Faculty of Computer Science and Engineering
Ho Chi Minh City University of Technology

Cryptography and Network Security
Assignment 1

Nguyen Huu Hieu

Ngày 17 tháng 2 năm 2019

1 Giới thiệu

Mã hoá là phương pháp giúp bảo vệ dữ liệu cá nhân nhạy cảm trên máy tính của bạn, cho dù bạn có gởi dữ liệu cho cá nhân, tổ chức nào đó qua mạng Internet, hay sao lưu dữ liệu cá nhân trên các máy chủ, Cloud,..., thì việc mã hoá sẽ ngăn chặn bất cứ ai có thể đọc được dữ liệu trước khi được sự cho phép của bạn.

Trong assignment này các bạn sẽ thực hiện một chương trình mã hóa để giữ cho các tập tin và thư mục trên máy tính của mình thật sự an toàn. Cụ thể là xây dựng chương trình mã hóa và giải mã các tập tin và thư mục sử dụng các giải thuật mã hóa được sử dụng phổ biến trong thực tế như DES, AES, RSA...

2 Mục tiêu

Mục tiêu của assignment:

- Hiện thực các giải thuật mã hóa/giải mã được học trên lớp.
- Tìm hiểu các giải thuật mã hóa khác, chứng minh tính an toàn của giải thuật được chọn và triển khai giải thuật đó để demo kết quả.
- Sinh viên có khả năng ứng dụng các thư viện lập trình mã hóa để xây dựng chương trình mã hóa và giải mã các tập tin và thư mục ứng dụng trong thực tế.

3 Yêu cầu

∗**Tính năng cơ bản**:

- Chương trình tích hợp ít nhất ba giải thuật mã hóa, trong đó bao gồm giải thuật mã hóa đối xứng, giải thuật mã hóa bất đối xứng và ít nhất một giải thuật mã hóa không được học trên lớp. Sinh viên cho biết lí do chọn giải thuật mã hóa, cơ sở lí thuyết tổng quan cũng như chứng minh độ an toàn cho giải thuật được chọn trong bài báo cáo.
- Chương trình có khả năng mã hóa một tập tin bất kì như hình ảnh, âm thanh, văn bản, pdf...Sinh viên trình bày rõ trong báo cáo một số loại tập tin mà chương trình hỗ trợ mã hóa/giải mã.

- Quá trình mã hóa: nhận input là tập tin bất kì và tập tin text chứa chìa khóa mã hóa (encryption key) và một số option khác (nếu cần), output là tập tin hay thư mực chứa dữ liệu đã được mã hóa.
- Quá trình giải mã: nhận input là tập tin hay thư mục chứa dữ liệu đã được mã hóa và tập tin text chứa chìa khóa giải mã (decryption key) và một số option khác (nếu cần), output chương trình là tập tin được giãi mã thành công. Sử dụng các hàm Hash như MD5, SHA để chứng minh. **tính toàn vẹn** giữa tập tin gốc ban đầu được chọn và tập tin output của quá trình giải mã.
- Trong bài báo cáo sinh viên cần trình bày quá trình phân tích và thiết kế chương trình, mô tả tổng quan cách hiện thực (giải thuật, thư viện lập trình, cấu trúc dữ liệu được sử dụng...), phân tích hiệu năng của chương trình (tính chính xác của quá trình mã hóa-giải mã, thời gian thực thi quá trình mã hóa-giải mã, độ lớn tối đa của file cần mã hoá/giải mã mà chương trình hỗ trợ,...), ưu khuyết điểm của chương trình, hướng phát triển thêm...

∗**Các tính năng nâng cao** (Khuyến khích Sinh viên tự đề xuất ý tưởng và thực hiện), bên dưới là một số ý tưởng tham khảo:

- Tích hợp lớp mã hoá vào các ứng dụng có sẵn, như ứng dụng chat, file sharing để bảo mật dữ liệu gởi, nhận.
- Hiện thực quá trình sinh khóa và phân phối khóa.
- Mã hóa giải mã toàn bộ tập tin trong một thư mục được chọn.
- Hiển thị thanh trạng thái trong quá trình mã hóa/giải mã.

∗**Ngôn ngữ lập trình**

- 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++, Perl, Scala, Go Programming, Python, NodeJS...
- Một số thư viện lập trình tham khảo: Pycrypto, Perl Crypto, Java Cryptography Architecture (JCA), Botan, Crypto++, Sage, OpenSSL...

4 Qui định nộp bài

Một số qui định về cách thức nộp bài:

- Deadline nộp bài: tuần 13 (tính theo tuần học của phòng đào tạo).
- Mỗi nhóm tối đa 04 sinh viên.
- Sinh viên không đăng ký làm bài tập lớn hoặc không tham gia làm chung với nhóm sẽ nhận điểm 0 phần bài tập lớn.
- Nộp mã nguồn chương trình, mã thực thi (nếu có), báo cáo, các tài liệu liên quan,... Sinh viên chuẩn bị để nộp ngay sau khi báo cáo tại lab.
- Báo cáo (hard copy) sinh viên in ra và nộp khi demo chương trình.
- Mỗi nhóm có tối đa 10 phút để demo chương trình trên lớp vào giờ học lab.

5 Báo cáo

Qui định nộp báo cáo:

- Bài báo cáo từ 15 đến 20 trang, định dạng PDF, khuyến khích sử dụng Latex khi trình bày.
- Thông thường bố cục bài báo cáo gồm các phần sau:

  1. Tóm tắt (abstract) — Tóm tắt ngắn gọn nội dung được trình bày trong báo cáo
  2. Giới thiệu (introduction) — Giới thiệu tổng quan về công việc đã làm, phạm vi, giới hạn của đề tài
  3. Thân bài (body) — Nội dung công việc đã làm
  4. Phân tích và kết luận (analysis and conclusions) — Tổng kết lại kết quả đạt được, đánh giá kết quả và mặt hạn chế
  5. Hướng phát triển (recommendations) — Nêu các công việc chưa được giải quyết và hướng phát triển trong tương lai
  6. Tham khảo (references) —Danh sách tài liệu tham khảo: sách, báo, các đường dẫn Internet...
- Trong bài báo cáo trình bày các nội dung đề ra trong mục Yêu cầu, sinh viên có thể bổ sung các nội dung khác nếu thấy cần thiết và hợp lí
- Phần Phụ lục 1: Ghi rõ nhiệm vụ, vai trò các thành viên trong nhóm, phần trăm tham gia hoàn thành bài tập lớn (Bảng đánh giá)
- Phần Phụ lục 2: Trình bày hướng dẫn sử dụng chương trình

LƯU Ý : *Trong báo cáo các nhóm chỉ viết cơ sở lí thuyết ngắn gọn, xúc tích. Thay vào đó nên tập trung vào cách phân tích, hiện thực và đánh giá kết quả đạt được. Điểm sẽ được đánh giá tập trung dựa vào những tiêu chí: nhận thức vấn đề, phân tích, hiện thực và cách đánh giá hệ thống đã xây dựng.*

6 Cách tính điểm

• Hoàn thành các tính năng cơ bản: **8 điểm** trong đó bao gồm 40% báo cáo + 60% demo

• Chương trình hỗ trợ các tính năng nâng cao, giao diện đẹp dễ sử dụng, trong suốt với người dùng, được cộng điểm tùy theo mức độ từ **0.5 đến 1 điểm** (Điểm tối đa cho assignment 1: 10 điểm)

• Báo cáo trễ mỗi tuần bị trừ 2 điểm.

HẾT