BÀI TẬP LỚN
Môn: MẬT MÃ VÀ AN NINH MẠNG
-o0o-

Đối với môn học này, mỗi sinh viên đều phải làm một bài tập lớn.
- Mỗi nhóm có nhiều nhất là 4 sinh viên và ít nhất là 2 sinh viên.
- Đề bài tập lớn được gán cho mỗi nhóm theo danh sách đính kèm.
- Hạn chót để đăng ký nhóm bài tập lớn là sau 1 tuần học.
- Mã nguồn và báo cáo cuối cùng phải được nộp theo deadline thông báo ở Bkel.

I. DANH SÁCH CÁC BÀI TẬP LỚN

1. Bài tập lớn số 1

Trong bài tập lớn này, bạn cần phải xây dựng một chương trình mã hóa/giải mã bằng một ngôn ngữ lập trình bất kỳ mà bạn chọn. Sau đó bạn sẽ tạo ra một số bản mã từ một bản rõ có ý nghĩa. Cuối cùng bạn sẽ cố gắng phân tích các bản mã trên. Cho đơn giản, chúng ta giả sử rằng đầu vào là chuỗi ký tự dạng UTF-8. Chương trình của bạn sẽ diễn tả các chức năng như sau:

- Từ một bản rõ tạo ra một bản mã dùng mã hóa thay thế đơn ký tự Cesar.
- Từ một bản rõ tạo ra một bản mã dùng mã hóa hoán vị Rail fence.
- Từ một bản rõ tạo ra một bản mã dùng mã hóa nhân dựa trên hai hàm nói trên. Giả sử mả hóa thay thế được dùng trước sau đó mã hóa hoán vị được dùng để mã hóa kết quả và lấy ra được bản mã cuối cùng.
- Tạo ba phương thức với ba hàm nói trên. Mỗi phương thức(với khóa cố định) bạn mã hóa bản rõ tiếng Anh với chiều dài tùy ý và ít nhất là 1000 ký tự.
- Sau đó bạn tạo ra các bản mã dùng một trong ba phương thức trên(với khóa khác nhau), bây giờ bạn bắt đầu phải thiết kế các phương pháp để tìm ra bản rõ tương ứng với bản mã đã có. Bắt đầu với (1), tiếp tục với (2).
  1. Cố gắng lấy các bản rõ từ các bản mã.
  2. Cố gắng lấy khóa đã sử dụng.

2. Bài tập lớn số 2

Trong bài tập lớn này, bạn cần phải hiện thực hệ mã RSA trên Java/C/C++. Bạn không được dùng các hiện thực RSA đã có từ web hay trong Java. Những gì bạn có thể dùng là:

- Java có lớp BigInteger được xây dựng sẵn.
- C++ có thư viện NTL(Library for doing Number Theory) or GMP (the GNU Multiple Precision Arithmetic Library).
- Bạn có thể dùng các hiện thực big-integer để quản lý dữ liệu của bạn và thực hiện phép toán **mod** nhưng không được dùng các phương thức đã hiện thực (gcd, power, tìm số nguyên tố, ..). Như vậy bạn phải tự hiện thực các phương thức này.

- Bạn có thể dùng hàm an toàn đang tồn tại để tạo ra các số ngẫu nhiên lớn. Ví dụ Java cung cấp các công cụ để tạo số ngẫu nhiên trong java.util.random hay java.security.SecureRandom. Tương tự C++ có rand() và srand() để tạo số ngẫu nhiên.

Trong hiện thực RSA của bạn, giả sử các số nguyên tố lớn ít nhất phải 500 bits(nhưng có thể lớn hơn) và bạn phải viết các hàm sau:

- Tìm số nguyên tố lớn khi cho số lượng bit của số nguyên tố lớn cần tìm.
- Tính ước số lớn nhất khi cho hai số nguyên lớn.
- Tính toán khóa giải mã d khi cho khoá mã hóa e và hai số nguyên tố lớn.
- Tạo bộ khóa ngẫu nhiên khi cho 2 số nguyên tố lớn.
- Mã hóa khi cho thông điệp và khóa mã hóa e và n.
- Giải mã khi cho thông điệp mã hóa và khóa giải mã d và n.

3. Bài tập lớn số 3

Trong bài tập lớn này, bạn cần phải triển khai một hệ thống quản lý định danh và truy cập(IAM - Identity and Access Management). Bạn có thể sử dụng các thư viện và mã nguồn mở từ web hay có trong các ngôn ngữ lập trình như: JCA/JCE, JAAS, OpenLDAP, Webmin, CAS, … hoặc tự xây dựng.

Hệ thống của bạn phải có các chức năng sau:

- Các chức năng quản lý người dùng: tạo, cập nhật, xóa, tìm kiếm thông tin định danh của người dùng với các dịch vụ thư mục như OpenLDAP.
- Các chức năng xác thực với các phương pháp: username và password, smart card và PIN(Personal Identification Number).
- Các chức năng nhật ký để quản lý các sự kiện xác thực, thay đổi các đối tượng thư mục.
- Các chức năng quản trị thông qua Web cho việc quản lý người dùng và nhật ký.

4. Bài tập lớn số 4

Trong bài tập lớn này, bạn cần phải triển khai một hệ thống bức tường lửa với nhiều chức năng bổ sung. Bạn có thể dùng các mã nguồn mở có trên web như pfSense Squid, SquidGuard, ClamAV, …

Hệ thống của bạn phải có các chức năng sau:

- **Firewall**: bộ lọc gói có trạng thái, không giới hạn số lượng giao tiếp mạng, nhiều giao tiếp mạng trên một zone và nhiều zone trên một giao tiếp, quản lý địa chỉ linh động(NAT, PAT).
- **Lọc Web:** chặn dựa trên URL/Keyword/Pharse, chặn Java Applet, Cookies, Active X.
- **Antivirus:** Hỗ trợ lọc trên các giao thức HTTP/HTTPS và cơ sở dữ liệu về virus được cập nhật tự động.
- **Quản trị:** Thông qua Web.

5. Bài tập lớn số 5

Trong bài tập lớn này, bạn cần tìm hiểu các giải pháp Single-Sign-On và xây dựng ứng dụng thử nghiệm trên nền Web.

Các nội dung cần thực hiện:

- Tìm hiểu khái niệm và nguyên lý hoạt động của các giải pháp Single-Sign-On
- Tìm hiểu, cài đặt và đánh giá điểm mạnh/điểm yếu của các giải pháp Single Sign On thông dụng: OpenID Connect, CAS, SAML, JOSSO

- Hiện thực tính năng đăng nhập cho Website sử dụng các giải pháp Single Sign On nói trên, bạn có thể chọn bất kỳ ngôn ngữ nào để hiện thực website, demo không được sử dụng các giải pháp xác thực có sẵn như của Google, Facebook,…
- Demo kết quả và giải thích cách thức hoạt động của chương trình.

6. Bài tập lớn số 6

Trong bài tập lớn này, bạn cần tìm hiểu cách thức hoạt động của tấn công DoS/DDoS trong mạng và các cách thức để phòng chống loại tấn công này

Các nội dung cần thực hiện:

- Tìm hiểu khái niệm về tấn công DoS/DDoS
- Tìm hiểu các kỹ thuật tấn công DoS trong mạng: Teardrop, Ping of Death, TCP SYN Flood, DNS Amplification Attack
- Tìm hiểu cách thức phòng chống cho các loại tấn công nói trên
- Demo, phân tích và đánh giá các kỹ thuật tấn công (có thể sử dụng các chương trình/mã nguồn có sẵn hoặc tự viết chương trình để demo)
- Hiện thực các kỹ thuật để phòng chống các loại tấn công nói trên và demo kết quả

II. NHỮNG GÌ MỘT NHÓM PHẢI NỘP

1. Mã nguồn và hướng dẫn sử dụng

Tổ chức cây thư mục bao gồm:

- Tập tin README.doc: hướng dẫn sử dụng chương trình/hệ thống mà bạn đã xây dựng.
- Thư mục srcs: chứa toàn bộ mã nguồn mà bạn đã hiện thực.
- Thư mục refs: chứa toàn bộ các tài liệu, mã nguồn mở mà bạn đã tham khảo và sử dụng.

2. Báo cáo kỹ thuật

Báo cáo kỹ thuật bao gồm các nội dung sau:

- **Chương 1 - Giới thiệu**: trình bày các yêu cầu của chương trình/hệ thống mà bạn cần xây dựng, nội dung chính của các chương tiếp theo.
- **Chương 2 - Phân tích và thiết kế hệ thống**: trình bày các bước phân tích và thiết kế hệ thống dựa trên các yêu cầu đặt ra.
- **Chương 3 - Hiện thực và đánh giá hệ thống**: trình bày phần hiện thực hệ thống, cách thức và kết quả đánh giá hệ thống đã xây dựng.
- **Chương 4 - Kết luận**: trình bày những gì hệ thống đã làm được và không làm được theo các yêu cầu đã đặt ra, ưu và nhược điểm của hệ thống, hướng phát triển của hệ thống.
- **Tài liệu tham khảo**
- **Phụ lục**: trình bày ngắn gọn thông tin về các môi trường phát triển ứng dụng, thư viện, mã nguồn mở mà bạn đã sử dụng.

Các phần chính trong báo cáo này là chương 2 và chương 3. Toàn bộ báo cáo này chỉ từ 20 đến 30 trang. Định dạng của báo cáo là MS WORD. Tên tập tin báo cáo là report.doc.

3. Đóng gói và nộp bài

Toàn bộ hai phần (1) và (2) sẽ được đóng gói và nén lại với ZIP thành một tập tin Assigment#.zip. Dấu # tương trưng cho số thứ tự của đề bài tập lớn. Ví dụ nhóm bạn đã đăng

ký đề bài tập lớn số 1 thì tập tin này là Assignmnent1.zip. Người đã đăng ký đề bài tập lớn sẽ thay mặt cho toàn bộ nhóm nộp bài.