# LAB REPORT: CODING DES & AES USING CRYTOPP LIBRARY

| | | |
|---|---|---|
| **Instructor** | **Đỗ Thị Phương Uyên** | |
| **Student 1:** | Tào Minh Đức | 23520315 |
| **Student 2:** | Mai Nguyễn Phúc Minh | 23520930 |

## LAB 1 REPORT'S TABLE OF CONTENTS

## 1. Hardware resource

| | |
|---|---|
| **Device:** | Lenovo Gaming Legion 5 15IAH7H |
| **Chip:** | Intel Core i5 12500H<br>- Cores: 12<br>- P-core: 4<br>- E-core: 8<br>- Logical processor: 16 |
| **Ram & Memory:** | DDR5-4800 – 16GB (RAM)<br>512 GB SSD x2 |
| **Operating Systems:** | Window 11<br>Ubuntu |

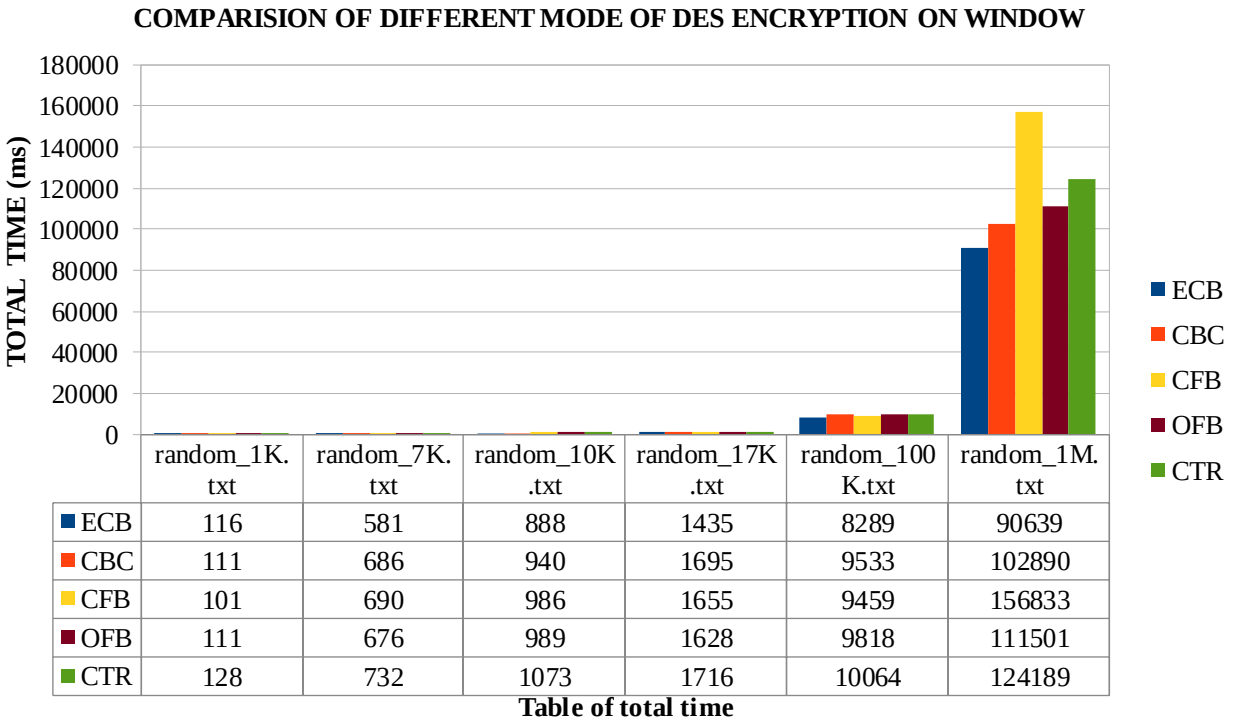
## 2. Input testcase

- Making a executed program to automatically generate a random input with 6 different testcase:
  - 1 KB input
  - 7 KB input
  - 10 KB input
  - 17 KB input
  - 100 KB input
  - 1 MB input
- **Note:** These testcase are generated randomly based on the program **makingtextcase.exe**

## 3. DES (Windows System)

- **Encryption (10000 times)**
  - **Abbreviation:**
    - TT: Total Time, AT: Average Time
  - **Note:**
    - All key and iv are randomly selected.
    - Using g++ compiler

| Mode / Input | ECB | CBC | CFB | OFB | CTR |
|---|---|---|---|---|---|
| **random_1K.txt** | TT: 116 ms<br>AT: 0.0116 ms | TT: 111 ms<br>AT: 0.0111 ms | TT: 101 ms<br>AT: 0.0101 ms | TT: 111 ms<br>AT: 0.0119 ms | TT: 128 ms<br>AT: 0.0117 ms |
| **random_7K.txt** | TT: 581 ms<br>AT: 0.0581 ms | TT: 686 ms<br>AT: 0.0686 ms | TT: 690 ms<br>AT: 0.069 ms | TT: 676 ms<br>AT: 0.0676 ms | TT: 732 ms<br>AT: 0.0732 ms |
| **random_10K.txt** | TT: 888 ms<br>AT: 0.0888 ms | TT: 940 ms<br>AT: 0.094 ms | TT: 986 ms<br>AT: 0.0986 ms | TT: 989 ms<br>AT: 0.0989 ms | TT: 1073 ms<br>AT: 0.1073 ms |
| **Random_17K.txt** | TT: 1435 ms<br>AT: 0.1435 ms | TT: 1695 ms<br>AT: 0.1695 ms | TT: 1655ms<br>AT: 0.1655 ms | TT: 1628 ms<br>AT: 0.1628 ms | TT: 1716 ms<br>AT: 0.1716 ms |
| **random_100K.txt** | TT: 8289 ms<br>AT: 0.8289 ms | TT: 9533 ms<br>AT: 0.9533 ms | TT: 9459 ms<br>AT: 0.9459 ms | TT: 9818 ms<br>AT: 0.9815 ms | TT: 10064 ms<br>AT: 1.0064 ms |
| **random_1M.txt** | TT: 90639 ms<br>AT: 9.0639 ms | TT: 102890 ms<br>AT: 10.289 ms | TT: 156833 ms<br>AT: 15.6833 ms | TT: 111501 ms<br>AT: 11.1501 ms | TT: 124189 ms<br>AT: 12.4189 ms |



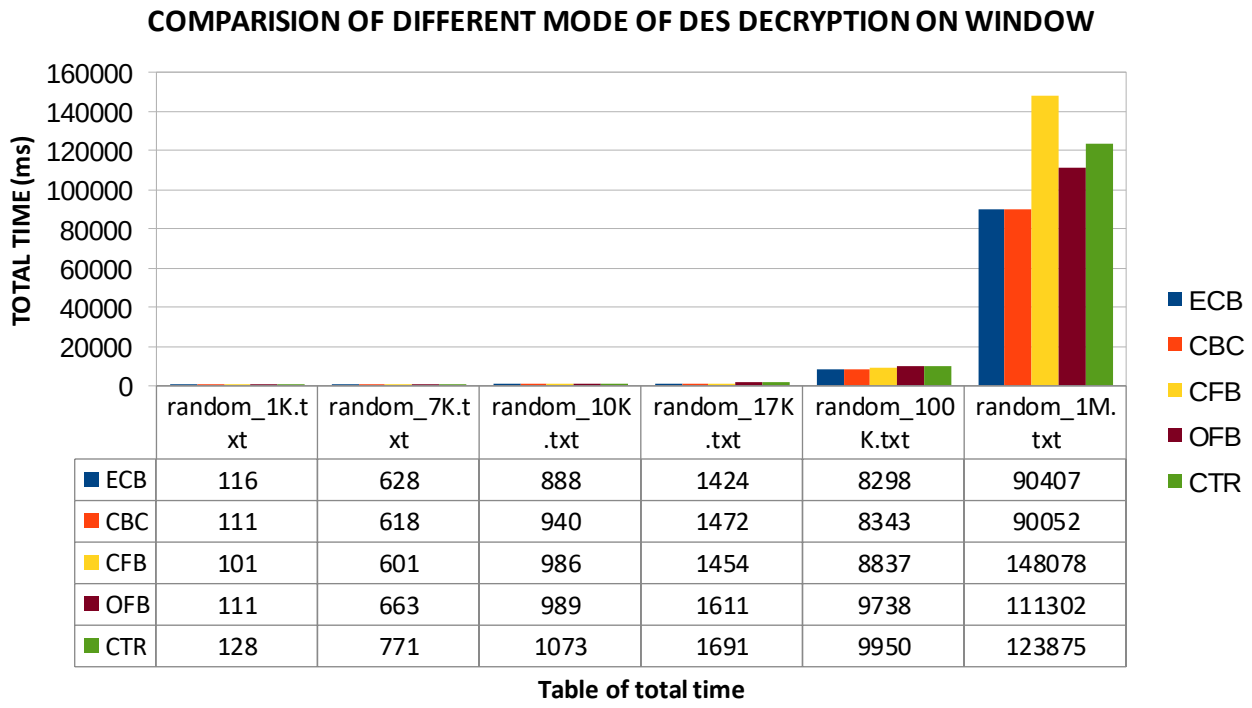

| | random_1K.txt | random_7K.txt | random_10K.txt | random_17K.txt | random_100K.txt | random_1M.txt |
|---|---|---|---|---|---|---|
| ECB | 116 | 581 | 888 | 1435 | 8289 | 90639 |
| CBC | 111 | 686 | 940 | 1695 | 9533 | 102890 |
| CFB | 101 | 690 | 986 | 1655 | 9459 | 156833 |
| OFB | 111 | 676 | 989 | 1628 | 9818 | 111501 |
| CTR | 128 | 732 | 1073 | 1716 | 10064 | 124189 |

**Table of total time**

- **Decryption (10000 times)**
  - **Abbreviation:**
    - TT: Total Time, AT: Average Time

- **Note:**
  - All key and iv are randomly selected.
  - Using g++ compiler

| Mode / Input | ECB | CBC | CFB | OFB | CTR |
|---|---|---|---|---|---|
| **random_1K.txt** | TT: 116 ms<br>AT: 0.0116 ms | TT: 111 ms<br>AT: 0.0111 ms | TT: 101 ms<br>AT: 0.0101 ms | TT: 111 ms<br>AT: 0.0119 ms | TT: 128 ms<br>AT: 0.0117 ms |
| **random_7K.txt** | TT: 628 ms<br>AT: 0.0628 ms | TT: 618 ms<br>AT: 0.0616 ms | TT: 601 ms<br>AT: 0.0601 ms | TT: 663 ms<br>AT: 0.0663 ms | TT: 771 ms<br>AT: 0.0771 ms |
| **random_10K.txt** | TT: 888 ms<br>AT: 0.0888 ms | TT: 940 ms<br>AT: 0.094 ms | TT: 986 ms<br>AT: 0.0986 ms | TT: 989 ms<br>AT: 0.0989 ms | TT: 1073 ms<br>AT: 0.1073 ms |
| **Random_17K.txt** | TT: 1424 ms<br>AT: 0.1424 ms | TT: 1472 ms<br>AT: 0.1472 ms | TT: 1454 ms<br>AT: 0.1454 ms | TT: 1611 ms<br>AT: 0.1611 ms | TT: 1691 ms<br>AT: 0.1691 ms |
| **random_100K.txt** | TT: 8298 ms<br>AT: 0.8298 ms | TT: 8343 ms<br>AT: 0.8343 ms | TT: 8837 ms<br>AT: 0.8837 ms | TT: 9738 ms<br>AT: 0.9738 ms | TT: 9950 ms<br>AT: 0.995 ms |
| **random_1M.txt** | TT: 90407 ms<br>AT: 9.0407 ms | TT: 90052 ms<br>AT: 9.0052 ms | TT: 148078 ms<br>AT: 14.8078 ms | TT: 111302 ms<br>AT: 11.1302 ms | TT: 123875 ms<br>AT: 12.3875 ms |




| | random_1K.txt | random_7K.txt | random_10K.txt | random_17K.txt | random_100K.txt | random_1M.txt |
|---|---|---|---|---|---|---|
| ECB | 116 | 628 | 888 | 1424 | 8298 | 90407 |
| CBC | 111 | 618 | 940 | 1472 | 8343 | 90052 |
| CFB | 101 | 601 | 986 | 1454 | 8837 | 148078 |
| OFB | 111 | 663 | 989 | 1611 | 9738 | 111302 |
| CTR | 128 | 771 | 1073 | 1691 | 9950 | 123875 |

Table of total time

## 4. AES (Windows System)

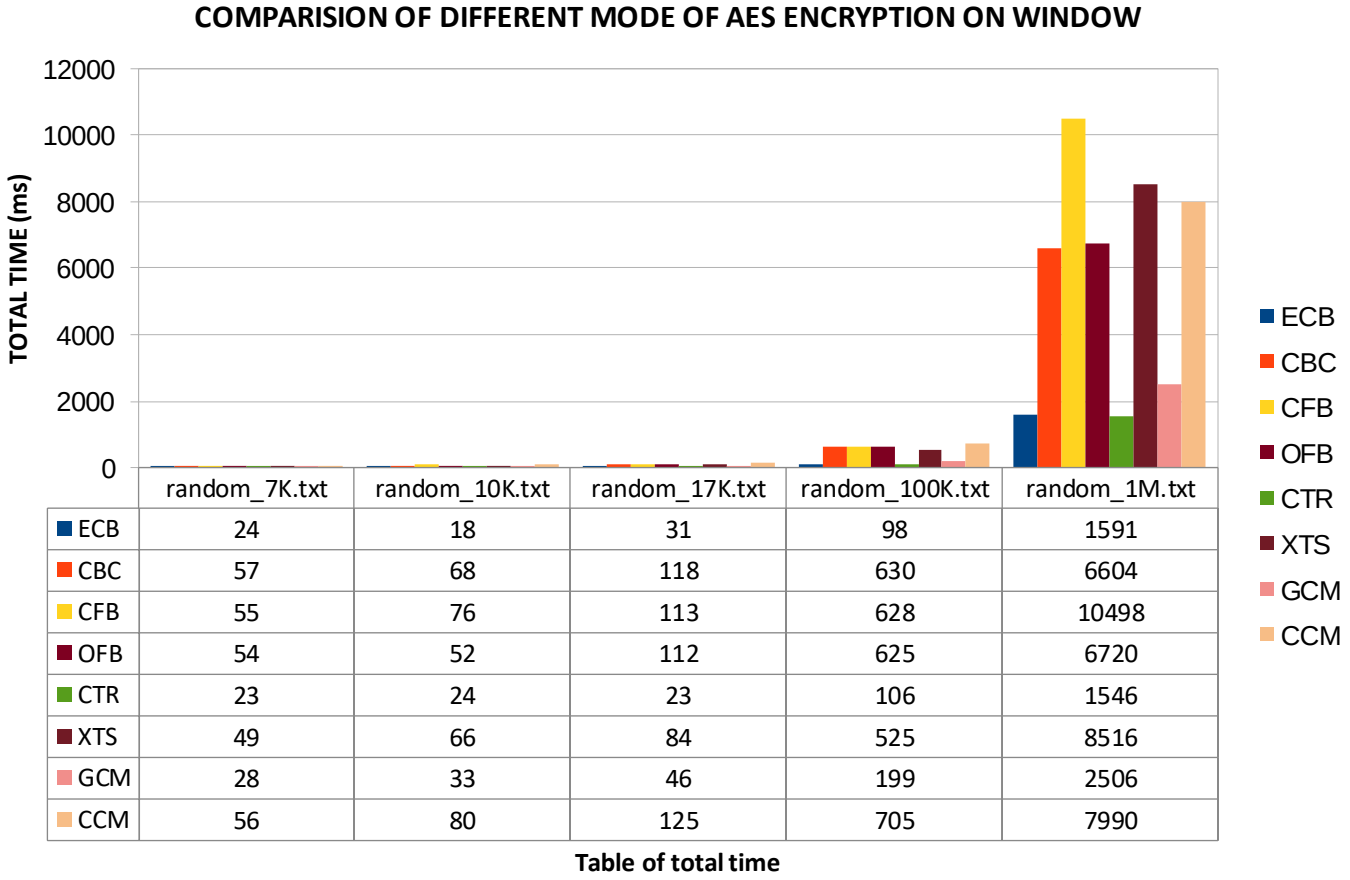
### - Encryption (10000 times)

- **Abbreviation:**
  - TT: Total Time, AT: Average Time
- **Note:**
  - All key and iv are randomly selected.
  - Using g++ compiler
  - 128 bits default
  - For XTS : 256 bits mode

| Mode / Input | ECB | CBC | CFB | OFB | CTR |
|---|---|---|---|---|---|
| **random_1K.txt** | TT: 11 ms<br>AT: 0.0011 ms | TT: 23 ms<br>AT: 0.0023 ms | TT: 17 ms<br>AT: 0.0017 ms | TT: 14 ms<br>AT: 0.0014 ms | TT: 13 ms<br>AT: 0.0013 ms |
| **random_7K.txt** | TT: 24 ms<br>AT: 0.0024 ms | TT: 57 ms<br>AT: 0.0057 ms | TT: 55 ms<br>AT: 0.0055 ms | TT: 54 ms<br>AT: 0.0054 ms | TT: 23 ms<br>AT: 0.0023 ms |
| **random_10K.txt** | TT: 18 ms<br>AT: 0.0018 ms | TT: 68 ms<br>AT: 0.0068 ms | TT: 76 ms<br>AT: 0.0076 ms | TT: 52 ms<br>AT: 0.0052 ms | TT: 24 ms<br>AT: 0.0024 ms |
| **random_17K.txt** | TT: 31 ms<br>AT: 0.0031 ms | TT: 118 ms<br>AT: 0.0118 ms | TT: 113 ms<br>AT: 0.0113 ms | TT: 112 ms<br>AT: 0.0112 ms | TT: 23 ms<br>AT: 0.0023 ms |
| **random_100K.txt** | TT: 98 ms<br>AT: 0.0098 ms | TT: 630 ms<br>AT: 0.063 ms | TT: 628 ms<br>AT: 0.0628 ms | TT: 625 ms<br>AT: 0.0625 ms | TT: 106 ms<br>AT: 1.0106 ms |
| **random_1M.txt** | TT: 1591 ms<br>AT: 0.1591 ms | TT: 6604 ms<br>AT: 0.6604 ms | TT: 10498 ms<br>AT: 1.0498 ms | TT: 6720 ms<br>AT: 0.6720 ms | TT: 1546 ms<br>AT: 0.1546 ms |

| Mode / Input | XTS | GCM | CCM |
|---|---|---|---|
| **random_1K.txt** | TT: 22 ms<br>AT: 0.0022 ms | TT: 12 ms<br>AT: 0.0012 ms | TT: 29 ms<br>AT: 0.0029 ms |
| **random_7K.txt** | TT: 49 ms<br>AT: 0.0049 ms | TT: 28 ms<br>AT: 0.0028 ms | TT: 56 ms<br>AT: 0.0056 ms |
| **random_10K.txt** | TT: 66 ms<br>AT: 0.0066 ms | TT: 33 ms<br>AT: 0.0033 ms | TT: 80 ms<br>AT: 0.008 ms |

| | | | |
|---|---|---|---|
| **random_17K.txt** | TT: 84 ms<br>AT: 0.0084 ms | TT: 46 ms<br>AT: 0.0046 ms | TT: 125 ms<br>AT: 0.0125 ms |
| **random_100K.txt** | TT: 525 ms<br>AT: 0.0525 ms | TT: 199 ms<br>AT: 0.0199 ms | TT: 705 ms<br>AT: 0.0705 ms |
| **random_1M.txt** | TT: 8615 ms<br>AT: 0.8615 ms | TT: 2506 ms<br>AT: 0.2506 ms | TT: 7990 ms<br>AT: 0.799 ms |



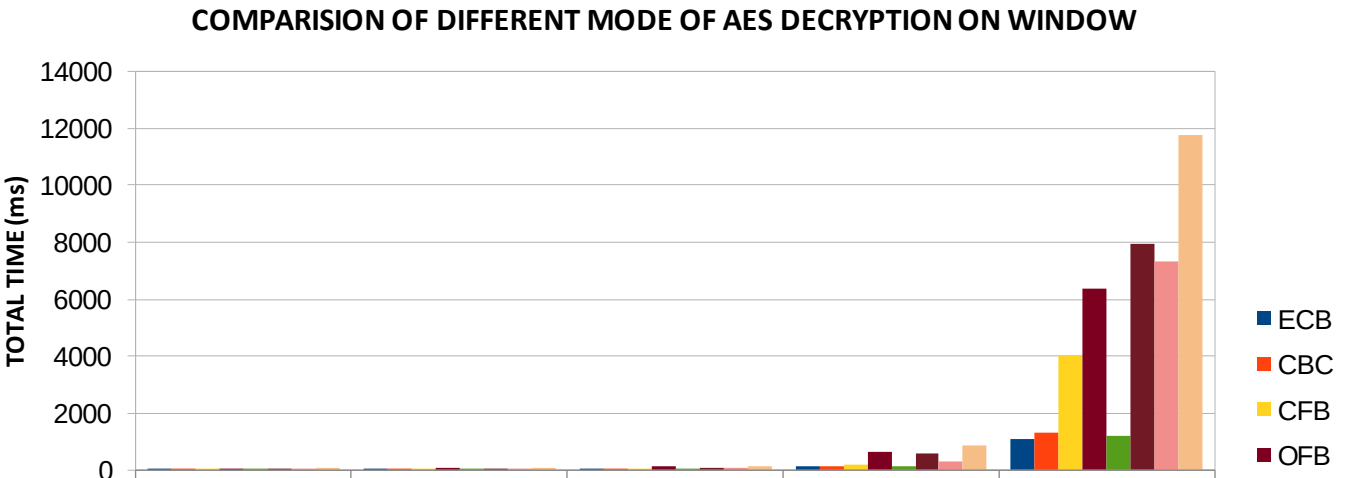

| | random_7K.txt | random_10K.txt | random_17K.txt | random_100K.txt | random_1M.txt |
|---|---|---|---|---|---|
| ECB | 24 | 18 | 31 | 98 | 1591 |
| CBC | 57 | 68 | 118 | 630 | 6604 |
| CFB | 55 | 76 | 113 | 628 | 10498 |
| OFB | 54 | 52 | 112 | 625 | 6720 |
| CTR | 23 | 24 | 23 | 106 | 1546 |
| XTS | 49 | 66 | 84 | 525 | 8516 |
| GCM | 28 | 33 | 46 | 199 | 2506 |
| CCM | 56 | 80 | 125 | 705 | 7990 |

**Table of total time**

- **Decryption (10000 times)**
  - **Abbreviation:**
    - TT: Total Time, AT: Average Time
  - **Note:**
    - All key and iv are randomly selected.
    - Using g++ compiler
    - GCM and CCM using input authentication: ***hello*** and default IV

| Mode / Input | ECB | CBC | CFB | OFB | CTR |
|---|---|---|---|---|---|
| **random_1K.txt** | TT: 11 ms<br>AT: 0.0011 ms | TT: 10 ms<br>AT: 0.001 ms | TT: 14 ms<br>AT: 0.0014 ms | TT: 18 ms<br>AT: 0.0018 ms | TT: 12 ms<br>AT: 0.0012 ms |
| **random_7K.txt** | TT: 12 ms<br>AT: 0.0012 ms | TT: 19 ms<br>AT: 0.0019 ms | TT: 27 ms<br>AT: 0.0027 ms | TT: 49 ms<br>AT: 0.0049 ms | TT: 17 ms<br>AT: 0.0017 ms |
| **random_10K.txt** | TT: 21 ms<br>AT: 0.0021 ms | TT: 31 ms<br>AT: 0.0031 ms | TT: 25 ms<br>AT: 0.0025 ms | TT: 82 ms<br>AT: 0.0082 ms | TT: 23 ms<br>AT: 0.023 ms |
| **random_17K.txt** | TT: 22 ms<br>AT: 0.0022 ms | TT: 26 ms<br>AT: 0.0026 ms | TT: 39 ms<br>AT: 0.0039 ms | TT: 117 ms<br>AT: 0.0117 ms | TT: 39 ms<br>AT: 0.0039 ms |
| **random_100K.txt** | TT: 120 ms<br>AT: 0.012 ms | TT: 116 ms<br>AT: 0.0116 ms | TT: 211 ms<br>AT: 0.0211 ms | TT: 622 ms<br>AT: 0.0622 ms | TT: 120 ms<br>AT: 0.012 ms |
| **random_1M.txt** | TT: 1066 ms<br>AT: 0.1066 ms | TT: 1319 ms<br>AT: 0.1319 ms | TT: 4035 ms<br>AT: 0.4035 ms | TT: 6361 ms<br>AT: 0.6361 ms | TT: 1218 ms<br>AT: 0.1218 ms |

| Mode / Input | XTS | GCM | CCM |
|---|---|---|---|
| **random_1K.txt** | TT: 30 ms<br>AT: 0.003 ms | TT: 34 ms<br>AT: 0.0034 ms | TT: 39 ms<br>AT: 0.0039 ms |
| **random_7K.txt** | TT: 44 ms<br>AT: 0.0044 ms | TT: 40 ms<br>AT: 0.004 ms | TT: 75 ms<br>AT: 0.0075 ms |
| **random_10K.txt** | TT: 55 ms<br>AT: 0.0055 ms | TT: 51 ms<br>AT: 0.0051 ms | TT: 93 ms<br>AT: 0.0093 ms |
| **random_17K.txt** | TT: 105 ms<br>AT: 0.0105 ms | TT: 64 ms<br>AT: 0.0064 ms | TT: 157 ms<br>AT: 0.0157 ms |
| **random_100K.txt** | TT: 563 ms<br>AT: 0.0563 ms | TT: 286 ms<br>AT: 0.0286 ms | TT: 846 ms<br>AT: 0.0846 ms |
| **random_1M.txt** | TT: 7941 ms<br>AT: 0.7941 ms | TT: 7333 ms<br>AT: 0.7333 ms | TT: 11769 ms<br>AT: 1.1769 ms |




| | random_7K.txt | random_10K.txt | random_17K.txt | random_100K.txt | random_1M.txt |
|---|---|---|---|---|---|
| ECB | 12 | 21 | 22 | 120 | 1066 |
| CBC | 19 | 31 | 26 | 116 | 1319 |
| CFB | 27 | 25 | 39 | 211 | 4035 |
| OFB | 49 | 82 | 117 | 622 | 6361 |
| CTR | 17 | 23 | 39 | 120 | 1218 |
| XTS | 44 | 55 | 105 | 563 | 7941 |
| GCM | 40 | 51 | 64 | 286 | 7333 |
| CCM | 75 | 93 | 157 | 846 | 11769 |

Table of total time

## 5. DES (Linux System)

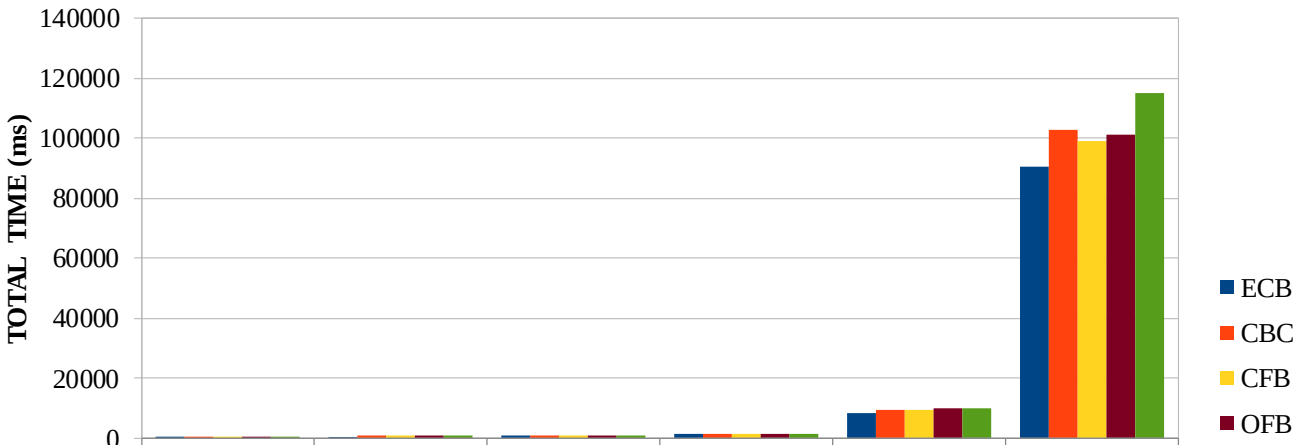
### - Encryption (10000 times)

- **Abbreviation:**
  - TT: Total Time, AT: Average Time
- **Note:**
  - All key and iv are randomly selected.
  - Using g++ compiler

| Mode / Input | ECB | CBC | CFB | OFB | CTR |
|---|---|---|---|---|---|
| **random_1K.txt** | TT: 116 ms<br>AT: 0.0116 ms | TT: 111 ms<br>AT: 0.0111 ms | TT: 101 ms<br>AT: 0.0101 ms | TT: 111 ms<br>AT: 0.0119 ms | TT: 128 ms<br>AT: 0.0117 ms |
| **random_7K.txt** | TT: 581 ms<br>AT: 0.0581 ms | TT: 686 ms<br>AT: 0.0686 ms | TT: 690 ms<br>AT: 0.069 ms | TT: 676 ms<br>AT: 0.0676 ms | TT: 732 ms<br>AT: 0.0732 ms |

| | | | | | |
|---|---|---|---|---|---|
| **random_10K.txt** | TT: 888 ms<br>AT: 0.0888 ms | TT: 940 ms<br>AT: 0.094 ms | TT: 986 ms<br>AT: 0.0986 ms | TT: 989 ms<br>AT: 0.0989 ms | TT: 1073 ms<br>AT: 0.1073 ms |
| **Random_17K.txt** | TT: 1435 ms<br>AT: 0.1435 ms | TT: 1695 ms<br>AT: 0.1695 ms | TT: 1655ms<br>AT: 0.1655 ms | TT: 1628 ms<br>AT: 0.1628 ms | TT: 1716 ms<br>AT: 0.1716 ms |
| **random_100K.txt** | TT: 8289 ms<br>AT: 0.8289 ms | TT: 9533 ms<br>AT: 0.9533 ms | TT: 9459 ms<br>AT: 0.9459 ms | TT: 9818 ms<br>AT: 0.9815 ms | TT: 10064 ms<br>AT: 1.0064 ms |
| **random_1M.txt** | TT: 90639 ms<br>AT: 9.0639 ms | TT: 102890 ms<br>AT: 10.289 ms | TT: 98806 ms<br>AT: 9.8806 ms | TT: 100898 ms<br>AT: 10.0898 ms | TT: 114857 ms<br>AT: 11.4857 ms |

**COMPARISION OF DIFFERENT MODE OF DES ENCRYPTION ON UBUNTU**



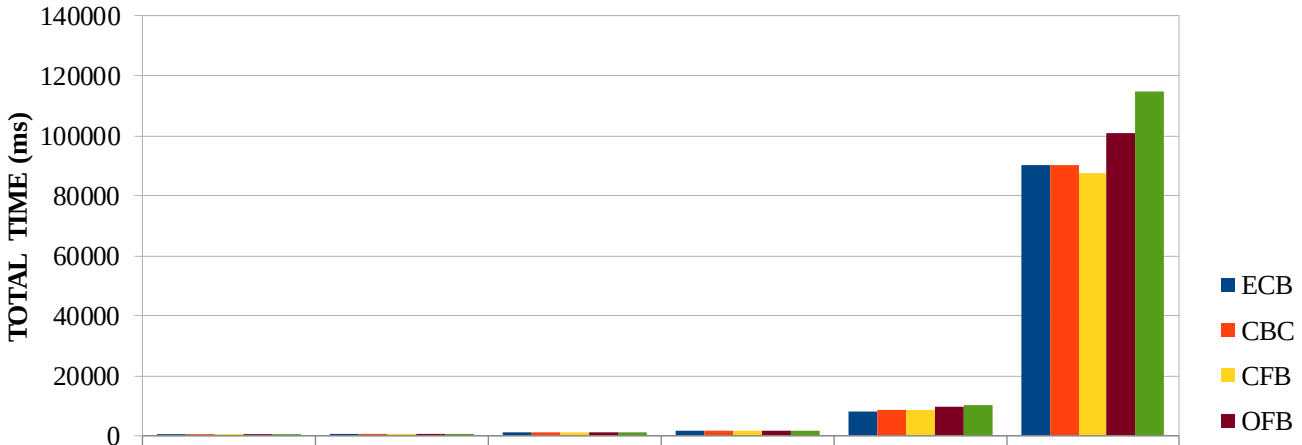

| | random_1K.txt | random_7K.txt | random_10K.txt | random_17K.txt | random_100K.txt | random_1M.txt |
|---|---|---|---|---|---|---|
| ECB | 116 | 581 | 888 | 1435 | 8289 | 90639 |
| CBC | 111 | 686 | 940 | 1695 | 9533 | 102890 |
| CFB | 101 | 690 | 986 | 1655 | 9459 | 98806 |
| OFB | 111 | 676 | 989 | 1628 | 9818 | 100898 |
| CTR | 128 | 732 | 1073 | 1716 | 10064 | 114857 |

**Table of total time**

- **Decryption (10000 times)**
  - **Abbreviation:**
    - TT: Total Time, AT: Average Time
  - **Note:**
    - All key and iv are randomly selected.
    - Using g++ compiler

| Mode / Input | ECB | CBC | CFB | OFB | CTR |
|---|---|---|---|---|---|
| **random_1K.txt** | TT: 116 ms<br>AT: 0.0116 ms | TT: 111 ms<br>AT: 0.0111 ms | TT: 101 ms<br>AT: 0.0101 ms | TT: 111 ms<br>AT: 0.0119 ms | TT: 128 ms<br>AT: 0.0117 ms |
| **random_7K.txt** | TT: 628 ms<br>AT: 0.0628 ms | TT: 618 ms<br>AT: 0.0616 ms | TT: 601 ms<br>AT: 0.0601 ms | TT: 663 ms<br>AT: 0.0663 ms | TT: 771 ms<br>AT: 0.0771 ms |
| **random_10K.txt** | TT: 888 ms<br>AT: 0.0888 ms | TT: 940 ms<br>AT: 0.094 ms | TT: 986 ms<br>AT: 0.0986 ms | TT: 989 ms<br>AT: 0.0989 ms | TT: 1073 ms<br>AT: 0.1073 ms |
| **Random_17K.txt** | TT: 1424 ms<br>AT: 0.1424 ms | TT: 1472 ms<br>AT: 0.1472 ms | TT: 1454 ms<br>AT: 0.1454 ms | TT: 1611 ms<br>AT: 0.1611 ms | TT: 1691 ms<br>AT: 0.1691 ms |
| **random_100K.txt** | TT: 8298 ms<br>AT: 0.8298 ms | TT: 8343 ms<br>AT: 0.8343 ms | TT: 8837 ms<br>AT: 0.8837 ms | TT: 9738 ms<br>AT: 0.9738 ms | TT: 9950 ms<br>AT: 0.995 ms |
| **random_1M.txt** | TT: 90407 ms<br>AT: 9.0407 ms | TT: 90052 ms<br>AT: 9.0052 ms | TT: 87243 ms<br>AT: 8.7243 ms | TT: 100909 ms<br>AT: 10.0909 ms | TT: 114943 ms<br>AT: 11.4943 ms |

**COMPARISION OF DIFFERENT MODE OF DES DECRYPTION ON UBUNTU**




| | random_1K.txt | random_7K.txt | random_10K.txt | random_17K.txt | random_100K.txt | random_1M.txt |
|---|---|---|---|---|---|---|
| ECB | 116 | 628 | 888 | 1424 | 8298 | 90407 |
| CBC | 111 | 618 | 940 | 1472 | 8343 | 90052 |
| CFB | 101 | 601 | 986 | 1454 | 8837 | 87243 |
| OFB | 111 | 663 | 989 | 1611 | 9738 | 100909 |
| CTR | 128 | 771 | 1073 | 1691 | 9950 | 114943 |

**Table of total time**

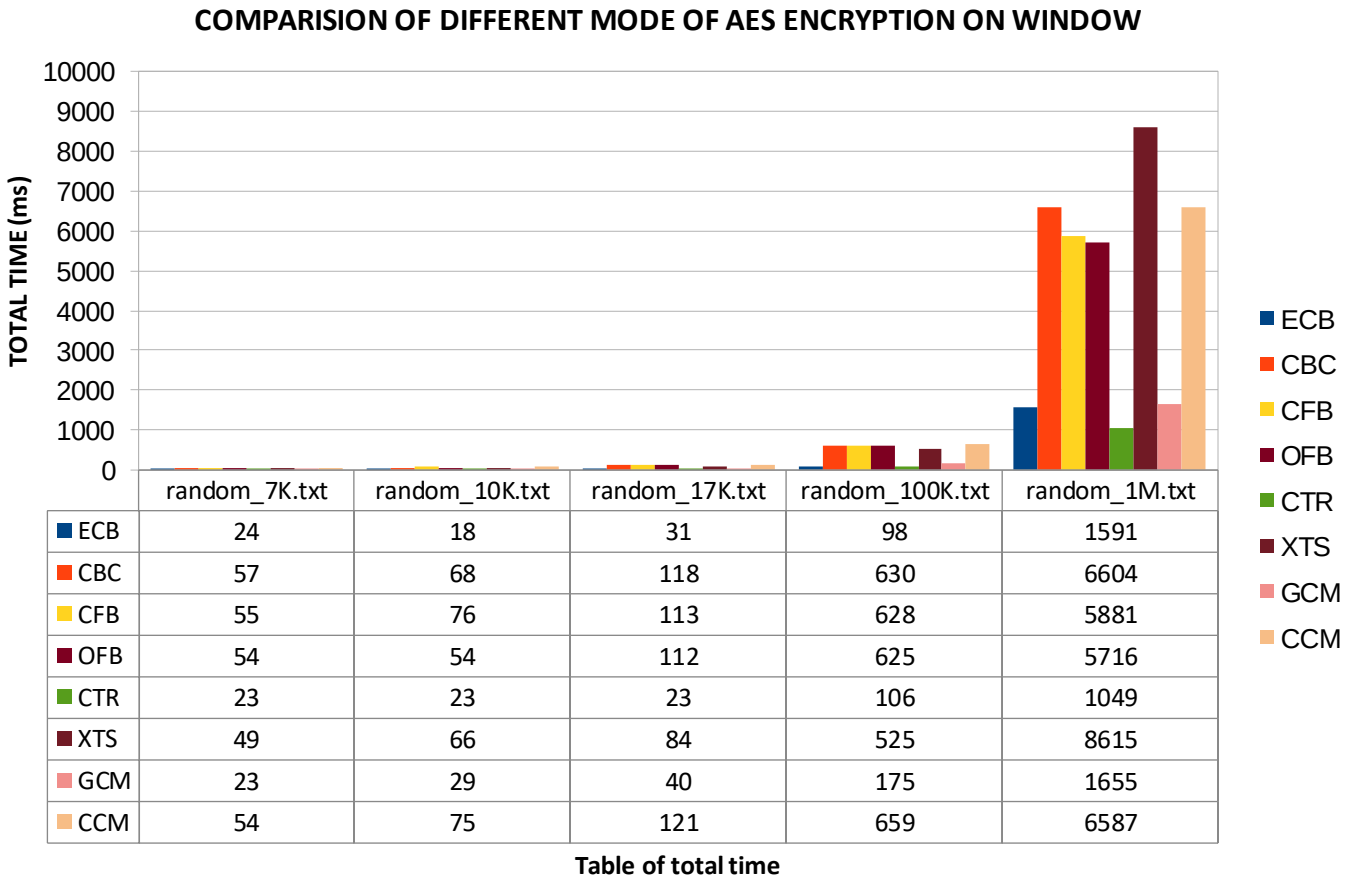
## 6. AES (Linux System)

- **Encryption (10000 times)**
  - **Abbreviation:**
    - TT: Total Time, AT: Average Time
  - **Note:**
    - All key and iv are randomly selected.
    - Using g++ compiler
    - 128 bits default
    - For XTS : 256 bits mode

| Mode / Input | ECB | CBC | CFB | OFB | CTR |
|---|---|---|---|---|---|
| random_1K.txt | TT: 11 ms<br>AT: 0.0011 ms | TT: 23 ms<br>AT: 0.0023 ms | TT: 17 ms<br>AT: 0.0017 ms | TT: 14 ms<br>AT: 0.0014 ms | TT: 13 ms<br>AT: 0.0013 ms |
| random_7K.txt | TT: 24 ms<br>AT: 0.0024 ms | TT: 57 ms<br>AT: 0.0057 ms | TT: 55 ms<br>AT: 0.0055 ms | TT: 54 ms<br>AT: 0.0054 ms | TT: 23 ms<br>AT: 0.0023 ms |
| random_10K.txt | TT: 18 ms<br>AT: 0.0018 ms | TT: 68 ms<br>AT: 0.0068 ms | TT: 76 ms<br>AT: 0.0076 ms | TT: 52 ms<br>AT: 0.0052 ms | TT: 24 ms<br>AT: 0.0024 ms |
| random_17K.txt | TT: 31 ms<br>AT: 0.0031 ms | TT: 118 ms<br>AT: 0.0118 ms | TT: 113 ms<br>AT: 0.0113 ms | TT: 112 ms<br>AT: 0.0112 ms | TT: 23 ms<br>AT: 0.0023 ms |
| random_100K.txt | TT: 98 ms<br>AT: 0.0098 ms | TT: 630 ms<br>AT: 0.063 ms | TT: 628 ms<br>AT: 0.0628 ms | TT: 625 ms<br>AT: 0.0625 ms | TT: 106 ms<br>AT: 1.0106 ms |
| random_1M.txt | TT: 1591 ms<br>AT: 0.1591 ms | TT: 6604 ms<br>AT: 0.6604 ms | TT: 5881 ms<br>AT: 0.5881 ms | TT: 5716 ms<br>AT: 0.5716 ms | TT: 1049 ms<br>AT: 0.1049 ms |

| Mode / Input | XTS | GCM | CCM |
|---|---|---|---|
| random_1K.txt | TT: 22 ms<br>AT: 0.0022 ms | TT: 11 ms<br>AT: 0.0011 ms | TT: 16 ms<br>AT: 0.0016 ms |
| random_7K.txt | TT: 49 ms<br>AT: 0.0049 ms | TT: 23 ms<br>AT: 0.0023 ms | TT: 54 ms<br>AT: 0.0054 ms |
| random_10K.txt | TT: 66 ms<br>AT: 0.0066 ms | TT: 29 ms<br>AT: 0.0029ms | TT: 75 ms<br>AT: 0.0075ms |
| random_17K.txt | TT: 84 ms | TT: 40 ms | TT: 121 ms |

| | | | |
|---|---|---|---|
| | AT: 0.0084 ms | AT: 0.004 ms | AT: 0.0121 ms |
| **random_100K.txt** | TT: 525 ms<br>AT: 0.0525 ms | TT: 175 ms<br>AT: 0.0175 ms | TT: 659 ms<br>AT: 0.0659ms |
| **random_1M.txt** | TT: 8615 ms<br>AT: 0.8615 ms | TT: 1655 ms<br>AT: 0.1655 ms | TT: 6587 ms<br>AT: 0.6587 ms |




| | random_7K.txt | random_10K.txt | random_17K.txt | random_100K.txt | random_1M.txt |
|---|---|---|---|---|---|
| ECB | 24 | 18 | 31 | 98 | 1591 |
| CBC | 57 | 68 | 118 | 630 | 6604 |
| CFB | 55 | 76 | 113 | 628 | 5881 |
| OFB | 54 | 54 | 112 | 625 | 5716 |
| CTR | 23 | 23 | 23 | 106 | 1049 |
| XTS | 49 | 66 | 84 | 525 | 8615 |
| GCM | 23 | 29 | 40 | 175 | 1655 |
| CCM | 54 | 75 | 121 | 659 | 6587 |

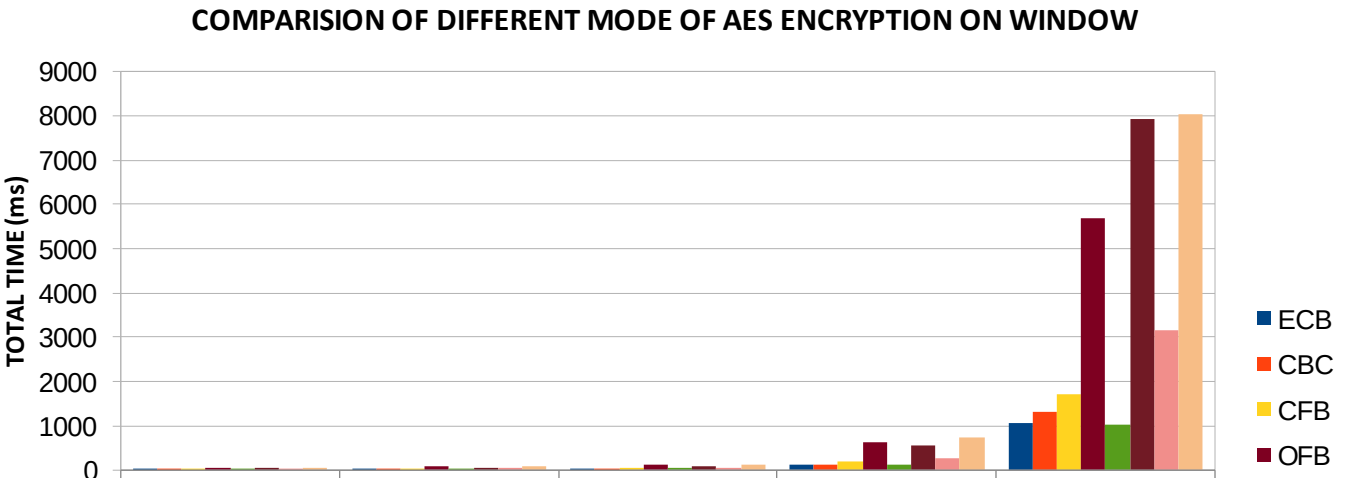
Table of total time

- **Decryption (10000 times)**
  - **Abbreviation:**
    - TT: Total Time, AT: Average Time
  - **Note:**
    - All key and iv are randomly selected.
    - Using g++ compiler

➢

| Mode / Input | ECB | CBC | CFB | OFB | CTR |
|---|---|---|---|---|---|
| **random_1K.txt** | TT: 11 ms<br>AT: 0.0011 ms | TT: 10 ms<br>AT: 0.001 ms | TT: 14 ms<br>AT: 0.0014 ms | TT: 18 ms<br>AT: 0.0018 ms | TT: 12 ms<br>AT: 0.0012 ms |
| **random_7K.txt** | TT: 12 ms<br>AT: 0.0012 ms | TT: 19 ms<br>AT: 0.0019 ms | TT: 27 ms<br>AT: 0.0027 ms | TT: 49 ms<br>AT: 0.0049 ms | TT: 17 ms<br>AT: 0.0017 ms |
| **random_10K.txt** | TT: 21 ms<br>AT: 0.0021 ms | TT: 31 ms<br>AT: 0.0031 ms | TT: 25 ms<br>AT: 0.0025 ms | TT: 82 ms<br>AT: 0.0082 ms | TT: 23 ms<br>AT: 0.023 ms |
| **random_17K.txt** | TT: 22 ms<br>AT: 0.0022 ms | TT: 26 ms<br>AT: 0.0026 ms | TT: 39 ms<br>AT: 0.0039 ms | TT: 117 ms<br>AT: 0.0117 ms | TT: 39 ms<br>AT: 0.0039 ms |
| **random_100K.txt** | TT: 120 ms<br>AT: 0.012 ms | TT: 116 ms<br>AT: 0.0116 ms | TT: 211 ms<br>AT: 0.0211 ms | TT: 622 ms<br>AT: 0.0622 ms | TT: 120 ms<br>AT: 0.012 ms |
| **random_1M.txt** | TT: 1066 ms<br>AT: 0.1066 ms | TT: 1319 ms<br>AT: 0.1319 ms | TT: 1728 ms<br>AT: 0.1728 ms | TT: 5681 ms<br>AT: 0.5681 ms | TT: 1019 ms<br>AT: 0.1019 ms |

| Mode / Input | XTS | GCM | CCM |
|---|---|---|---|
| **random_1K.txt** | TT: 30 ms<br>AT: 0.003 ms | TT: 18 ms<br>AT: 0.0018 ms | TT: 22 ms<br>AT: 0.0022 ms |
| **random_7K.txt** | TT: 44 ms<br>AT: 0.0044 ms | TT: 33 ms<br>AT: 0.0033 ms | TT: 63 ms<br>AT: 0.0063 ms |
| **random_10K.txt** | TT: 55 ms<br>AT: 0.0055 ms | TT: 41 ms<br>AT: 0.0041 ms | TT: 86 ms<br>AT: 0.0086ms |
| **random_17K.txt** | TT: 105 ms<br>AT: 0.0105 ms | TT: 57 ms<br>AT: 0.0057 ms | TT: 136 ms<br>AT: 0.0136 ms |
| **random_100K.txt** | TT: 563 ms<br>AT: 0.0563 ms | TT: 262 ms<br>AT: 0.0262 ms | TT: 741 ms<br>AT: 0.0741 ms |
| **random_1M.txt** | TT: 7941 ms<br>AT: 0.7941 ms | TT: 3161 ms<br>AT: 0.3161 ms | TT: 8022 ms<br>AT: 0.8022ms |




| | random_7K.txt | random_10K.txt | random_17K.txt | random_100K.txt | random_1M.txt |
|---|---|---|---|---|---|
| ECB | 12 | 21 | 22 | 120 | 1066 |
| CBC | 19 | 31 | 26 | 116 | 1319 |
| CFB | 27 | 25 | 39 | 211 | 1728 |
| OFB | 49 | 82 | 117 | 622 | 5681 |
| CTR | 17 | 23 | 39 | 120 | 1019 |
| XTS | 44 | 55 | 105 | 563 | 7941 |
| GCM | 33 | 41 | 57 | 262 | 3161 |
| CCM | 63 | 86 | 136 | 741 | 8022 |

**Table of total time**

## 7. Conclusion

- AES is faster than DES based on the run time result.

  + AES using 128-bit block size, compared to DES (only 64-bit block size)

  + The algorithm of AES is fewer (only 10, 12 or 14 rounds depending on keys size while DES have to loop 16 rounds

  + AES is suitable for implementation on hardware and software based on it efficient.

- Shifting to the output result of the report when executing both DES and AES, we can clearly see that the bigger the file is, the higher it takes to complete 10000 times of functioning.

⇨ From a security standpoint, DES has been considered obsolete since 2001 due to vulnerabilities in its 56-bit key length, making it susceptible to brute-force attacks. AES, on the other hand, has become the standard for modern symmetric encryption, offering a more robust and secure alternative for protecting sensitive data.

⇨ The result indicates that encryption and decryption time increase as files grow, which is expected due to the nature of symmetric cryptographic operators.

- On Window, AES consistently achieves lower execution times compared to DES across all file sizes and encryption modes. However, execution times tend to be slightly higher than on Linux.
- On Linux, AES and DES exhibit slightly better performance in most cases. This could be due to Linux's more efficient scheduling process and lower system overhead compared to Windows.
- When focusing on execution time, using the same key for all test cases results in the best performance on Linux, while Windows maintains more consistent execution across different scenarios.

⇨ In conclusion, this lab report is only a brief comparison of DES and AES based on it time performance and how it was built based on the crytopp library in C++.