ĐỒ ÁN NHÓM MÔN AN TOÀN MẠNG MÁY TÍNH

Mỗi nhóm gồm 2-3 sinh viên. Nhóm có thể chọn 1 trong 2 phần sau để làm đồ án: viết ứng dụng và tạo video bài giảng

A. Viết ứng dụng

Viết ứng dụng cho các giải thuật mã hoá sau:

1. Mã hoá PlayFair
2. Mã hoá RSA

B. Tạo video bài giảng

- **Yêu cầu**
    - Tạo video với nội dung là các đề tài đính kèm
    - Mỗi video có độ dài 8-15 phút
    - Video phải có thuyết minh bằng giọng nói, có thể bổ sung phụ đề
    - Cần xây dựng kịch bản nghiêm túc, chất lượng (mở đầu, giới thiệu, nội dung, kết luận…)
    - Mỗi nhóm thực hiện 5-6 video từ danh sách 9 đề tài. Thời hạn nộp bài là trước buổi học cuối học kỳ.

Đề tài

1. Nêu chức năng và cách sử dụng một số công cụ sau đây:
    a. Netstat
    b. Fport
    c. TCPView
    d. CurrPorts Tool
    e. Process Viewer
    f. What's running
    g. One file exe maker
2. Tạo Virus, Worm, Trojan với các công cụ tạo tự động (Terabit Virus maker, Internet Worm Maker Thing…).
3. Sử dụng công cụ Cryptool, cho ví dụ về mã hoá và giải mã một chuỗi ký tự với giải thuật PlayFair và giải thuật Hill.
4. Cho ví dụ về mã hoá và giải mã một chuỗi ký tự với giải thuật RSA
    a. Tạo cặp khoá
    b. Chuyển chuỗi ký tự sang dạng số
    c. Mã hoá chuỗi số để tạo ciphertext
    d. Giải mã ciphertext để thu được chuỗi số, chuyển đổi sang chuỗi ký tự plaintext ban đầu
5. Cho ví dụ về tấn công chuỗi băm
    a. Sử dụng công cụ Cryptool (menu Analysis – Hash – Attack on the…)

    b. Thực hiện tấn công với 2 file có nội dung khác nhau
    c. Mô tả quá trình thực hiện và kết quả đạt được
6. Cho ví dụ về tạo chữ ký số
    a. Sử dụng công cụ Cryptool (menu Digital Signatures/PKI)
    b. Thực hiện các bước tạo khoá, ký vào văn bản, kiểm tra chữ ký số…
7. Mô tả quá trình tạo chữ ký số
    a. Sử dụng công cụ Cryptool (menu Indiv. Procedures – RSA Cryptosystem – Signature Demontration)
    b. Mô tả các bước theo lưu đồ
8. Mô tả quá trình bảo mật Email
    a. Sử dụng công cụ Cryptool (menu Indiv. Procedures – Protocol – Secure Email with S/MIME)
    b. Mô tả các bước thực hiện
9. Thực hiện cuộc tấn công lên Access Point được cấu hình với mã hoá yếu (crack passowrd wifi)
    a. Nhận diện các mạng wifi trong khu vực (các công cụ như inSSIDer, NetSurvisor)
    b. Sử dụng các công cụ thuộc bộ aircrack-ng để crack password wifi
    c. Mô tả quá trình thực hiện và kết quả thu được