HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

VIỆN KHOA HỌC KỸ THUẬT BƯU ĐIỆN

ĐỀ CƯƠNG CHI TIẾT

AN TOÀN VÀ BẢO MẬT HỆ THỐNG THÔNG TIN

THỰC HÀNH TẠO VÀ XÁC THỰC CHỮ KÝ SỐ

Lớp học phần	**:** INT1303-20242-13
Giảng viên hướng dẫn	**:** PGS.TS Trần Đức Sự
Nhóm thực hiện	**:**
Nguyễn Khả Phong	B23DCCC129
Phạm Tiến Công	B23DCCC025
Đinh Hoàng Long	B23DCCC102

Hà Nội – 04/2025

MỤC LỤC

TÊN CHỦ ĐỀ

Thực hành triển khai hệ thống tạo và xác thực chữ ký số sử dụng thuật toán RSA và DSA

NỘI DUNG CHÍNH

1. Mục tiêu của bài thực hành

- Hiểu được cơ chế hoạt động và vai trò của chữ ký số trong bảo mật thông tin
- Nắm vững nguyên lý của các thuật toán RSA và DSA trong ứng dụng chữ ký số
- Thực hành triển khai hệ thống tạo và xác thực chữ ký số
- So sánh hiệu suất và độ an toàn giữa các thuật toán chữ ký số

2. Chức năng và tính năng kỹ thuật

2.1 Sinh khóa

- Chức năng: Tạo cặp khóa (khóa công khai, khóa riêng tư) cho người dùng
- Tính năng kỹ thuật:
    - Sinh số nguyên tố an toàn
    - Tạo khóa với các độ dài khác nhau (1024, 2048, 3072, 4096 bit)
    - Lưu trữ khóa dưới định dạng an toàn
    - Bảo vệ khóa riêng tư bằng mật khẩu

2.2 Tạo chữ ký số

- Chức năng: Tạo chữ ký số cho dữ liệu đầu vào (văn bản, tập tin)
- Tính năng kỹ thuật:
    - Hỗ trợ băm dữ liệu với SHA-256/SHA-3
    - Ký dữ liệu sử dụng khóa riêng
    - Đóng gói chữ ký vào định dạng tiêu chuẩn
    - Hỗ trợ ký các loại tập tin khác nhau

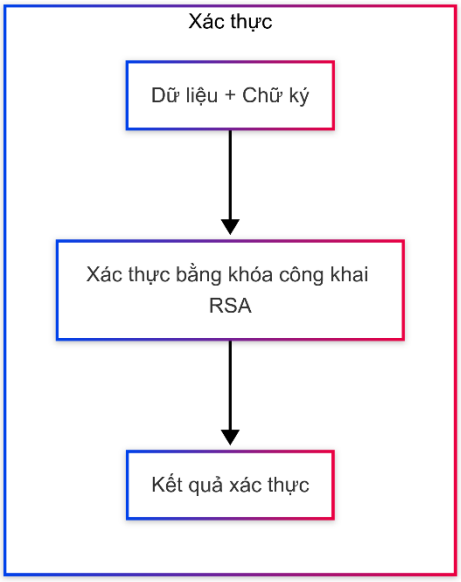
2.3 Xác thực chữ ký số

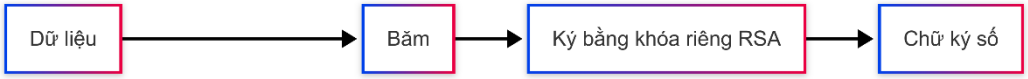
- Chức năng: Kiểm tra tính hợp lệ của chữ ký số
- Tính năng kỹ thuật:
  - Xác thực sử dụng khóa công khai
  - Kiểm tra tính toàn vẹn của dữ liệu
  - Xác minh nguồn gốc của chữ ký
  - Báo cáo kết quả xác thực chi tiết

3. Mô hình và quy trình thực hiện thuật toán

3.1 Thuật toán RSA

Sơ đồ tổng quát:





Các bước thực hiện:

a. Sinh khóa RSA:

- Bước 1: Chọn hai số nguyên tố lớn p và q
- Bước 2: Tính n = p * q
- Bước 3: Tính giá trị hàm Euler φ(n) = (p-1) * (q-1)
- Bước 4: Chọn e sao cho 1 < e < φ(n) và gcd(e, φ(n)) = 1
- Bước 5: Tính d = e^(-1) mod φ(n)
- Bước 6: Khóa công khai: (n, e), Khóa riêng: (n, d)

b. Tạo chữ ký RSA:

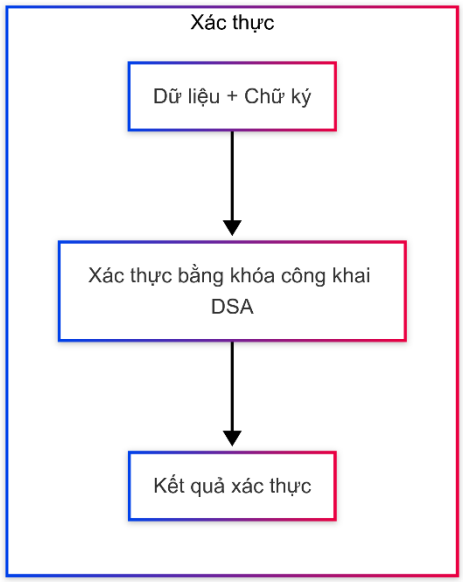
- Bước 1: Tính giá trị băm h = Hash(M) của thông điệp M
- Bước 2: Chuyển đổi h thành số nguyên m
- Bước 3: Tính chữ ký s = m^d mod n
- Bước 4: Kết quả là cặp (M, s)

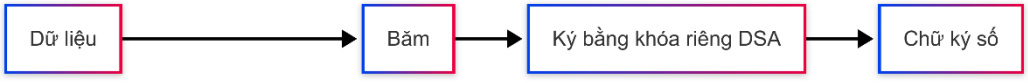
c. Xác thực chữ ký RSA:

- Bước 1: Tính m' = s^e mod n
- Bước 2: Tính giá trị băm h' = Hash(M) của thông điệp M nhận được
- Bước 3: Chuyển đổi h' thành số nguyên m"
- Bước 4: Nếu m' = m" thì chữ ký hợp lệ, ngược lại là không hợp lệ

3.2 Thuật toán DSA

Sơ đồ tổng quát:





Các bước thực hiện:

a. Sinh khóa DSA:

- Bước 1: Chọn một số nguyên tố p (độ dài 2048 bit)
- Bước 2: Chọn một số nguyên tố q (độ dài 256 bit) là ước của p-1
- Bước 3: Tính g = h^((p-1)/q) mod p, với h < p-1 sao cho g > 1

- Bước 4: Chọn khóa riêng x ngẫu nhiên, 0 < x < q
- Bước 5: Tính khóa công khai y = g^x mod p
- Bước 6: Khóa công khai: (p, q, g, y), Khóa riêng: x

b. Tạo chữ ký DSA:

- Bước 1: Tính giá trị băm h = Hash(M) của thông điệp M
- Bước 2: Chọn một số k ngẫu nhiên, 0 < k < q
- Bước 3: Tính r = (g^k mod p) mod q
- Bước 4: Tính s = (k^(-1) * (h + x*r)) mod q
- Bước 5: Kết quả chữ ký là cặp (r, s)

c. Xác thực chữ ký DSA:

- Bước 1: Kiểm tra 0 < r < q và 0 < s < q, nếu không thỏa thì chữ ký không hợp lệ
- Bước 2: Tính w = s^(-1) mod q
- Bước 3: Tính giá trị băm h = Hash(M) của thông điệp M
- Bước 4: Tính u1 = h * w mod q
- Bước 5: Tính u2 = r * w mod q
- Bước 6: Tính v = ((g^u1 * y^u2) mod p) mod q
- Bước 7: Nếu v = r thì chữ ký hợp lệ, ngược lại là không hợp lệ

4. Triển khai mã nguồn

4.1 Cấu trúc chương trình

- Ngôn ngữ lập trình: Python
- Thư viện mật mã: Các thư viện mã nguồn mở như Cryptography, PyCryptodome

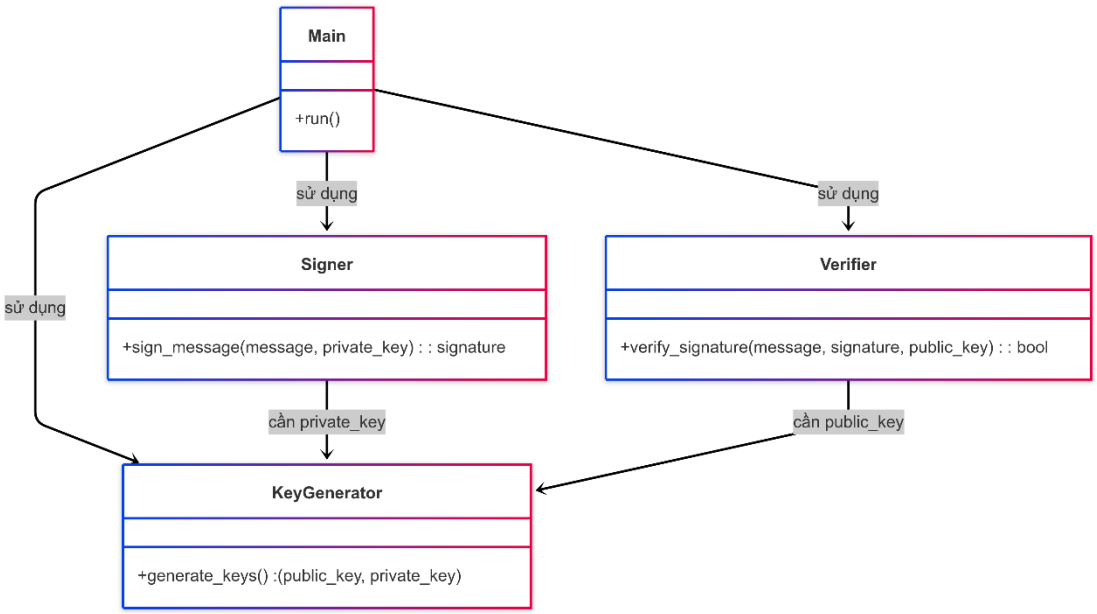
4.2 Các module chính

- Module sinh khóa: Triển khai các thuật toán sinh khóa RSA và DSA
- Module tạo chữ ký: Triển khai các thuật toán tạo chữ ký số
- Module xác thực: Triển khai các thuật toán xác thực chữ ký
- Giao diện người dùng: Command-line hoặc GUI

4.3 Mã nguồn triển khai

- Mô tả các lớp và hàm quan trọng
- Mã giả hoặc đoạn code mẫu cho các thuật toán chính

- Sơ đồ UML mô tả cấu trúc phần mềm



Giải thích sơ đồ

- KeyGenerator: tạo cặp khóa công khai & bí mật.
- Signer: ký thông điệp bằng khóa bí mật.
- Verifier: kiểm tra chữ ký với thông điệp và khóa công khai.
- Main: điểm khởi động chính, điều phối toàn bộ các module.

- Mã nguồn xử lý các trường hợp đặc biệt/ngoại lệ

4.4 Công cụ

- Môi trường phát triển: Visual Studio Code, PyCharm
- Công cụ kiểm thử: Pytest, Unitest

4.5 Hướng dẫn cài đặt và sử dụng

- Yêu cầu hệ thống và môi trường
- Các bước cài đặt
- Hướng dẫn sử dụng cơ bản
- Ví dụ minh họa các tính năng chính

5. Kịch bản thử nghiệm

5.1 Thử nghiệm chức năng sinh khóa

- Mục tiêu: Kiểm tra khả năng sinh cặp khóa đúng định dạng và an toàn

- Kịch bản:
  - Sinh khóa RSA với các độ dài khác nhau (1024, 2048, 4096 bit)
  - Sinh khóa DSA với các tham số khác nhau
  - Kiểm tra tính đúng đắn của cặp khóa
  - Đo thời gian sinh khóa và lưu trữ kết quả

5.2 Thử nghiệm tạo chữ ký số

- Mục tiêu: Kiểm tra khả năng tạo chữ ký đúng cho các dữ liệu khác nhau
- Kịch bản:
  - Tạo chữ ký cho văn bản ngắn
  - Tạo chữ ký cho tập tin có kích thước khác nhau
  - Đo thời gian tạo chữ ký trên cùng dữ liệu giữa thuật toán RSA và DSA

5.3 Thử nghiệm xác thực chữ ký số

- Mục tiêu: Kiểm tra khả năng xác thực chính xác
- Kịch bản:
  - Xác thực chữ ký hợp lệ
  - Xác thực chữ ký với dữ liệu đã bị sửa đổi
  - Xác thực chữ ký với khóa công khai không khớp
  - Đo thời gian xác thực giữa thuật toán RSA và DSA

5.4 Thử nghiệm hiệu suất

- Mục tiêu: So sánh hiệu suất giữa các thuật toán
- Kịch bản:
  - So sánh thời gian sinh khóa RSA và DSA
  - So sánh thời gian tạo chữ ký với từng thuật toán
  - So sánh thời gian xác thực chữ ký
  - Phân tích sự thay đổi hiệu suất theo kích thước dữ liệu

6. Đánh giá và nhận xét

6.1 So sánh thuật toán RSA và DSA

- So sánh về độ an toàn lý thuyết
- So sánh về tốc độ xử lý

- So sánh về kích thước khóa và chữ ký
- Phân tích ưu nhược điểm của mỗi thuật toán

6.2 Đánh giá hiệu quả hệ thống

- Đánh giá độ chính xác trong xác thực
- Đánh giá khả năng phát hiện sửa đổi dữ liệu
- Đánh giá tính ổn định của hệ thống
- Phân tích giới hạn và hạn chế

6.3 Kết luận và đề xuất

- Tóm tắt kết quả nghiên cứu
- Đề xuất cải tiến và phát triển
- Hướng ứng dụng thực tiễn

TÀI LIỆU THAM KHẢO

[1] William Stallings – Cryptography and Network Security, Pearson..

[2] https://en.wikipedia.org/wiki/Digital_signature.

[3] https://docs.python.org/3/library/cryptography.html.