UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTER NETWORK AND COMMUNICATION

Logo, company name

Description automatically generated

**REPORT**

Subject: Cryptography

Semester I (2024 – 2025)

**Report Lab 3**

Nhóm :13

Student: Võ Hoài Nam

Student ID Number: 23520990

Student: Nguyễn Huỳnh Nhân

Student ID Number: 23521080

Class: NT219.P22.ANTT

University of Information Technology

Report Lab 3

**Student Information**

Full Name: Nguyễn Huỳnh Nhân

Student ID Number: 23520180

Class: ATTT2023.2

Full Name: Võ Hoài Nam

Student ID Number: 23520990

Class: ATTT2023.2

**Device Information**

CPU: 11th Gen Intel(R) Core(TM) i5-1135G7

Ram: 16 GB DDR4 3200MHz

SSD PCle: 512GB

**RSA**

key: AD12463E840DCE194EFB330E3C5D751C1D90A286A8DDFE3A4AB76D46B637ABDD

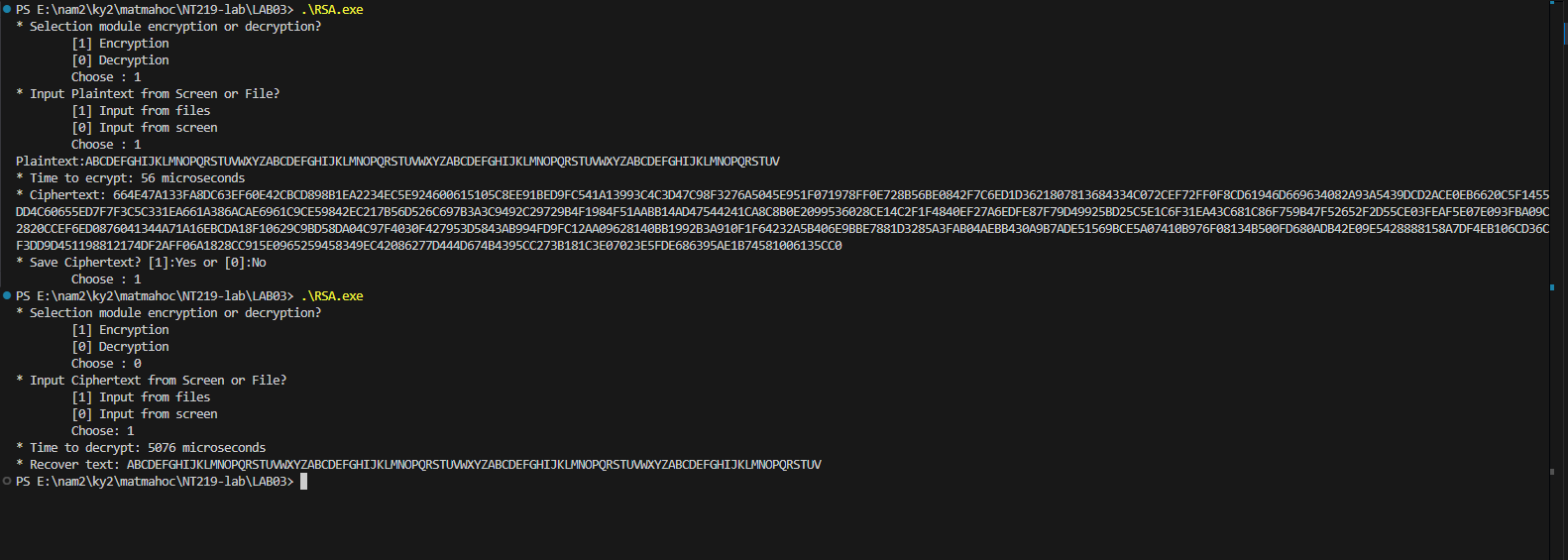
iv:018C53B1CA0FBBFCB571C82191F32265

**Plain1KB.txt**

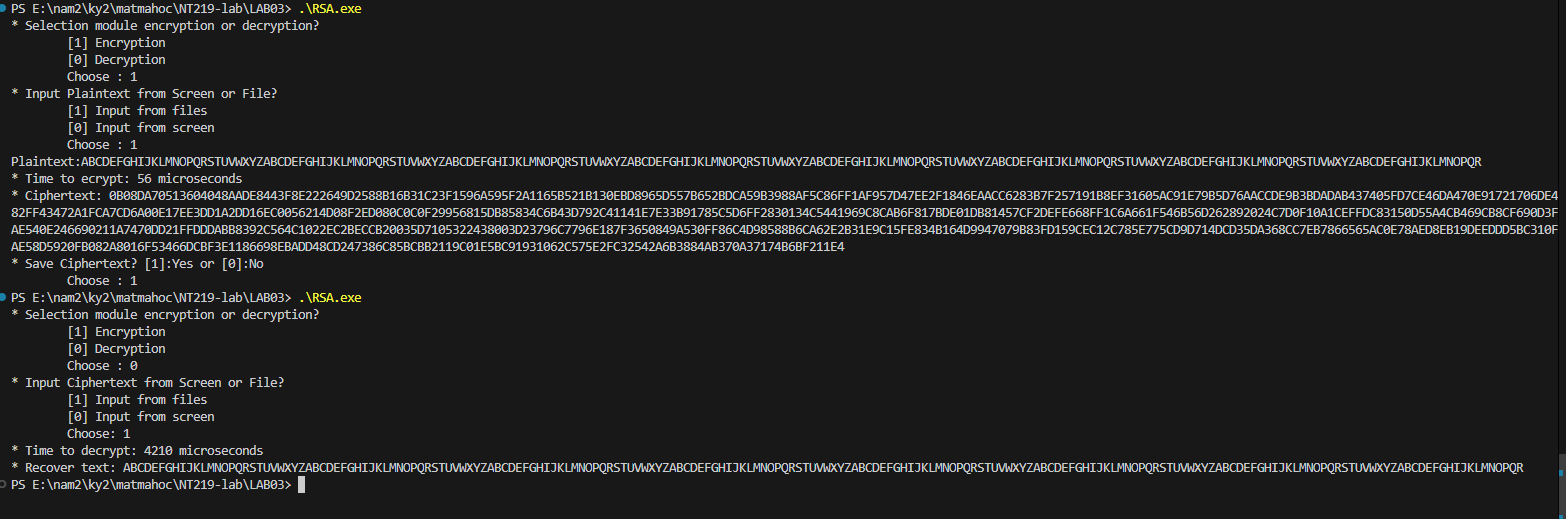
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| 100 Bytes | 56 ms | 5076 ms | 58.6 ms | 3573 ms |
| 200 Bytes | 56 ms | 4210 ms | 58.5 ms | 3579 ms |
| 300 Bytes | 58 ms | 4408 ms | 58.9 ms | 3630 ms |

**Window:**

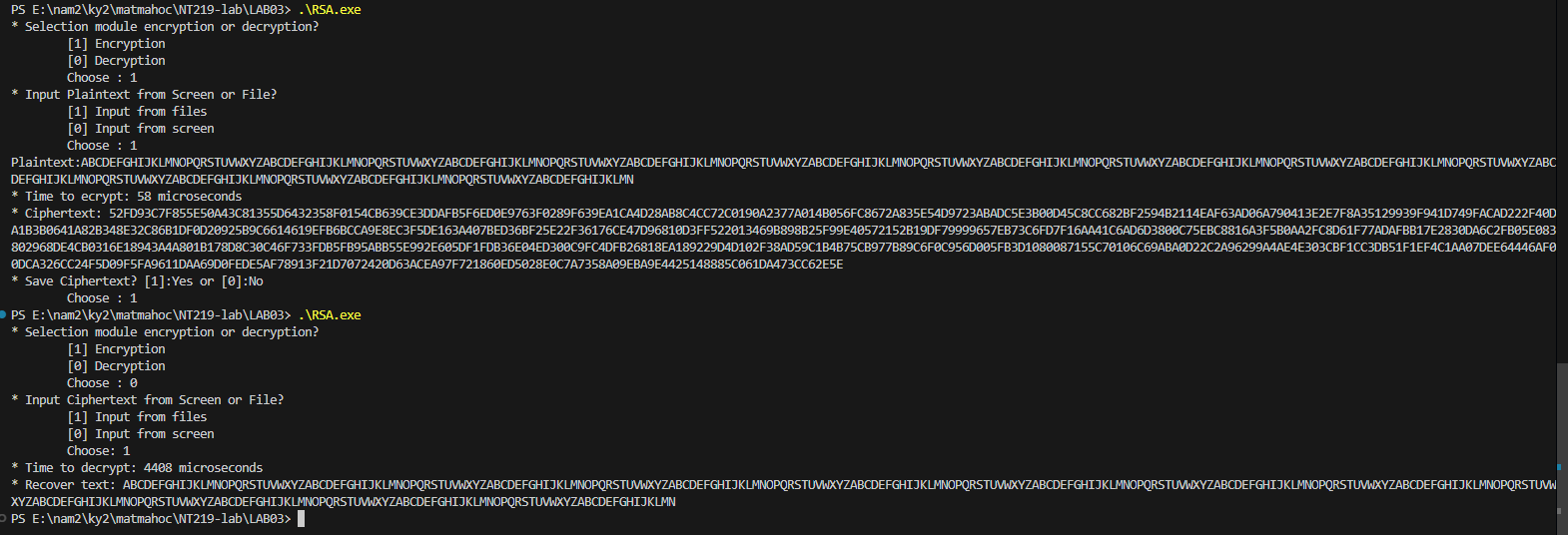
100 bytes



200 bytes



300 bytes



**Linux:**

100 bytes

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

200 bytes

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình

Nội dung do AI tạo ra có thể không chính xác.

300 bytes:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Nhận xét:**

\_Quá trình mã hóa và giải mã trên cùng 1 hệ điều hành không chênh lệch thời gian nhiều.

\_Mã hóa rất nhanh và không đổi nhiều khi tăng kích thước dữ liệu. Vì khi mã hóa RSA chỉ thực sự xử lý một khối dữ liệu có kích thước bằng đúng padding block bất kể dữ liệu vào.

\_Giải mã thì chậm hơn vì decrypt luôn thực hiện một số phép tính toán học cố định (modular exponentiation) trên toàn block, nên dung lượng dữ liệu thêm vào thực sự không ảnh hưởng đáng kể.

\_Sự khác biệt giữa Windows và Linux phần lớn xuất phát từ cách thư viện BigInteger/BN thực thi phép nhân và khai triển CRT trong private‐key operations.