UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTER NETWORK AND COMMUNICATION

Logo, company name

Description automatically generated

**REPORT**

Subject: Cryptography

Semester I (2024 – 2025)

**Report Lab 1**

Student: Nguyễn Huỳnh Nhân

Student ID Number: 23520180

Class: NT219.P22.ANTT

University of Information Technology

Report Lab 1

**Student Information**

Full Name: Nguyễn Huỳnh Nhân

Student ID Number: 23520180

Class: ATTT2023.2

**Device Information**

CPU: 11th Gen Intel(R) Core(TM) i5-1135G7

Ram: 16 GB DDR4 3200MHz

SSD PCle: 512GB

**DES**

key: 1895B914382E36C0

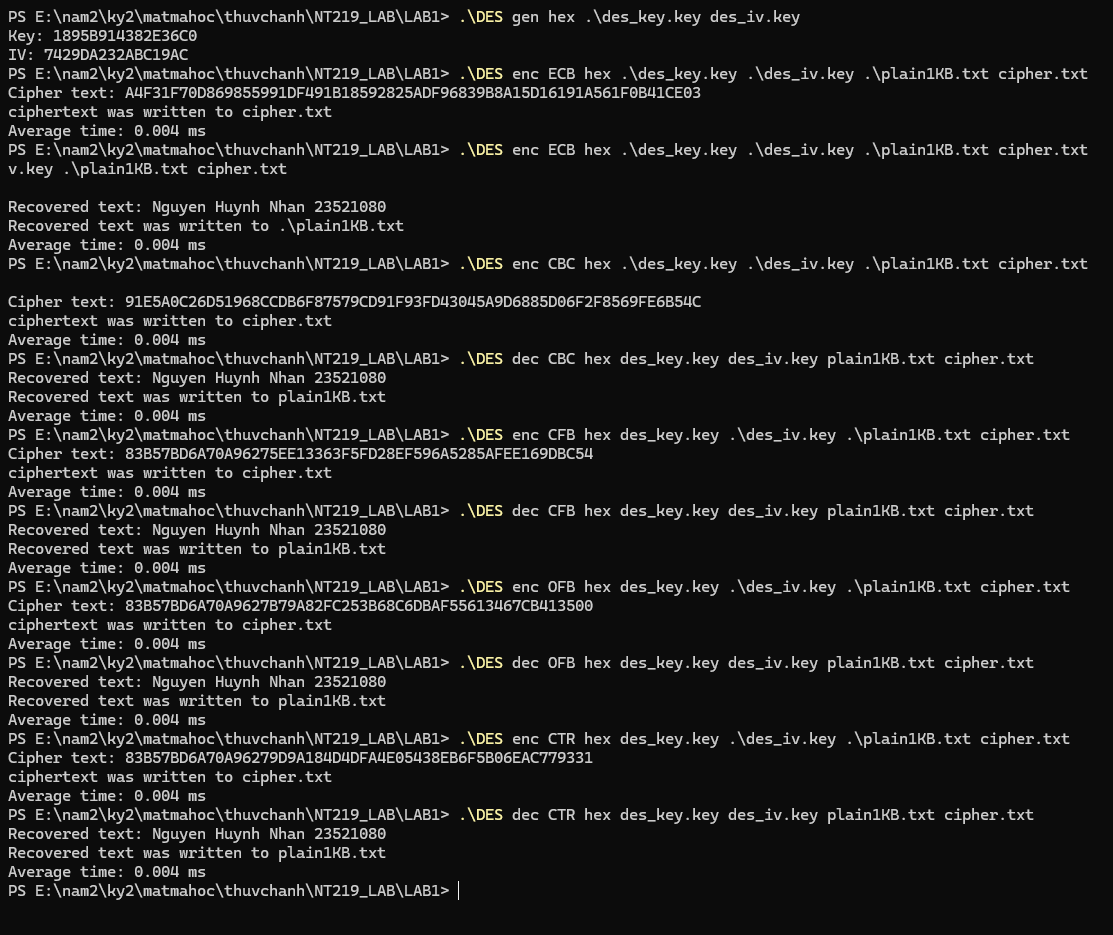
iv:7429DA232ABC19AC

**Plain1KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.004 ms | 0.004 ms | 0.007 ms | 0.007 ms |
| CBC | 0.004 ms | 0.004 ms | 0.007 ms | 0.007 ms |
| CFB | 0.004 ms | 0.004 ms | 0.007 ms | 0.007 ms |
| OFB | 0.004 ms | 0.004 ms | 0.007 ms | 0.007 ms |
| CTR | 0.004 ms | 0.004 ms | 0.008 ms | 0.008 ms |

A computer screen with text

Description automatically generated

A screen shot of a computer screen

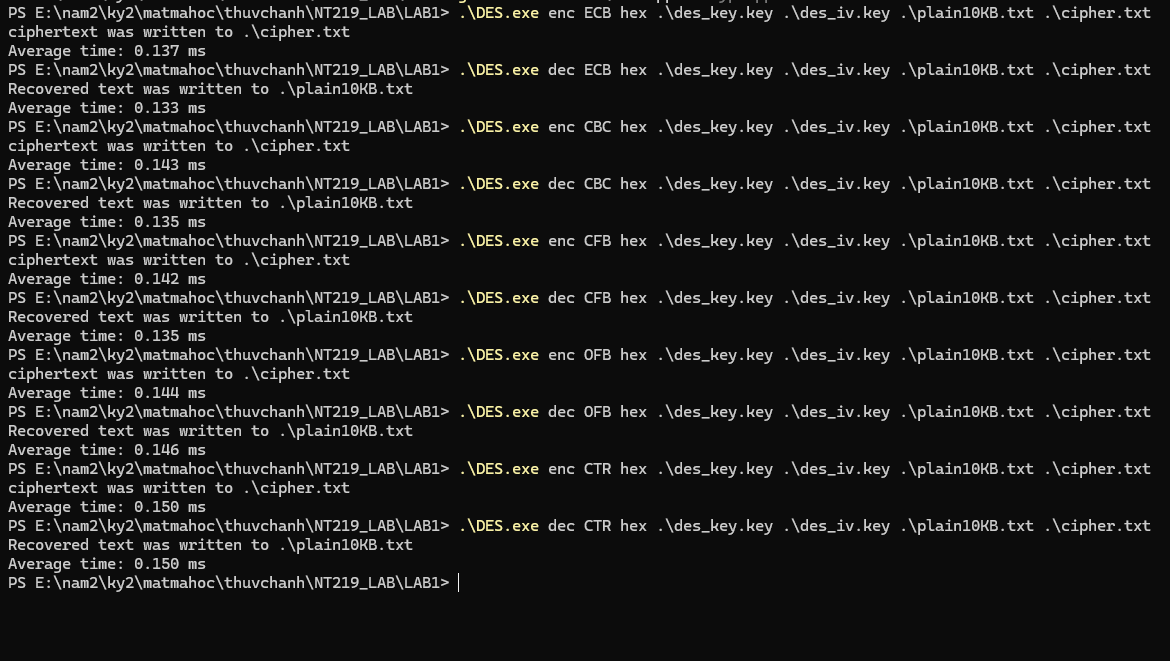
Description automatically generated

A screenshot of a computer program

Description automatically generated

**Plain10KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.137 ms | 0.133 ms | 0.096 ms | 0.093 ms |
| CBC | 0.143 ms | 0.135 ms | 0.107 ms | 0.096 ms |
| CFB | 0.142 ms | 0.135 ms | 0.103 ms | 0.094 ms |
| OFB | 0.144 ms | 0.146 ms | 0.103 ms | 0.103 ms |
| CTR | 0.150 ms | 0.150 ms | 0.111 ms | 0.108 ms |

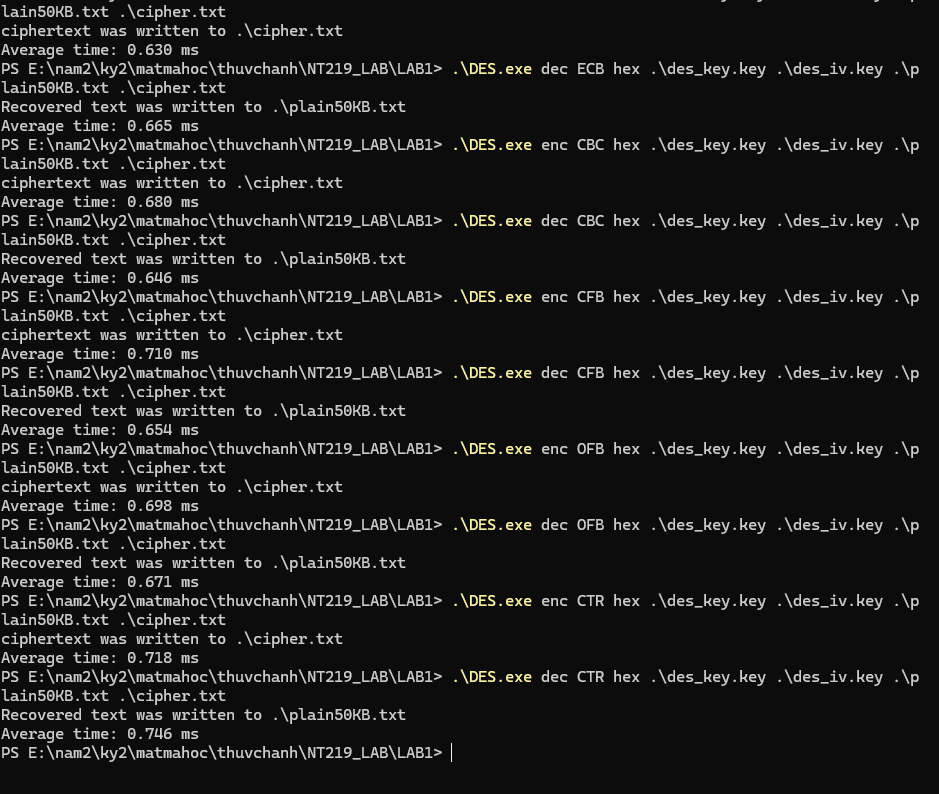


A screenshot of a computer program

Description automatically generated

**Plain50KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.630 ms | 0.665 ms | 0.448 ms | 0.447 ms |
| CBC | 0.680 ms | 0.646 ms | 0.497 ms | 0.450 ms |
| CFB | 0.710 ms | 0.645 ms | 0.497 ms | 0.451 ms |
| OFB | 0.698 ms | 0.671 ms | 0.495 ms | 0.484 ms |
| CTR | 0.718 ms | 0.746 ms | 0.535 ms | 0.520 ms |

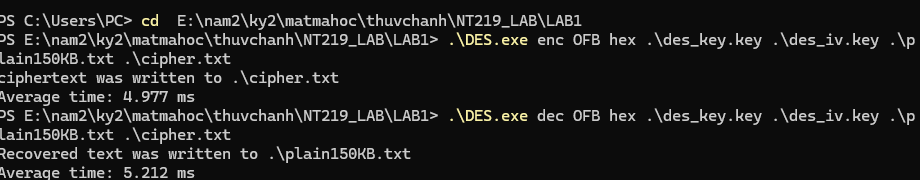


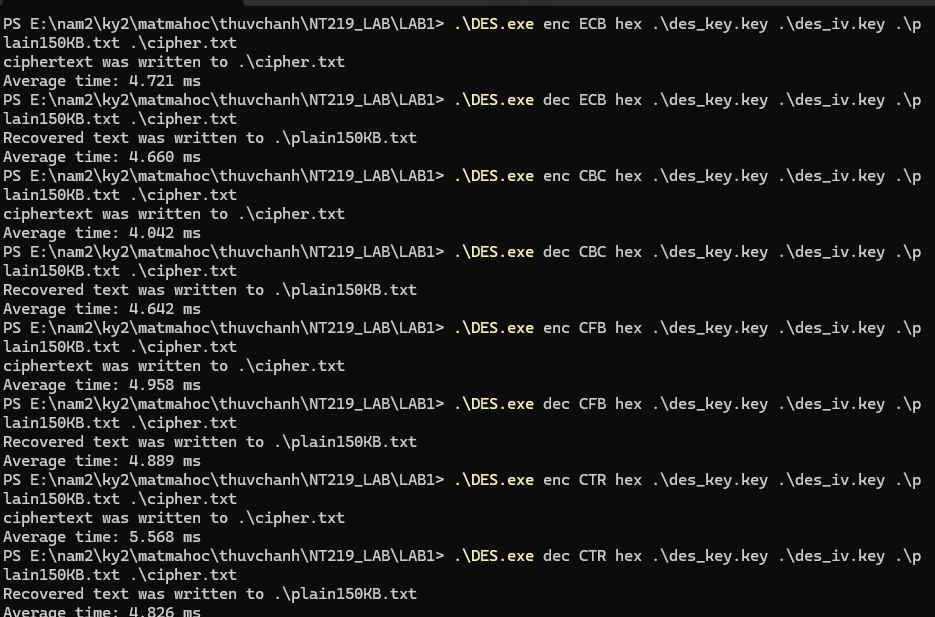
A screenshot of a computer program

Description automatically generated

**Plain150KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 4.721 ms | 4.660 ms | 1.358 ms | 1.351 ms |
| CBC | 4.042 ms | 4.642 ms | 1.508 ms | 1.359 ms |
| CFB | 4.958 ms | 4.889 ms | 1.460 ms | 1.364 ms |
| OFB | 4.977 ms | 5.212 ms | 1.462 ms | 1.458 ms |
| CTR | 5.568 ms | 4.826 ms | 1.585 ms | 1.592 ms |



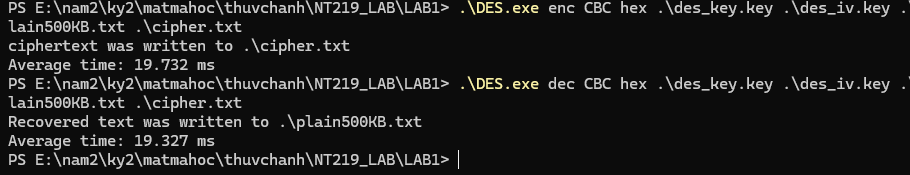
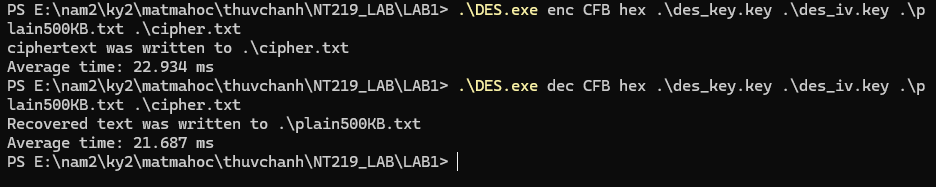
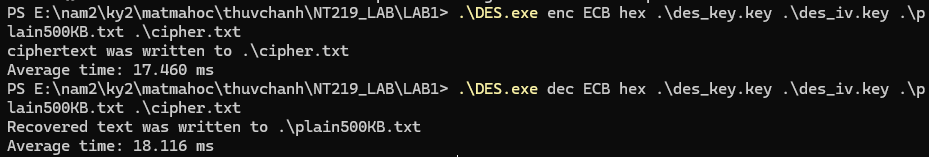
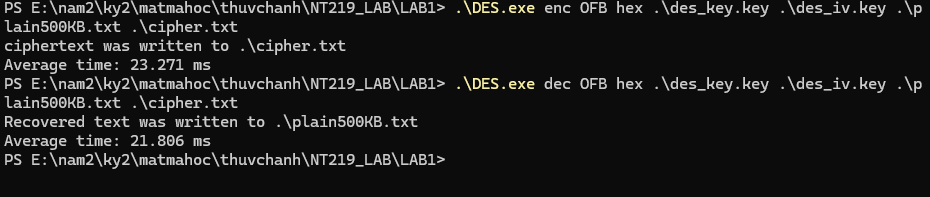
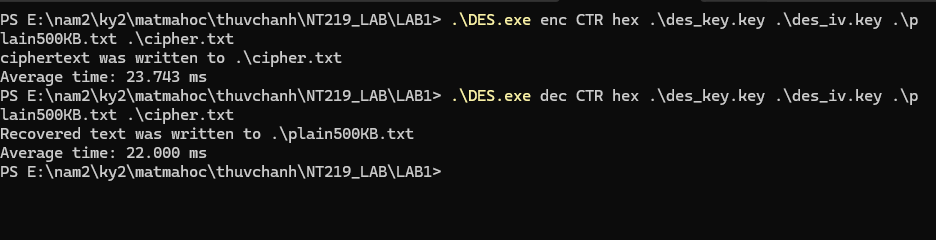


A screenshot of a computer program

Description automatically generated

**Plain500KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 17.460 ms | 18.116 ms | 4.517 ms | 4.507 ms |
| CBC | 19.732 ms | 19.327 ms | 5.072 ms | 4.537 ms |
| CFB | 22.934 ms | 21.687 ms | 4.866 ms | 4.537 ms |
| OFB | 23.271 ms | 21.806 ms | 4.909 ms | 4.870 ms |
| CTR | 23.743 ms | 22.000 ms | 5.281 ms | 5.285 ms |

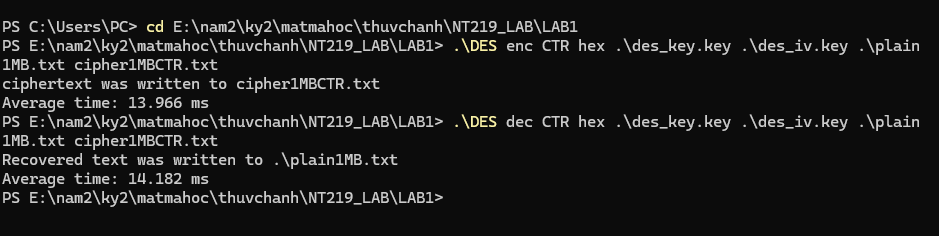
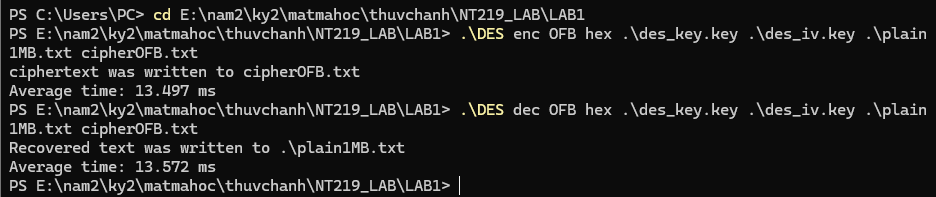
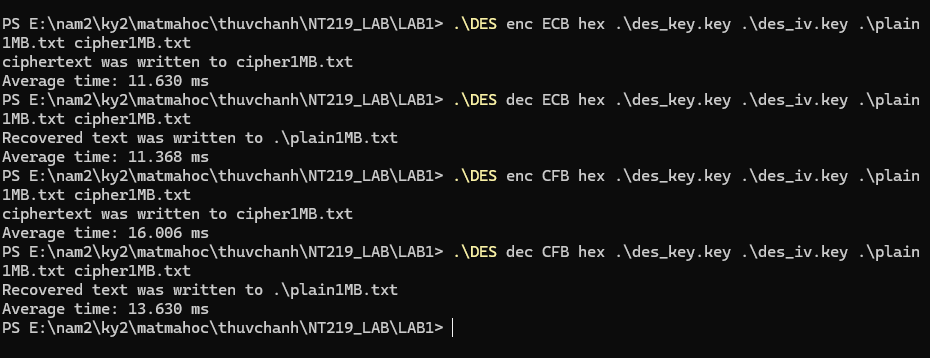


A screenshot of a computer program

Description automatically generated

**Plain1MB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 11.630 ms | 11.368 ms | 9.310 ms | 9.339 ms |
| CBC | 15.726 ms | 13.387 ms | 10.347 ms | 9.502 ms |
| CFB | 13.497 ms | 13.630 ms | 10.011 ms | 9.393 ms |
| OFB | 13.497 ms | 13.572 ms | 10.121 ms | 10.116 ms |
| CTR | 13.966 ms | 14.182 ms | 10.828 ms | 10.831 ms |



A computer screen with white text

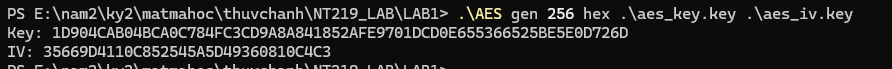
Description automatically generated

A screenshot of a computer program

Description automatically generated

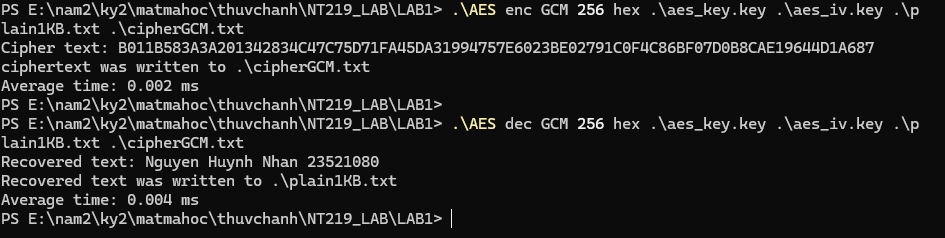
**AES**

Key: 1D904CAB04BCA0C784FC3CD9A8A841852AFE9701DCD0E655366525BE5E0D726D

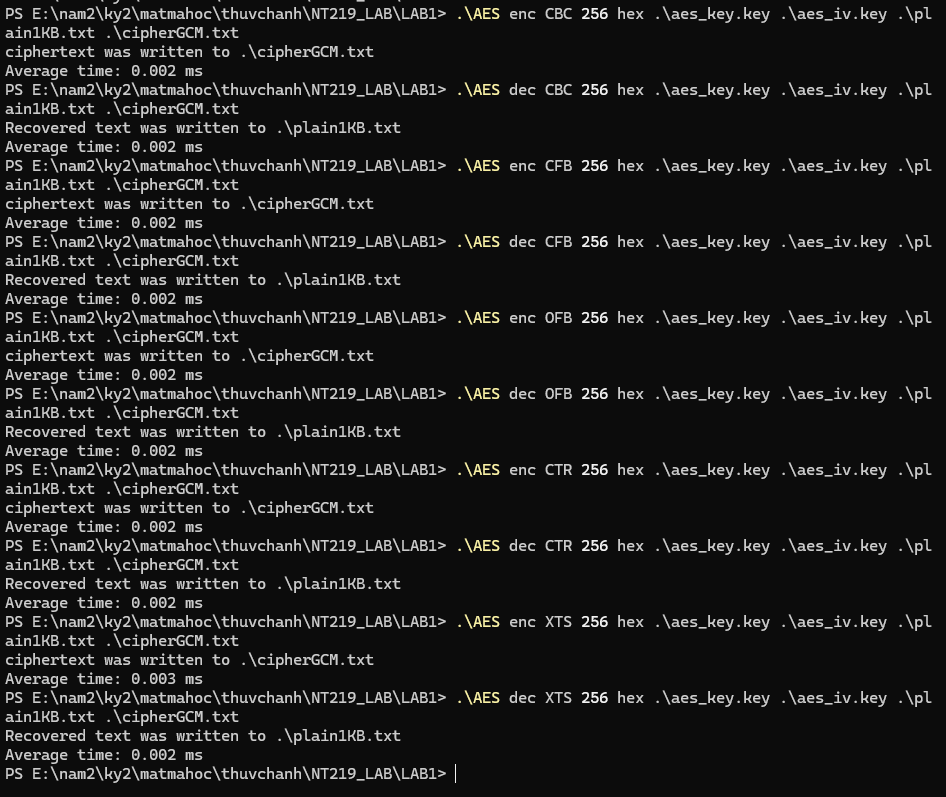
IV: 35669D4110C852545A5D49360810C4C3

**Plain1KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.002 ms | 0.002 ms | 0.002 ms | 0.002 ms |
| CBC | 0.002 ms | 0.002 ms | 0.002 ms | 0.002 ms |
| CFB | 0.002 ms | 0.002 ms | 0.002 ms | 0.002 ms |
| OFB | 0.002 ms | 0.002 ms | 0.002 ms | 0.002 ms |
| CTR | 0.002 ms | 0.002 ms | 0.002 ms | 0.002 ms |
| XTS | 0.003 ms | 0.002 ms | 0.002 ms | 0.002 ms |
| GCM | 0.002 ms | 0.004 ms | 0.002 ms | 0.003 ms |



A computer screen with white text

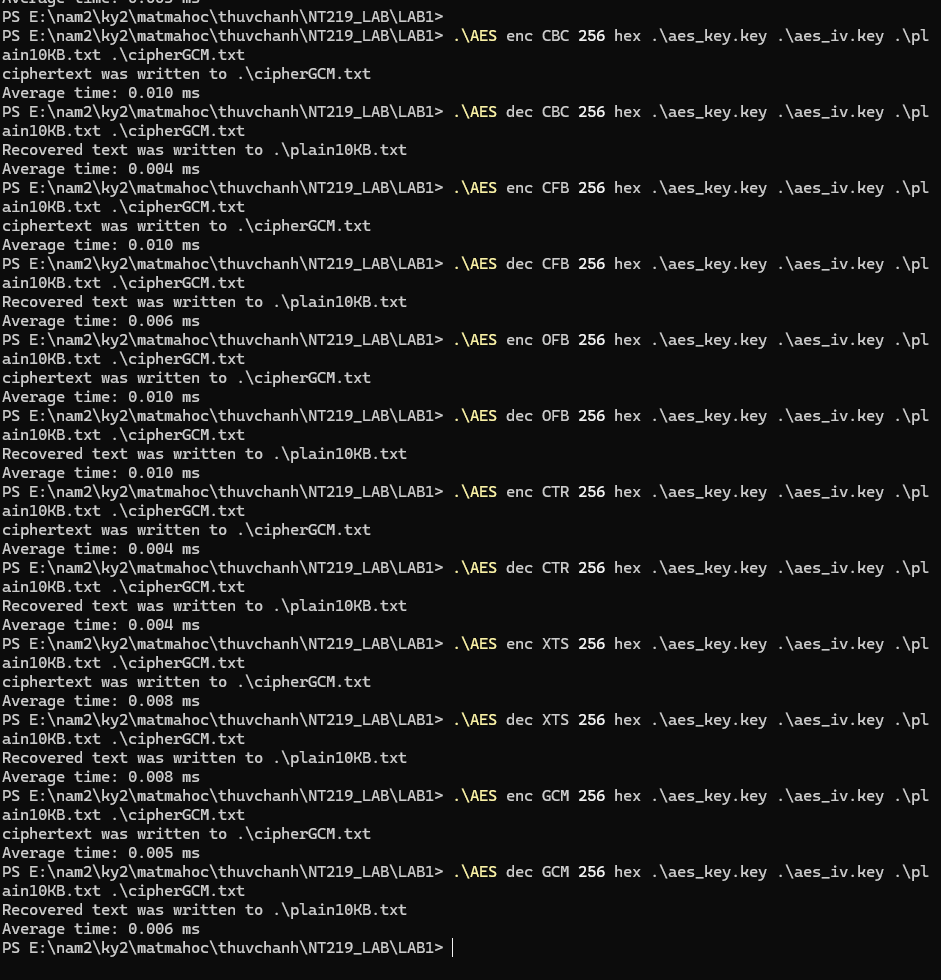
Description automatically generated

A screenshot of a computer program

Description automatically generated

**Plain10KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.003 ms | 0.003 ms | 0.007 ms | 0.007 ms |
| CBC | 0.010 ms | 0.004 ms | 0.015 ms | 0.008 ms |
| CFB | 0.010 ms | 0.006 ms | 0.015 ms | 0.007 ms |
| OFB | 0.010 ms | 0.010 ms | 0.015 ms | 0.015 ms |
| CTR | 0.004 ms | 0.004 ms | 0.007 ms | 0.007 ms |
| XTS | 0.008 ms | 0.008 ms | 0.012 ms | 0.014 ms |
| GCM | 0.005 ms | 0.006 ms | 0.009 ms | 0.010 ms |

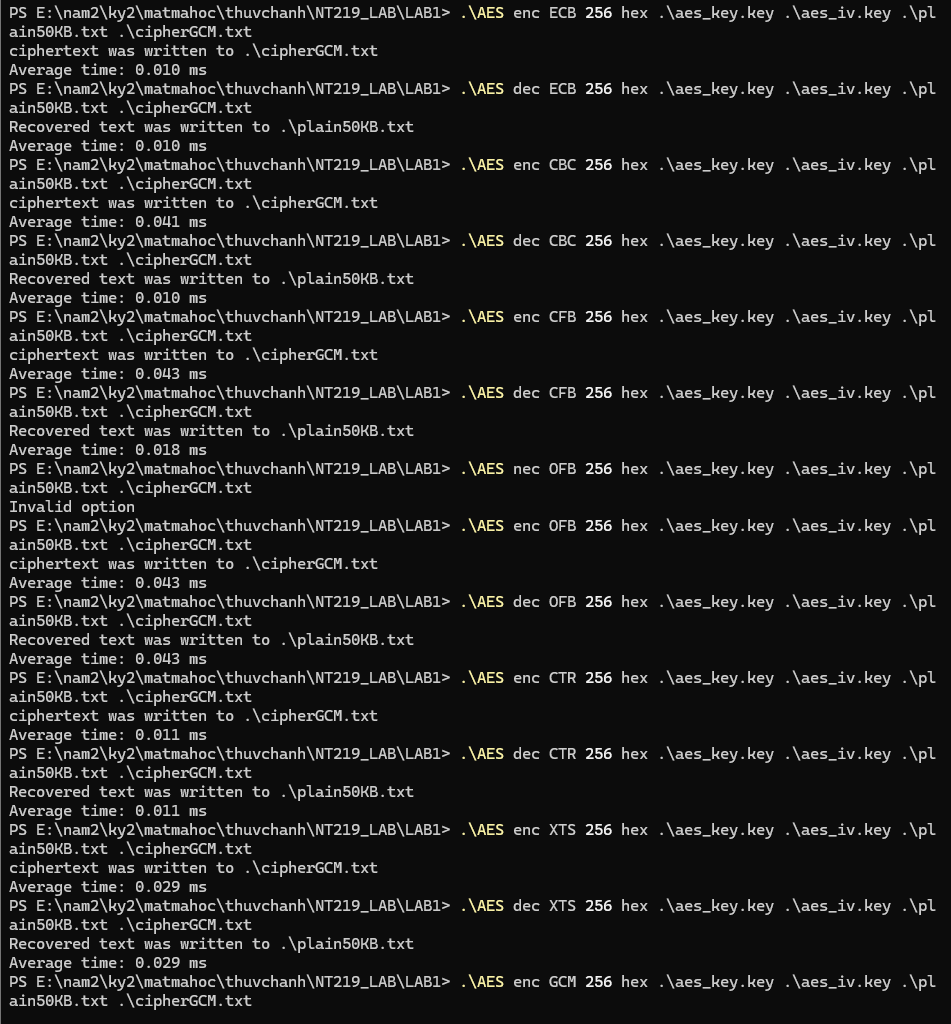


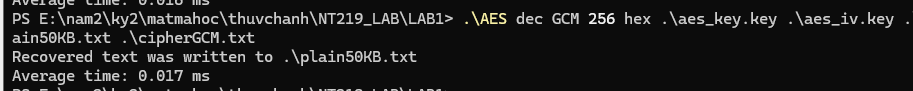
A screenshot of a computer program

Description automatically generated

**Plain50KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.010 ms | 0.010 ms | 0.029 ms | 0.029 ms |
| CBC | 0.041 ms | 0.010 ms | 0.067 ms | 0.042 ms |
| CFB | 0.043 ms | 0.018 ms | 0.081 ms | 0.040 ms |
| OFB | 0.043 ms | 0.043 ms | 0.081 ms | 0.080 ms |
| CTR | 0.011 ms | 0.011 ms | 0.043 ms | 0.044 ms |
| XTS | 0.029 ms | 0.029 ms | 0.053 ms | 0.067 ms |
| GCM | 0.016 ms | 0.017 ms | 0.038 ms | 0.038 ms |



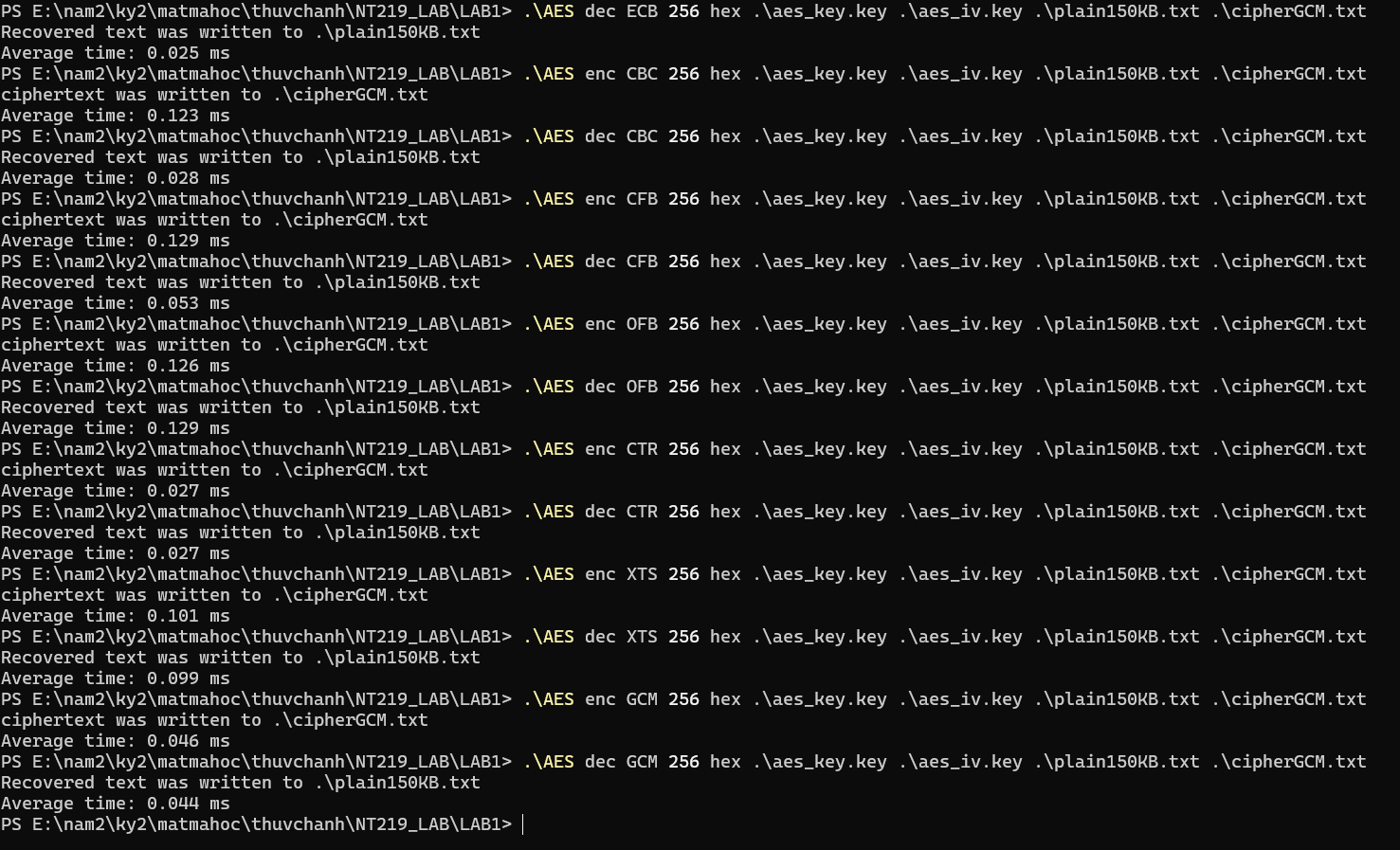


A screenshot of a computer program

Description automatically generated

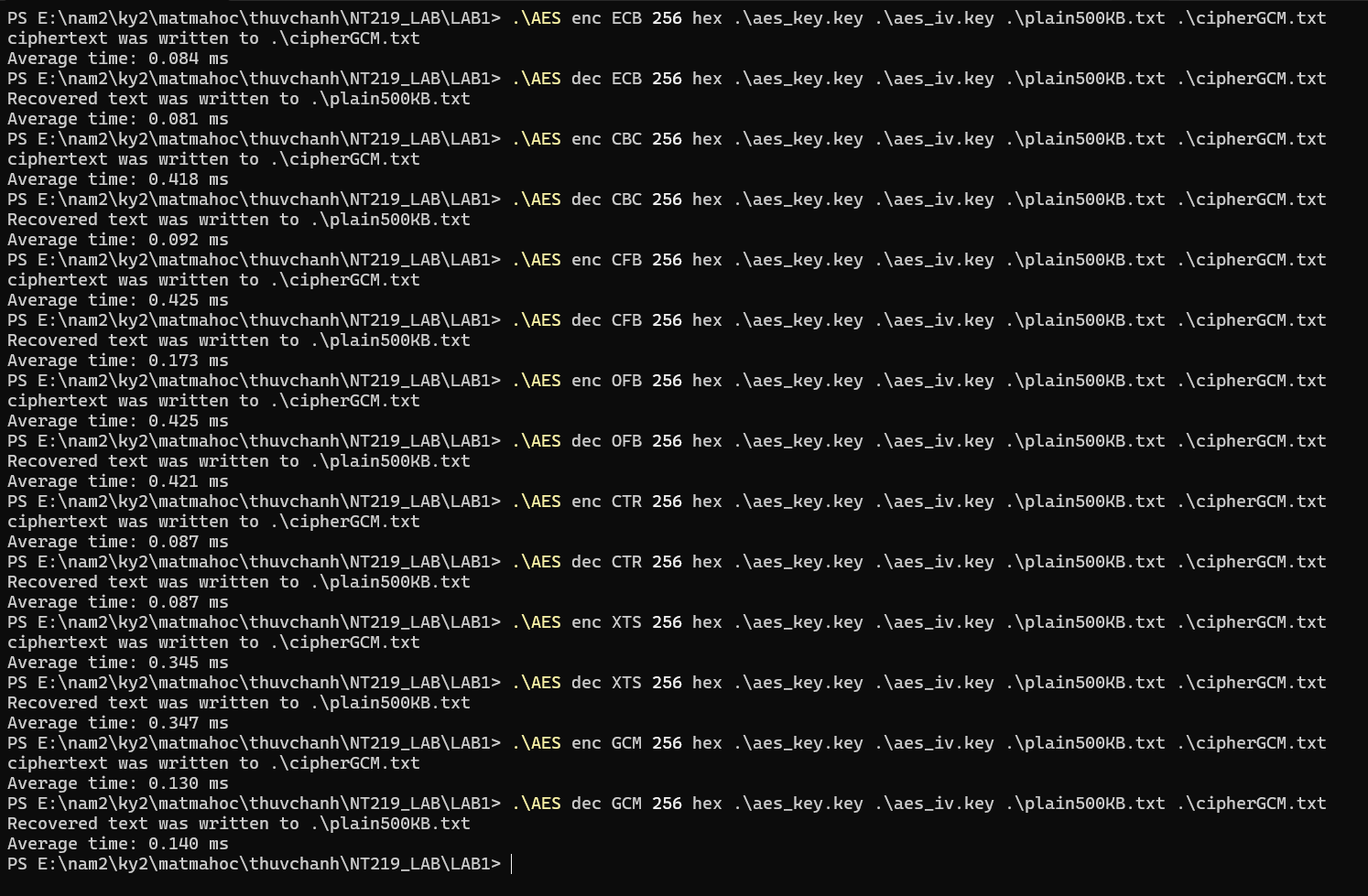
**Plain150KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.025 ms | 0.025 ms | 0.086 ms | 0.090 ms |
| CBC | 0.123 ms | 0.028 ms | 0.202 ms | 0.129 ms |
| CFB | 0.129 ms | 0.053 ms | 0.201 ms | 0.124 ms |
| OFB | 0.126 ms | 0.129 ms | 0.202 ms | 0.243 ms |
| CTR | 0.027 ms | 0.027 ms | 0.091 ms | 0.132 ms |
| XTS | 0.101 ms | 0.099 ms | 0.167 ms | 0.205 ms |
| GCM | 0.046 ms | 0.044 ms | 0.112 ms | 0.111 ms |



**Plain500KB.txt**

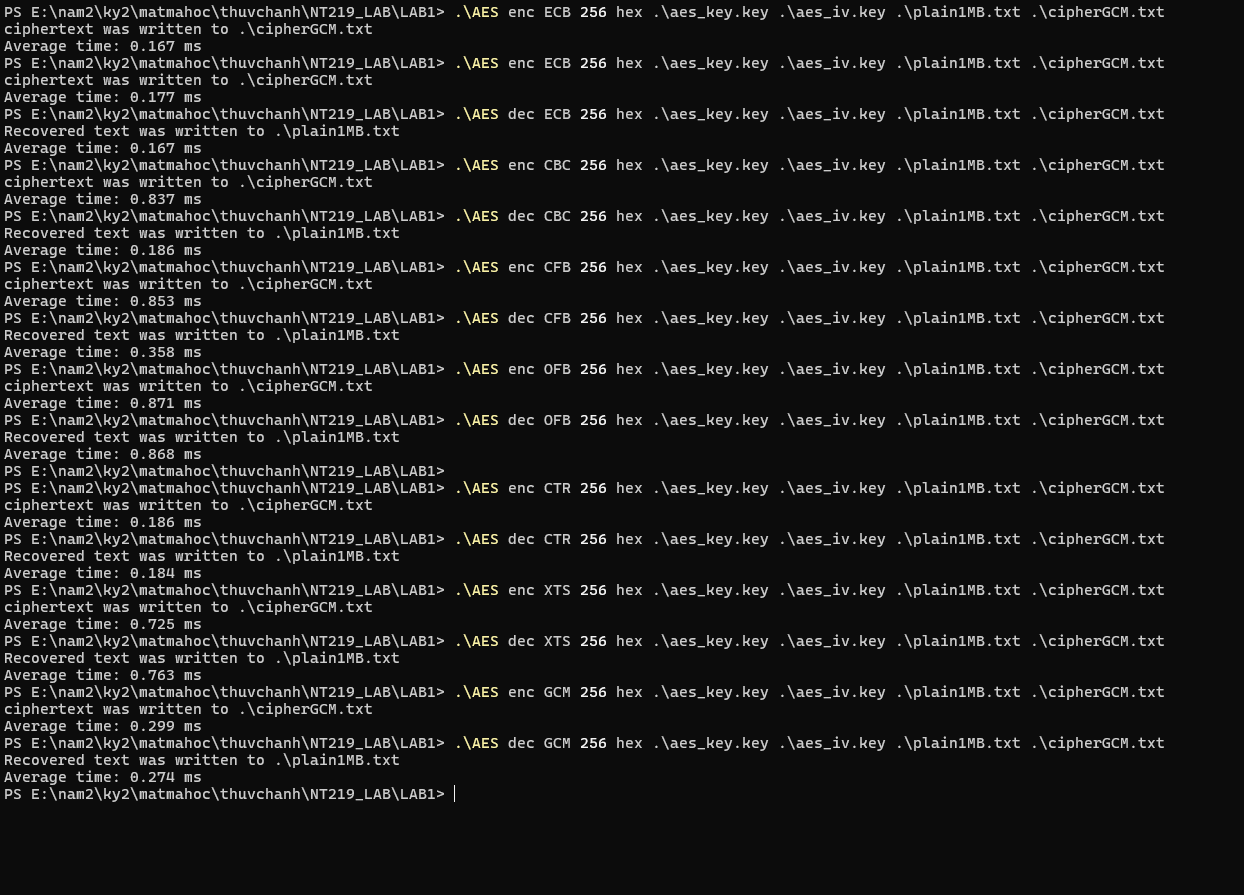
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.084 ms | 0.081 ms | 0.288 ms | 0.289 ms |
| CBC | 0.418 ms | 0.092 ms | 0.667 ms | 0.296 ms |
| CFB | 0.425 ms | 0.173 ms | 0.665 ms | 0.270 ms |
| OFB | 0.425 ms | 0.421 ms | 0.672 ms | 0.674 ms |
| CTR | 0.087 ms | 0.087 ms | 0.302 ms | 0.305 ms |
| XTS | 0.345 ms | 0.347 ms | 0.547 ms | 0.543 ms |
| GCM | 0.130 ms | 0.140 ms | 0.373 ms | 0.366 ms |

A screenshot of a computer program

Description automatically generated

**Plain1MB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.177 ms | 0.167 ms | 0.585 ms | 0.581 ms |
| CBC | 0.837 ms | 0.186 ms | 1.356 ms | 0.608 ms |
| CFB | 0.853 ms | 0.358 ms | 1.377 ms | 0.544 ms |
| OFB | 0.871 ms | 0.868 ms | 1.371 ms | 1.389 ms |
| CTR | 0.186 ms | 0.184 ms | 0.628 ms | 0.620 ms |
| XTS | 0.725 ms | 0.763 ms | 1.129 ms | 1.117 ms |
| GCM | 0.299 ms | 0.274 ms | 0.760 ms | 0.763 ms |



A screenshot of a computer program

Description automatically generated

**Comments and Comparison:**

* Executing the code in Linux is faster than Window in 6 testcases
* Time execute increase as same as the increase of file size
* There are not much different in time execute in 5 modes in DES among 6 testcases
* There are not much different in time execute in 7 modes in AES among 6 testcases
* AES is much faster than DES
* AES\_GCM mode has more execute time than other mode on Window