**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

A blue logo with a black background

Description automatically generated

**BÁO CÁO THỰC HÀNH**

**LAB 5: DIGITAL SIGNATURE WITH CRYPTOPP/OPENSSL**

**MÔN HỌC: MẬT MÃ HỌC**

**Họ và tên: LẠI QUAN THIÊN**

**Mã số sinh viên: 22521385**

**Lớp: NT219.O21.ANTT**

**TP. HỒ CHÍ MINH, THÁNG 07 NĂM 2024**

**MỤC LỤC**

[PHẦN I: TỔNG QUAN VÀ MÔ TẢ 2](#_Toc171035851)

[1.1. Thông tin cá nhân: 2](#_Toc171035852)

[1.2. Thông tin thiết bị: 2](#_Toc171035853)

[PHẦN II: NỘI DUNG THỰC HÀNH 2](#_Toc171035854)

[2.1. Hash Functions: 2](#_Toc171035855)

[2.1.1. Hash Functions GUI 2](#_Toc171035856)

[2.1.2. Hash Functions CLI 3](#_Toc171035857)

# PHẦN I: TỔNG QUAN VÀ MÔ TẢ

## 1.1. Thông tin cá nhân:

Họ và tên: Lại Quan Thiên

Mã số sinh viên: 22521385

Lớp thực hành: NT219.O21.ANTT.1

Link Github: [Cryptography-Course/Labs/OffClass/Lab\_1 at main · WanThinnn/Cryptography-Course (github.com)](https://github.com/WanThinnn/Cryptography-Course/tree/main/Labs/OffClass/Lab_1)

## 1.2. Thông tin thiết bị:

**- Thiết bị:** Macbook Air 2019 – RAM 8GB (LPDDR3 2133MHz) – SSD 128GB

**- Hệ điều hành:**

+ Windows 11 Pro 21H2 (cài đặt thông qua Bootcamp của Apple)

+ Ubuntu 22.04 Jammy Jellyfish (cài đặt thông qua [t2linux.org](https://t2linux.org/))

**- Bộ xử lý:**

+ Intel Core i5 8210Y – 1.60GHz – Turbo Boost 3.60Ghz

+ Intel UHD Graphics 617

+ Apple T2 Security Chip

**- Thông tin về bộ xử lý:**

+ [Intel Core i58210Y Processor 4M Cache up to 3.60 GHz Thông số kỹ thuật sản phẩm](https://ark.intel.com/content/www/vn/vi/ark/products/189912/intel-core-i5-8210y-processor-4m-cache-up-to-3-60-ghz.html)

+ [Hỗ trợ Intel® UHD Graphics 617](https://www.intel.vn/content/www/vn/vi/support/products/189913/graphics/processor-graphics/intel-uhd-graphics-family/intel-uhd-graphics-617.html)

+ [Apple T2 Security Chip: Security Overview](https://www.apple.com/jp/mac/docs/Apple_T2_Security_Chip_Overview.pdf)

- Các thực nghiệm được thực thi trong quá trình laptop cắm điện, nhiệt độ phòng

A screenshot of a computer

Description automatically generated

Ảnh 1: Thông tin thiết bị

**1.3. Tổng quan:**

Bài báo cáo gồm các Task 1, 2của Lab 5. Các chương trình được code bằng ngôn ngữ C++ và sử dụng thư viện CryptoPP, OpenSSL.

- Task 1: ECDSA

+ Đối với CLI: sau khi xây dựng code xong thì tiến hành tạo 5 file test với kích thước khác nhau từ 2.5 MB đến 30 MB, thực hiện đo thời gian 1000 Ký/Xác thực trên cả hai Hệ điều hành Windows và Linux. Sau đó vẽ bảng thống kê số liệu và vẽ biểu đồ phân tích và so sánh.

+ Đối với GUI: xuất file dll để build GUI trên Winform.

- Task 2: RSASS-PSS (Tương tự Task 1)

# PHẦN II: NỘI DUNG THỰC HÀNH

## 2.1. ECDSA:

### 2.1.1. ECDSA GUI

Sau khi code xong phần CLI, em xuất file sang dll để có thể build được giao diện. Sử dụng Visual Studio 2022 để build giao diện Winform. Dưới đây là một số ảnh minh hoạ:

A screenshot of a computer

Description automatically generated

Ảnh 2: Tạo key với định dạng PEM

A screenshot of a computer

Description automatically generated

Ảnh 3: Ký file PDF

A screenshot of a computer

Description automatically generated

Ảnh 4: Xác minh file PDF

### 2.1.2. ECDSA CLI

- Dưới đây là hình ảnh minh hoạ cách sử dụng ECDSA CLI App:

A computer screen with text

Description automatically generated

Ảnh 5: Minh hoạ cách sử dụng ECDSA CLI App (Thời gian đo 1000 lần Sign/Verify)

- Dưới đây là hình ảnh minh hoạ phần code chạy 1000 lần của các hàm Sign/Verify. Thời gian thực nghiệm được đo là tổng của bao gồm toàn bộ quá trình load file, check format, thực hiện sign/verify và lưu/xuất file:

A computer screen shot of a program code

Description automatically generated

Ảnh 6: Minh hoạ phần code Sign chạy 1000 lần

A computer screen shot of a program code

Description automatically generated

Ảnh 7: Minh hoạ phần code Verify chạy 1000 lần

##### 2.1.2.1 Bảng thống kê số liệu thực nghiệm

Dưới đây là bảng thống kê chi tiết thời gian trung bình thời gian băm của từng thuật toán (đơn vị thời gian: ***ms***):



Ảnh 8: Bảng thời gian trung bình 1000 lần Sign/Verify trên Windows 11



Ảnh 9: Bảng thời gian trung bình 1000 lần Sign/Verify trên Ubuntu 22.04

##### 2.1.2.2 Biểu đồ cột so sánh các thuật toán băm

Dựa theo số liệu từ các bảng ở trên, vẽ biểu đồ để dễ dàng so sánh một cách trực quan:

Ảnh 10: Biểu đồ thời gian trung bình 1000 lần Sign/Verify trên Windows 11

Ảnh 11: Biểu đồ thời gian trung bình 1000 lần Sign/Verify trên Ubuntu 22.04

##### 2.1.2.3 Biểu đồ đường so sánh thời gian thực thi trên hai hệ điều hành

Vì các test case với file nhỏ không phản ánh sự khác biệt quá rõ ràng. Vì vậy để trực quan hơn về việc so sánh thời gian thực thi giữa 2 hệ điều hành, em xin so sánh chi tiết thời gian băm của File\_3 (30.5 MB). Dưới đây là biểu đồ so sánh thời gian băm 2 file đó trên 2 hệ điều hành:

Ảnh 12: Biểu đồ so sánh thời gian trung bình Sign/Verify 1000 lần file 30.5 MB trên 2 hệ điều hành

##### 2.1.2.4. Phân tích và so sánh

**- Thời gian ký (Sign):**

* + Trên cả hai hệ điều hành, thời gian ký số tăng lên khi kích thước tệp tăng lên.
  + Windows 11 có thời gian ký số lâu hơn so với Ubuntu 22.04 cho tất cả các kích thước tệp.

- **Thời gian xác minh (Verify):**

* + Thời gian xác minh cũng tăng lên khi kích thước tệp tăng lên trên cả hai hệ điều hành.
  + Windows 11 có thời gian xác minh lâu hơn so với Ubuntu 22.04 cho tất cả các kích thước tệp.
  + Thời gian xác minh hầu như đều nhanh hơn thời gian ký

- **Tổng quan:**

* + Ubuntu 22.04 có hiệu suất tốt hơn so với Windows 11 trong việc thực thi thuật toán ECDSA 1000 lần cho cả hai thao tác ký số và xác minh.
  + Sự chênh lệch thời gian giữa hai hệ điều hành không quá lớn, nhưng Ubuntu 22.04 vẫn thể hiện hiệu suất vượt trội hơn.

**- Kết luận:** Kết quả cho thấy Ubuntu 22.04 cho thời gian chạy nhanh hơn so với Windows 11 trong việc thực thi thuật toán ECDSA 1000 lần cho cả ký số và xác minh. Điều này cho thấy rằng Ubuntu có thể được tối ưu hóa tốt hơn cho các tác vụ mật mã học, khả năng quản lý tài nguyên hiệu quả hơn và cấu trúc hệ điều hành có thể hỗ trợ tốt hơn cho các hoạt động tính toán nặng.

## 2.2. RSASS-PSS:

### 2.2.1. RSASS-PSS GUI

Sau khi code xong phần CLI, em xuất file sang dll để có thể build được giao diện. Sử dụng Visual Studio 2022 để build giao diện Winform. Dưới đây là một số ảnh minh hoạ:

A screenshot of a computer

Description automatically generated

Ảnh 2: Tạo key 3072 bits với định dạng PEM

A screenshot of a computer

Description automatically generated

Ảnh 3: Ký file PDF

A screenshot of a computer

Description automatically generated

Ảnh 4: Xác minh file PDF

### 2.2.2. RSASS-PSS CLI

- Dưới đây là hình ảnh minh hoạ cách sử dụng RSASS-PSS CLI App:

A black screen with white text

Description automatically generated

Ảnh 5: Minh hoạ cách sử dụng RSASS-PSS CLI App (Thời gian đo 1000 lần Sign/Verify)

- Dưới đây là hình ảnh minh hoạ phần code chạy 1000 lần của các hàm Sign/Verify. Thời gian thực nghiệm được đo là tổng của bao gồm toàn bộ quá trình load file, check format, thực hiện sign/verify và lưu/xuất file:

A computer screen shot of a program code

Description automatically generated

Ảnh 6: Minh hoạ phần code Sign chạy 1000 lần

A screen shot of a computer code

Description automatically generated

Ảnh 7: Minh hoạ phần code Verify chạy 1000 lần

##### 2.2.2.1 Bảng thống kê số liệu thực nghiệm

Dưới đây là bảng thống kê chi tiết thời gian trung bình thời gian băm của từng thuật toán (đơn vị thời gian: ***ms***):



Ảnh 8: Bảng thời gian trung bình 1000 lần Sign/Verify trên Windows 11



Ảnh 9: Bảng thời gian trung bình 1000 lần Sign/Verify trên Ubuntu 22.04

##### 2.2.2.2 Biểu đồ cột so sánh các thuật toán băm

Dựa theo số liệu từ các bảng ở trên, vẽ biểu đồ để dễ dàng so sánh một cách trực quan:

Ảnh 10: Biểu đồ thời gian trung bình 1000 lần Sign/Verify trên Windows 11

Ảnh 11: Biểu đồ thời gian trung bình 1000 lần Sign/Verify trên Ubuntu 22.04

##### 2.2.2.3 Biểu đồ đường so sánh thời gian thực thi trên hai hệ điều hành

Vì các test case với file nhỏ không phản ánh sự khác biệt quá rõ ràng. Vì vậy để trực quan hơn về việc so sánh thời gian thực thi giữa 2 hệ điều hành, em xin so sánh chi tiết thời gian băm của File\_3 (30.5 MB). Dưới đây là biểu đồ so sánh thời gian băm 2 file đó trên 2 hệ điều hành:

Ảnh 12: Biểu đồ so sánh thời gian trung bình Sign/Verify 1000 lần file 30.5 MB trên 2 hệ điều hành

##### 2.2.2.4. Phân tích và so sánh

**- Thời gian ký (Sign):**

* + Trên cả hai hệ điều hành, thời gian ký số tăng lên khi kích thước tệp tăng lên.
  + Windows 11 có thời gian ký số lâu hơn so với Ubuntu 22.04 cho tất cả các kích thước tệp.

- **Thời gian xác minh (Verify):**

* + Thời gian xác minh cũng tăng lên khi kích thước tệp tăng lên trên cả hai hệ điều hành.
  + Windows 11 có thời gian xác minh lâu hơn so với Ubuntu 22.04 cho tất cả các kích thước tệp.
  + Thời gian xác minh hầu như đều nhanh hơn thời gian ký

- **Tổng quan:**

* + Ubuntu 22.04 có hiệu suất tốt hơn so với Windows 11 trong việc thực thi thuật toán RSASS-PSS 1000 lần cho cả hai thao tác ký số và xác minh.
  + Sự chênh lệch thời gian giữa hai hệ điều hành không quá lớn, nhưng Ubuntu 22.04 vẫn thể hiện hiệu suất vượt trội hơn.

**- Kết luận:** Kết quả cho thấy Ubuntu 22.04 cho thời gian chạy nhanh hơn so với Windows 11 trong việc thực thi thuật toán RSASS-PSS 1000 lần cho cả ký số và xác minh. Điều này cho thấy rằng Ubuntu có thể được tối ưu hóa tốt hơn cho các tác vụ mật mã học, khả năng quản lý tài nguyên hiệu quả hơn và cấu trúc hệ điều hành có thể hỗ trợ tốt hơn cho các hoạt động tính toán nặng.