**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** 2](#_Toc193734277)

[**2.** **Input testcase** 2](#_Toc193734278)

[**3.** **DES (Windows System)** 2](#_Toc193734279)

[- **Encryption (10000 times)** 2](#_Toc193734280)

[- **Decryption (10000 times)** 3](#_Toc193734281)

[**4.** **AES (Windows System)** 5](#_Toc193734282)

[- **Encryption (10000 times)** 5](#_Toc193734283)

[- **Decryption (10000 times)** 6](#_Toc193734284)

[**5.** **DES (Linux System)** 8](#_Toc193734285)

[- **Encryption (10000 times)** 8](#_Toc193734286)

[- **Decryption (10000 times)** 9](#_Toc193734287)

[**6.** **AES (Linux System)** 10](#_Toc193734288)

[- **Encryption (10000 times)** 11](#_Toc193734289)

[- **Decryption (10000 times)** 12](#_Toc193734290)

[**7.** **Conclusion** 14](#_Toc193734291)

1. **Hardware resource**

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

1. **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**

1. **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  AT: 0.0116 ms | TT: 111 ms  AT: 0.0111 ms | TT: 101 ms  AT: 0.0101 ms | TT: 111 ms  AT: 0.0119 ms | TT: 128 ms  AT: 0.0117 ms |
| **random\_7K.txt** | TT: 581 ms  AT: 0.0581 ms | TT: 686 ms  AT: 0.0686 ms | TT: 690 ms  AT: 0.069 ms | TT: 676 ms  AT: 0.0676 ms | TT: 732 ms  AT: 0.0732 ms |
| **random\_10K.txt** | TT: 888 ms  AT: 0.0888 ms | TT: 940 ms  AT: 0.094 ms | TT: 986 ms  AT: 0.0986 ms | TT: 989 ms  AT: 0.0989 ms | TT: 1073 ms  AT: 0.1073 ms |
| **Random\_17K.txt** | TT: 1435 ms  AT: 0.1435 ms | TT: 1695 ms  AT: 0.1695 ms | TT: 1655ms  AT: 0.1655 ms | TT: 1628 ms  AT: 0.1628 ms | TT: 1716 ms  AT: 0.1716 ms |
| **random\_100K.txt** | TT: 8289 ms  AT: 0.8289 ms | TT: 9533 ms  AT: 0.9533 ms | TT: 9459 ms  AT: 0.9459 ms | TT: 9818 ms  AT: 0.9815 ms | TT: 10064 ms  AT: 1.0064 ms |
| **random\_1M.txt** | TT: 90639 ms  AT: 9.0639 ms | TT: 102890 ms  AT: 10.289 ms | TT: 156833 ms  AT: 15.6833 ms | TT: 111501 ms  AT: 11.1501 ms | TT: 124189 ms  AT: 12.4189 ms |

* **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  AT: 0.0116 ms | TT: 111 ms  AT: 0.0111 ms | TT: 101 ms  AT: 0.0101 ms | TT: 111 ms  AT: 0.0119 ms | TT: 128 ms  AT: 0.0117 ms |
| **random\_7K.txt** | TT: 628 ms  AT: 0.0628 ms | TT: 618 ms  AT: 0.0616 ms | TT: 601 ms  AT: 0.0601 ms | TT: 663 ms  AT: 0.0663 ms | TT: 771 ms  AT: 0.0771 ms |
| **random\_10K.txt** | TT: 888 ms  AT: 0.0888 ms | TT: 940 ms  AT: 0.094 ms | TT: 986 ms  AT: 0.0986 ms | TT: 989 ms  AT: 0.0989 ms | TT: 1073 ms  AT: 0.1073 ms |
| **Random\_17K.txt** | TT: 1424 ms  AT: 0.1424 ms | TT: 1472 ms  AT: 0.1472 ms | TT: 1454 ms  AT: 0.1454 ms | TT: 1611 ms  AT: 0.1611 ms | TT: 1691 ms  AT: 0.1691 ms |
| **random\_100K.txt** | TT: 8298 ms  AT: 0.8298 ms | TT: 8343 ms  AT: 0.8343 ms | TT: 8837 ms  AT: 0.8837 ms | TT: 9738 ms  AT: 0.9738 ms | TT: 9950 ms  AT: 0.995 ms |
| **random\_1M.txt** | TT: 90407 ms  AT: 9.0407 ms | TT: 90052 ms  AT: 9.0052 ms | TT: 148078 ms  AT: 14.8078 ms | TT: 111302 ms  AT: 11.1302 ms | TT: 123875 ms  AT: 12.3875 ms |

1. **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  AT: 0.0011 ms | TT: 23 ms  AT: 0.0023 ms | TT: 17 ms  AT: 0.0017 ms | TT: 14 ms  AT: 0.0014 ms | TT: 13 ms  AT: 0.0013 ms |
| **random\_7K.txt** | TT: 24 ms  AT: 0.0024 ms | TT: 57 ms  AT: 0.0057 ms | TT: 55 ms  AT: 0.0055 ms | TT: 54 ms  AT: 0.0054 ms | TT: 23 ms  AT: 0.0023 ms |
| **random\_10K.txt** | TT: 18 ms  AT: 0.0018 ms | TT: 68 ms  AT: 0.0068 ms | TT: 76 ms  AT: 0.0076 ms | TT: 52 ms  AT: 0.0052 ms | TT: 24 ms  AT: 0.0024 ms |
| **random\_17K.txt** | TT: 31 ms  AT: 0.0031 ms | TT: 118 ms  AT: 0.0118 ms | TT: 113 ms  AT: 0.0113 ms | TT: 112 ms  AT: 0.0112 ms | TT: 23 ms  AT: 0.0023 ms |
| **random\_100K.txt** | TT: 98 ms  AT: 0.0098 ms | TT: 630 ms  AT: 0.063 ms | TT: 628 ms  AT: 0.0628 ms | TT: 625 ms  AT: 0.0625 ms | TT: 106 ms  AT: 1.0106 ms |
| **random\_1M.txt** | TT: 1591 ms  AT: 0.1591 ms | TT: 6604 ms  AT: 0.6604 ms | TT: 10498 ms  AT: 1.0498 ms | TT: 6720 ms  AT: 0.6720 ms | TT: 1546 ms  AT: 0.1546 ms |

|  |  |  |  |
| --- | --- | --- | --- |
| **Mode**  **Input** | **XTS** | **GCM** | **CCM** |
| **random\_1K.txt** | TT: 22 ms  AT: 0.0022 ms | TT: 12 ms  AT: 0.0012 ms | TT: 29 ms  AT: 0.0029 ms |
| **random\_7K.txt** | TT: 49 ms  AT: 0.0049 ms | TT: 28 ms  AT: 0.0028 ms | TT: 56 ms  AT: 0.0056 ms |
| **random\_10K.txt** | TT: 66 ms  AT: 0.0066 ms | TT: 33 ms  AT: 0.0033 ms | TT: 80 ms  AT: 0.008 ms |
| **random\_17K.txt** | TT: 84 ms  AT: 0.0084 ms | TT: 46 ms  AT: 0.0046 ms | TT: 125 ms  AT: 0.0125 ms |
| **random\_100K.txt** | TT: 525 ms  AT: 0.0525 ms | TT: 199 ms  AT: 0.0199 ms | TT: 705 ms  AT: 0.0705 ms |
| **random\_1M.txt** | TT: 8615 ms  AT: 0.8615 ms | TT: 2506 ms  AT: 0.2506 ms | TT: 7990 ms  AT: 0.799 ms |

* **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  AT: 0.0011 ms | TT: 10 ms  AT: 0.001 ms | TT: 14 ms  AT: 0.0014 ms | TT: 18 ms  AT: 0.0018 ms | TT: 12 ms  AT: 0.0012 ms |
| **random\_7K.txt** | TT: 12 ms  AT: 0.0012 ms | TT: 19 ms  AT: 0.0019 ms | TT: 27 ms  AT: 0.0027 ms | TT: 49 ms  AT: 0.0049 ms | TT: 17 ms  AT: 0.0017 ms |
| **random\_10K.txt** | TT: 21 ms  AT: 0.0021 ms | TT: 31 ms  AT: 0.0031 ms | TT: 25 ms  AT: 0.0025 ms | TT: 82 ms  AT: 0.0082 ms | TT: 23 ms  AT: 0.023 ms |
| **random\_17K.txt** | TT: 22 ms  AT: 0.0022 ms | TT: 26 ms  AT: 0.0026 ms | TT: 39 ms  AT: 0.0039 ms | TT: 117 ms  AT: 0.0117 ms | TT: 39 ms  AT: 0.0039 ms |
| **random\_100K.txt** | TT: 120 ms  AT: 0.012 ms | TT: 116 ms  AT: 0.0116 ms | TT: 211 ms  AT: 0.0211 ms | TT: 622 ms  AT: 0.0622 ms | TT: 120 ms  AT: 0.012 ms |
| **random\_1M.txt** | TT: 1066 ms  AT: 0.1066 ms | TT: 1319 ms  AT: 0.1319 ms | TT: 4035 ms  AT: 0.4035 ms | TT: 6361 ms  AT: 0.6361 ms | TT: 1218 ms  AT: 0.1218 ms |

|  |  |  |  |
| --- | --- | --- | --- |
| **Mode**  **Input** | **XTS** | **GCM** | **CCM** |
| **random\_1K.txt** | TT: 30 ms  AT: 0.003 ms | TT: 34 ms  AT: 0.0034 ms | TT: 39 ms  AT: 0.0039 ms |
| **random\_7K.txt** | TT: 44 ms  AT: 0.0044 ms | TT: 40 ms  AT: 0.004 ms | TT: 75 ms  AT: 0.0075 ms |
| **random\_10K.txt** | TT: 55 ms  AT: 0.0055 ms | TT: 51 ms  AT: 0.0051 ms | TT: 93 ms  AT: 0.0093 ms |
| **random\_17K.txt** | TT: 105 ms  AT: 0.0105 ms | TT: 64 ms  AT: 0.0064 ms | TT: 157 ms  AT: 0.0157 ms |
| **random\_100K.txt** | TT: 563 ms  AT: 0.0563 ms | TT: 286 ms  AT: 0.0286 ms | TT: 846 ms  AT: 0.0846 ms |
| **random\_1M.txt** | TT: 7941 ms  AT: 0.7941 ms | TT: 7333 ms  AT: 0.7333 ms | TT: 11769 ms  AT: 1.1769 ms |

1. **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  AT: 0.0116 ms | TT: 111 ms  AT: 0.0111 ms | TT: 101 ms  AT: 0.0101 ms | TT: 111 ms  AT: 0.0119 ms | TT: 128 ms  AT: 0.0117 ms |
| **random\_7K.txt** | TT: 581 ms  AT: 0.0581 ms | TT: 686 ms  AT: 0.0686 ms | TT: 690 ms  AT: 0.069 ms | TT: 676 ms  AT: 0.0676 ms | TT: 732 ms  AT: 0.0732 ms |
| **random\_10K.txt** | TT: 888 ms  AT: 0.0888 ms | TT: 940 ms  AT: 0.094 ms | TT: 986 ms  AT: 0.0986 ms | TT: 989 ms  AT: 0.0989 ms | TT: 1073 ms  AT: 0.1073 ms |
| **Random\_17K.txt** | TT: 1435 ms  AT: 0.1435 ms | TT: 1695 ms  AT: 0.1695 ms | TT: 1655ms  AT: 0.1655 ms | TT: 1628 ms  AT: 0.1628 ms | TT: 1716 ms  AT: 0.1716 ms |
| **random\_100K.txt** | TT: 8289 ms  AT: 0.8289 ms | TT: 9533 ms  AT: 0.9533 ms | TT: 9459 ms  AT: 0.9459 ms | TT: 9818 ms  AT: 0.9815 ms | TT: 10064 ms  AT: 1.0064 ms |
| **random\_1M.txt** | TT: 90639 ms  AT: 9.0639 ms | TT: 102890 ms  AT: 10.289 ms | TT: 98806 ms  AT: 9.8806 ms | TT: 100898 ms  AT: 10.0898 ms | TT: 114857 ms  AT: 11.4857 ms |

* **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  AT: 0.0116 ms | TT: 111 ms  AT: 0.0111 ms | TT: 101 ms  AT: 0.0101 ms | TT: 111 ms  AT: 0.0119 ms | TT: 128 ms  AT: 0.0117 ms |
| **random\_7K.txt** | TT: 628 ms  AT: 0.0628 ms | TT: 618 ms  AT: 0.0616 ms | TT: 601 ms  AT: 0.0601 ms | TT: 663 ms  AT: 0.0663 ms | TT: 771 ms  AT: 0.0771 ms |
| **random\_10K.txt** | TT: 888 ms  AT: 0.0888 ms | TT: 940 ms  AT: 0.094 ms | TT: 986 ms  AT: 0.0986 ms | TT: 989 ms  AT: 0.0989 ms | TT: 1073 ms  AT: 0.1073 ms |
| **Random\_17K.txt** | TT: 1424 ms  AT: 0.1424 ms | TT: 1472 ms  AT: 0.1472 ms | TT: 1454 ms  AT: 0.1454 ms | TT: 1611 ms  AT: 0.1611 ms | TT: 1691 ms  AT: 0.1691 ms |
| **random\_100K.txt** | TT: 8298 ms  AT: 0.8298 ms | TT: 8343 ms  AT: 0.8343 ms | TT: 8837 ms  AT: 0.8837 ms | TT: 9738 ms  AT: 0.9738 ms | TT: 9950 ms  AT: 0.995 ms |
| **random\_1M.txt** | TT: 90407 ms  AT: 9.0407 ms | TT: 90052 ms  AT: 9.0052 ms | TT: 87243 ms  AT: 8.7243 ms | TT: 100909 ms  AT: 10.0909 ms | TT: 114943 ms  AT: 11.4943 ms |

1. **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  AT: 0.0011 ms | TT: 23 ms  AT: 0.0023 ms | TT: 17 ms  AT: 0.0017 ms | TT: 14 ms  AT: 0.0014 ms | TT: 13 ms  AT: 0.0013 ms |
| **random\_7K.txt** | TT: 24 ms  AT: 0.0024 ms | TT: 57 ms  AT: 0.0057 ms | TT: 55 ms  AT: 0.0055 ms | TT: 54 ms  AT: 0.0054 ms | TT: 23 ms  AT: 0.0023 ms |
| **random\_10K.txt** | TT: 18 ms  AT: 0.0018 ms | TT: 68 ms  AT: 0.0068 ms | TT: 76 ms  AT: 0.0076 ms | TT: 52 ms  AT: 0.0052 ms | TT: 24 ms  AT: 0.0024 ms |
| **random\_17K.txt** | TT: 31 ms  AT: 0.0031 ms | TT: 118 ms  AT: 0.0118 ms | TT: 113 ms  AT: 0.0113 ms | TT: 112 ms  AT: 0.0112 ms | TT: 23 ms  AT: 0.0023 ms |
| **random\_100K.txt** | TT: 98 ms  AT: 0.0098 ms | TT: 630 ms  AT: 0.063 ms | TT: 628 ms  AT: 0.0628 ms | TT: 625 ms  AT: 0.0625 ms | TT: 106 ms  AT: 1.0106 ms |
| **random\_1M.txt** | TT: 1591 ms  AT: 0.1591 ms | TT: 6604 ms  AT: 0.6604 ms | TT: 5881 ms  AT: 0.5881 ms | TT: 5716 ms  AT: 0.5716 ms | TT: 1049 ms  AT: 0.1049 ms |

|  |  |  |  |
| --- | --- | --- | --- |
| **Mode**  **Input** | **XTS** | **GCM** | **CCM** |
| **random\_1K.txt** | TT: 22 ms  AT: 0.0022 ms | TT: 11 ms  AT: 0.0011 ms | TT: 16 ms  AT: 0.0016 ms |
| **random\_7K.txt** | TT: 49 ms  AT: 0.0049 ms | TT: 23 ms  AT: 0.0023 ms | TT: 54 ms  AT: 0.0054 ms |
| **random\_10K.txt** | TT: 66 ms  AT: 0.0066 ms | TT: 29 ms  AT: 0.0029ms | TT: 75 ms  AT: 0.0075ms |
| **random\_17K.txt** | TT: 84 ms  AT: 0.0084 ms | TT: 40 ms  AT: 0.004 ms | TT: 121 ms  AT: 0.0121 ms |
| **random\_100K.txt** | TT: 525 ms  AT: 0.0525 ms | TT: 175 ms  AT: 0.0175 ms | TT: 659 ms  AT: 0.0659ms |
| **random\_1M.txt** | TT: 8615 ms  AT: 0.8615 ms | TT: 1655 ms  AT: 0.1655 ms | TT: 6587 ms  AT: 0.6587 ms |

* **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  AT: 0.0011 ms | TT: 10 ms  AT: 0.001 ms | TT: 14 ms  AT: 0.0014 ms | TT: 18 ms  AT: 0.0018 ms | TT: 12 ms  AT: 0.0012 ms |
| **random\_7K.txt** | TT: 12 ms  AT: 0.0012 ms | TT: 19 ms  AT: 0.0019 ms | TT: 27 ms  AT: 0.0027 ms | TT: 49 ms  AT: 0.0049 ms | TT: 17 ms  AT: 0.0017 ms |
| **random\_10K.txt** | TT: 21 ms  AT: 0.0021 ms | TT: 31 ms  AT: 0.0031 ms | TT: 25 ms  AT: 0.0025 ms | TT: 82 ms  AT: 0.0082 ms | TT: 23 ms  AT: 0.023 ms |
| **random\_17K.txt** | TT: 22 ms  AT: 0.0022 ms | TT: 26 ms  AT: 0.0026 ms | TT: 39 ms  AT: 0.0039 ms | TT: 117 ms  AT: 0.0117 ms | TT: 39 ms  AT: 0.0039 ms |
| **random\_100K.txt** | TT: 120 ms  AT: 0.012 ms | TT: 116 ms  AT: 0.0116 ms | TT: 211 ms  AT: 0.0211 ms | TT: 622 ms  AT: 0.0622 ms | TT: 120 ms  AT: 0.012 ms |
| **random\_1M.txt** | TT: 1066 ms  AT: 0.1066 ms | TT: 1319 ms  AT: 0.1319 ms | TT: 1728 ms  AT: 0.1728 ms | TT: 5681 ms  AT: 0.5681 ms | TT: 1019 ms  AT: 0.1019 ms |

|  |  |  |  |
| --- | --- | --- | --- |
| **Mode**  **Input** | **XTS** | **GCM** | **CCM** |
| **random\_1K.txt** | TT: 30 ms  AT: 0.003 ms | TT: 18 ms  AT: 0.0018 ms | TT: 22 ms  AT: 0.0022 ms |
| **random\_7K.txt** | TT: 44 ms  AT: 0.0044 ms | TT: 33 ms  AT: 0.0033 ms | TT: 63 ms  AT: 0.0063 ms |
| **random\_10K.txt** | TT: 55 ms  AT: 0.0055 ms | TT: 41 ms  AT: 0.0041 ms | TT: 86 ms  AT: 0.0086ms |
| **random\_17K.txt** | TT: 105 ms  AT: 0.0105 ms | TT: 57 ms  AT: 0.0057 ms | TT: 136 ms  AT: 0.0136 ms |
| **random\_100K.txt** | TT: 563 ms  AT: 0.0563 ms | TT: 262 ms  AT: 0.0262 ms | TT: 741 ms  AT: 0.0741 ms |
| **random\_1M.txt** | TT: 7941 ms  AT: 0.7941 ms | TT: 3161 ms  AT: 0.3161 ms | TT: 8022 ms  AT: 0.8022ms |

1. **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++.