# REPORT CRYTOGRAPHY – TASK 1

---

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 các thuật toán mã hóa AES và DES. Mục tiêu của báo cáo là so sánh thời gian mã hóa và giải mã của từng thuật toán 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, chúng tôi đã triển khai và đánh giá các mode mã hóa như ECB, CBC, CFB, OFB, CTR, XTS, CCM, và GCM. Kết quả thu được sẽ giúp đưa ra nhận định về hiệu suất và khả năng ứng dụng của từng thuật toán trong các môi trường khác nhau.

## 3. Thống kê và biểu đồ.

### a. Thống kê thời gian.

Windows - AES:

| Runtime in WINDOWS (ms) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Encrypt** | **ECB** | **CBC** | **CFB** | **OFB** | **CTR** | **XTS** | **GCM** | **CCM** |
| File 1 (1KBs) | 0.108 | 0.086 | 0.106 | 0.123 | 0.11 | 0.098 | 0.148 | 0.13 |
| File 2 (50KBs) | 0.296 | 0.311 | 0.33 | 0.394 | 0.208 | 0.393 | 0.26 | 0.427 |
| File 3 (100KBs) | 0.342 | 0.579 | 0.604 | 0.631 | 0.31 | 0.778 | 0.406 | 0.734 |
| File 4 (500KBs) | 1.048 | 2.698 | 2.622 | 2.82 | 1.179 | 3.017 | 1.572 | 3.147 |
| File 5(1MBs) | 2.67 | 5.902 | 5.156 | 5.512 | 2.205 | 6.014 | 2.938 | 6.48 |
| File 6 (2MBs) | 3.936 | 9.983 | 9.61 | 10.198 | 3.88 | 11.245 | 5.174 | 12.33 |

| **Decrypt** | **ECB** | **CBC** | **CFB** | **OFB** | **CTR** | **XTS** | **GCM** | **CCM** |
|---|---|---|---|---|---|---|---|---|
| File 1 (1KBs) | 0.105 | 0.09 | 0.1 | 0.116 | 0.108 | 0.103 | 0.145 | 0.132 |
| File 2 (50KBs) | 0.298 | 0.315 | 0.335 | 0.4 | 0.217 | 0.381 | 0.364 | 0.453 |
| File 3 (100KBs) | 0.36 | 0.576 | 0.61 | 0.599 | 0.305 | 0.771 | 0.412 | 0.754 |
| File 4 (500KBs) | 1.104 | 2.841 | 2.433 | 2.562 | 1.12 | 2.726 | 1.447 | 3.118 |
| File 5(1MBs) | 2.698 | 5.822 | 5.161 | 5.531 | 2.212 | 6.36 | 2.886 | 6.665 |
| File 6 (2MBs) | 3.93 | 9.96 | 9.638 | 10.184 | 3.903 | 11.67 | 5.202 | 12.225 |

Windows - DES:

| Runtime in WINDOWS (ms) | | | | | |
|---|---|---|---|---|---|
| **Encrypt** | **ECB** | **CBC** | **CFB** | **OFB** | **CTR** |
| File 1 (1KBs) | 0.138 | 0.18 | 0.147 | 0.158 | 0.794 |
| File 2 (50KBs) | 3.02 | 3.456 | 3.22 | 3.32 | 3.28 |
| File 3 (100KBs) | 6.04 | 6.91 | 6.53 | 6.6 | 6.47 |
| File 4 (500KBs) | 30.7 | 31.9 | 30.15 | 30.84 | 31.75 |
| File 5(1MBs) | 61.75 | 64.62 | 62.46 | 62.33 | 64.2 |
| File 6 (2MBs) | 122.37 | 129.05 | 122.1 | 123.67 | 137.87 |

| Decrypt | ECB | CBC | CFB | OFB | CTR |
|---|---|---|---|---|---|
| File 1 (1KBs) | 0.299 | 0.156 | 0.153 | 0.161 | 0.155 |
| File 2 (50KBs) | 3.331 | 3.363 | 3.307 | 3.508 | 3.563 |
| File 3 (100KBs) | 6.838 | 6.357 | 6.375 | 6.588 | 6.6 |
| File 4 (500KBs) | 33.581 | 32.136 | 33.546 | 32.675 | 35.171 |
| File 5(1MBs) | 66.295 | 67.179 | 65.869 | 65.645 | 65.728 |
| File 6 (2MBs) | 128.153 | 127.329 | 141.393 | 129.806 | 129.911 |

Linux - AES:

| Runtime AES in LINUX (ms) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Encrypt** | **ECB** | **CBC** | **CFB** | **OFB** | **CTR** | **XTS** | **GCM** | **CCM** |
| File 1 (1KBs) | 0.024 | 0.022 | 0.019 | 0.019 | 0.056 | 0.019 | 0.026 | 0.019 |
| File 2 (50KBs) | 0.048 | 0.086 | 0.09 | 0.069 | 0.071 | 0.07 | 0.049 | 0.14 |
| File 3 (100KBs) | 0.07 | 0.22 | 0.18 | 0.15 | 0.095 | 0.227 | 0.13 | 0.223 |
| File 4 (500KBs) | 0.612 | 0.888 | 0.898 | 1.283 | 0.45 | 1.279 | 0.48 | 1.2 |
| File 5(1MBs) | 1.257 | 1.788 | 2.069 | 2.412 | 1.505 | 1.538 | 2.351 | 2.467 |
| File 6 (2MBs) | 1.753 | 3.313 | 3.807 | 4.446 | 2.869 | 4.395 | 4.109 | 5.162 |
| | | | | | | | | |
| **Decrypt** | **ECB** | **CBC** | **CFB** | **OFB** | **CTR** | **XTS** | **GCM** | **CCM** |
| File 1 (1KBs) | 0.013 | 0.025 | 0.041 | 0.014 | 0.013 | 0.02 | 0.058 | 0.02 |
| File 2 (50KBs) | 0.032 | 0.041 | 0.046 | 0.087 | 0.04 | 0.067 | 0.078 | 0.097 |
| File 3 (100KBs) | 0.129 | 0.071 | 0.138 | 0.198 | 0.077 | 0.135 | 0.095 | 0.207 |
| File 4 (500KBs) | 0.397 | 0.776 | 0.43 | 0.824 | 0.411 | 0.72 | 0.47 | 0.983 |
| File 5(1MBs) | 0.83 | 0.943 | 0.961 | 2.187 | 0.844 | 1.35 | 1.231 | 1.704 |
| File 6 (2MBs) | 2.861 | 3.484 | 3.664 | 3.941 | 3.299 | 2.883 | 3.286 | 4.345 |

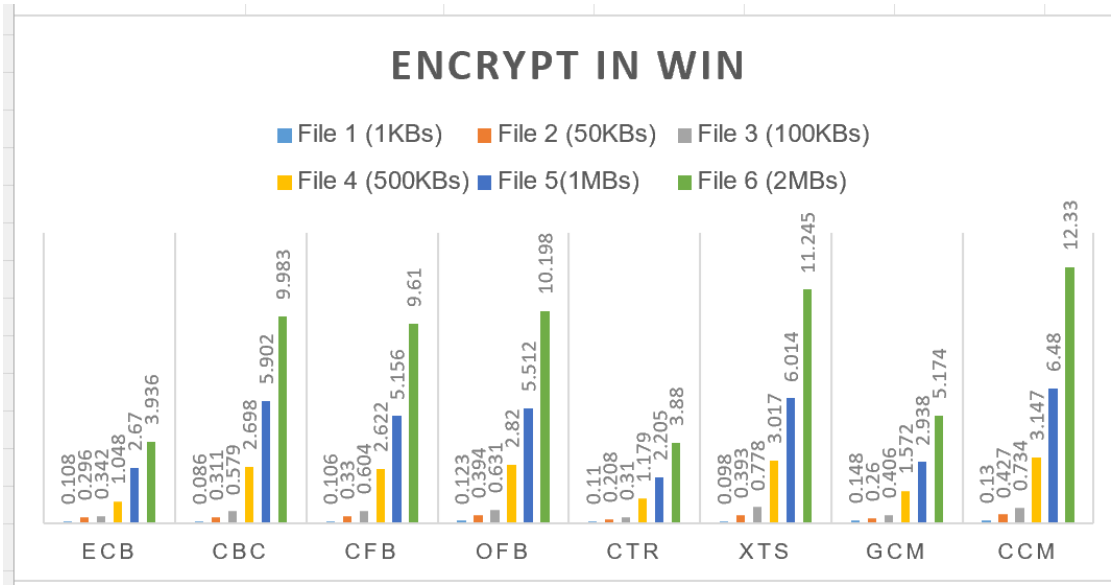
Linux - DES:

| Runtime DES in Linux (ms) | | | | | |
|---|---|---|---|---|---|
| **Encrypt** | **ECB** | **CBC** | **CFB** | **OFB** | **CTR** |
| File 1 (1KBs) | 0.125 | 0.126 | 0.129 | 0.14 | 0.177 |
| File 2 (50KBs) | 0.696 | 1.193 | 0.694 | 0.679 | 0.806 |
| File 3 (100KBs) | 1.772 | 1.352 | 1.632 | 1.989 | 1.374 |
| File 4 (500KBs) | 6.07 | 7.7 | 7.62 | 6.58 | 6.947 |
| File 5(1MBs) | 12.87 | 13.47 | 11.9 | 11.91 | 12.48 |
| File 6 (2MBs) | 21.62 | 24.72 | 23.54 | 24.12 | 24.8 |
| | | | | | |
| **Decrypt** | **ECB** | **CBC** | **CFB** | **OFB** | **CTR** |
| File 1 (1KBs) | 0.166 | 0.104 | 0.113 | 0.125 | 0.112 |
| File 2 (50KBs) | 0.654 | 0.955 | 1.2436 | 0.766 | 13.81 |
| File 3 (100KBs) | 1.642 | 1.243 | 1.366 | 1.571 | 1.8 |
| File 4 (500KBs) | 6.823 | 7.76 | 6.747 | 7.353 | 7.801 |
| File 5(1MBs) | 14.28 | 13.81 | 13.881 | 13.434 | 13.757 |
| File 6 (2MBs) | 42.324 | 24.38 | 32.771 | 35.221 | 35.125 |

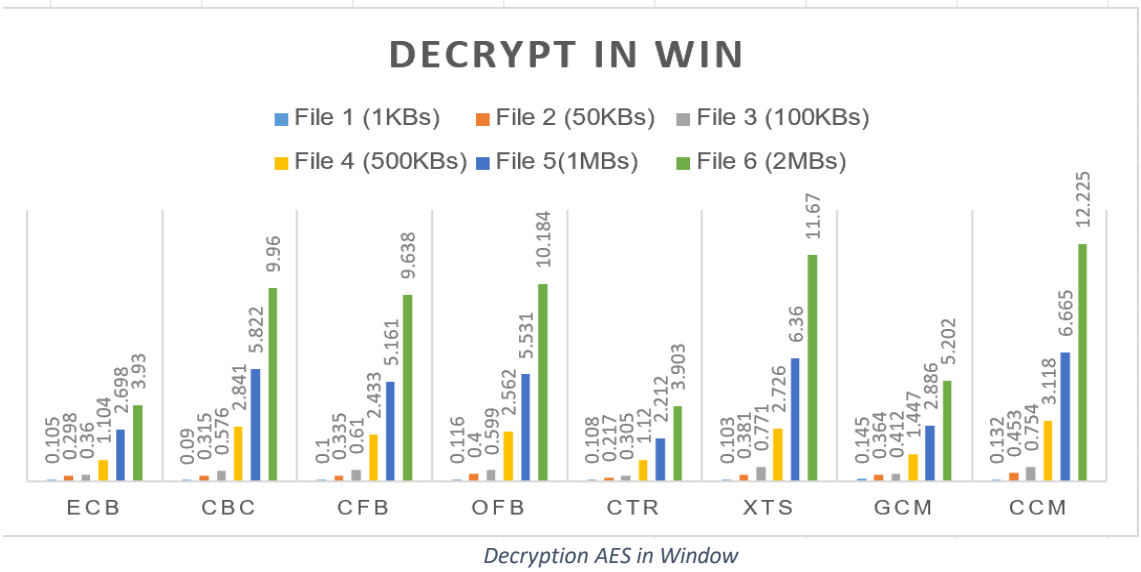
## b. Biểu đồ so sánh.

### 1. Biểu đồ bảng thống kê:

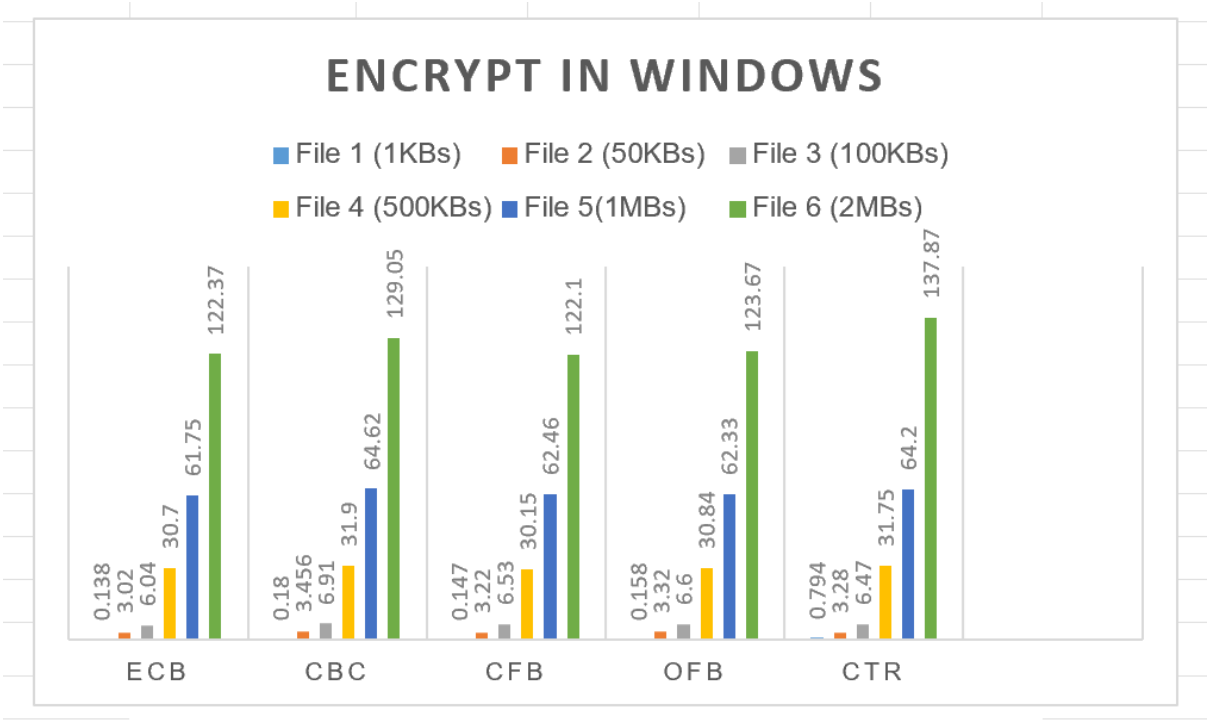
Window :



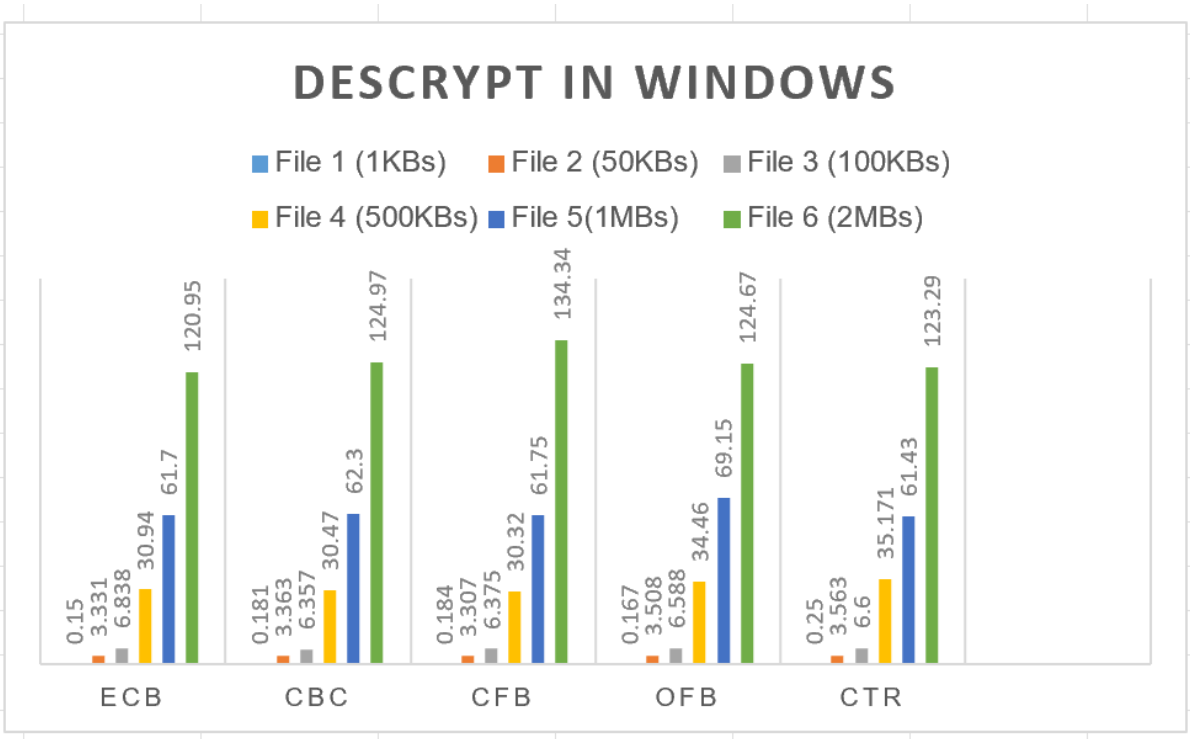

*Encryption AES in Window*




*Decryption AES in Window*

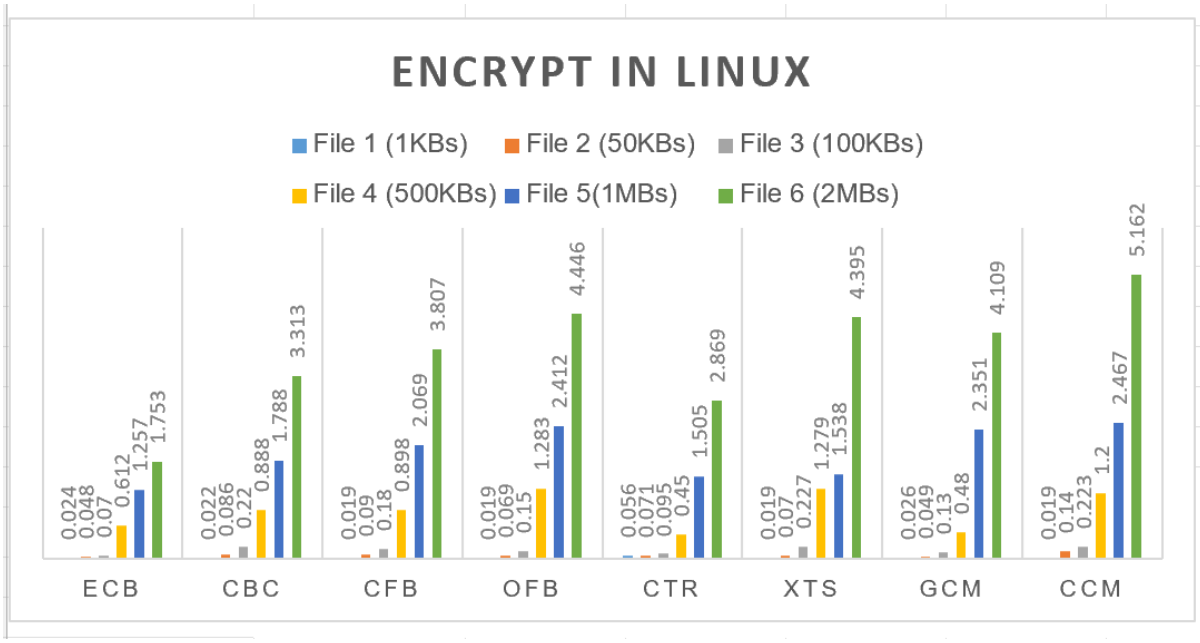



*Encryption DES in Window*

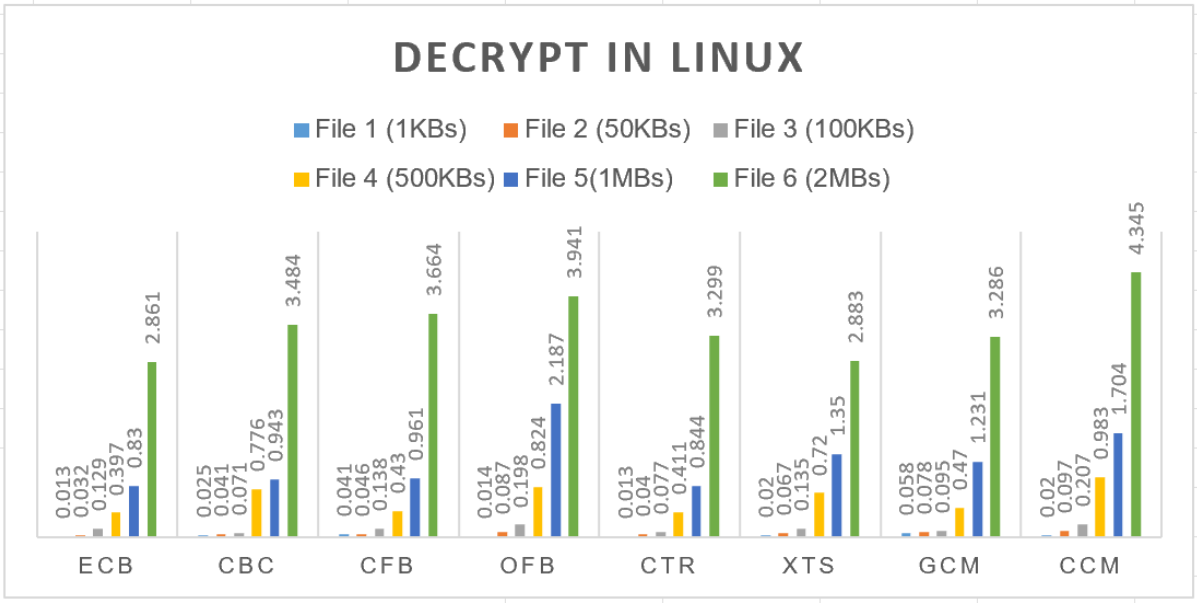



*Decryption DES in Window*

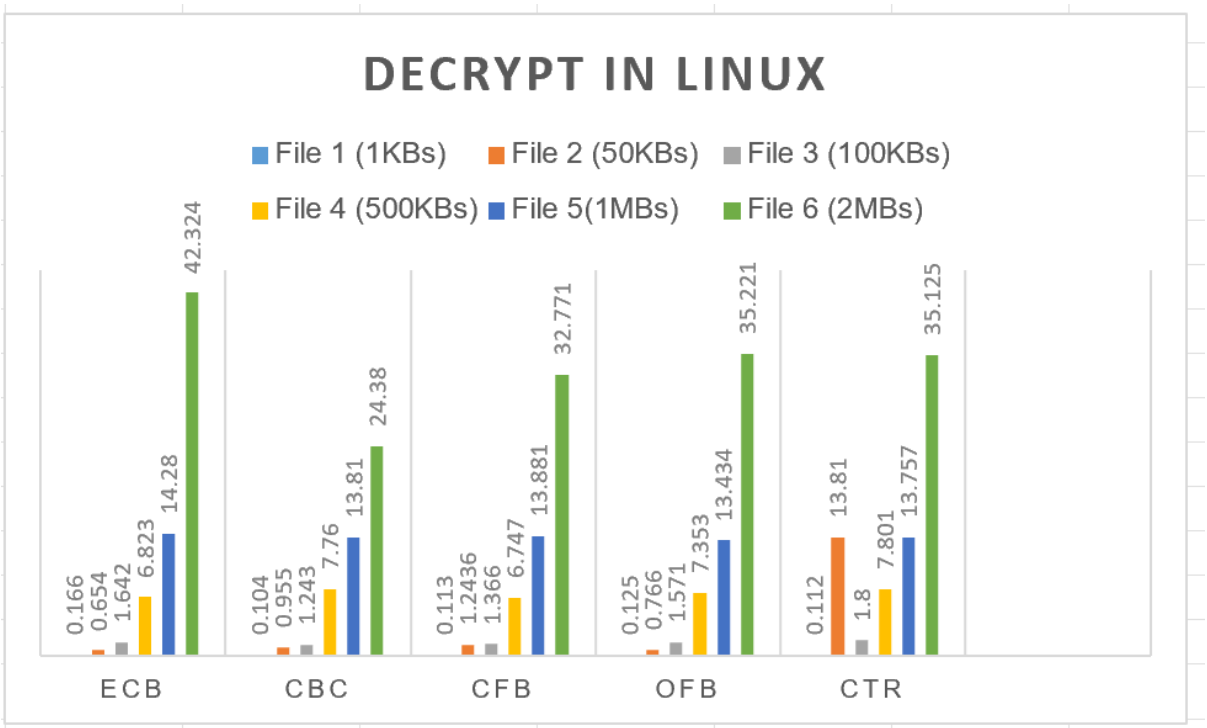
Linux :



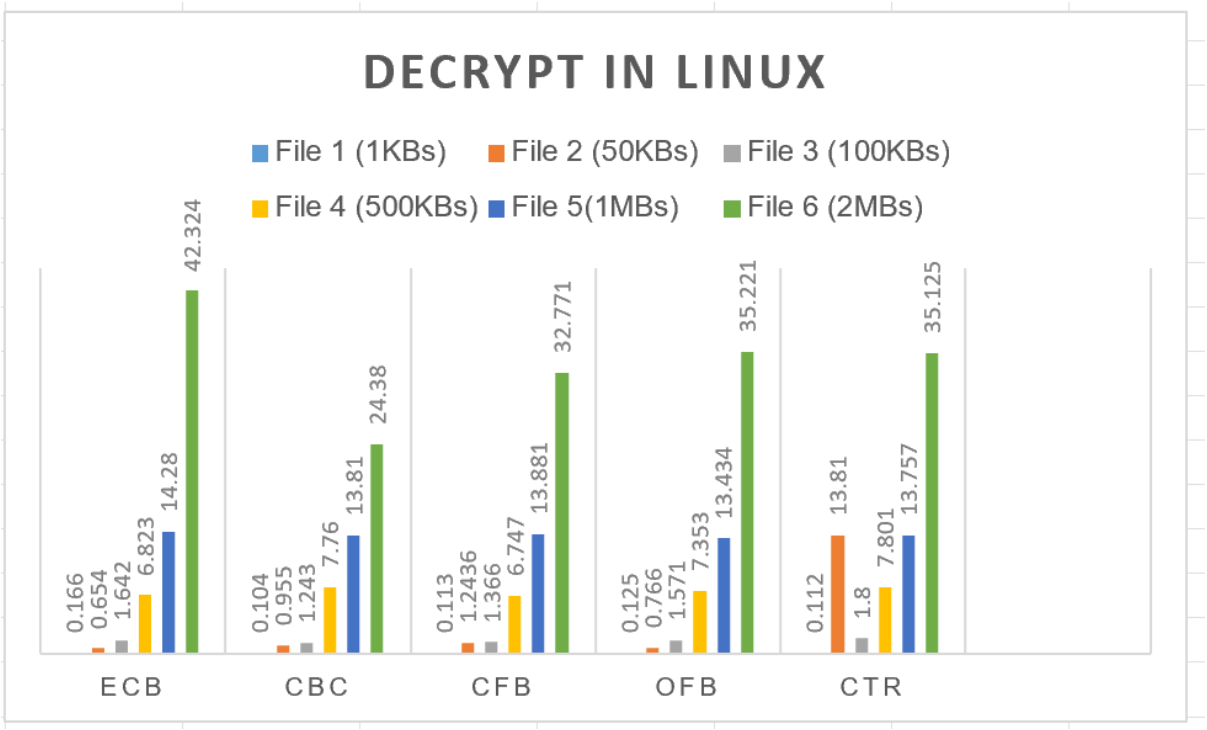

*Encryption AES in Linux*




*Decryption AES in Linux*

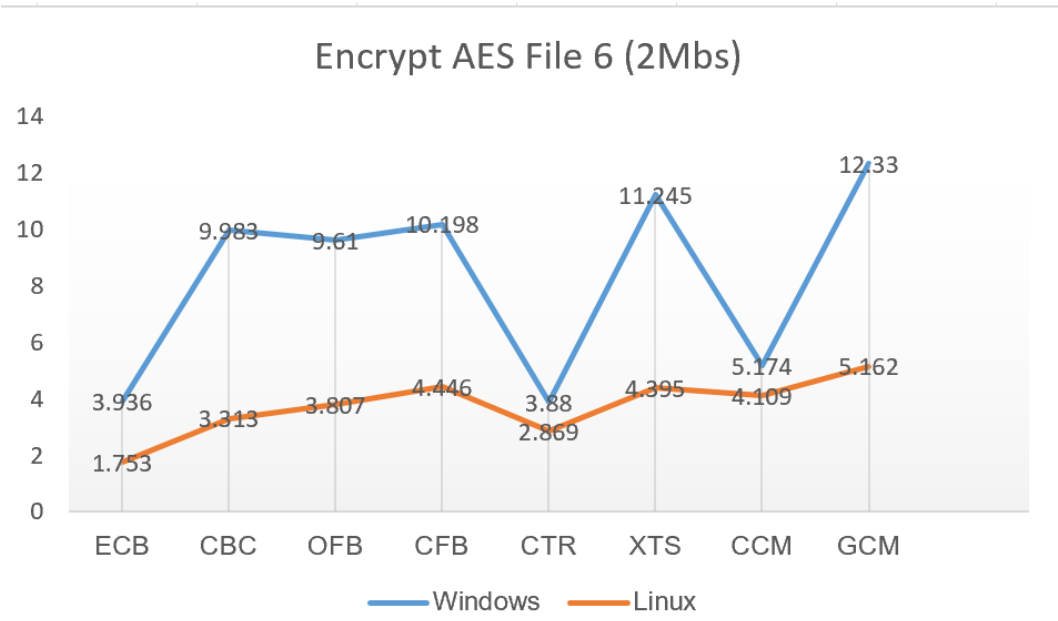


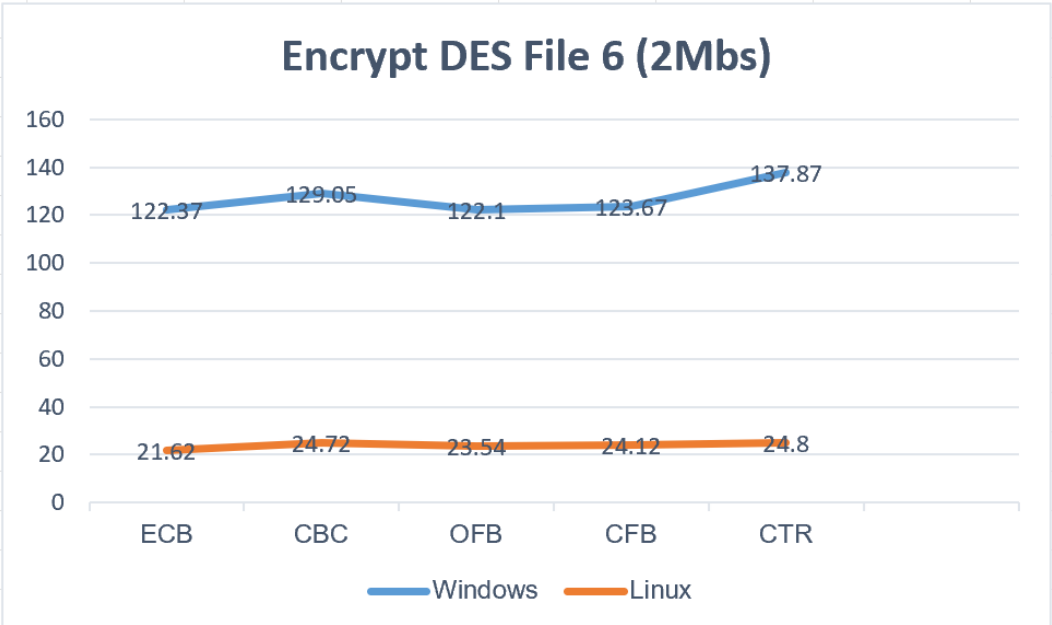

*Encryption DES in Linux*




*Decryption DES in Linux*

**2.So Sánh Windows và Linux :**




## 4. So Sánh :

**AES**: Thời gian mã hóa trên Windows thường chậm hơn so với Linux. Điều này đặc biệt rõ ràng ở các mode CBC, OFB, CFB, XTS và GCM. Điều này có thể cho thấy sự tối ưu hóa của Linux tốt hơn đối với các thuật toán mã hóa hiện đại như AES.

**DES**: Thời gian mã hóa trên Windows cũng chậm hơn đáng kể so với Linux trong tất cả các mode, cho thấy rằng Linux có thể có sự tối ưu hóa tốt hơn cho cả các thuật toán mã hóa cũ như DES.

**Kết Luận**: Linux dường như là hệ điều hành hiệu quả hơn cho việc thực hiện các thuật toán mã hóa, có thể do sự tối ưu hóa trong hệ thống hoặc phần cứng tốt hơn.

Windows, trong trường hợp này, chậm hơn đáng kể cho cả AES và DES, có thể ảnh hưởng đến hiệu suất của các ứng dụng yêu cầu mã hóa nhanh.

## 5. Tổng Kết :

Em đã học cách sử dụng thư viện CryptoPP để thực hiện mã hóa và giải mã AES, cũng như viết mã implement cho các tác vụ này. Em đã biết cách xây dựng và triển khai các task lập trình, thiết lập hệ thống dual boot để kiểm thử trên cả Linux và Windows. Qua việc so sánh thời gian thực thi của các mode mã hóa khác nhau, em nhận thấy hiệu suất của Linux cao hơn so với Windows.