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

3

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

Thuật toán mã hoá RSA

Thực hành môn Mật mã học

Tháng 3/2023

Lưu hành nội bộ

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 thuật toán RSA.
- 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

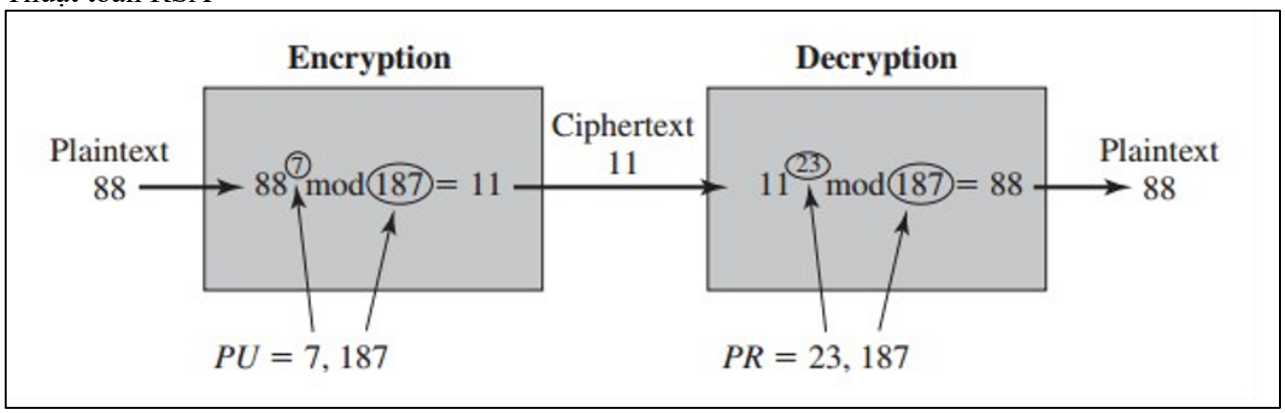
2. Hệ điều hành

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

C. THỰC HÀNH

1. Tìm hiểu mã hoá RSA sử dụng thư viện cryptopp

Thuật toán RSA



a) Tạo khoá

- Lựa chọn 2 số nguyên tố lớn p và q (p≠q) sau đó tính toán **n=pq**
- Tính $\boldsymbol{\phi(n) = (p-1)(q-1)}$
- Lựa chọn 1 số **e** sao cho **1<e<** $\boldsymbol{\phi(n)}$ *và* **gcd(e,** $\boldsymbol{\phi(n)}$**)=1**
- Tính d sao cho $\boldsymbol{e.d \equiv 1\ mod\ \phi(n)}$.
- Public key (PU) sẽ là **n** và **e**
- Private key (PK) sẽ là **p,q** và **d**

b) Mã hoá:

- Sẽ có 2 kiểu sử dụng khoá để mã hoá dữ liệu

- Mã hoá để bảo mật plain text: **C = E(M,PU) = M^e mod n** với **M** là dữ liệu cần mã hoá và **C** là dữ liệu được mã hoá. Quá trình này sử dụng **public key** để mã hoá
- Mã hoá để đảm bảo tính toàn vẹn: **C = E(M,PR) = M^d mod n .** Quá trình mã hoá sẽ sử dụng **private key** để mã hoá

c) Giải mã

- Quá trình giải mã sẽ ngược lại với quá trình mã hoá
- Giải mã sử dụng private key: **M = D(C, PR) = C^d mod n.** Dữ liệu truyền đi sẽ bí mật, do khoá private key được giữ bí mật với bên ngoài.
- Giải mã sử dụng public key: **M = D(C,PU) = C^emod n.** Dữ liệu truyền đi ai có key cũng có thể xem được, tuy nhiên không chỉnh sửa được, đảm bảo tính toàn vẹn của dữ liệu.

d) Thực hành viết chương trình mã hoá sử dụng thuật toán mã hoá RSA bằng thư viện cryptopp.

- **Bước 1**: Sử dụng code mẫu được cung cấp:
- Tạo khoá

```
// Generate keys
AutoSeededRandomPool rng;

InvertibleRSAFunction parameters;
parameters.GenerateRandomWithKeySize( rng, 1024 );

RSA::PrivateKey privateKey( parameters );
RSA::PublicKey publicKey( parameters );
```

Chậm lại và suy nghĩ 1: Hàm GenerateRandomWithKeySize đang làm gì, InvertibleRSAFunction có nhiệm vụ gì trong việc tạo khoá?

- **Bước 2**: Mã hoá:
- **Bài tập 1:** Sử dụng code mẫu sample_rsa.cpp được cung cấp, chỉnh sửa và mã hoá đoạn plaintext sau: "RSA Encryption Schemes". Kết quả xuất ra màn hình
- **Bài tập 2:** Sử dụng private key để mã hoá đoạn plaintext trên và giải mã bằng public key. Kết quả xuất ra màn hình.
- **Bước 3**: Giải mã:
- **Bài tập 3:** Tương tự với quá trình mã hoá, phần này yêu cầu **ciphertext** được nhập từ **file** để phục vụ quá trình giải mã. Key được set cố định trong chương trình.
- **Bài tập 4:** plaintext hỗ trợ đầu vào bao gồm các kí tự thuộc UTF-16
- **Bài tập 5:** Đầu vào plaintext được nhập thủ công vào chương trình.
- **Bài tập 6:** Key được load lên từ file. Giá trị key >= 3072 bits.

2. Tấn công thuật toán và lược đồ

- **Bài tập 7:** Tìm hiểu một kiểu tấn công trên thuật toán mã hoá RSA và biểu diễn code demo chương trình. Khuyến khích mỗi nhóm tìm hiểu 1 kiểu tấn công và sử dụng các kịch bản khác nhau. Tham khảo thêm tại: https://crypto.stanford.edu/~dabo/pubs/papers/RSA-survey.pdf

3. Bài tập luyện tập

- **Bài tập luyện tập 1:** Đánh giá hiệu năng của thuật toán RSA
  1. Trường hợp 1: Dữ liệu dạng utf-16
  2. Trường hợp 2: Dữ liệu lớn hơn 100 MB
  3. Báo cáo với 2 thông số Cycles Per Byte và MiB/Second. Có thể tham khảo công cụ đánh giá tại https://www.cryptopp.com/wiki/Benchmarks
- **Bài tập luyện tập 2:** Viết chương trình RSA mã hoá chữ ký (có thể nhập từ file). Sử dụng **private key** để mã hoá. Yêu cầu là file chữ ký sẽ được truyền đi cùng trong qúa trình truyền dữ liệu. (Quá trình truyền có thể giả sử nhưng cần mô tả cách thức làm).

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!