Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin

4

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

Thuật toán mã hoá Elliptic Curve và hàm băm

Thực hành môn Mật mã học

Tháng 3/2023

Lưu hành nội bộ

<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

Mọi góp ý về tài liệu, vui lòng gửi về email inseclab@uit.edu.vn

BEE SECURE
INSECLAB

A. TỔNG QUAN

1. Mục tiêu

- Hiểu được ECC và một số hàm băm.
- Lập trình sử dụng được thư viện cryptopp trên đa nền tảng (window và linux)
- Tìm hiểu được một vài cuộc tấn công trên các thuật toán này

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

1. Phần mềm visual studio code

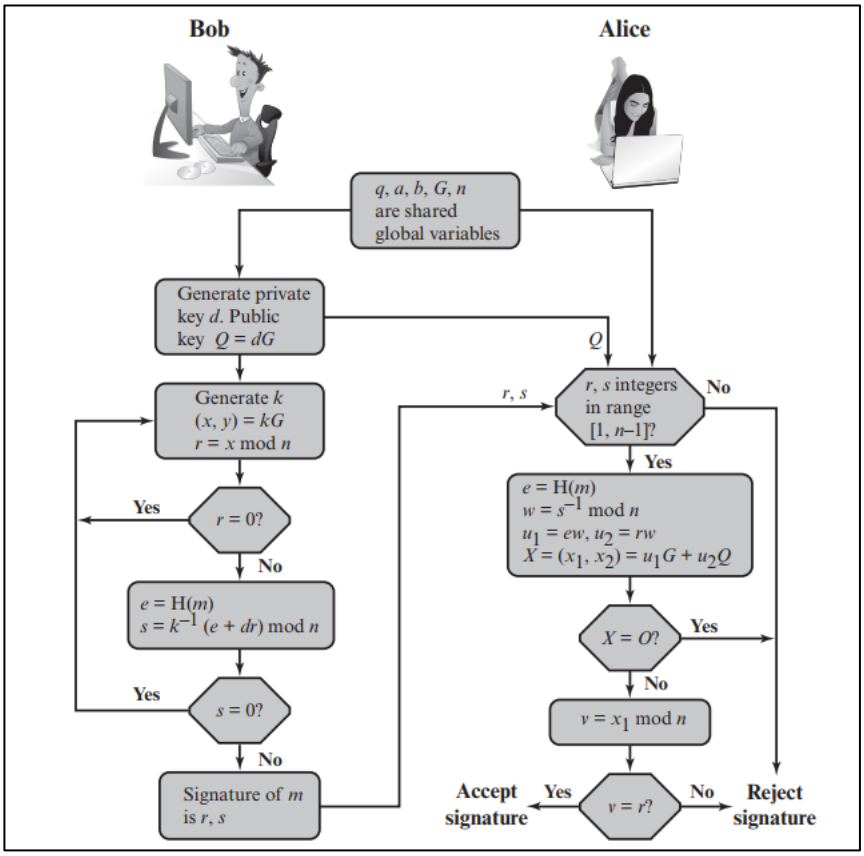
2. Hệ điều hành

- Sử dụng cả hệ điều hành linux và window để kiểm tra thuật toán.

C. THỰC HÀNH

1. Tìm hiểu ECDSA sử dụng thư viện cryptopp

ECDSA(The Elliptic Curve Digital Signature Algorithm)



a) Quá trình ký số

Thuật toán ký số ECDSA được thực hiện như luồng dữ liệu phía trên. Quá trình sẽ được diễn ra như sau:

- Người ký sẽ lựa chọn một số $\boldsymbol{d}$ làm khoá bí mật
- Từ khoá bí mật $\boldsymbol{d}$, người ký sẽ tạo ra khoá công khai $\boldsymbol{Q = dG}$
- Sử dụng hàm băm $\boldsymbol{H}$, người ký tạo ra giá trị tóm tắt $\boldsymbol{e}$ của văn bản $\boldsymbol{m}$
- Chữ ký số sẽ là cặp $(\boldsymbol{r}, \boldsymbol{s})$ được tính ở lược đồ phía trên

b) Quá trình xác thực văn bản

- Sau đó, người xác thực chữ ký nhận được văn bản $\boldsymbol{m}$ và chữ ký số $(\boldsymbol{r}, \boldsymbol{s})$ của người ký.
- Tính giá trị $\boldsymbol{e}$ của văn bản $\boldsymbol{m}$ thông qua hàm băm $\boldsymbol{H}$
- Sau đó tính các giá trị khác thông qua các tham số có được và tiến hành so sánh với cặp chữ ký số $(\boldsymbol{r}, \boldsymbol{s})$ được cung cấp để xác thực chữ ký có bị giả mạo hoặc sửa đổi hay bị lỗ do đường truyền hay không.

c) Thực hành viết chương trình mã hoá sử dụng ECDSA bằng thư viện cryptopp.

- **Bài tập 1:** Sử dụng code mẫu **sample_ecdsa.cpp** được cung cấp, chỉnh sửa và ký tập tin **UIT.png** đính kèm.
- **Bài tập 2:** Thay đổi thuật toán mã hoá sha1 thành sha256 và mô tả điểm khác biệt trong chương trình.
- **Bài tập 3:** Load chữ ký số $(\boldsymbol{r}, \boldsymbol{s})$ và văn bản $\boldsymbol{m}$ từ file và xác thực.

2. Hàm băm và hash Collision

- **Bài tập 4:** Viết chương trình C++ sử dụng switch case với các trường hợp hàm băm sau MD5, SHA224, SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256.
- Input đầu vào cần băm sẽ được nhập từ bàn phím, kết quả xuất ra đoạn mã hash.
- Tham khảo các thư viện:
- `#include <cryptopp/md5.h>`
- `#include <cryptopp/sha3.h>`
- `#include <cryptopp/sha.h>`
- `#include <cryptopp/shake.h>`
- **Bài tập 6:** Tìm hiểu phương pháp tấn công collision trong hàm băm và mô tả chi tiết lại quá trình tấn công sử dụng hàm băm md5.
- Tham khảo https://en.wikipedia.org/wiki/Collision_attack
- **Bài tập 7:** Tìm hiểu tấn công length extension trong hàm băm và mô tả lại chi tiết quá trình sử dụng hàm băm sha256.
- Tham khảo https://en.wikipedia.org/wiki/Length_extension_attack

3. Bài tập luyện tập

- **Bài tập luyện tập 1:** So sánh thuật toán RSA và ECC trong xác thực chữ ký, ưu và nhược điểm của 2 phương pháp. Luyện tập tìm hiểu và khai thác lỗi thiết kế ecdsa tại https://web.cryptohack.org/digestive/
- **Bài tập luyện tập 2:** So sánh HMAC và MAC. Làm bài luyện tập khai thác lỗi tại https://cryptohack.org/static/challenges/13407_1f10afb29e0cabd0f02d6c2305298173.py
- `nc socket.cryptohack.org 13407`

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.
- Nộp báo cáo kết quả gồm Code, CSDL được export và chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Báo cáo:
  - File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
  - Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1.
  - Ví dụ: [NT219.K11.ANTN.1]-Lab1_1852xxxx-.
  - Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
  - Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!