Cryptography Report – Task 1

Student - ID: Trần Minh Hiếu – 22520445

Class: NT1219.O21.ANTT

Lecturer: Nguyễn Ngọc Tự

I/ Hardware Resources

1. Windows

Item	Value
OS Name	Microsoft Windows 11 Home Single Language
Version	10.0.22631 Build 22631
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	LAPTOP-LUB6K53Q
System Manufacturer	ASUSTeK COMPUTER INC.
System Model	ASUS TUF Gaming A15 FA507RE_FA507RE
System Type	x64-based PC
System SKU	
Processor	AMD Ryzen 7 6800H with Radeon Graphics, 3201 Mhz, 8 Core(s), 16 Logical...
BIOS Version/Date	American Megatrends International, LLC. FA507RE.315, 11/30/2022
SMBIOS Version	3.4
Embedded Controller Version	3.07
BIOS Mode	UEFI
BaseBoard Manufacturer	ASUSTeK COMPUTER INC.
BaseBoard Product	FA507RE
BaseBoard Version	1.0
Platform Role	Mobile
Secure Boot State	On
PCR7 Configuration	Elevation Required to View
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "10.0.22621.2506"
User Name	LAPTOP-LUB6K53Q\Admin

Item	Value
Secure Boot State	On
PCR7 Configuration	Elevation Required to View
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "10.0.22621.2506"
User Name	LAPTOP-LUB6K53Q\Admin
Time Zone	SE Asia Standard Time
Installed Physical Memory (RA...	8.00 GB
Total Physical Memory	7.25 GB
Available Physical Memory	858 MB
Total Virtual Memory	13.7 GB
Available Virtual Memory	1.72 GB
Page File Space	6.43 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	On
Virtualization-based security	Running
Virtualization-based security ...	
Virtualization-based security ...	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Read...
Virtualization-based security S...	
Virtualization-based security S...	
Windows Defender Applicatio...	Enforced
Windows Defender Applicatio...	Off
Device Encryption Support	Elevation Required to View
A hypervisor has been detecte...	

2. Linux (Ubuntu)

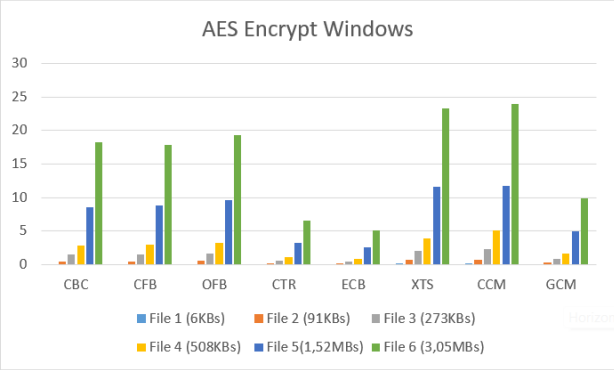
```
hieriss@hieriss-ASUS-TUF-Gaming-A15-FA507RE-FA507RE:~$ lscpu
Architecture:            x86_64
  CPU op-mode(s):        32-bit, 64-bit
  Address sizes:         48 bits physical, 48 bits virtual
  Byte Order:            Little Endian
CPU(s):                  16
  On-line CPU(s) list:   0-15
Vendor ID:               AuthenticAMD
  Model name:            AMD Ryzen 7 6800H with Radeon Graphics
    CPU family:          25
    Model:               68
    Thread(s) per core:  2
    Core(s) per socket:  8
    Socket(s):           1
    Stepping:            1
    CPU max MHz:         4785,0000
    CPU min MHz:         400,0000
    BogoMIPS:            6388.02
    Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mc
                         a cmov pat pse36 clflush mmx fxsr sse sse2 ht syscall n
                         x mmxext fxsr_opt pdpe1gb rdtscp lm constant_tsc rep_go
                         od nopl nonstop_tsc cpuid extd_apicid aperfmperf rapl p
                         ni pclmulqdq monitor ssse3 fma cx16 sse4_1 sse4_2 x2api
                         c movbe popcnt aes xsave avx f16c rdrand lahf_lm cmp_le
                         gacy svm extapic cr8_legacy abm sse4a misalignsse 3dnow
                         prefetch osvw ibs skinit wdt tce topoext perfctr_core p
                         erfctr_nb bpext perfctr_llc mwaitx cpb cat_l3 cdp_l3 hw
                         _pstate ssbd mba ibrs ibpb stibp vmmcall fsgsbase bmi1
                         avx2 smep bmi2 invpcid cqm rdt_a rdseed adx smap clflus
                         hopt clwb sha_ni xsaveopt xsavec xgetbv1 xsaves cqm_llc
                          cqm_occup_llc cqm_mbm_total cqm_mbm_local clzero irper
                         f xsaveerptr rdpru wbnoinvd cppc arat npt lbrv svm_lock
                          nrip_save tsc_scale vmcb_clean flushbyasid decodeassis
                         ts pausefilter pfthreshold avic v_vmsave_vmload vgif v_
                         spec_ctrl umip pku ospke vaes vpclmulqdq rdpid overflow
                         _recov succor smca
Virtualization features:
  Virtualization:        AMD-V
Caches (sum of all):
  L1d:                   256 KiB (8 instances)
  L1i:                   256 KiB (8 instances)
  L2:                    4 MiB (8 instances)
  L3:                    16 MiB (1 instance)
NUMA:
  NUMA node(s):          1
  NUMA node0 CPU(s):     0-15
Vulnerabilities:
  Gather data sampling:  Not affected
  Itlb multihit:         Not affected
  L1tf:                  Not affected
  Mds:                   Not affected
```

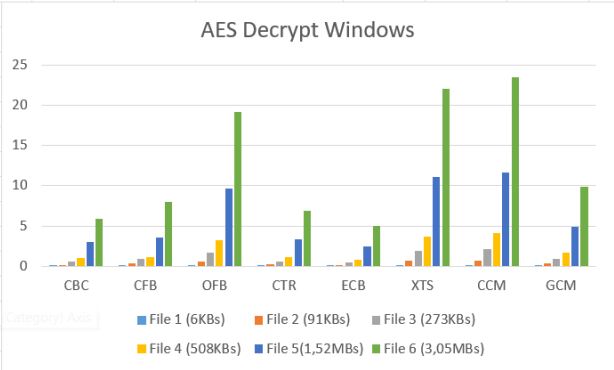
II/ Performance computation on Windows and Ubuntu

- Em tạo 6 testcases với kích thước tăng dần và tiến hành chạy với toàn bộ 8 modes và thu được kết quả ở OS Windows và Ubuntu như sau:
- Windows:

AES Runtime in WINDOWS (s)								
Encrypt	**CBC**	**CFB**	**OFB**	**CTR**	**ECB**	**XTS**	**CCM**	**GCM**
File 1 (6KBs)	0.041	0.042	0.142	0.055	0.043	0.179	0.18	0.085
File 2 (91KBs)	0.524	0.536	0.58	0.204	0.152	0.704	0.722	0.305
File 3 (273KBs)	1.529	1.595	1.71	0.596	0.449	2.105	2.382	0.897
File 4 (508KBs)	2.849	2.961	3.207	1.081	0.839	3.876	5.185	1.629
File 5(1,52MBs)	8.574	8.86	9.59	3.29	2.545	11.665	11.691	4.937
File 6 (3,05MBs)	18.265	17.807	19.299	6.532	5.147	23.319	23.924	9.851

AES Runtime in WINDOWS (s)								
Decrypt	**CBC**	**CFB**	**OFB**	**CTR**	**ECB**	**XTS**	**CCM**	**GCM**
File 1 (6KBs)	0.017	0.055	0.139	0.055	0.04	0.172	0.183	0.087
File 2 (91KBs)	0.179	0.412	0.566	0.208	0.154	0.661	0.712	0.305
File 3 (273KBs)	0.532	0.882	1.722	0.604	0.45	1.96	2.087	0.899
File 4 (508KBs)	0.997	1.108	3.194	1.132	0.822	3.656	4.133	1.656
File 5(1,52MBs)	3.015	3.561	9.605	3.39	2.451	11.062	11.622	4.895
File 6 (3,05MBs)	5.923	8.023	19.188	6.867	5.036	21.998	23.469	9.83

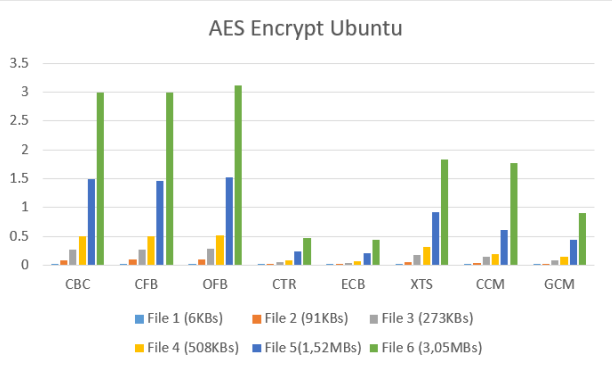


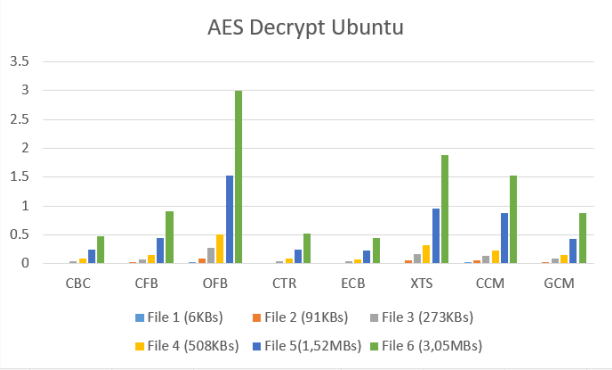


- Linux:

AES Runtime in UBUNTU(s)								
Encrypt	**CBC**	**CFB**	**OFB**	**CTR**	**ECB**	**XTS**	**CCM**	**GCM**
File 1 (6KBs)	0.021	0.022	0.022	0.004	0.003	0.012	0.024	0.007
File 2 (91KBs)	0.089	0.091	0.093	0.014	0.012	0.052	0.035	0.026
File 3 (273KBs)	0.268	0.266	0.276	0.044	0.037	0.168	0.143	0.078
File 4 (508KBs)	0.498	0.493	0.514	0.083	0.071	0.315	0.196	0.149
File 5(1,52MBs)	1.495	1.464	1.522	0.244	0.207	0.921	0.604	0.445
File 6 (3,05MBs)	2.987	2.989	3.118	0.469	0.431	1.838	1.772	0.907

AES Runtime in UBUNTU (s)								
Decrypt	**CBC**	**CFB**	**OFB**	**CTR**	**ECB**	**XTS**	**CCM**	**GCM**
File 1 (6KBs)	0.004	0.007	0.022	0.004	0.004	0.016	0.025	0.007
File 2 (91KBs)	0.014	0.025	0.093	0.014	0.013	0.052	0.062	0.026
File 3 (273KBs)	0.044	0.079	0.271	0.044	0.039	0.167	0.131	0.081
File 4 (508KBs)	0.083	0.148	0.504	0.081	0.071	0.324	0.224	0.148
File 5(1,52MBs)	0.242	0.451	1.527	0.247	0.222	0.949	0.871	0.43
File 6 (3,05MBs)	0.482	0.909	2.999	0.521	0.44	1.881	1.523	0.872





- Comparisons and Comments:
  - ⇨ Các mode CTR, GCM và ECB mã hóa và giải mã nhanh hơn nhờ cơ chế **parallelizable.**
  - ⇨ Mode OFB mã hóa và giải mã chậm nhất vì không có cơ chế **parallelizable.**
  - ⇨ Tổng quan thì kết quả chạy trên Ubuntu nhanh hơn Windows với mọi file (ở moi kích thước).
  - ⇨ Khác biệt rõ rang nhất thể hiện ở file testcase6:

AES Runtime Comparison								
	CBC	**CFB**	**OFB**	**CTR**	**ECB**	**XTS**	**CCM**	**GCM**
Windows	24.188	25.83	38.487	13.399	10.183	45.317	47.393	19.681
Linux	3.469	3.898	6.117	0.99	0.871	3.719	3.295	1.779