UNIVERSITY OF INFORMATION TECHNOLOGY
FACULTY OF COMPUTER NETWORK AND COMMUNICATION


# CRYPTOGRAPHY

## Report Lab 1

## Coding DES, AES using Crypto++ Library

| | |
|---|---|
| Lecturer: | Nguyễn Ngọc Tự |
| Class: | NT219.O21.ANTT.2 |
| Student: | Trần Thế Hữu Phúc |
| Student ID Number: | 22521143 |

**Hồ Chí Minh City, June 2024**

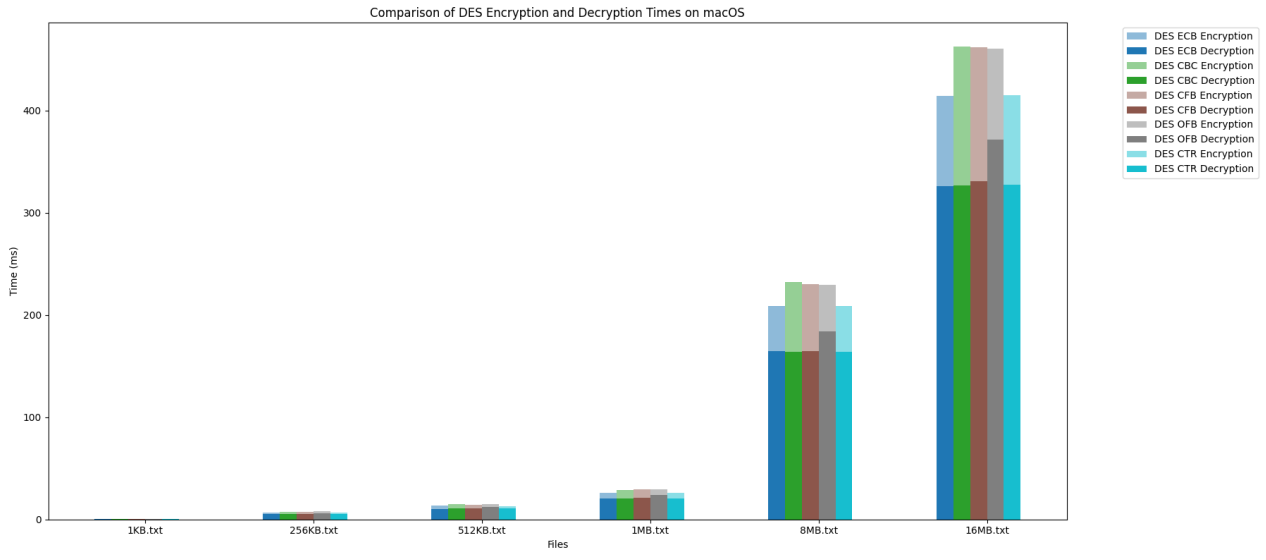
## 1. Hardware Resources

| | |
|---|---|
| **Device** | MacBook Pro |
| **Chip** | Apple M1<br>• 8-core CPU<br>• 8-core GPU<br>• 16-core Neural Engine |
| **Memory** | 8GB LPDDR4 |
| **Storage** | 256GB SSD |
| **Operating Systems** | • macOS 14.5 Sonoma<br>• Windows 11 Pro Version 23H2<br>• Ubuntu 22.04.4 LTS |

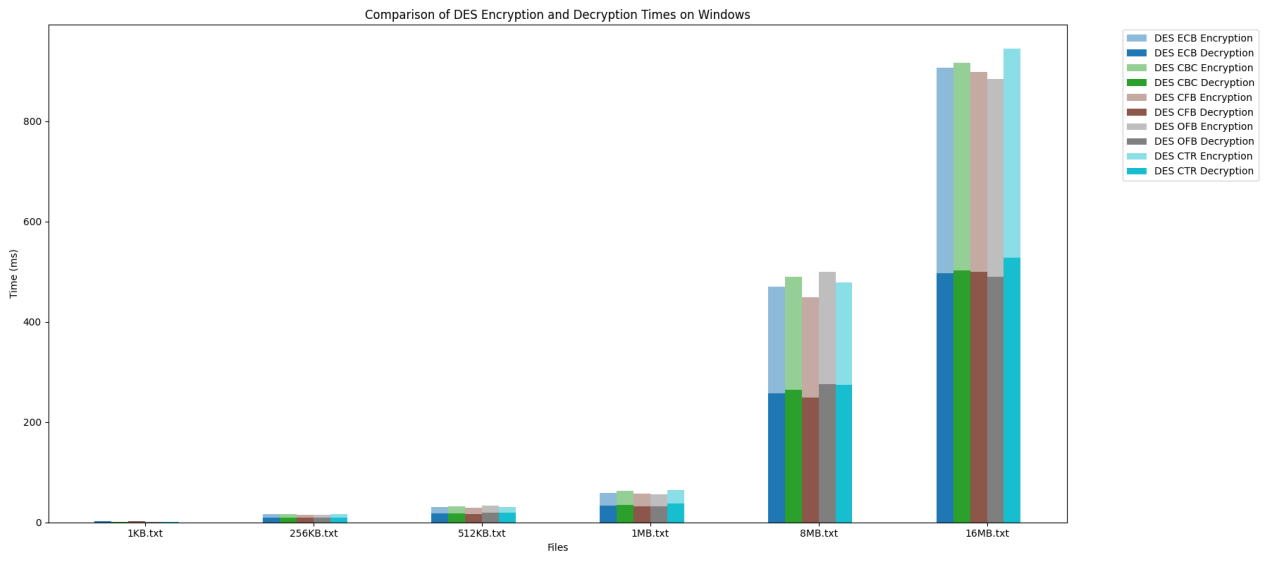
## 2. Computation performance on macOS, Windows and Linux

### 2.1. DES

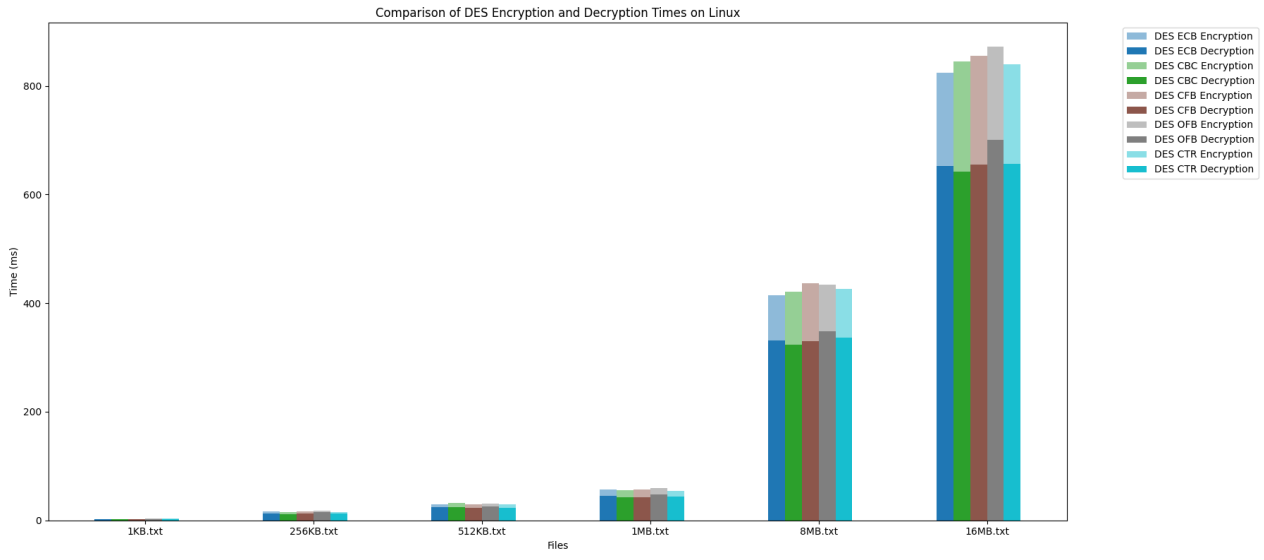
| DES on macOS (miliseconds) | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Mode** | | **Input Size** | | | | | |
| | | 1KB | 256KB | 512KB | 1MB | 8MB | 16MB |
| ECB | Encrypt | 0.308 | 6.838 | 13.381 | 25.723 | 208.715 | 414.391 |
| | Decrypt | 0.299 | 5.492 | 10.418 | 20.527 | 164.746 | 326.309 |
| CBC | Encrypt | 0.292 | 7.581 | 15.051 | 29.117 | 232.079 | 462.694 |
| | Decrypt | 0.262 | 5.360 | 11.107 | 20.681 | 163.626 | 326.994 |
| CFB | Encrypt | 0.492 | 7.418 | 14.611 | 29.125 | 230.480 | 462.094 |
| | Decrypt | 0.311 | 5.611 | 10.758 | 21.031 | 164.601 | 330.927 |
| OFB | Encrypt | 0.296 | 7.915 | 14.971 | 29.580 | 229.204 | 460.819 |
| | Decrypt | 0.298 | 6.115 | 12.158 | 23.617 | 184.228 | 371.256 |
| CTR | Encrypt | 0.274 | 6.731 | 13.201 | 26.203 | 208.843 | 415.047 |
| | Decrypt | 0.471 | 5.367 | 10.521 | 20.333 | 164.139 | 327.084 |



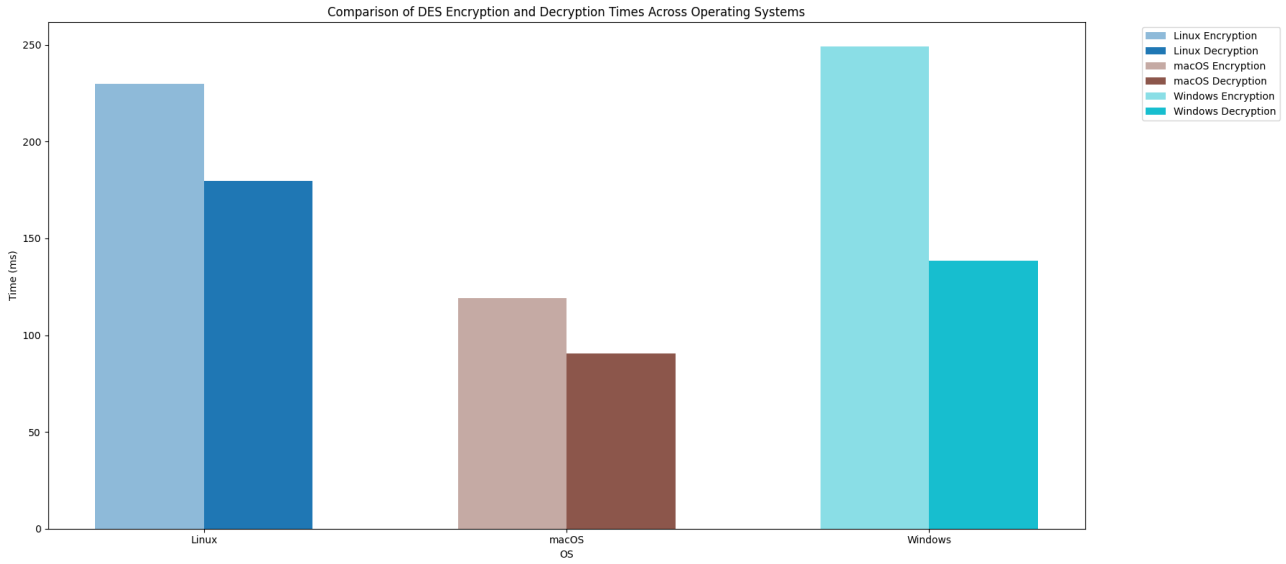
| DES on Windows (miliseconds) | | | | | | | |
|---|---|---|---|---|---|---|---|
| Mode | | Input Size | | | | | |
| | | 1KB | 256KB | 512KB | 1MB | 8MB | 16MB |
| ECB | Encrypt | 1.749 | 16.176 | 31.003 | 58.132 | 469.446 | 906.108 |
| | Decrypt | 1.849 | 9.545 | 18.258 | 33.564 | 256.731 | 497.112 |
| CBC | Encrypt | 1.415 | 16.303 | 31.739 | 63.048 | 489.060 | 916.883 |
| | Decrypt | 1.418 | 9.254 | 18.302 | 35.143 | 263.849 | 502.390 |
| CFB | Encrypt | 1.538 | 15.319 | 29.135 | 58.010 | 449.334 | 897.383 |
| | Decrypt | 1.876 | 8.965 | 17.070 | 31.930 | 249.480 | 498.955 |
| OFB | Encrypt | 1.324 | 15.386 | 33.586 | 55.393 | 499.417 | 883.596 |
| | Decrypt | 1.366 | 9.155 | 19.576 | 32.455 | 275.786 | 489.752 |
| CTR | Encrypt | 1.444 | 16.366 | 30.840 | 64.517 | 478.107 | 944.655 |
| | Decrypt | 1.484 | 10.077 | 18.996 | 37.828 | 274.338 | 528.299 |



| DES on Linux (miliseconds) | | | | | | | |
|---|---|---|---|---|---|---|---|
| Mode | | Input Size | | | | | |
| | | 1KB | 256KB | 512KB | 1MB | 8MB | 16MB |
| ECB | Encrypt | 2.841 | 16.358 | 29.534 | 56.571 | 414.142 | 824.044 |
| | Decrypt | 2.465 | 13.205 | 24.002 | 45.275 | 331.320 | 652.671 |
| CBC | Encrypt | 2.640 | 15.351 | 31.559 | 55.844 | 421.462 | 844.333 |
| | Decrypt | 2.276 | 11.961 | 23.731 | 42.374 | 323.494 | 642.364 |
| CFB | Encrypt | 2.724 | 16.030 | 29.561 | 56.235 | 437.044 | 855.609 |
| | Decrypt | 2.376 | 12.694 | 22.826 | 42.757 | 330.025 | 655.350 |
| OFB | Encrypt | 3.184 | 17.755 | 31.118 | 59.151 | 434.276 | 872.360 |
| | Decrypt | 2.802 | 14.625 | 25.514 | 47.643 | 348.711 | 699.945 |
| CTR | Encrypt | 3.056 | 15.716 | 29.010 | 53.974 | 426.793 | 839.246 |
| | Decrypt | 2.847 | 12.879 | 23.404 | 43.269 | 335.897 | 656.808 |



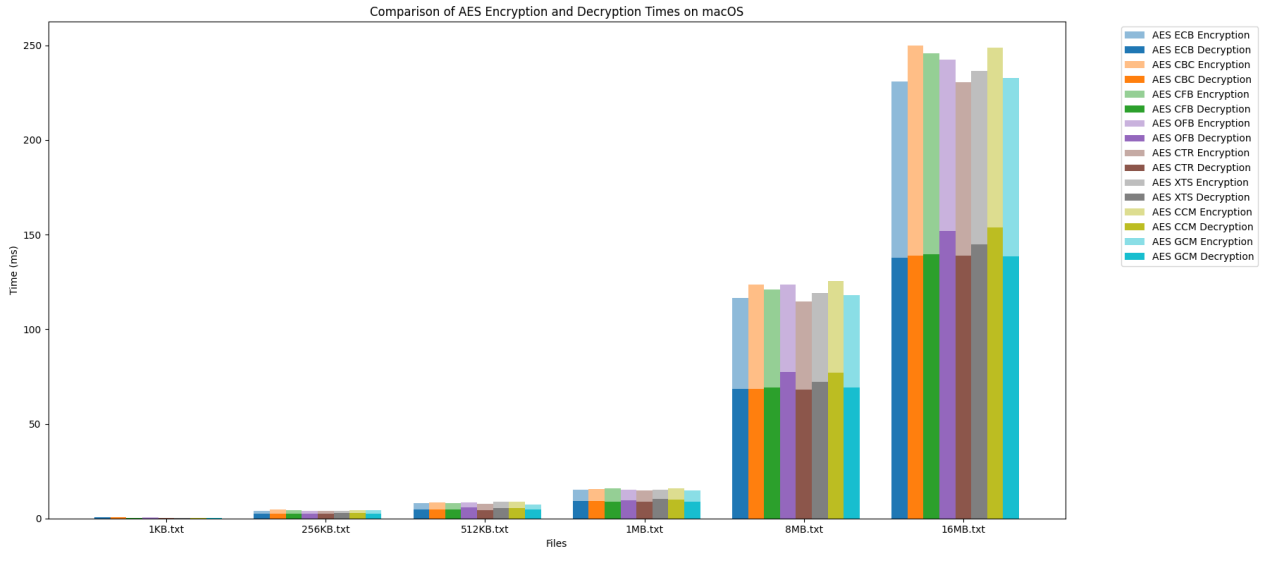
## ⌥ Phân tích và so sánh



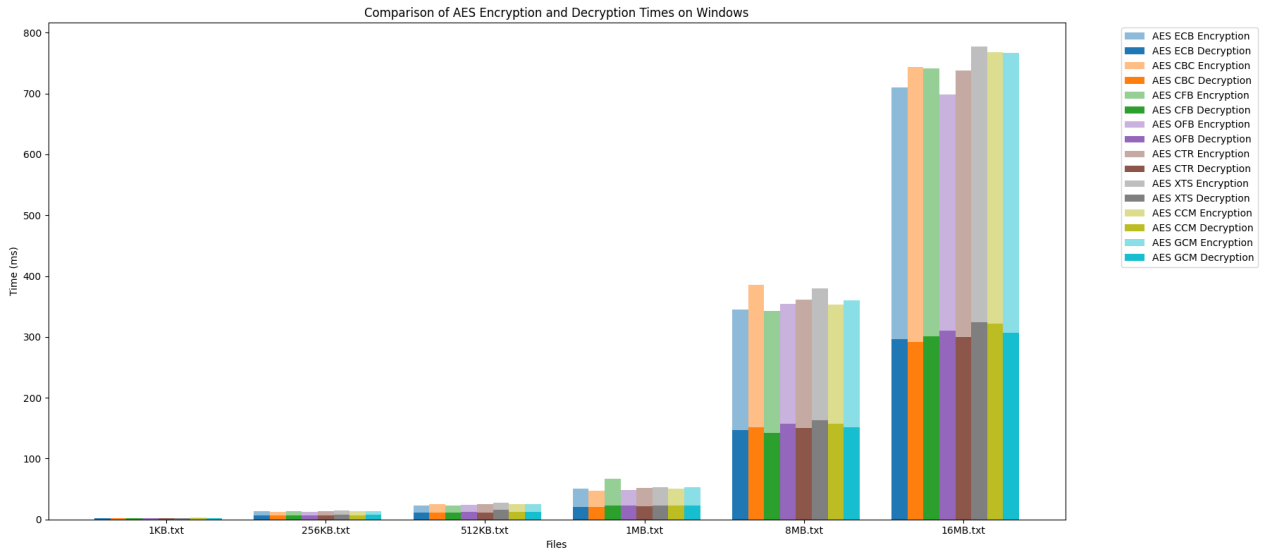

- **Kích thước đầu vào:**
  - Có mối tương quan rõ ràng giữa kích thước đầu vào và thời gian cần thiết cho cả mã hóa và giải mã.
  - Kích thước đầu vào lớn hơn làm tăng đáng kể thời gian cần thiết trên tất cả các chế độ và hệ điều hành.
- **Hệ điều hành:**
  - **macOS** là hiệu quả nhất cho các thao tác DES, thích hợp cho các ứng dụng cần mã hóa và giải mã nhanh chóng.
  - **Windows** có hiệu suất trung bình, thích hợp cho các ứng dụng đa mục đích nhưng có thể không lý tưởng cho nhu cầu hiệu suất cao.
  - **Linux** có thời gian cao nhất, cho thấy có thể không phải là lựa chọn tốt nhất cho các môi trường mà hiệu suất DES là quan trọng.
- **Chế độ:**
  - Chế độ ECB và CTR thường nhanh hơn trên tất cả các hệ điều hành, trong khi chế độ OFB và CBC có xu hướng chậm hơn.
  - Với các ứng dụng cần mã hóa và giải mã nhanh, chế độ ECB hoặc CTR có thể là lựa chọn ưu tiên.

## 2.1. AES

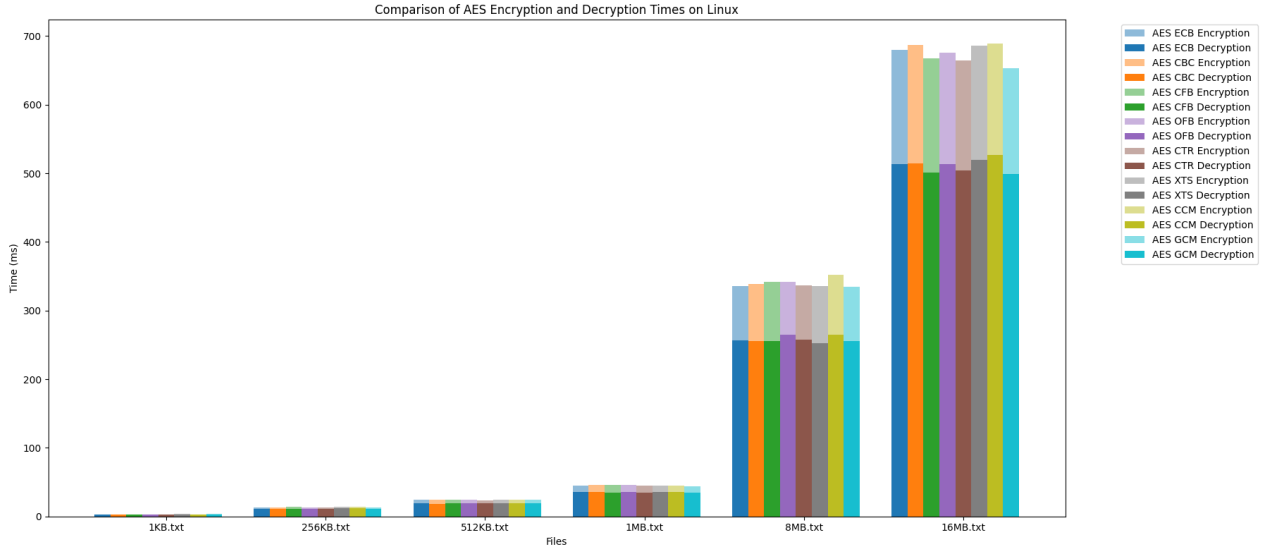
| AES on macOS (miliseconds) | | | | | | | |
|---|---|---|---|---|---|---|---|
| Mode | | Input Size | | | | | |
| | | 1KB | 256KB | 512KB | 1MB | 8MB | 16MB |
| ECB | Encrypt | 0.355 | 3.955 | 8.201 | 15.229 | 116.483 | 230.736 |
| | Decrypt | 0.763 | 2.442 | 4.557 | 9.261 | 68.492 | 137.700 |
| CBC | Encrypt | 0.302 | 4.808 | 8.472 | 15.535 | 123.728 | 249.950 |
| | Decrypt | 0.482 | 2.462 | 4.559 | 9.097 | 68.618 | 138.897 |
| CFB | Encrypt | 0.440 | 4.374 | 8.008 | 15.915 | 121.095 | 245.648 |
| | Decrypt | 0.427 | 2.648 | 4.811 | 9.019 | 69.198 | 139.552 |
| OFB | Encrypt | 0.562 | 4.180 | 8.384 | 15.307 | 123.711 | 242.482 |
| | Decrypt | 0.266 | 2.676 | 5.689 | 9.616 | 77.396 | 152.069 |
| CTR | Encrypt | 0.311 | 3.941 | 7.579 | 14.713 | 114.567 | 230.642 |
| | Decrypt | 0.272 | 2.533 | 4.495 | 8.776 | 68.254 | 139.037 |
| XTS | Encrypt | 0.294 | 4.164 | 8.885 | 15.009 | 119.132 | 236.559 |
| | Decrypt | 0.263 | 2.699 | 5.390 | 10.176 | 72.173 | 144.968 |
| CCM | Encrypt | 0.313 | 4.424 | 8.688 | 16.046 | 125.360 | 248.669 |
| | Decrypt | 0.285 | 2.698 | 5.472 | 9.970 | 76.975 | 153.927 |
| GCM | Encrypt | 0.333 | 4.362 | 7.484 | 14.929 | 118.042 | 232.754 |
| | Decrypt | 0.273 | 2.475 | 4.781 | 8.804 | 69.027 | 138.586 |



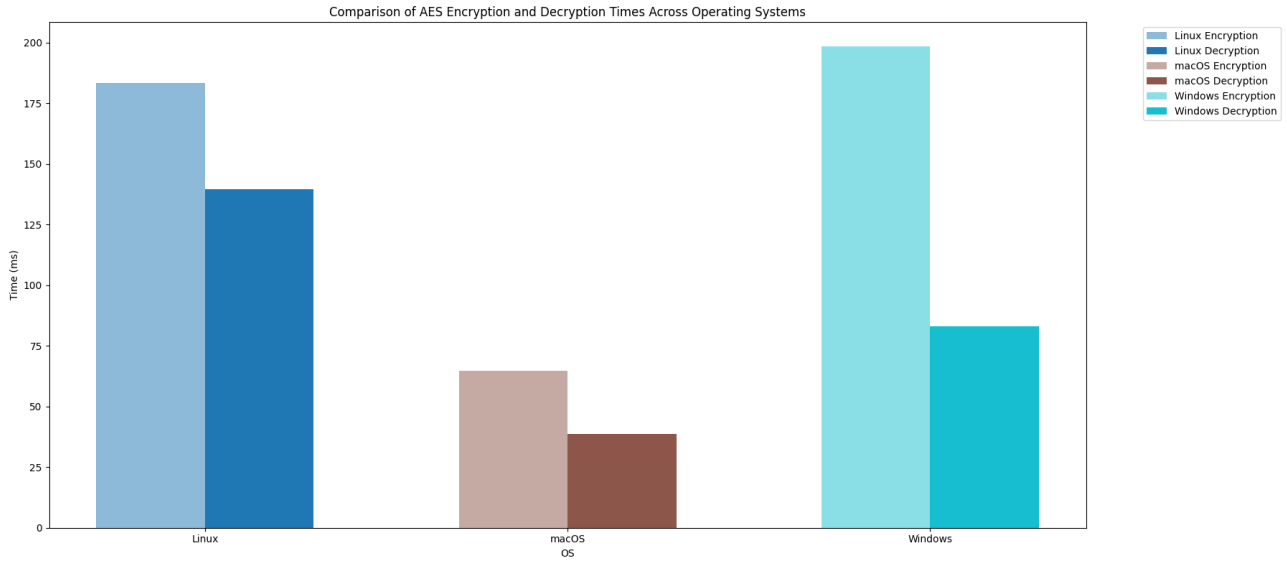
| AES on Windows (miliseconds) | | | | | | | |
|---|---|---|---|---|---|---|---|
| Mode | | Input Size | | | | | |
| | | 1KB | 256KB | 512KB | 1MB | 8MB | 16MB |
| ECB | Encrypt | 1.615 | 13.626 | 23.423 | 50.485 | 345.394 | 710.134 |
| | Decrypt | 1.563 | 6.559 | 10.914 | 20.670 | 146.274 | 295.836 |
| CBC | Encrypt | 1.816 | 12.897 | 25.030 | 47.684 | 385.328 | 743.532 |
| | Decrypt | 1.869 | 12.897 | 11.392 | 20.976 | 151.803 | 291.423 |
| CFB | Encrypt | 2.085 | 13.158 | 23.401 | 67.096 | 342.873 | 741.030 |
| | Decrypt | 2.142 | 6.078 | 10.833 | 23.258 | 141.869 | 300.841 |
| OFB | Encrypt | 2.035 | 12.755 | 24.217 | 48.048 | 354.539 | 698.635 |
| | Decrypt | 1.689 | 6.796 | 11.992 | 22.381 | 157.622 | 309.955 |
| CTR | Encrypt | 1.619 | 13.644 | 24.777 | 52.207 | 361.702 | 737.262 |
| | Decrypt | 1.697 | 6.849 | 11.673 | 21.969 | 150.501 | 300.224 |
| XTS | Encrypt | 1.815 | 14.388 | 27.942 | 53.053 | 379.708 | 777.379 |
| | Decrypt | 1.767 | 7.332 | 15.541 | 22.977 | 162.501 | 323.844 |
| CCM | Encrypt | 3.204 | 13.137 | 24.882 | 50.471 | 353.002 | 768.523 |
| | Decrypt | 1.636 | 7.024 | 12.210 | 23.053 | 157.195 | 321.505 |
| GCM | Encrypt | 1.669 | 14.132 | 25.706 | 52.586 | 360.258 | 767.286 |
| | Decrypt | 1.689 | 7.215 | 12.159 | 23.376 | 151.773 | 306.978 |



| AES on Linux (miliseconds) | | | | | | | |
|---|---|---|---|---|---|---|---|
| Mode | | Input Size | | | | | |
| | | 1KB | 256KB | 512KB | 1MB | 8MB | 16MB |
| ECB | Encrypt | 3.071 | 13.437 | 24.074 | 45.403 | 335.756 | 680.132 |
| | Decrypt | 2.896 | 11.033 | 19.386 | 35.977 | 256.161 | 512.986 |
| CBC | Encrypt | 3.107 | 13.376 | 24.039 | 46.225 | 339.206 | 687.068 |
| | Decrypt | 2.898 | 10.514 | 18.230 | 35.172 | 255.471 | 514.746 |
| CFB | Encrypt | 3.295 | 14.031 | 24.326 | 46.450 | 341.966 | 667.923 |
| | Decrypt | 2.965 | 10.980 | 19.149 | 34.631 | 255.694 | 500.652 |
| OFB | Encrypt | 3.172 | 13.187 | 24.448 | 46.039 | 341.496 | 676.208 |
| | Decrypt | 2.842 | 11.037 | 19.182 | 35.520 | 265.076 | 513.552 |
| CTR | Encrypt | 3.090 | 13.164 | 23.668 | 44.550 | 336.817 | 664.127 |
| | Decrypt | 2.862 | 10.685 | 19.316 | 34.865 | 257.316 | 504.428 |
| XTS | Encrypt | 3.466 | 13.803 | 24.871 | 44.888 | 335.208 | 685.987 |
| | Decrypt | 3.079 | 11.551 | 19.590 | 35.437 | 252.668 | 519.391 |
| CCM | Encrypt | 3.246 | 13.752 | 24.695 | 45.440 | 351.919 | 689.321 |
| | Decrypt | 3.164 | 11.729 | 19.613 | 35.226 | 264.968 | 527.235 |
| GCM | Encrypt | 3.358 | 13.200 | 24.361 | 44.039 | 334.331 | 652.911 |
| | Decrypt | 3.113 | 11.218 | 652.911 | 34.435 | 255.861 | 499.543 |



## ⌥ Phân tích và so sánh




### Nhận xét chung:

- **Ảnh hưởng của kích thước đầu vào:**
  - Khi kích thước đầu vào tăng lên, thời gian mã hóa và giải mã cũng tăng lên trên tất cả các chế độ và hệ điều hành.
- **So sánh hệ điều hành:**
  - macOS có thời gian thấp nhất cho cả mã hóa và giải mã trên tất cả các chế độ và kích thước đầu vào.
  - Windows có thời gian cao hơn macOS nhưng thấp hơn Linux, đặc biệt là với các kích thước đầu vào lớn.
  - Linux có thời gian cao nhất cho cả mã hóa và giải mã trên hầu hết các chế độ và kích thước đầu vào.

### Phân tích chi tiết:

**macOS:**

- **Hiệu suất:**
  - Thời gian mã hóa và giải mã là thấp nhất trên tất cả các chế độ và kích thước đầu vào.
  - Cho thấy sự gia tăng thời gian tương đối tuyến tính khi kích thước đầu vào tăng lên.
- **So sánh các chế độ:**
  - Chế độ ECB và CTR có thời gian thấp nhất cho mã hóa và giải mã.
  - Chế độ OFB và CCM có thời gian cao hơn so với các chế độ khác, đặc biệt là với các kích thước đầu vào lớn.

**Windows:**

- **Hiệu suất:**
  - Thời gian cao hơn macOS nhưng thấp hơn Linux.
  - Thời gian mã hóa cao hơn đáng kể so với thời gian giải mã cho các kích thước đầu vào lớn.

- **So sánh các chế độ:**
    - Chế độ ECB nhanh hơn cho giải mã so với mã hóa.
    - Chế độ OFB và CTR có thời gian cao hơn, đặc biệt là với các kích thước đầu vào lớn.

**Linux:**

- **Hiệu suất:**
    - Thời gian cao nhất cho cả mã hóa và giải mã trên hầu hết các chế độ và kích thước đầu vào.
    - Cho thấy sự gia tăng thời gian đáng kể khi kích thước đầu vào tăng lên.
- **So sánh các chế độ:**
    - Chế độ ECB và CFB tương đối nhanh hơn so với các chế độ khác cho các kích thước đầu vào nhỏ.
    - Chế độ OFB và CTR có thời gian cao nhất, đặc biệt là với các kích thước đầu vào lớn.