**Report Lab 1 – 2**

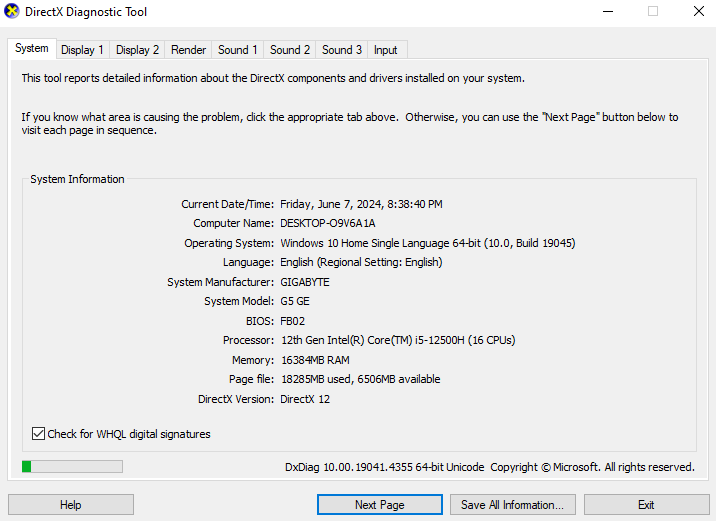
**Student Information**

Full Name: Mai Nguyễn Nam Phương

Student ID Number: 22521164

Class: NT219.O21.ANTT

**Device Information**



**DES**

**TEST CASE  
Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động**

number of iterations: 10000

time counter: mili seconds

**testcase1.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.1464 | 0.1509 | 0.0895 | 0.0741 |
| CBC | 0.1474 | 0.148 | 0.0921 | 0.0856 |
| CFB | 0.1464 | 0.1456 | 0.0907 | 0.0832 |
| OFB | 0.1493 | 0.1474 | 0.0953 | 0.0901 |
| CTR | 0.1504 | 0.1485 | 0.0928 | 0.0898 |

**testcase2.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.2525 | 0.2569 | 0.1368 | 0.1012 |
| CBC | 0.2811 | 0.2811 | 0.1468 | 0.1252 |
| CFB | 0.2703 | 0.2628 | 0.1615 | 0.1145 |
| OFB | 0.2647 | 0.2724 | 0.1373 | 0.1447 |
| CTR | 0.2733 | 0.2799 | 0.2031 | 0.1519 |

**testcase3.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.6169 | 0.6749 | 0.3853 | 0.4042 |
| CBC | 0.6853 | 0.708 | 0.422831 | 0.4124 |
| CFB | 0.6821 | 0.6947 | 0.4112 | 0.4353 |
| OFB | 0.6782 | 0.765 | 0.4176 | 0.4273 |
| CTR | 0.7139 | 0.7943 | 0.4388 | 0.4253 |

**testcase4.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 1.0777 | 1.2338 | 0.7413 | 1.1921 |
| CBC | 1.203 | 1.2559 | 0.8326 | 1.2536 |
| CFB | 1.2027 | 1.2659 | 0.7513 | 1.3157 |
| OFB | 1.2024 | 1.3763 | 0.7895 | 1.2347 |
| CTR | 1.2668 | 1.437 | 0.865 | 1.2952 |

**testcase5.txt**

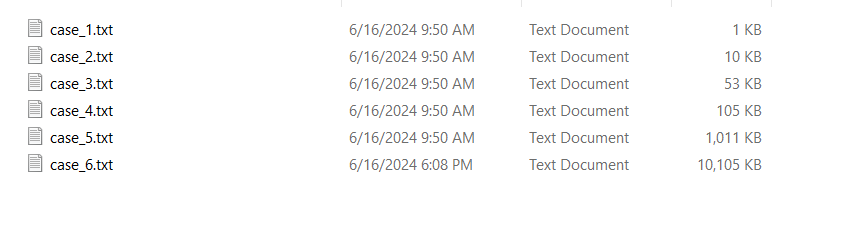
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 9.7304 | 11.2758 | 7.1663 | 7.46251 |
| CBC | 10.9102 | 11.3073 | 7.59732 | 7.61452 |
| CFB | 10.8456 | 11.3405 | 7.44374 | 7.53211 |
| OFB | 10.8881 | 12.427 | 7.46393 | 7.44125 |
| CTR | 11.3694 | 13.0129 | 8.0824 | 7.62015 |

**testcase6.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 103.5968 | 135.7987 | 97.3562 | 116.8541 |
| CBC | 114.9517 | 145.5042 | 100.2148 | 117.0142 |
| CFB | 114.6407 | 121.1586 | 102.215 | 116.9521 |
| OFB | 121.5736 | 142.5898 | 105.3148 | 116.3652 |
| CTR | 150.0025 | 134.907 | 105.3654 | 116.4221 |

**AES**

**TEST CASE**



number of iterations: 10000

time counter: mili seconds

**testcase1.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.1412 | 0.1439 | 0.1302 | 0.1203 |
| CBC | 0.1646 | 0.1681 | 0.1427 | 0.1247 |
| CFB | 0.1602 | 0.1547 | 0.1558 | 0.1652 |
| OFB | 0.1553 | 0.157 | 0.1564 | 0.1329 |
| CTR | 0.156 | 0.1693 | 0.1430 | 0.1306 |
| XTS | 0.1706 | 0.16311 | 0.1664 | 0.1596 |
| GCM | 0.1616 | 0.1589 | 0.132 | 0.1228 |
| CCM | 0.1585 | 0.1701 | 0.1354 | 0.1454 |

**testcase2.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.1691 | 0.1726 | 0.1435 | 0.1548 |
| CBC | 0.1951 | 0.1881 | 0.1624 | 0.1658 |
| CFB | 0.1891 | 0.2161 | 0.1589 | 0.1599 |
| OFB | 0.1898 | 0.199 | 0.1593 | 0.1639 |
| CTR | 0.1779 | 0.1942 | 0.1501 | 0.1507 |
| XTS | 0.1973 | 0.2136 | 0.1785 | 0.2031 |
| GCM | 0.1804 | 0.1906 | 0.1479 | 0.1455 |
| CCM | 0.1987 | 0.2089 | 0.1798 | 0.1652 |

**testcase3.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.2324 | 0.3376 | 0.2011 | 0.2721 |
| CBC | 0.2724 | 0.351 | 0.2354 | 0.3441 |
| CFB | 0.2702 | 0.3619 | 0.2112 | 0.2985 |
| OFB | 0.2687 | 0.396 | 0.2432 | 0.2977 |
| CTR | 0.2567 | 0.3615 | 0.219 | 0.2509 |
| XTS | 0.2592 | 0.3777 | 0.265 | 0.3111 |
| GCM | 0.2638 | 0.3857 | 0.2178 | 0.2741 |
| CCM | 0.277 | 0.4073 | 0.2314 | 0.3386 |

**testcase4.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 0.2874 | 0.4692 | 0.2324 | 0.2416 |
| CBC | 0.3779 | 0.4984 | 0.2741 | 0.2789 |
| CFB | 0.3709 | 0.5151 | 0.2831 | 0.2796 |
| OFB | 0.3658 | 0.552 | 0.2749 | 0.2985 |
| CTR | 0.3072 | 0.5049 | 0.2561 | 0.2541 |
| XTS | 0.3443 | 0.5405 | 0.2614 | 0.3014 |
| GCM | 0.3173 | 0.5073 | 0.2458 | 0.2589 |
| CCM | 0.3828 | 0.5854 | 0.3064 | 0.2997 |

**testcase5.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 1.8701 | 3.1582 | 1.5212 | 2.5521 |
| CBC | 2.5114 | 3.2074 | 2.1033 | 2.8546 |
| CFB | 2.5372 | 3.3084 | 2.1547 | 2.9215 |
| OFB | 2.5291 | 3.814 | 2.2541 | 2.4154 |
| CTR | 1.9326 | 3.2109 | 1.6512 | 2.7214 |
| XTS | 2.3967 | 4.009 | 2.3214 | 2.3142 |
| GCM | 1.9978 | 3.3065 | 1.5655 | 1.9555 |
| CCM | 2.6853 | 3.9143 | 2.4125 | 2.2475 |

**testcase6.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| ECB | 27.319 | 40.133 | 24.1358 | 28.3216 |
| CBC | 31.9361 | 40.9138 | 28.3216 | 34.489 |
| CFB | 32.4516 | 44.4555 | 27.6998 | 32.2616 |
| OFB | 32.3685 | 48.6126 | 30.2989 | 39.1541 |
| CTR | 26.5027 | 42.3426 | 24.0121 | 40.3123 |
| XTS | 30.894 | 46.3901 | 29.2316 | 39.6154 |
| GCM | 27.0162 | 42.0421 | 25.3369 | 32.3172 |
| CCM | 33.4652 | 48.3897 | 30.6984 | 39.3187 |

**Comments and Comparison:**

* Thuật toán AES nhanh hơn so với DES trong 7 test case trên cả hệ điều hành Windows và Linux. Điều này cho thấy AES có hiệu suất cao hơn so với DES
* Việc thực hiện mã hóa và giải mã trên Windows chậm hơn Linux( Ubuntu) trong tất cả các test case.
* Thời gian thực hiện tăng theo sự gia tăng của kích thước file. Điều này là dễ hiểu vì dữ liệu lớn hơn yêu cầu nhiều thời gian xử lý hơn
* Trong thuật toán DES thì chế độ ECB thường sẽ thực hiện nhanh nhất, còn các chế độ còn lại thì có hiệu xuất khá tương đồng nhau
* Trong thuật toán AES, các chế độ ECB, CTR, và GCM có thời gian thực hiện nhanh hơn so với các chế độ khác.

**AES-MANUAL**

**TEST CASE**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, đại số

Mô tả được tạo tự động

number of iterations: 10000

time counter: mili seconds

**testcase1.txt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test case | Encrypt (Window) | Decrypt (Window) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| Test case 1 | 0.2228 | 0.2666 | 0.1958 | 0.2216 |
| Test case 2 | 1.384 | 1.4559 | 1.0214 | 1.6231 |
| Test case 3 | 3.5363 | 5.0883 | 3.6323 | 4.8772 |
| Test case 4 | 6.5564 | 8.7003 | 6.0117 | 8.2364 |
| Test case 5 | 377.2107 | 380.7047 | 360.1476 | 377.3234 |
| Test case 6 | 5813.5387 | 7431.7336 | 5412.218 | 7652.3226 |

**Comments and Comparison:**

* Tương tự như AES có sử dụng thư viện Crypto thì việc mã hoá và giải mã bên ubuntu vẫn nhanh hơn bên window ở tất cả các test case
* Thời gian thực hiện tăng theo sự gia tăng của kích thước file. Điều này là dễ hiểu vì dữ liệu lớn hơn yêu cầu nhiều thời gian xử lý hơn
* Thời gian chạy mã hoá và giải mã là lâu hơn so với có sử dụng thư viện vì code này chưa được tối ưu hoá