**LAB REPORT: RSA-OAEP Cipher using CryptoPP**

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

LAB 3 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 3 different testcase:
  + 1 KB input
  + 10 KB input
  + 1 MB input
* **Note:** These testcase are generated randomly based on the program **makingtextcase.exe**

1. **RSA-OAEP (Windows System)**

* **Key using throughout all files:** *public.pem* (for public key) and *private.pem* (for private key)
* **Key size:** 3072
* **File encrypted:** *cipher.bin*
* **File plaintext after decrypted:** *output.txt || decrypted.txt*
* **Usage format:**

+ D:\CRYPTO\LAB\rsaoaep.exe gen <keysize> <format> <privateKeyFile> <publicKeyFile> (*e.g:* .\rsaoecp.exe gen 3072 PEM private.pem public.pem)

+ D:\CRYPTO\LAB\rsaoaep.exe enc <format> <publicKeyFile> <plainFile> <cipherFile> (*e.g:* .\rsaoecp.exe enc PEM public.pem random\_1K.txt cipher.bin)

+D:\CRYPTO\LAB\rsaoaep.exe dec <format> <privateKeyFile> <plainFile> <cipherFile> *(e.g:* .\rsaoecp.exe dec PEM private.pem output.txt cipher.bin)

* **Abbreviations:** TT (Total Time), AT (Average Time)
* **Time counter:** Mili second (ms)
* **Execution Time (average of 10000 executions):**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **1KB** | **10KB** | **1MB** |
| **Encrytion** | TT: 144329  AT: 14.4329 | TT:  AT: | TT:  AT: |
| **Decryption** | TT: 270723  AT: 27.0723 | TT:  AT: | TT:  AT: |

1. **RSA-OAEP (Linux System)**

* **Key using throughout all files:** *public.pem* (for public key) and *private.pem* (for private key)
* **Key size:** 3072
* **File encrypted:** *cipher.bin*
* **File plaintext after decrypted:** *output.txt || decrypted.txt*
* **Usage format:**

+ D:\CRYPTO\LAB\rsaoaep.exe gen <keysize> <format> <privateKeyFile> <publicKeyFile> (*e.g:* .\rsaoecp.exe gen 3072 PEM private.pem public.pem)

+ D:\CRYPTO\LAB\rsaoaep.exe enc <format> <publicKeyFile> <plainFile> <cipherFile> (*e.g:* .\rsaoecp.exe enc PEM public.pem random\_1K.txt cipher.bin)

+D:\CRYPTO\LAB\rsaoaep.exe dec <format> <privateKeyFile> <plainFile> <cipherFile> *(e.g:* .\rsaoecp.exe dec PEM private.pem output.txt cipher.bin)

* **Abbreviations:** TT (Total Time), AT (Average Time)
* **Time counter:** Mili second (ms)
* **Execution Time (average of 10000 executions):**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **1KB** | **10KB** | **1MB** |
| **Encrytion** | TT: 144329  AT: 14.4329 | TT:  AT: | TT:  AT: |
| **Decryption** | TT: 270723  AT: 27.0723 | TT:  AT: | TT:  AT: |

1. **Sample images**

* **Generate public/private key:**

****

* **Encrypted text:**

**A screenshot of a computer code

AI-generated content may be incorrect.**

* **Decrypted text:**

1. **Conclusion**