**LAB REPORT: CODING AES WITHOUT OTHER CRYPTOGRAPHIC EXTERNAL LIBRARIES**

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

LAB 2 REPORT’S TABLE OF CONTENTS

[**1.** **Hardware resource** 2](#_Toc197346521)

[**2.** **Input testcase** 2](#_Toc197346522)

[**3.** **AES (Windows System)** 2](#_Toc197346523)

[**4.** **AES (Linux System)** 3](#_Toc197346524)

[**5.** **Conclusion** 4](#_Toc197346525)

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. **AES (Windows System)**

* **Key using throughout all files:** 2352031523520930
* **IV (Initialized Vector) using throughout all files:** MinhDucPhucMinh
* **Mode:** CBC
* **Abbreviations:** TT (Total Time), AT (Average Time)
* **Time counter:** Mili second (ms)
* **Execution Time (average of 10000 times execution):**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **1KB** | **7KB** | **10KB** | **17KB** | **100KB** | **1MB** |
| **Encrytion** | TT: 12924  AT: 1.2924 | TT: 117564  AT: 11.7564 | TT: 166372  AT: 16.6372 | TT: 314123  AT: 31.4123 | TT: 1552400  AT: 155.24 | TT: 14349968  AT: 1434.9968 |
| **Decryption** | TT: 30818  AT: 1.0818 | TT: 125313  AT: 12.5313 | TT: 196376  AT: 19.6376 | TT: 286180  AT: 28.618 | TT: 1522924  AT: 152.2924 | TT: 16326545  AT: 1632.6545 |

1. **AES (Linux System)**

* **Key using throughout all files:** 2352031523520930
* **IV (Initialized Vector) using throughout all files:** MinhDucPhucMinh
* **Mode:** CBC
* **Abbreviations:** TT (Total Time), AT (Average Time)
* **Time counter:** Mili second (ms)
* **Execution Time (average of 10000 times execution):**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **1KB** | **7KB** | **10KB** | **17KB** | **100KB** | **1MB** |
| **Encrytion** | TT: 102463  AT: 10.2463 | TT: 28.8974  AT: 28.8974 | TT: 389977  AT: 38.9977 | TT: 665899  AT: 66.5899 | TT: 3486754  AT: 348.6754 | TT: 35588678  AT: 3558.8678 |
| **Decryption** | TT: 39984  AT: 3.9984 | TT: 240084  AT: 24.0084 | TT: 346474  AT: 34.6474 | TT: 605112  AT: 60.5112 | TT: 3448779  AT: 344.8779 | TT: 35333679  AT: 3533.3679 |

1. **Conclusion**

* We observed that the execution time on both Linux and Windows is significantly higher compared to Lab 1, where external libraries were allowed to optimize AES algorithm efficiency.
* Although Linux is theoretically expected to have better execution times than Windows, our implementation showed slower performance on Linux, as reflected in the code and results.
* A factor contributing to the slower performance of our code is vector initialization. Since the size is fixed in the algorithm, using an array instead of a vector would be more efficient.
* In conclusion, this lab report summarizes the work we have done and demonstrates that our code is not the most efficient implementation of the AES algorithm, due to the use of inappropriate data structures and nested loops that unintentionally increased execution time.