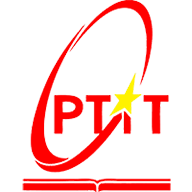
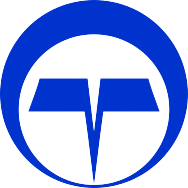
 **HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**VIỆN KHOA HỌC KỸ THUẬT BƯU ĐIỆN**



**BÁO CÁO THỰC HÀNH**

**MÔN: AN TOÀN VÀ BẢO MẬT**

**HỆ THỐNG THÔNG TIN**

**ĐỀ TÀI: TẠO VÀ XÁC THỰC CHỮ KÝ SỐ**

|  |  |
| --- | --- |
| **Lớp học phần** | **:** RIPT1302-DHCQ20232-01 |
| **Giảng viên hướng dẫn** | **:** Nguyễn Mạnh Dũng |
| **Nhóm thực hiện** | **:** |
| Nguyễn Khả Phong | B23DCCC129 |
| Phạm Tiến Công | B23DCCC025 |
| Đinh Hoàng Long | B23DCCC102 |

***Hà Nội – 04/2025***

MỤC LỤC

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

LỜI CẢM ƠN

# GIỚI THIỆU

## Mục tiêu của báo cáo thực hành

Báo cáo thực hành này nhằm mục đích:

* Hiểu rõ và triển khai các thuật toán chữ ký số phổ biến (RSA và DSA) trong môi trường thực tế
* Xây dựng các module phần mềm cho phép tạo khóa, tạo chữ ký số và xác thực chữ ký số
* So sánh hiệu năng và tính ứng dụng của các thuật toán chữ ký số khác nhau trong thực tế
* Cung cấp một nền tảng thực hành để hiểu sâu hơn về nguyên lý hoạt động của các hệ thống chữ ký số

Kết quả mong đợi từ báo cáo thực hành là một ứng dụng hoàn chỉnh với khả năng tạo và xác thực chữ ký số, minh họa cụ thể cho các nguyên lý đã được học trong phần lý thuyết.

## Tóm tắt về chữ ký số và vai trò trong bảo mật thông tin

Chữ ký số là một cơ chế bảo mật thông tin dựa trên hệ thống mã hóa khóa công khai (PKI), đóng vai trò quan trọng trong các hệ thống thông tin hiện đại bằng cách cung cấp:

* **Xác thực nguồn gốc:** Xác nhận chính xác danh tính của người gửi thông điệp, đảm bảo rằng thông điệp thực sự đến từ nguồn được tuyên bố.
* **Tính toàn vẹn dữ liệu:** Đảm bảo thông điệp không bị thay đổi trong quá trình truyền từ người gửi đến người nhận.
* **Tính không thể chối bỏ:** Người gửi không thể phủ nhận việc đã gửi thông điệp, tạo cơ sở pháp lý cho các giao dịch điện tử.
* **Tính duy nhất:** Mỗi chữ ký số chỉ có thể được sử dụng một lần, gắn liền với thông điệp cụ thể.

Chữ ký số tạo nền tảng cho nhiều ứng dụng thiết yếu trong thời đại số như:

* Giao dịch tài chính và ngân hàng trực tuyến
* Ký kết hợp đồng điện tử
* Xác thực phần mềm và cập nhật
* Chứng thực tài liệu số
* Trao đổi thông tin bảo mật giữa các tổ chức

## Phạm vi thực hành của báo cáo

Báo cáo thực hành sẽ tập trung vào các nội dung sau:

* **Triển khai thuật toán:** Xây dựng module tạo và xác thực chữ ký số sử dụng thuật toán RSA và DSA
* **Xây dựng ứng dụng:** Phát triển ứng dụng với giao diện người dùng cho phép:
  + Tạo và lưu cặp khóa (công khai/riêng tư)
  + Ký số cho các loại dữ liệu khác nhau (văn bản, tập tin)
  + Xác thực chữ ký số
* **Thử nghiệm và đánh giá:**
  + So sánh hiệu năng giữa các thuật toán
  + Kiểm tra độ bền vững trước các tình huống tấn công cơ bản
  + Đánh giá khả năng ứng dụng thực tế

Phạm vi không bao gồm:

* Triển khai đầy đủ hệ thống PKI
* Cài đặt chi tiết hệ thống quản lý chứng chỉ số
* Xây dựng hệ thống phân phối khóa
* Tối ưu hóa thuật toán ở mức cao

# CƠ SỞ LÝ THUYẾT

## Khái niệm cơ bản về chữ ký số

**Chữ ký số** là một chuỗi dữ liệu được tạo ra bằng kỹ thuật mật mã, gắn liền với một thông điệp cụ thể và có thể xác minh được bởi người nhận. Chữ ký số đóng vai trò tương tự như chữ ký tay trong môi trường điện tử, nhưng cung cấp mức độ bảo mật và xác thực cao hơn.

**Các khái niệm quan trọng:**

* **Hệ thống chữ ký số:** Tập hợp các thuật toán và quy trình cho phép tạo và xác thực chữ ký số, bao gồm:
  + Thuật toán sinh khóa
  + Thuật toán tạo chữ ký
  + Thuật toán xác thực chữ ký
* **Hàm băm mật mã (Cryptographic Hash Function):** Hàm toán học một chiều biến đổi dữ liệu đầu vào có độ dài bất kỳ thành một chuỗi có độ dài cố định, đóng vai trò quan trọng trong quá trình tạo chữ ký số.
* **Cặp khóa công khai/riêng tư:** Hai khóa liên kết toán học với nhau, trong đó:
  + Khóa riêng tư được giữ bí mật và dùng để tạo chữ ký
  + Khóa công khai được phân phối rộng rãi và dùng để xác thực chữ ký

**Tính chất cơ bản của chữ ký số:**

* **Tính xác thực (Authentication):** Người nhận có thể xác minh chính xác nguồn gốc của thông điệp.
* **Tính toàn vẹn (Integrity):** Bất kỳ sự thay đổi nào đối với thông điệp sẽ làm cho quá trình xác thực thất bại.
* **Tính không thể chối bỏ (Non-repudiation):** Người gửi không thể phủ nhận việc đã tạo và gửi thông điệp.
* **Tính duy nhất (Uniqueness):** Mỗi chữ ký số chỉ áp dụng cho một thông điệp cụ thể, không thể sử dụng lại cho thông điệp khác.

## Quy trình tạo và kiểm tra chữ ký số

### Quy trình tạo chữ ký số:

* Tạo chuỗi đại diện: Sử dụng hàm băm để tạo ra một chuỗi đại diện (message digest/hash value) có độ dài cố định từ thông điệp gốc.
* Ký chuỗi đại diện: Sử dụng khóa riêng tư để mã hóa chuỗi đại diện, tạo thành chữ ký số.
* Đóng gói: Kết hợp thông điệp gốc với chữ ký số và thông tin liên quan (như thông tin về thuật toán sử dụng).
* Gửi đi: Chuyển thông điệp đã được ký cho người nhận.

### Quy trình kiểm tra chữ ký số:

* Tách thông tin: Tách thông điệp gốc và chữ ký số từ thông điệp đã ký nhận được.
* Tính toán chuỗi đại diện: Sử dụng cùng một hàm băm để tính toán chuỗi đại diện từ thông điệp gốc (MD1).
* Giải mã chữ ký: Sử dụng khóa công khai của người gửi để giải mã chữ ký số, thu được chuỗi đại diện ban đầu (MD2).
* So sánh: So sánh hai chuỗi đại diện MD1 và MD2:
  + Nếu MD1 = MD2: Chữ ký hợp lệ, xác nhận tính xác thực và toàn vẹn của thông điệp.
  + Nếu MD1 ≠ MD2: Chữ ký không hợp lệ, thông điệp có thể đã bị thay đổi hoặc không đến từ nguồn được tuyên bố.

## Giới thiệu các thuật toán sẽ sử dụng trong thực hành

### Thuật toán RSA (Rivest-Shamir-Adleman)

RSA là một trong những thuật toán mã hóa khóa công khai được sử dụng rộng rãi nhất, có thể được áp dụng cho cả mã hóa và chữ ký số.

**Đặc điểm chính:**

* Dựa trên bài toán khó về phân tích số nguyên lớn thành các thừa số nguyên tố
* Có thể sử dụng linh hoạt cho cả mã hóa và chữ ký số
* Quá trình kiểm tra chữ ký tương đối nhanh
* Được sử dụng rộng rãi trong các ứng dụng thực tế

**Quy trình sinh khóa RSA:**

* Chọn hai số nguyên tố lớn p và q
* Tính n = p × q
* Tính φ(n) = (p-1) × (q-1)
* Chọn số mũ công khai e sao cho 1 < e < φ(n) và gcd(e, φ(n)) = 1
* Tính số mũ bí mật d sao cho (d × e) mod φ(n) = 1
* Khóa công khai: (n, e)
* Khóa riêng tư: (n, d)

**Quy trình tạo và xác thực chữ ký RSA:**

* Tạo chữ ký: signature = (hash(message)^d) mod n
* Xác thực chữ ký: hash(message) == (signature^e) mod n

### Thuật toán DSA (Digital Signature Algorithm)

DSA là thuật toán chữ ký số được Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) phát triển, chỉ dùng cho chữ ký số không như RSA.

**Đặc điểm chính:**

* Dựa trên bài toán logarit rời rạc
* Chỉ được sử dụng để tạo và xác thực chữ ký số, không dùng cho mã hóa
* Quá trình tạo chữ ký nhanh hơn RSA
* Sinh khóa nhanh hơn RSA

**Quy trình sinh khóa DSA:**

* Chọn số nguyên tố p và q (q là ước số của p-1)
* Chọn g với bậc q trong Z\*p
* Chọn số riêng tư x (0 < x < q)
* Tính y = g^x mod p
* Khóa công khai: (p, q, g, y)
* Khóa riêng tư: x

**Quy trình tạo và xác thực chữ ký DSA:**

* Tạo chữ ký:
  + Chọn số ngẫu nhiên k (0 < k < q)
  + Tính r = (g^k mod p) mod q
  + Tính s = k^-1(hash(message) + x\*r) mod q
  + Chữ ký là cặp (r, s)
* Xác thực chữ ký:
* Tính w = s^-1 mod q
* Tính u1 = hash(message) \* w mod q
* Tính u2 = r \* w mod q
* Tính v = ((g^u1 \* y^u2) mod p) mod q
* Chữ ký hợp lệ nếu v = r

### So sánh RSA và DSA:

|  |  |  |
| --- | --- | --- |
| **Tiêu chí** | **RSA** | **DSA** |
| Cơ sở toán học | Phân tích số nguyên thành thừa số | Logarit rời rạc |
| Tốc độ sinh khóa | Chậm hơn | Nhanh hơn |
| Tốc độ tạo chữ ký | Chậm hơn | Nhanh hơn |
| Tốc độ xác thực chữ ký | Nhanh hơn | Chậm hơn |
| Ứng dụng | Mã hóa và chữ ký số | Chỉ chữ ký số |
| Độ dài khóa đề xuất | Tối thiểu 2048 bit | 2048 bit cho p và 224 bit cho q |
| Phổ biến | Cao | Trung bình |

# THIẾT KẾ ỨNG DỤNG THỰC HÀNH

## Yêu cầu chức năng

**Tạo cặp khóa (khóa công khai/khóa riêng)**

* Sinh cặp khóa RSA với độ dài tùy chọn (1024, 2048, 3072, 4096 bits)
* Sinh cặp khóa DSA với độ dài tùy chọn
* Lưu khóa vào tập tin với định dạng PEM
* Tải khóa từ tập tin có sẵn
* Hỗ trợ bảo vệ khóa riêng bằng mật khẩu

**Ký một thông điệp/tập tin**

* Ký văn bản trực tiếp nhập từ giao diện
* Ký tập tin từ hệ thống
* Hỗ trợ nhiều thuật toán băm (SHA-256, SHA-384, SHA-512)
* Lưu chữ ký vào tập tin

**Xác thực chữ ký số**

* Xác thực chữ ký trên văn bản nhập trực tiếp
* Xác thực chữ ký trên tập tin
* Hiển thị kết quả xác thực rõ ràng
* Hỗ trợ tải chữ ký từ tập tin

**Giao diện người dùng**

* Giao diện đồ họa thân thiện với người dùng sử dụng Tkinter Python
* Bố cục tab cho từng chức năng: quản lý khóa, ký văn bản/tập tin, xác thực chữ ký
* Hỗ trợ tiếng Việt
* Hiển thị thông báo lỗi và trạng thái rõ ràng

## Môi trường phát triển

**Ngôn ngữ lập trình sử dụng**

* Python 3.8+: Ngôn ngữ chính để phát triển ứng dụng
* Ưu điểm: đa nền tảng, dễ học, có nhiều thư viện mã hóa mạnh mẽ

**Thư viện mã hóa/bảo mật sử dụng**

* cryptography: Thư viện mã hóa hiện đại cho Python với API cao cấp
  + Hỗ trợ RSA, DSA, và các thuật toán băm hiện đại
  + Cung cấp chức năng quản lý khóa, ký và xác thực
* pycryptodome (dự phòng): Phiên bản cải tiến của PyCrypto, cung cấp các thuật toán mã hóa

**Các công cụ hỗ trợ**

* Tkinter: Thư viện giao diện đồ họa tiêu chuẩn của Python
* pipenv/venv: Quản lý môi trường ảo và phụ thuộc
* pytest: Framework kiểm thử cho Python
* Git: Hệ thống quản lý phiên bản

## Kiến trúc phần mềm

**Sơ đồ các module chính**

digital\_signature\_app/

├── main.py # Điểm khởi đầu ứng dụng, khởi tạo giao diện

├── modules/

│ ├── \_\_init\_\_.py

│ ├── key\_generator.py # Module quản lý và sinh khóa

│ ├── signature.py # Module tạo và xác thực chữ ký

│ └── utils.py # Các tiện ích hỗ trợ

├── gui/

│ ├── \_\_init\_\_.py

│ ├── app.py # Lớp ứng dụng chính

│ ├── key\_tab.py # Tab quản lý khóa

│ ├── sign\_tab.py # Tab ký số

│ └── verify\_tab.py # Tab xác thực chữ ký

└── requirements.txt # Các phụ thuộc của dự án

**Luồng dữ liệu**

**Mô tả giao diện**

Ứng dụng sử dụng giao diện đồ họa dựa trên Tkinter với bố cục tab:

**Tab Quản lý khóa**

* Phần sinh khóa mới:
  + Lựa chọn thuật toán (RSA/DSA)
  + Lựa chọn độ dài khóa (dropdown)
  + Nút "Sinh cặp khóa"
* Phần lưu khóa:
* Trường nhập đường dẫn lưu khóa riêng
* Trường nhập đường dẫn lưu khóa công khai
* Nút "Lưu khóa riêng" và "Lưu khóa công khai"
* Phần tải khóa:
* Nút "Tải khóa riêng" và "Tải khóa công khai"
* Trạng thái khóa đã tải

**Tab Ký số**

* Lựa chọn kiểu đầu vào (File/Văn bản)
* Đầu vào văn bản: Hộp văn bản đa dòng
* Đầu vào file: Trường đường dẫn và nút "Chọn file"
* Lựa chọn thuật toán băm (SHA-256, SHA-384, SHA-512)
* Nút "Ký"
* Phần chữ ký: Nút "Lưu chữ ký"

**Tab Xác thực chữ ký**

* Lựa chọn kiểu đầu vào (File/Văn bản)
* Đầu vào văn bản: Hộp văn bản đa dòng
* Đầu vào file: Trường đường dẫn và nút "Chọn file"
* Trường đường dẫn file chữ ký và nút "Chọn file"
* Lựa chọn thuật toán băm (phải trùng với thuật toán khi ký)
* Nút "Xác thực"
* Phần kết quả: Hiển thị kết quả xác thực