**Report Lab 4 – 5**

**Student Information**

Full Name: Mai Nguyễn Nam Phương

Student ID Number: 22521164

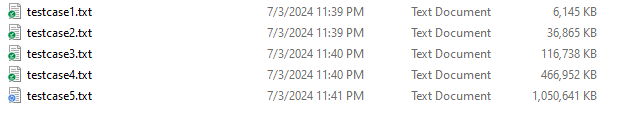
Class: NT219.O21.ANTT

**Device Information**



**TASK 4.1**

**TEST CASE**

****

number of iterations: 1000

time counter: mili seconds

**Window**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Testcase1  (6,145 KB) | Testcase2  (36,865 KB) | Testcase3  (116,738 KB) | Testcase4  (466,952 KB) | Testcase6  (1,050,641 KB) |
| SHA224 | 4 | 20 | 56 | 221 | 535 |
| SHA256 | 4 | 23 | 58 | 221 | 547 |
| SHA384 | 9 | 56 | 163 | 671 | 1655 |
| SHA512 | 9 | 58 | 164 | 734 | 1534 |
| SHA3\_224 | 12 | 74 | 216 | 925 | 1957 |
| SHA3\_256 | 12 | 77 | 228 | 960 | 2106 |
| SHA3\_384 | 16 | 101 | 292 | 1241 | 2679 |
| SHA3\_512 | 22 | 146 | 422 | 1877 | 3832 |
| SHAKE128 (d=256) | 10 | 63 | 181 | 803 | 1676 |
| SHAKE128 (d=256) | 13 | 75 | 225 | 987 | 2058 |

**Ảnh có chứa văn bản, ảnh chụp màn hình

Mô tả được tạo tự độngẢnh có chứa văn bản, ảnh chụp màn hình

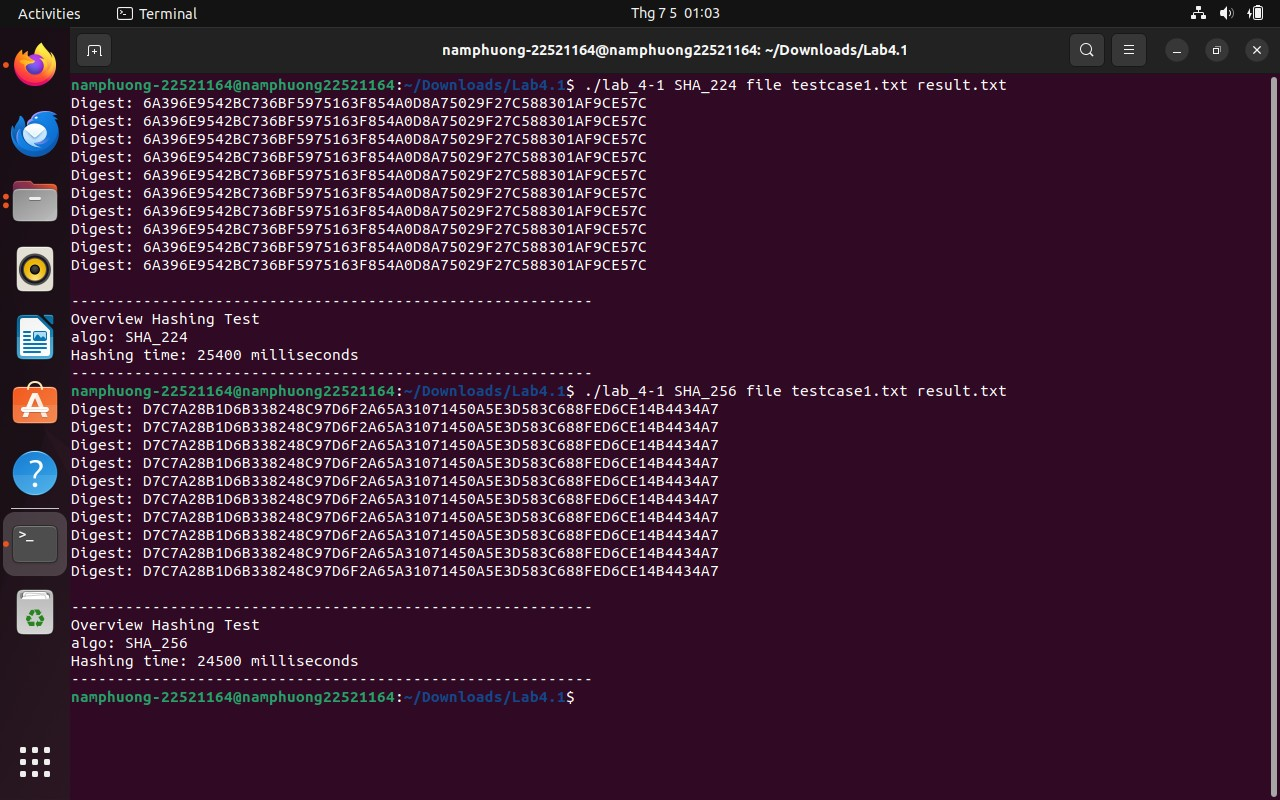
Mô tả được tạo tự động**

**Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Mô tả được tạo tự động**

**Ubuntu**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Testcase1  (6,145 KB) | Testcase2  (36,865 KB) | Testcase3  (116,738 KB) | Testcase4  (466,952 KB) | Testcase6  (1,050,641 KB) |
| SHA224 | 2.54 | 16.65 | 44.16 | 200.12 | 497.5 |
| SHA256 | 2.45 | 17.54 | 48.54 | 204.65 | 500 |
| SHA384 | 5.63 | 43.76 | 123.43 | 603.12 | 1534.46 |
| SHA512 | 6.12 | 46.88 | 126.7 | 689.86 | 1645.65 |
| SHA3\_224 | 6.76 | 68.5 | 187.98 | 843.32 | 1767.84 |
| SHA3\_256 | 7 | 73.23 | 205.23 | 864.65 | 2067.74 |
| SHA3\_384 | 8.65 | 88.65 | 268.34 | 1123.98 | 2536.79 |
| SHA3\_512 | 11.54 | 121.32 | 387.88 | 1771.53 | 3566.75 |
| SHAKE128 (d=256) | 8.63 | 56.43 | 145.66 | 730.34 | 1574.87 |
| SHAKE128 (d=256) | 9.36 | 62.12 | 208.56 | 779.23 | 1802.93 |



Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

**Comment**

* Trên cả 2 hệ điều hành, ta có thể thấy với input size càng lớn thì thời gian chạy càng lâu
* Khi so sánh thời gian chạy giữa 2 hệ điều hành thì chênh lệch thởi gian là có nhưng không đánh kể só với sự khác biệt trong AES và DES
* Các thuật toán HASH càng phức tạp thì sẽ cho thời gian chạy càng lâu, tuy nhiên là độ bảo mật được tang lên đáng kể
* Nếu xét thời gian chạy của cả 2 hệ điều hành trên cùng 1 thuật toán và cùng thuật toán tương đương nhau thì đa phần Ubuntu sẽ nhanh hơn Window tầm khoảng từ 10-15%

**TASK 4.2**

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Mô tả được tạo tự động

**TASK 4.3**

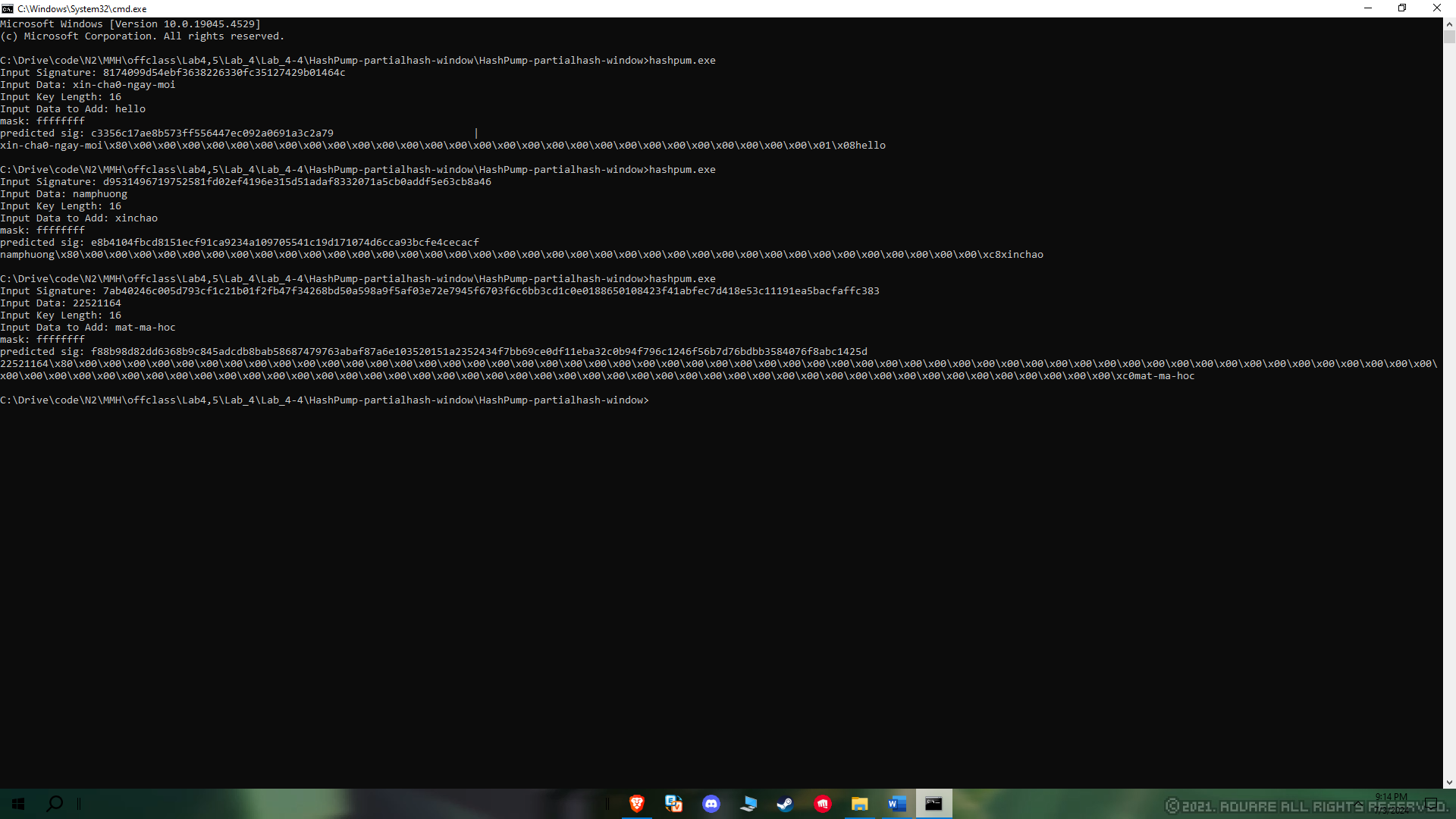
* Đây là kết quả sau khi chạy tool hashclash để tạo 2 file có cùng giá trị hash MD5 và có cùng prefix cho trước rồi kiểm tra nội dung 2 file bằng cách check hexdump:  
  Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

  Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phông chữ

Mô tả được tạo tự động

Đây là kết quả sau khi chạy tool hashclash để tạo ra file MD5 collision với 2 prefix là 2 file thực thi của 2 chương trình C++ khác nhau  
Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động  
**TASK 4.4**  


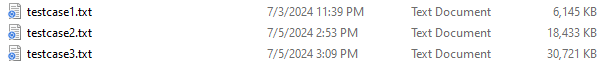
**TASK 4.5**

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

**TASK 5.1 - ECDSA**

**TEST CASE**



number of iterations: 1000

time counter: mili seconds

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ECDSA | Window | | Ubuntu | |
| Sign | Verify | Sign | Verify |
| File 1 (6,145 KB) | 13,176 | 12,949 | 7,421 | 6,921 |
| File 2 (18,433 KB) | 37,426 | 38,482 | 28.978 | 28.453 |
| File 3 (30,721 KB) | 58,865 | 59,034 | 56.312 | 53.411 |

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Mô tả được tạo tự động|  
Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Mô tả được tạo tự động  
Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Mô tả được tạo tự động  
Ảnh có chứa văn bản, ảnh chụp màn hình, thực đơn

Mô tả được tạo tự động  
Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

**COMMENT**

* Về thời gian ký ( Sign )  
  **+** Trên cả 2 hệ điều hành thì thời gian ký tăng lên khi kích thước tệp tăng lên

+ Ubuntu có thời gian kí nhanh hơn so với Window trên cả tất cả các tệp

* Về thời gian xác minh ( Verìy )  
  + Thời gian xác minh cũng tăng khi kích thước tệp tăng lên ở cả 2 hệ điều hành

+ Ubuntu có thời gian kí nhanh hơn so với Window trên cả tất cả  
+ Thời gian xác minh và ký khá tương đồng

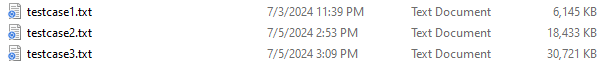
* Nhìn chung

+ 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

**TASK 5.2 - RSASS-PSS**

**TEST CASE**



number of iterations: 1000

time counter: mili seconds

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RSASS-PSS | Window | | Ubuntu | |
| Sign | Verify | Sign | Verify |
| File 1 (6,145 KB) | 20,156 | 11,474 | 18,421 | 9,921 |
| File 2 (18,433 KB) | 57,013 | 35,45 | 55.259 | 33.52 |
| File 3 (30,721 KB) | 90,007 | 55,552 | 83.312 | 53.411 |

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Mô tả được tạo tự độngẢnh có chứa văn bản, ảnh chụp màn hình, màn hình, phần mềm

Mô tả được tạo tự động  
  
  
Ảnh có chứa văn bản, ảnh chụp màn hình, thực đơn, Phông chữ

Mô tả được tạo tự độngẢnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

**COMMENT**

* Về thời gian ký ( Sign )  
  **+** Trên cả 2 hệ điều hành thì thời gian ký tăng lên khi kích thước tệp tăng lên

+ Ubuntu có thời gian kí nhanh hơn so với Window trên cả tất cả các tệp

* Về thời gian xác minh ( Verify )  
  + Thời gian xác minh cũng tăng khi kích thước tệp tăng lên ở cả 2 hệ điều hành

+ Ubuntu có thời gian kí nhanh hơn so với Window trên cả tất cả  
+ Thời gian xác minh sẽ luôn nhanh hơn so với thời gian ký

* Nhìn chung

+ 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