**ASSIGNMENT REPORT: CLASSICAL ENCRYPTION**

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

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**

* 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

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **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 |  |  |  |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **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 |  |  |  |

1. **AES (Windows System)**
   1. **GCC compiler**

* **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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **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 |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **XTS** | **GCM** | **CCM** |
| **random\_1K.txt** | TT: 22 ms  AT: 0.0022 ms |  |  |
| **random\_7K.txt** | TT: 49 ms  AT: 0.0049 ms |  |  |
| **random\_10K.txt** | TT: 66 ms  AT: 0.0066 ms |  |  |
| **random\_17K.txt** | TT: 84 ms  AT: 0.0084 ms |  |  |
| **random\_100K.txt** | TT: 525 ms  AT: 0.0525 ms |  |  |
| **random\_1M.txt** | TT: 8615 ms  AT: 0.8615 ms |  |  |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **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 |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **XTS** | **GCM** | **CCM** |
| **random\_1K.txt** | TT: 30 ms  AT: 0.003 ms |  |  |
| **random\_7K.txt** | TT: 44 ms  AT: 0.0044 ms |  |  |
| **random\_10K.txt** | TT: 55 ms  AT: 0.0055 ms |  |  |
| **random\_17K.txt** | TT: 105 ms  AT: 0.0105 ms |  |  |
| **random\_100K.txt** | TT: 563 ms  AT: 0.0563 ms |  |  |
| **random\_1M.txt** | TT: 7941 ms  AT: 0.7941 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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **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 |  |  |  |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **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 |  |  |  |

1. **AES (Linux System)**
   1. **GCC compiler**

* **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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **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 |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **XTS** | **GCM** | **CCM** |
| **random\_1K.txt** | TT: 22 ms  AT: 0.0022 ms |  |  |
| **random\_7K.txt** | TT: 49 ms  AT: 0.0049 ms |  |  |
| **random\_10K.txt** | TT: 66 ms  AT: 0.0066 ms |  |  |
| **random\_17K.txt** | TT: 84 ms  AT: 0.0084 ms |  |  |
| **random\_100K.txt** | TT: 525 ms  AT: 0.0525 ms |  |  |
| **random\_1M.txt** | TT: 8615 ms  AT: 0.8615 ms |  |  |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **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 |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **XTS** | **GCM** | **CCM** |
| **random\_1K.txt** | TT: 30 ms  AT: 0.003 ms |  |  |
| **random\_7K.txt** | TT: 44 ms  AT: 0.0044 ms |  |  |
| **random\_10K.txt** | TT: 55 ms  AT: 0.0055 ms |  |  |
| **random\_17K.txt** | TT: 105 ms  AT: 0.0105 ms |  |  |
| **random\_100K.txt** | TT: 563 ms  AT: 0.0563 ms |  |  |
| **random\_1M.txt** | TT: 7941 ms  AT: 0.7941 ms |  |  |