UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTER NETWORK AND COMMUNICATION

Logo, company name

Description automatically generated

**REPORT**

Subject: Cryptography

Semester II (2023 – 2024)

**Report Lab 1**

Student: Võ Ngọc Bảo

Student ID Number: 22520127

Class: NT219.O22.ANTT

University of Information Technology

Lecturer: Nguyễn Ngọc Tự

**Hồ Chí Minh City, June 2024**

Report Lab 1

**Student Information**

Full Name: Võ Ngọc Bảo

Student ID Number: 22520127

Class: ATTT2022.1

**Device Information**

CPU: AMD Ryzen 5 5600H 3.30 GHz

Ram: 8 GB DDR4 3200MHz

SSD PCle: 512GB

**DES**

key: F1C06DD52A2FF0C1

iv: 0E6AB8F0DBBE91C7

A black background with white text

Description automatically generated

**Plain1KB.txt**

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

A screen shot of a computer screen

Description automatically generated

A computer screen with text

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

**Plain10KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.096 ms | 0.097 ms | 0.096 ms | 0.093 ms |
| CBC | 0.110 ms | 0.098 ms | 0.107 ms | 0.096 ms |
| CFB | 0.106 ms | 0.098 ms | 0.103 ms | 0.094 ms |
| OFB | 0.107 ms | 0.106 ms | 0.103 ms | 0.103 ms |
| CTR | 0.115 ms | 0.115 ms | 0.111 ms | 0.108 ms |

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

**Plain50KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.468 ms | 0.468 ms | 0.448 ms | 0.447 ms |
| CBC | 0.533 ms | 0.473 ms | 0.497 ms | 0.450 ms |
| CFB | 0.515 ms | 0.469 ms | 0.497 ms | 0.451 ms |
| OFB | 0.515 ms | 0.517 ms | 0.495 ms | 0.484 ms |
| CTR | 0.555 ms | 0.553 ms | 0.535 ms | 0.520 ms |

**A screenshot of a computer screen

Description automatically generated**

A screenshot of a computer program

Description automatically generated

**Plain150KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 1.429 ms | 1.437 ms | 1.358 ms | 1.351 ms |
| CBC | 1.628 ms | 1.439 ms | 1.508 ms | 1.359 ms |
| CFB | 1.567 ms | 1.563 ms | 1.460 ms | 1.364 ms |
| OFB | 1.563 ms | 1.571 ms | 1.462 ms | 1.458 ms |
| CTR | 1.683 ms | 1.679 ms | 1.585 ms | 1.592 ms |

**A screenshot of a computer program

Description automatically generated**

A screenshot of a computer program

Description automatically generated

**Plain500KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 4.811 ms | 4.782 ms | 4.517 ms | 4.507 ms |
| CBC | 5.406 ms | 4.846 ms | 5.072 ms | 4.537 ms |
| CFB | 5.238 ms | 4.808 ms | 4.866 ms | 4.537 ms |
| OFB | 5.219 ms | 5.229 ms | 4.909 ms | 4.870 ms |
| CTR | 5.623 ms | 5.621 ms | 5.281 ms | 5.285 ms |

**A screenshot of a computer program

Description automatically generated**

A screenshot of a computer program

Description automatically generated

**Plain1MB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 9.757 ms | 9.716 ms | 9.310 ms | 9.339 ms |
| CBC | 11.039 ms | 9.797 ms | 10.347 ms | 9.502 ms |
| CFB | 10.704 ms | 9.986 ms | 10.011 ms | 9.393 ms |
| OFB | 10.715 ms | 10.817 ms | 10.121 ms | 10.116 ms |
| CTR | 11.486 ms | 11.507 ms | 10.828 ms | 10.831 ms |

**A screenshot of a computer program

Description automatically generated**

A computer screen with white text

Description automatically generated

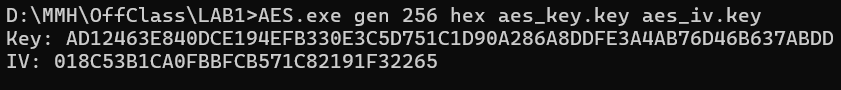
A screenshot of a computer program

Description automatically generated

**AES**

key: AD12463E840DCE194EFB330E3C5D751C1D90A286A8DDFE3A4AB76D46B637ABDD

iv: 018C53B1CA0FBBFCB571C82191F32265



**Plain1KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.003 ms | 0.003 ms | 0.002 ms | 0.002 ms |
| CBC | 0.004 ms | 0.004 ms | 0.002 ms | 0.002 ms |
| CFB | 0.004 ms | 0.004 ms | 0.002 ms | 0.002 ms |
| OFB | 0.004 ms | 0.004 ms | 0.002 ms | 0.002 ms |
| CTR | 0.004 ms | 0.004 ms | 0.002 ms | 0.002 ms |
| XTS | 0.004 ms | 0.004 ms | 0.002 ms | 0.002 ms |
| GCM | 0.005 ms | 0.006 ms | 0.002 ms | 0.003 ms |

A black and white screen with white text

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

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 | 0.046 ms | 0.048 ms | 0.007 ms | 0.007 ms |
| CBC | 0.048 ms | 0.048 ms | 0.015 ms | 0.008 ms |
| CFB | 0.047 ms | 0.047 ms | 0.015 ms | 0.007 ms |
| OFB | 0.047 ms | 0.048 ms | 0.015 ms | 0.015 ms |
| CTR | 0.047 ms | 0.052 ms | 0.007 ms | 0.007 ms |
| XTS | 0.045 ms | 0.045 ms | 0.012 ms | 0.014 ms |
| GCM | 0.058 ms | 0.058 ms | 0.009 ms | 0.010 ms |

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

**Plain50KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.224 ms | 0.225 ms | 0.029 ms | 0.029 ms |
| CBC | 0.232 ms | 0.229 ms | 0.067 ms | 0.042 ms |
| CFB | 0.229 ms | 0.231 ms | 0.081 ms | 0.040 ms |
| OFB | 0.228 ms | 0.228 ms | 0.081 ms | 0.080 ms |
| CTR | 0.231 ms | 0.230 ms | 0.043 ms | 0.044 ms |
| XTS | 0.211 ms | 0.201 ms | 0.053 ms | 0.067 ms |
| GCM | 0.272 ms | 0.277 ms | 0.038 ms | 0.038 ms |

**A screenshot of a computer program

Description automatically generated**

**A computer screen with white text

Description automatically generated**

A screenshot of a computer program

Description automatically generated

**Plain150KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.689 ms | 0.683 ms | 0.086 ms | 0.090 ms |
| CBC | 0.712 ms | 0.692 ms | 0.202 ms | 0.129 ms |
| CFB | 0.687 ms | 0.688 ms | 0.201 ms | 0.124 ms |
| OFB | 0.691 ms | 0.691 ms | 0.202 ms | 0.243 ms |
| CTR | 0.687 ms | 0.696 ms | 0.091 ms | 0.132 ms |
| XTS | 0.621 ms | 0.627 ms | 0.167 ms | 0.205 ms |
| GCM | 0.850 ms | 0.839 ms | 0.112 ms | 0.111 ms |

**A screenshot of a computer screen

Description automatically generated**

**A computer screen with white text

Description automatically generated**

A screenshot of a computer program

Description automatically generated

**Plain500KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 2.297 ms | 2.288 ms | 0.288 ms | 0.289 ms |
| CBC | 2.380 ms | 2.291 ms | 0.667 ms | 0.296 ms |
| CFB | 2.316 ms | 2.309 ms | 0.665 ms | 0.270 ms |
| OFB | 2.335 ms | 2.334 ms | 0.672 ms | 0.674 ms |
| CTR | 2.334 ms | 2.329 ms | 0.302 ms | 0.305 ms |
| XTS | 2.101 ms | 2.089 ms | 0.547 ms | 0.543 ms |
| GCM | 2.867 ms | 2.802 ms | 0.373 ms | 0.366 ms |

**A screenshot of a computer program

Description automatically generated**

**A computer screen with white text

Description automatically generated**

A screenshot of a computer program

Description automatically generated

**Plain1MB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 4.723 ms | 4.763 ms | 0.585 ms | 0.581 ms |
| CBC | 4.876 ms | 4.783 ms | 1.356 ms | 0.608 ms |
| CFB | 4.756 ms | 4.776 ms | 1.377 ms | 0.544 ms |
| OFB | 4.868 ms | 4.744 ms | 1.371 ms | 1.389 ms |
| CTR | 4.790 ms | 4.818 ms | 0.628 ms | 0.620 ms |
| XTS | 4.346 ms | 4.276 ms | 1.129 ms | 1.117 ms |
| GCM | 5.975 ms | 5.998 ms | 0.760 ms | 0.763 ms |

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

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