REPORT CRYTOGRAPHY – TASK 3

Student: Huỳnh Trung Thuận

ID: 22521444

Lecturer: Nguyễn Ngọc Tự

---

1. Hardware resources.

a. Windows

System Information

Current Date/Time:	Saturday, June 15, 2024, 3:25:43 PM
Computer Name:	LAPTOP-B42TB1HN
Operating System:	Windows 11 Home Single Language 64-bit (10.0, Build 22631)
Language:	English (Regional Setting: English)
System Manufacturer:	ASUSTeK COMPUTER INC.
System Model:	Vivobook_ASUSLaptop X1403ZA_A1403ZA
BIOS:	X1403ZA.300
Processor:	12th Gen Intel(R) Core(TM) i5-12500H (16 CPUs), ~2.5GHz
Memory:	16384MB RAM
Page file:	17426MB used, 12686MB available
DirectX Version:	DirectX 12

b. Linux (ubuntu)

```
thuanht@HuynhTrungThuan-22521444:~$ lscpu
Architecture:            x86_64
  CPU op-mode(s):        32-bit, 64-bit
  Address sizes:         39 bits physical, 48 bits virtual
  Byte Order:            Little Endian
CPU(s):                  16
  On-line CPU(s) list:   0-15
Vendor ID:               GenuineIntel
  Model name:            12th Gen Intel(R) Core(TM) i5-12500H
    CPU family:          6
    Model:               154
    Thread(s) per core:  2
    Core(s) per socket:  12
    Socket(s):           1
    Stepping:            3
    CPU max MHz:         4500.0000
    CPU min MHz:         400.0000
    BogoMIPS:            6220.80
    Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mc
                         a cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss
                         ht tm pbe syscall nx pdpe1gb rdtscp lm constant_tsc art
                          arch_perfmon pebs bts rep_good nopl xtopology nonstop_
                         tsc cpuid aperfmperf tsc_known_freq pni pclmulqdq dtes6
                         4 monitor ds_cpl vmx smx est tm2 ssse3 sdbg fma cx16 xt
                         pr pdcm sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_
                         timer aes xsave avx f16c rdrand lahf_lm abm 3dnowprefet
                         ch cpuid_fault epb cat_l2 cdp_l2 ssbd ibrs ibpb stibp i
                         brs enhanced tpr_shadow flexpriority ept vpid ept_ad fs
                         gsbase tsc_adjust bmi1 avx2 smep bmi2 erms invpcid rdt_
                         a rdseed adx smap clflushopt clwb intel_pt sha_ni xsave
                         opt xsavec xgetbv1 xsaves split_lock_detect avx_vnni dt
                         herm ida arat pln pts hwp hwp_notify hwp_act_window hwp
                         _epp hwp_pkg_req hfi vnmi umip pku ospke waitpkg gfni v
                         aes vpclmulqdq rdpid movdiri movdir64b fsrm md_clear se
                         rialize arch_lbr ibt flush_l1d arch_capabilities
Virtualization features:
  Virtualization:        VT-x
Caches (sum of all):
  L1d:                   448 KiB (12 instances)
  L1i:                   640 KiB (12 instances)
  L2:                    9 MiB (6 instances)
  L3:                    18 MiB (1 instance)
NUMA:
  NUMA node(s):          1
  NUMA node0 CPU(s):     0-15
Vulnerabilities:
  Gather data sampling:  Not affected
```

2. Giới thiệu.

Báo cáo này trình bày quá trình thực hiện và kết quả kiểm thử hiệu suất của thuật toán mã hóa RSA. Mục tiêu của báo cáo là so sánh thời gian mã hóa và giải mã của RSA khi thực thi trên hai hệ điều hành khác nhau, Windows và Linux, với mỗi tác vụ được chạy 10,000 lần để đảm bảo tính chính xác và ổn định của kết quả. Thông qua việc sử dụng thư viện CryptoPP, em đã triển khai và đánh giá RSA với các kích thước tệp khác nhau. Kết quả thu được sẽ giúp đưa ra nhận định về hiệu suất và khả năng ứng dụng của thuật toán RSA trong các môi trường khác nhau.

3. Thống kê .

Kết quả thử nghiệm thời gian mã hóa và giải mã bằng RSA với khóa có kích thước 7086 bits.

Windows :

Time (ms)	Encrypt Windows	Decrypt Windows
File1 (342 Byte)	3.7286	48.361
File2 (462 byte)	3.8534	49.936
File3 (712 bytes)	3.9659	54.221

Linux :

Time (ms)	Encrypt Linux	Decrypt Linux
File1 (342 Byte)	0.8	62.6
File2 (462 byte)	1	63.5
File3 (712 bytes)	1.2	63.8

4. So Sánh:

Dựa trên bảng thời gian mã hóa và giải mã bằng RSA trên hai hệ điều hành (Windows và Linux) cho ba tệp có kích thước khác nhau, em có những nhận xét sau:

Thời gian mã hóa:

- Trên Windows, thời gian mã hóa dao động từ 3.7286 ms đến 3.9659 ms, tăng nhẹ theo kích thước tệp.

- Trên Linux, thời gian mã hóa ngắn hơn nhiều so với Windows, từ 0.8 ms đến 1.2 ms, cũng tăng nhẹ theo kích thước tệp.

Thời gian giải mã:

- Trên Windows, thời gian giải mã dài hơn đáng kể so với thời gian mã hóa, từ 48.361 ms đến 54.221 ms, tăng nhẹ theo kích thước tệp.
- Trên Linux, thời gian giải mã từ 62.6 ms đến 63.8 ms, cũng tăng nhẹ theo kích thước tệp và dài hơn thời gian giải mã trên Windows.

So sánh giữa Windows và Linux:

- Linux thực hiện mã hóa nhanh hơn đáng kể so với Windows.
- Windows thực hiện giải mã nhanh hơn so với Linux.
- Trên cả hai hệ điều hành, thời gian giải mã dài hơn thời gian mã hóa.

5. Tổng Kết

Kết quả thử nghiệm thời gian mã hóa và giải mã bằng RSA trên Windows và Linux cho thấy sự khác biệt rõ rệt về hiệu suất giữa hai hệ điều hành. Cụ thể, Linux thực hiện mã hóa nhanh hơn nhiều so với Windows, trong khi Windows lại thực hiện giải mã nhanh hơn so với Linux. Trên cả hai hệ điều hành, thời gian mã hóa tốn ít thời gian hơn so với giải mã và thời gian này tăng nhẹ khi kích thước tệp tăng lên. Nhìn chung, RSA có hiệu suất mã hóa tốt hơn trên Linux và giải mã tốt hơn trên Windows