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

Full Name: Võ Hoài Nam

Student ID Number: 23520990

Class: ATTT2023.2

**Device Information**

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

Ram: 16 GB DDR4 3200MHz

SSD PCle: 512GB

**DES**

key: AD12463E840DCE194EFB330E3C5D751C1D90A286A8DDFE3A4AB76D46B637ABDD

iv:018C53B1CA0FBBFCB571C82191F32265

**Plain1KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| OFB | 49479 ms | 56678 ms | 25628 ms | 25707 ms |
| CBC | 53940 ms | 53172 ms | 24623 ms | 24636 ms |
| CFB | 50542 ms | 50059 ms | 25368 ms | 24581 ms |
| CTR | 44356 ms | 49652 ms | 26607 ms | 25744 ms |
| ECB | 50197 ms | 42826 ms | 24487 ms | 23274 ms |

**Plain10KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| OFB | 1581297 ms | 1673324 ms | 1150395 ms | 1146395 ms |
| CBC | 1566812 ms | 1740870 ms | 24623 ms | 24636 ms |
| CFB | 1597197 ms | 1550475 ms | 1142931 ms | 1125103 ms |
| CTR | 1649770 ms | 1642217 ms | 1213091 ms | 1234587 ms |
| ECB | 1492925 ms | 1499107 ms | 1088060 ms | 1105877 ms |

**Plain50KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| OFB | 7636492 ms | 7857023 ms | 5726249 ms | 6142738 ms |
| CBC | 8002911ms | 7529173 ms | 5836370 ms | 5826878 ms |
| CFB | 7656502 ms | 7515139 ms | 6083239 ms | 5866195 ms |
| CTR | 8041717 ms | 8316898 ms | 6310332 ms | 6437265 ms |
| ECB | 7345578 ms | 7476803 ms | 5795102 ms | 5770358 ms |

**Plain150KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| OFB | 54660269 ms | 46636663 ms | 18910176 ms | 20915051 ms |
| CBC | 26118190 ms | 22889235 ms | 28256917 ms | 29507654 ms |
| CFB | 47388900 ms | 33455335 ms | 26717763 ms | 29268392 ms |
| CTR | 27881204 ms | 28205558 ms | 19395454 ms | 20967484 ms |
| ECB | 50647311 ms | 30974153 ms | 20387040 ms | 23803927ms |

**Plain500KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| OFB | 75002002 ms | 74016245 ms | 84383919 ms | 81887990 ms |
| CBC | 75615545 ms | 167146889 ms | 57075953 ms | 54016344 ms |
| CFB | 74676781 ms | 58444931 ms | 56437639 ms | 54396471 ms |
| CTR | 60792107 ms | 60430567 ms | 59358327 ms | 59151395 ms |
| ECB | 56627724 ms | 55634313 ms | 53622930 ms | 53727623 ms |

**Plain1MB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 139653754 ms | 135316368 ms | 116267993 ms | 116362356 ms |
| CBC | 128759676 ms | 127838733 ms | 116324119 ms | 110961447 ms |
| CFB | 129565634 ms | 122402005 ms | 115521352 ms | 111983714 ms |
| OFB | 129227232 ms | 124116777 ms | 121332037 ms | 121462232 ms |
| CTR | 120833878 ms | 126558553 ms | 110363807 ms | 109999559 ms |

**AES**

Key: AD12463E840DCE194EFB330E3C5D751C1D90A286A8DDFE3A4AB76D46B637ABDD

IV: 018C53B1CA0FBBFCB571C82191F32265

**Plain1KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| XTS | 20995 ms | 61069 ms | 12952 ms | 12312 ms |
| CBC | 17014 ms | 16207 ms | 9556 ms | 9580 ms |
| CFB | 17344 ms | 14655 ms | 10322 ms | 10912 ms |
| CTR | 19689 ms | 15713 ms | 10416 ms | 10425 ms |
| ECB | 16265 ms | 14817 ms | 8665 ms | 8862 ms |
| GCM | 17588 ms | 31969 ms | 10352 ms | 10151 ms |
| OFB | 17520 ms | 15706 ms | 12952 ms | 12312 ms |

**Plain10KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| XTS | 108620 ms | 77917 ms | 65013 ms | 64159 ms |
| CBC | 107730 ms | 41581 ms | 93104 ms | 31543 ms |
| CFB | 117531 ms | 57088 ms | 94985 ms | 46367 ms |
| CTR | 47483 ms | 41759 ms | 35270 ms | 34491 ms |
| ECB | 53616 ms | 38329ms | 29922 ms | 28140 ms |
| GCM | 53654 ms | 75212 ms | 41811 ms | 55478 ms |
| OFB | 111778 ms | 108146 ms | 96982 ms | 95825 ms |

**Plain50KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| XTS | 371558 ms | 309488 ms | 289518 ms | 286569 ms |
| CBC | 500280 ms | 137913 ms | 415976 ms | 116348 ms |
| CFB | 515649 ms | 206908 ms | 426089 ms | 190298 ms |
| CTR | 217151 ms | 139479 ms | 124705 ms | 123537 ms |
| ECB | 201778 ms | 129385 ms | 108581 ms | 102816 ms |
| GCM | 253302 ms | 237200 ms | 161513 ms | 210437 ms |
| OFB | 527048 ms | 453099 ms | 425258 ms | 425393 ms |

**Plain150KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| XTS | 1163158 ms | 1074892 ms | 997471 ms | 980036 ms |
| CBC | 1474861 ms | 397010 ms | 1264298 ms | 335170 ms |
| CFB | 1489244 ms | 1489244 ms | 1309926 ms | 556541 ms |
| CTR | 557301 ms | 391305 ms | 363758 ms | 356554 ms |
| ECB | 519876 ms | 352241 ms | 323082 ms | 314526 ms |
| GCM | 670237 ms | 665865 ms | 479365 ms | 645485 ms |
| OFB | 1514397 ms | 1346240 ms | 1293110 ms | 1298653 ms |

**Plain500KB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| XTS | 4273497 ms | 3977403 ms | 3650958 ms | 3597193 ms |
| CBC | 5299716 ms | 1762345 ms | 4342541 ms | 1193689 ms |
| CFB | 5040900 ms | 2498912 ms | 4394781 ms | 1935761 ms |
| CTR | 1921159 ms | 1568997ms | 1273369 ms | 1301342 ms |
| ECB | 1699804 ms | 1565992 ms | 1133520 ms | 1043746 ms |
| GCM | 2831266 ms | 3341819 ms | 1674455 ms | 3335583 ms |
| OFB | 5019708 ms | 5013321 ms | 4413584 ms | 4539780 ms |

**Plain1MB.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| XTS | 12760689 ms | 12692551 ms | 7547422 ms | 7403347 ms |
| CBC | 15720209 ms | 7642246 ms | 9290746 ms | 2719085 ms |
| CFB | 18818243 ms | 30446956 ms | 9531973 ms | 4186385 ms |
| CTR | 21686111 ms | 26111969 ms | 2669152 ms | 2739508 ms |
| ECB | 30151847 ms | 18637230 ms | 2824648 ms | 2286324 ms |
| GCM | 17746394 ms | 25054526 ms | 3926617 ms | 5743832 ms |
| OFB | 23337051 ms | 19828240 ms | 9337180 ms | 9126852 ms |

**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