REPORT CRYTOGRAPHY – TASK 5

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
```

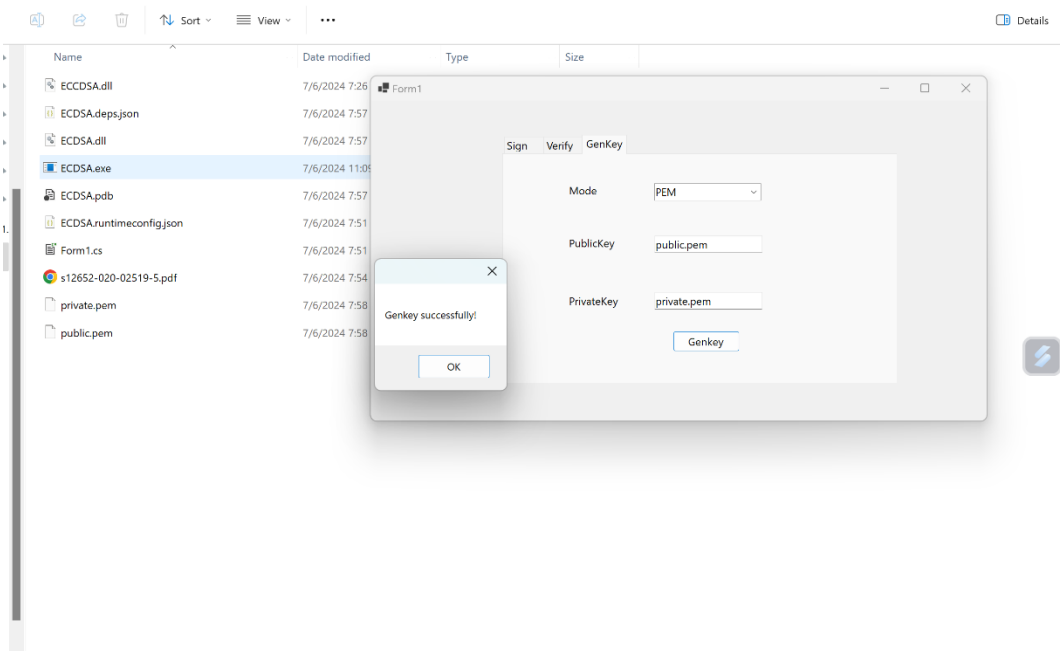
2. Giới thiệu.

Báo cáo này trình bày quá trình thực hiện và kết quả kiểm thử hiệu suất của hai thuật toán ký số: ECDSA và RSA-PSS. Mục tiêu của báo cáo là so sánh thời gian thực hiện ký và xác thực của từng thuật toán khi thực thi trên hai hệ điều hành khác nhau, Windows và Linux. Để đảm bảo tính chính xác và ổn định của kết quả, mỗi tác vụ được chạy 1000 lần.

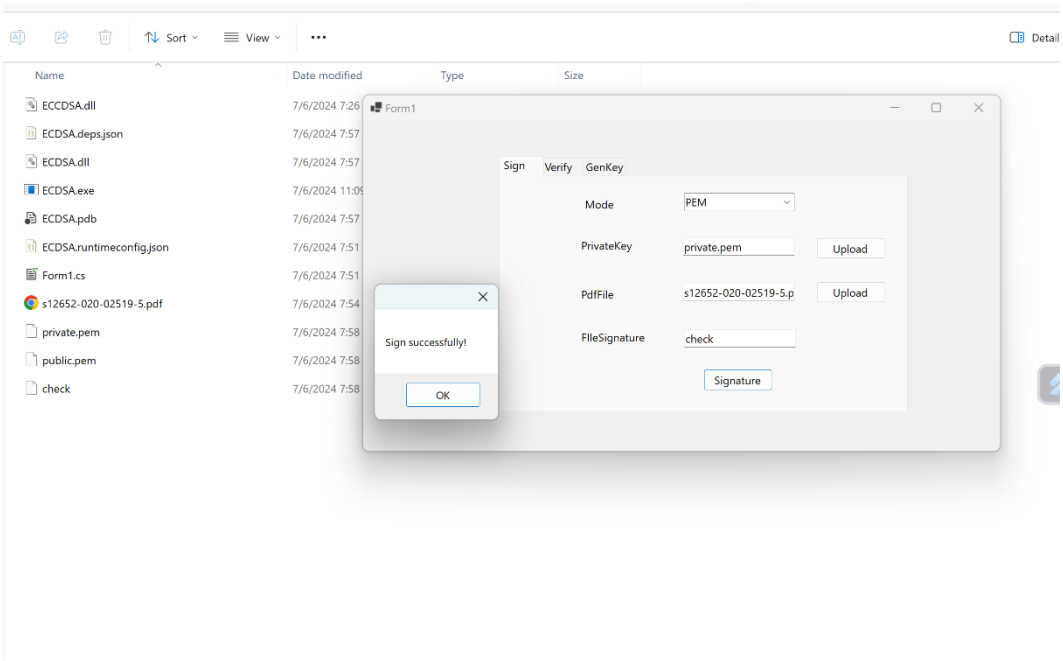
3. Digital signature with CryptoPP/Openssl

3.1 Thực hiện demo

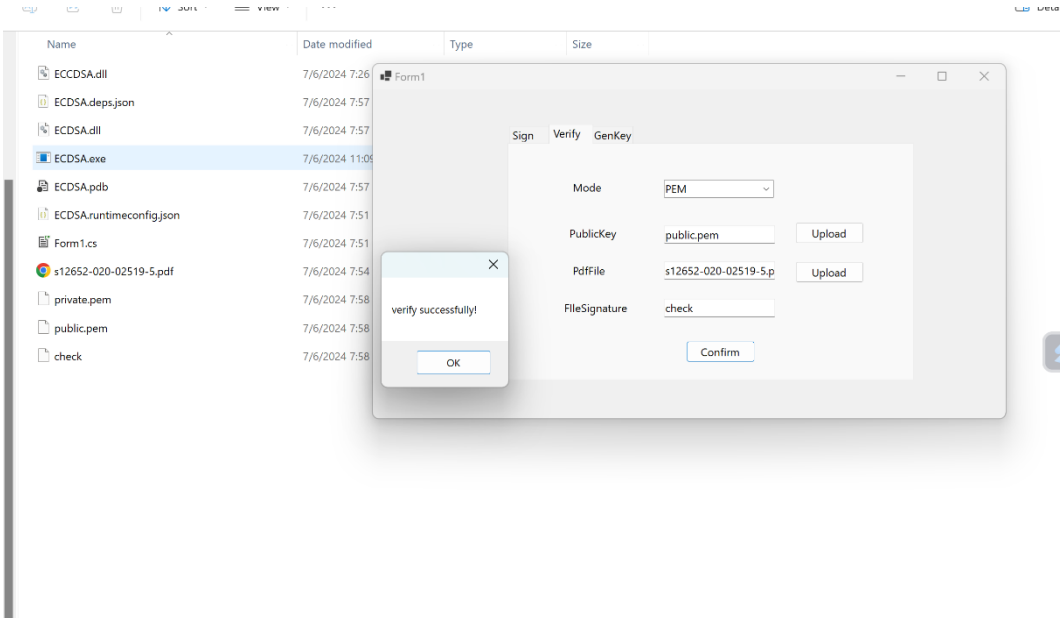
Thực hiện bước genkey :



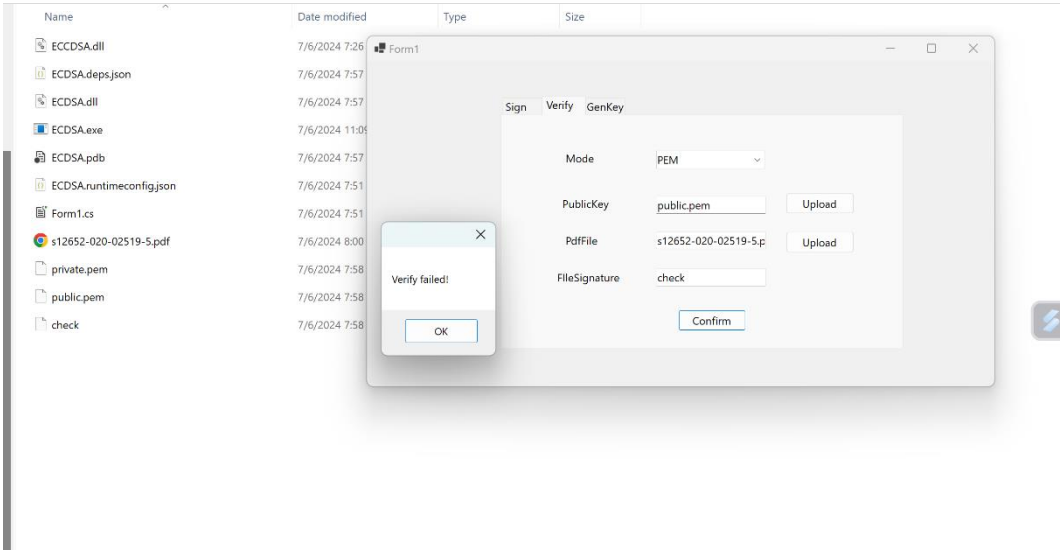
Thực hiện Signature :



Thực hiện Verify :



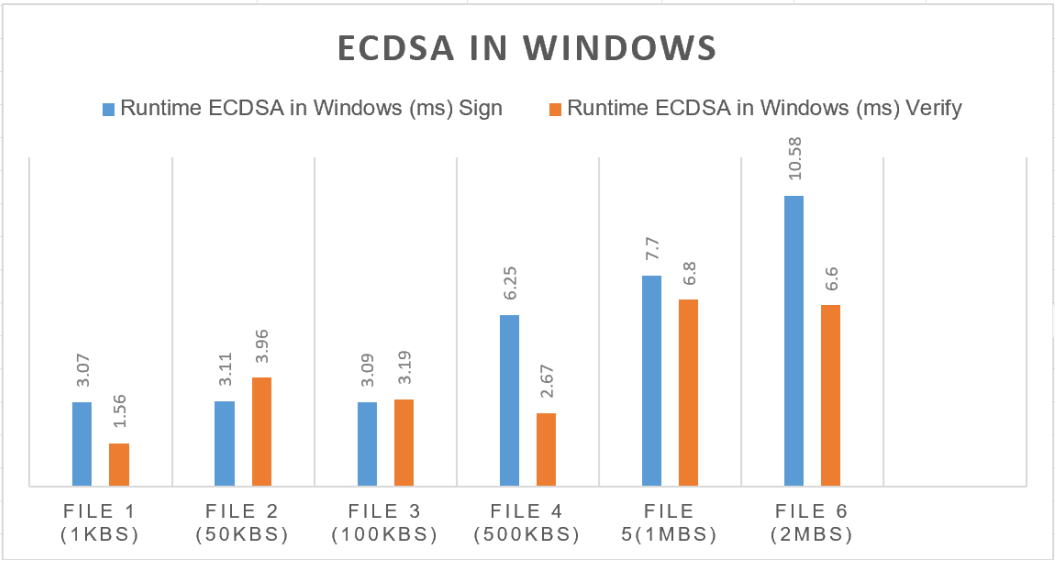
Tiến hành thử nghiệm thay đổi nội dung của file và kết quả :



3.2 ECDSA và RSA-PSS :

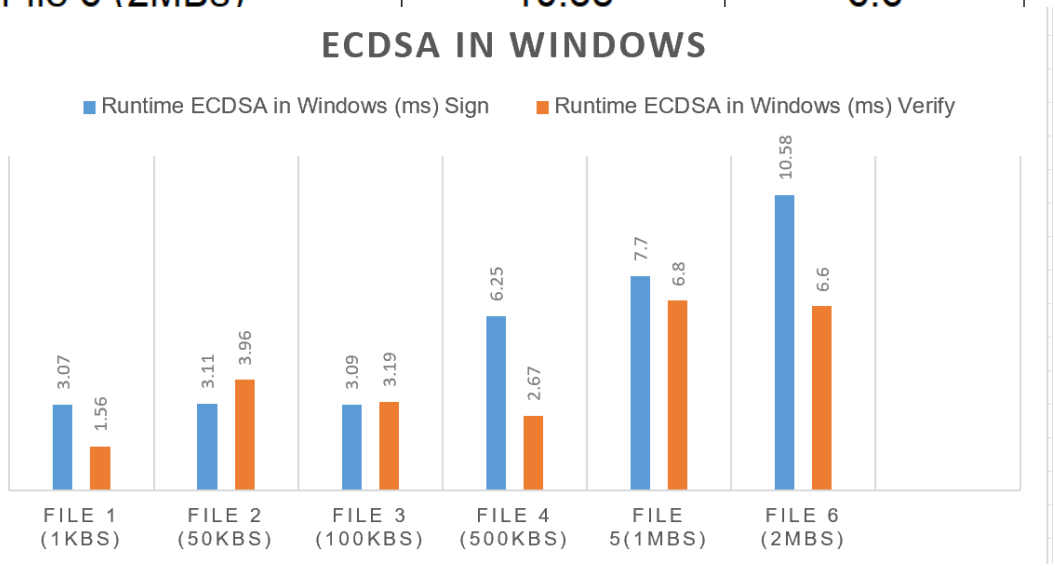
ECDSA thực hiện trên windows: (đơn vị ms)

Runtime ECDSA in Windows (ms)		
	Sign	**Verify**
File 1 (1KBs)	3.07	1.56
File 2 (50KBs)	3.11	3.96
File 3 (100KBs)	3.09	3.19
File 4 (500KBs)	6.25	2.67
File 5(1MBs)	7.7	6.8
File 6 (2MBs)	10.58	6.6



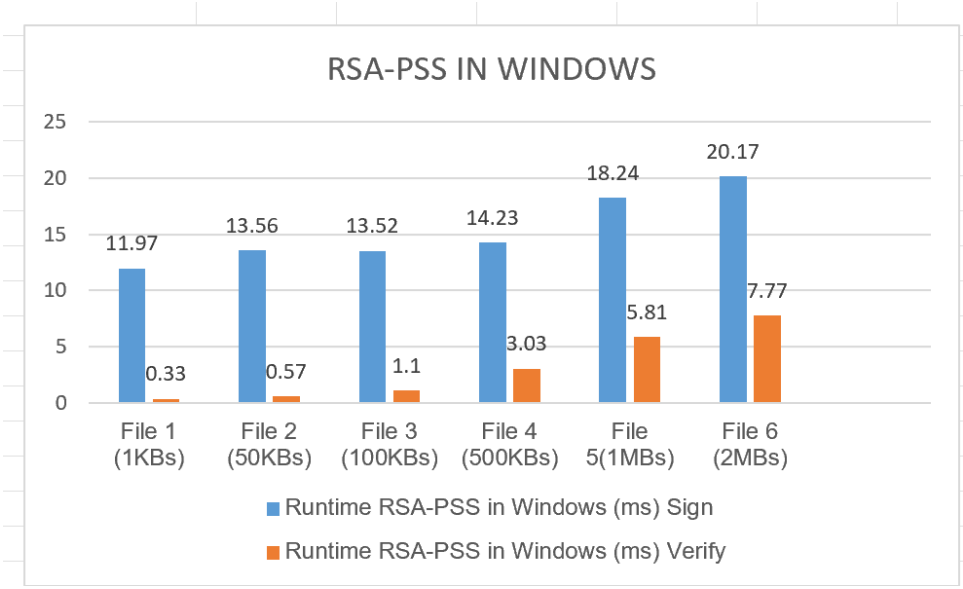
ECDSA thực hiện trên Linux: (đơn vị ms)

Runtime ECDSA in Windows (ms)		
	Sign	**Verify**
File 1 (1KBs)	3.07	1.56
File 2 (50KBs)	3.11	3.96
File 3 (100KBs)	3.09	3.19
File 4 (500KBs)	6.25	2.67
File 5(1MBs)	7.7	6.8
File 6 (2MBs)	10.58	6.6



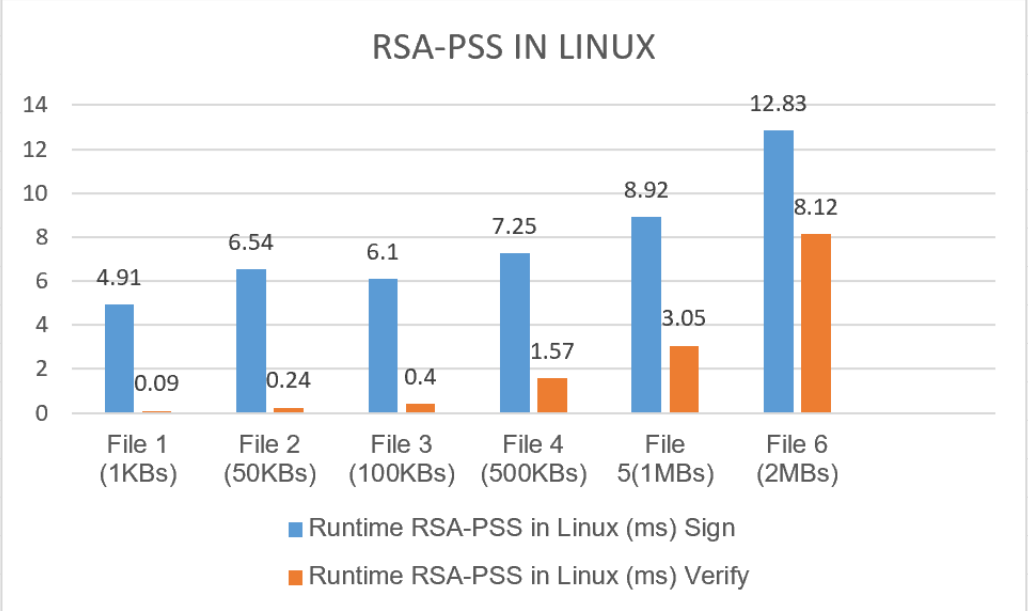
RSA-PSS thực hiện trên windows: (đơn vị ms)

Runtime RSA-PSS in Windows (ms)		
	Sign	**Verify**
File 1 (1KBs)	11.97	0.33
File 2 (50KBs)	13.56	0.57
File 3 (100KBs)	13.52	1.1
File 4 (500KBs)	14.23	3.03
File 5(1MBs)	18.24	5.81
File 6 (2MBs)	20.17	7.77



RSA-PSS thực hiện trên Linux: (đơn vị ms)

Runtime RSA-PSS in Linux (ms)		
	Sign	**Verify**
File 1 (1KBs)	4.91	0.09
File 2 (50KBs)	6.54	0.24
File 3 (100KBs)	6.1	0.4
File 4 (500KBs)	7.25	1.57
File 5(1MBs)	8.92	3.05
File 6 (2MBs)	12.83	8.12



3.3 So Sánh :

Hiệu suất trên Linux vượt trội hơn:Cả RSA-PSS và ECDSA đều cho thấy thời gian ký và xác thực nhanh hơn đáng kể trên Linux so với Windows. Điều này chứng tỏ Linux có khả năng tối ưu hóa tốt hơn cho các tác vụ mã hóa, có thể nhờ vào việc quản lý tài nguyên hiệu quả và cấu trúc hệ điều hành tối ưu.

ECDSA có hiệu suất cao hơn RSA-PSS: Trên cả hai hệ điều hành, ECDSA luôn cho thấy thời gian thực thi nhanh hơn so với RSA-PSS, đặc biệt là trong tác vụ ký số. Điều này làm cho ECDSA trở thành lựa chọn ưu việt khi yêu cầu về hiệu suất và tốc độ.

3.4 Nhận Xét :

- **Linux là lựa chọn tốt hơn cho mã hóa:** Hiệu suất tốt hơn của Linux đối với cả hai thuật toán mã hóa cho thấy nó là lựa chọn ưu tiên cho các hệ thống yêu cầu xử lý mã hóa nhanh chóng và hiệu quả.
- **ECDSA ưu việt hơn cho hiệu suất:** Với tốc độ thực thi nhanh hơn, ECDSA là lựa chọn tốt hơn so với RSA-PSS trong hầu hết các trường hợp, đặc biệt là khi cần ký số nhanh và hiệu quả.