khai căn bằng phương pháp toán học (Newton, căn bậc ba nguyên)
- Thiết kế phần mềm minh họa:
    - Xây dựng chương trình cho phép sinh khóa RSA với e=3
    - Mã hóa bản rõ nhỏ và hiển thị quá trình tấn công bằng cách khai căn

    - Mô phỏng tấn công Håstad trong trường hợp nhiều người nhận
- Chức năng chính:
    - Sinh khóa RSA với tham số tùy chỉnh
    - Mã hóa và giải mã bản rõ
    - Tấn công: hiển thị rõ quá trình khai căn để tìm lại bản rõ
    - Giao diện trực quan hoặc mô tả từng bước (nếu là ứng dụng dòng lệnh)
- Công nghệ áp dụng:
    - Ngôn ngữ gợi ý: Python (sử dụng thư viện Crypto, gmpy2, sympy)
    - Giao diện: dòng lệnh (CLI) hoặc giao diện đơn giản với Tkinter/Web
    - Có thể tích hợp mã nguồn mở (như rsatool, Cryptool) để minh họa
- Kiểm thử và đánh giá:
    - Thử nghiệm với nhiều bản rõ khác nhau và so sánh độ dễ/khó khi tấn công
    - Kiểm tra khả năng phục hồi bản rõ trong các điều kiện khác nhau
- Tài liệu và báo cáo:
    - Quyển báo cáo đề tài

4. Yêu cầu nhóm và học viên.

- Yêu cầu đối với nhóm thực hiện:
    - Nhóm từ 2–4 sinh viên để dễ dàng phối hợp.
    - Mỗi thành viên cần đảm nhiệm một phần cụ thể: lý thuyết, lập trình, mô phỏng tấn công, viết báo cáo.
    - Làm việc nhóm hiệu quả, cập nhật tiến độ định kỳ và hỗ trợ nhau hoàn thành sản phẩm.
- Yêu cầu đối với từng học viên:
    - Hiểu rõ cơ chế hoạt động của RSA và rủi ro khi dùng số mũ công khai nhỏ.
    - Có khả năng lập trình với các thư viện mã hóa cơ bản.
    - Chủ động nghiên cứu và tìm hiểu các công trình/thực nghiệm liên quan.
    - Viết báo cáo rõ ràng, trình bày logic và dễ hiểu.
    - Tham gia đầy đủ vào quá trình phát triển, kiểm thử và thuyết trình.