UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTER NETWORK AND COMMUNICATION

Logo, company name

Description automatically generated

**REPORT**

Subject: Cryptography

Semester II (2021 – 2022)

**Report Lab 1 – 2**

Student: Võ Anh Kiệt

Student ID Number: 20520605

Class: NT219.M21.ANTN

University of Information Technology

Lecturer: Nguyễn Ngọc Tự

**Hồ Chí Minh City, March 2022**

Report Lab 1 – 2

**Student Information**

Full Name: Võ Anh Kiệt

Student ID Number: 20520605

Class: ANTN2020

**Device Information**

CPU: Intel core i5 – 8250U @ 1.60 GHz

Ram: 16 GB DDR3L

SSD M2 SATA: 500GB

HDD: 1000GB

Display chip name: UHD 620

**DES**

plaintext: Võ Anh Kiệt - 20520605 - ANTN2020 (testcase1)

key: F192C3EBC709CA47

iv: A40C475837067905

number of iterations: 10000

time counter: mili seconds

**testcase1.txt (1 KB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.0036 | 0.0039 | 0.0051551 | 0.0052945 |
| CBC | 0.0046 | 0.0044 | 0.0063048 | 0.0062123 |
| CFB | 0.0037 | 0.0039 | 0.0061273 | 0.0062332 |
| OFB | 0.0042 | 0.0046 | 0.0063858 | 0.0064095 |
| CTR | 0.0038 | 0.0038 | 0.0053758 | 0.0053945 |

**testcase2.txt (20 KB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.2305 | 0.2365 | 0.236888 | 0.237512 |
| CBC | 0.2485 | 0.2516 | 0.249958 | 0.251452 |
| CFB | 0.2379 | 0.2412 | 0.244691 | 0.230145 |
| OFB | 0.2456 | 0.2532 | 0.246537 | 0.245147 |
| CTR | 0.2337 | 0.2433 | 0.257170 | 0.258412 |

**testcase3.txt (50 KB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.5756 | 0.5809 | 0.585340 | 0.575142 |
| CBC | 0.6111 | 0.6121 | 0.622831 | 0.612050 |
| CFB | 0.6053 | 0.6102 | 0.611240 | 0.602153 |
| OFB | 0.6200 | 0.6233 | 0.617063 | 0.621743 |
| CTR | 0.6996 | 0.7013 | 0.639851 | 0.642153 |

**testcase4.txt (100 KB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 1.2067 | 1.2169 | 1.18152 | 1.19215 |
| CBC | 1.3095 | 1.3395 | 1.24920 | 1.25362 |
| CFB | 1.2809 | 1.2656 | 1.31088 | 1.31574 |
| OFB | 1.2677 | 1.2699 | 1.23865 | 1.23475 |
| CTR | 1.3382 | 1.3445 | 1.29039 | 1.29521 |

**testcase5.txt (200 KB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 2.5046 | 2.5546 | 2.45663 | 2.46251 |
| CBC | 2.8631 | 2.7439 | 2.59732 | 2.61452 |
| CFB | 2.7933 | 2.8133 | 2.44374 | 2.53211 |
| OFB | 2.7547 | 2.7017 | 2.46393 | 2.44125 |
| CTR | 2.8573 | 2.9005 | 2.55824 | 2.62015 |

**testcase6.txt (1024 KB = 1 MB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 12.9249 | 11.7676 | 16.0346 | 16.8541 |
| CBC | 13.8128 | 14.2356 | 16.9888 | 17.0142 |
| CFB | 13.5349 | 13.7852 | 16.7735 | 16.9521 |
| OFB | 14.7828 | 13.9878 | 13.6756 | 13.3652 |
| CTR | 15.2765 | 14.9578 | 14.2031 | 14.4221 |

**testcase7.txt (5 MB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 77.2391 | 78.2410 | 82.8954 | 83.2513 |
| CBC | 82.4812 | 81.3652 | 87.8335 | 86.2513 |
| CFB | 81.3122 | 83.1475 | 86.3837 | 87.2521 |
| OFB | 78.2260 | 77.2152 | 79.1061 | 79.1452 |
| CTR | 80.7086 | 81.2365 | 81.3674 | 81.6742 |

**AES**

plaintext: Võ Anh Kiệt - 20520605 - ANTN2020 (testcase1)

key: 9800A318AEFF1DD5CEF5925B04A4217A195833F2FA095762CD61DDF12BF4AAB0

iv: 64FF5E940E349F043D8EF87A4EEE4041

iv: 64FF5E940E349F04 (8 bytes CCM)

auth data: 20520605

time counter: mili seconds

**testcase1.txt (1 KB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.0018 | 0.0019 | 0.0033103 | 0.0034002 |
| CBC | 0.0021 | 0.0020 | 0.0036827 | 0.0037102 |
| CFB | 0.0030 | 0.0032 | 0.0029874 | 0.0030210 |
| OFB | 0.0014 | 0.0015 | 0.0030240 | 0.0030902 |
| CTR | 0.0024 | 0.0024 | 0.0038196 | 0.0039014 |
| XTS | 0.0036 | 0.0036 | 0.0038260 | 0.0038324 |
| GCM | 0.0026 | 0.0025 | 0.0032228 | 0.0033620 |
| CCM | 0.0030 | 0.0029 | 0.0041249 | 0.0042471 |

**testcase2.txt (20 KB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.0105 | 0.0115 | 0.0087086 | 0.0089201 |
| CBC | 0.0300 | 0.0320 | 0.0291228 | 0.0302103 |
| CFB | 0.0315 | 0.0376 | 0.0291984 | 0.0280123 |
| OFB | 0.0239 | 0.0269 | 0.0282953 | 0.0027321 |
| CTR | 0.0074 | 0.0079 | 0.0098595 | 0.0097851 |
| XTS | 0.0166 | 0.0167 | 0.0204288 | 0.0210521 |
| GCM | 0.0136 | 0.0136 | 0.0125633 | 0.0125012 |
| CCM | 0.0371 | 0.0392 | 0.0340690 | 0.0363210 |

**testcase3.txt (50 KB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.0125 | 0.0136 | 0.0183947 | 0.0195214 |
| CBC | 0.0537 | 0.0539 | 0.0669401 | 0.0670123 |
| CFB | 0.0523 | 0.0523 | 0.0662011 | 0.0672143 |
| OFB | 0.0543 | 0.0555 | 0.0670936 | 0.0681420 |
| CTR | 0.0158 | 0.0154 | 0.0180896 | 0.0184102 |
| XTS | 0.0464 | 0.0455 | 0.0485905 | 0.0471252 |
| GCM | 0.0197 | 0.0193 | 0.0264517 | 0.0263517 |
| CCM | 0.0628 | 0.0629 | 0.0801763 | 0.0802014 |

**testcase4.txt (100 KB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.0336 | 0.0327 | 0.0325843 | 0.0337514 |
| CBC | 0.1383 | 0.1421 | 0.1322160 | 0.1420240 |
| CFB | 0.1322 | 0.1389 | 0.1356760 | 0.1375214 |
| OFB | 0.1377 | 0.1417 | 0.1329210 | 0.1324853 |
| CTR | 0.0365 | 0.0366 | 0.0337018 | 0.0347512 |
| XTS | 0.0887 | 0.0915 | 0.0970175 | 0.0915142 |
| GCM | 0.0460 | 0.0498 | 0.0488964 | 0.0452032 |
| CCM | 0.1592 | 0.1610 | 0.1212740 | 0.1356201 |

**testcase5.txt (200 KB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.0628 | 0.0628 | 0.0461604 | 0.0452173 |
| CBC | 0.2589 | 0.2589 | 0.1921180 | 0.2014253 |
| CFB | 0.2950 | 0.3010 | 0.1949320 | 0.2102541 |
| OFB | 0.2950 | 0.3100 | 0.1978380 | 0.1952302 |
| CTR | 0.0670 | 0.0683 | 0.0493176 | 0.0486231 |
| XTS | 0.1993 | 0.2028 | 0.1878430 | 0.1935620 |
| GCM | 0.1033 | 0.1202 | 0.0743966 | 0.0813201 |
| CCM | 0.3349 | 0.3474 | 0.2343270 | 0.2475325 |

**testcase6.txt (1024 KB = 1 MB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.3386 | 0.3478 | 0.326627 | 0.331456 |
| CBC | 1.3581 | 1.3783 | 1.325160 | 1.312521 |
| CFB | 1.3203 | 1.3333 | 1.116080 | 1.214232 |
| OFB | 1.3474 | 1.3299 | 1.389250 | 1.365215 |
| CTR | 0.3273 | 0.3390 | 0.240121 | 0.253123 |
| XTS | 0.9273 | 0.9302 | 0.947407 | 0.938215 |
| GCM | 0.4562 | 0.4589 | 0.415180 | 0.423652 |
| CCM | 1.6049 | 1.6179 | 1.233940 | 1.223145 |

**testcase7.txt (5 MB)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 1.6831 | 1.7621 | 1.62723 | 1.71202 |
| CBC | 6.6201 | 6.7320 | 5.71980 | 5.82301 |
| CFB | 6.9617 | 6.9751 | 7.18960 | 7.12501 |
| OFB | 7.0753 | 7.1423 | 7.41209 | 7.36201 |
| CTR | 1.8967 | 1.9366 | 1.96609 | 1.94203 |
| XTS | 6.7403 | 6.8523 | 6.94557 | 6.83620 |
| GCM | 2.9064 | 2.9302 | 3.06292 | 3.01236 |
| CCM | 8.3611 | 8.4123 | 8.74701 | 8.85213 |

**Comments and Comparison:**

* AES mode is faster than DES mode in 7 testcases in both Window and Linux
* Executing the code in Window is faster than Linux in 7 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 7 testcases
* Mode ECB, CTR, GCM have the time execute faster than the other modes in scheme AES
* With the files, the size of which are under 1 MB have the time execute faster than the file from 1 MB and above. With the file greater than 1 MB, must have the clean data function to cut down the time execute