Tên: Lâm Thanh Ngân

MSSV: 19521884

REPORT LAB3

RSA Cipher (Encryption/Decryption) using CryptoPP

Required:

+) Separation Encryption function and Decryption function (using switch case)

+) Plaintext:

- Support Vietnamse (using setmod, UTF-16)

- Input from screen or from file (using switch case)

+) Ciphertex:

- Input from screen or from file (using switch case)

+) Secret key/public key

- The keys load from files (for both two functions)

- The public key: >= 3072 bits

+) OS platforms

- Your code can compile on both Windows and Linux;

+) Performance

- Report your hardware resources

- Report computation performance for all operations on both Windows and Linux

### **Hardware specifications**

Intel Core i7-85650U CPU @ 1.80 GHz

RAM: 8GB

Plaintext in file plaintext.txt :

file test Tiếng Việt

19521884 - Lâm Thanh Ngân - 19521884

NT219.L21.ANTN

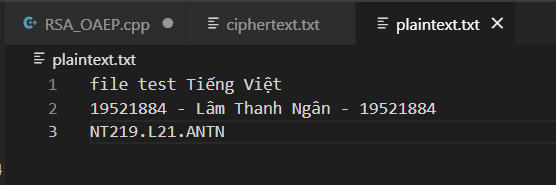
Vòng: 1000 lần

\* Key length : 3072 bits

TABLE 1

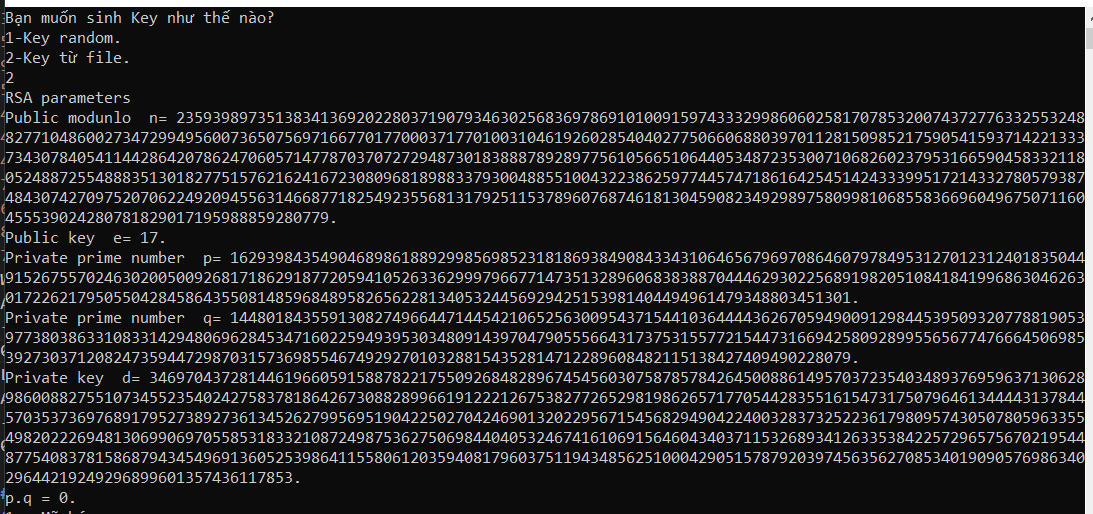
|  |  |  |
| --- | --- | --- |
| ECDSA | Time (ms) | |
| Windown | Linux |
| Encryption time | 0.042 | 0.071742 |
| Decryption time | 0.891 | 0.918016 |

File plaintext.txt



\* Sinh key và in ra các paragram:

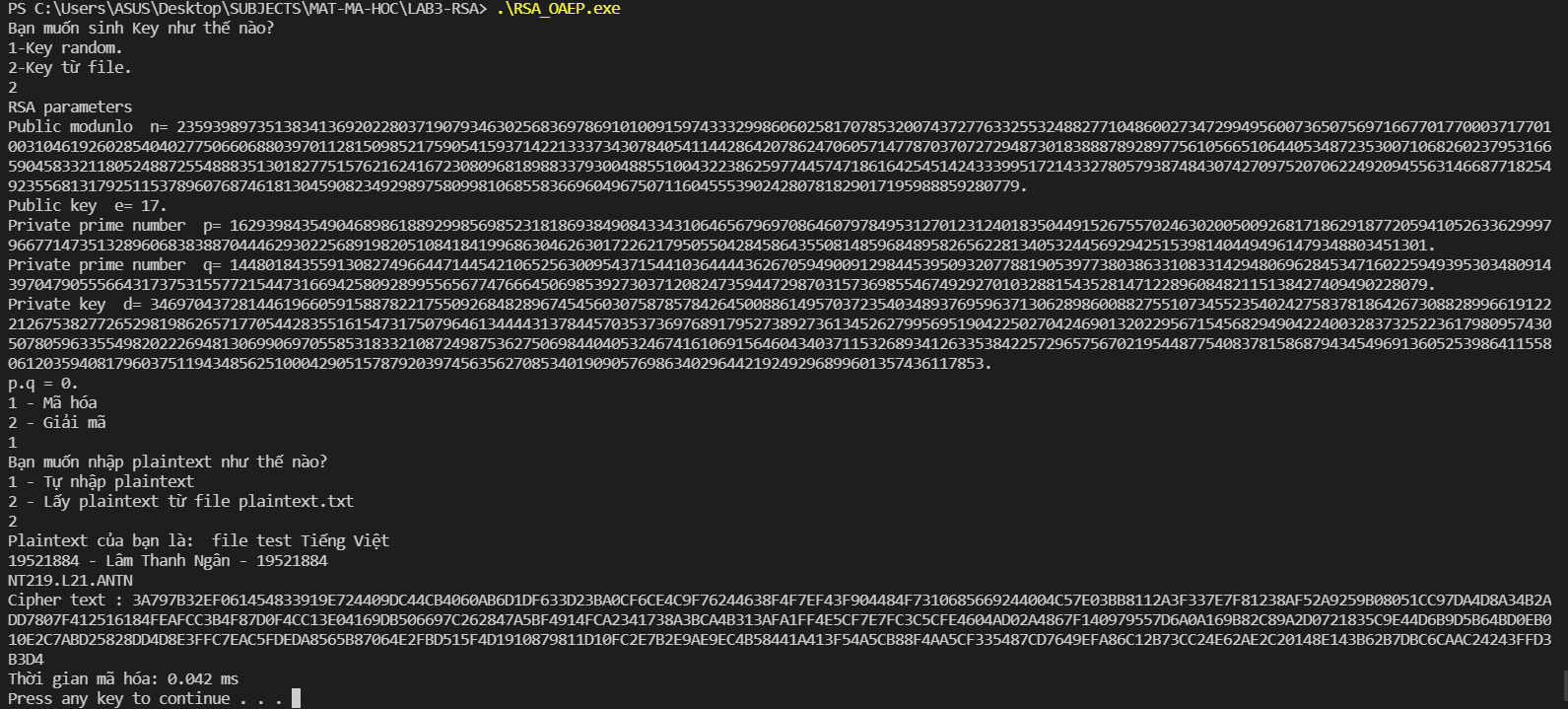
Cho phép chọn giữa random hoặc input từ file.



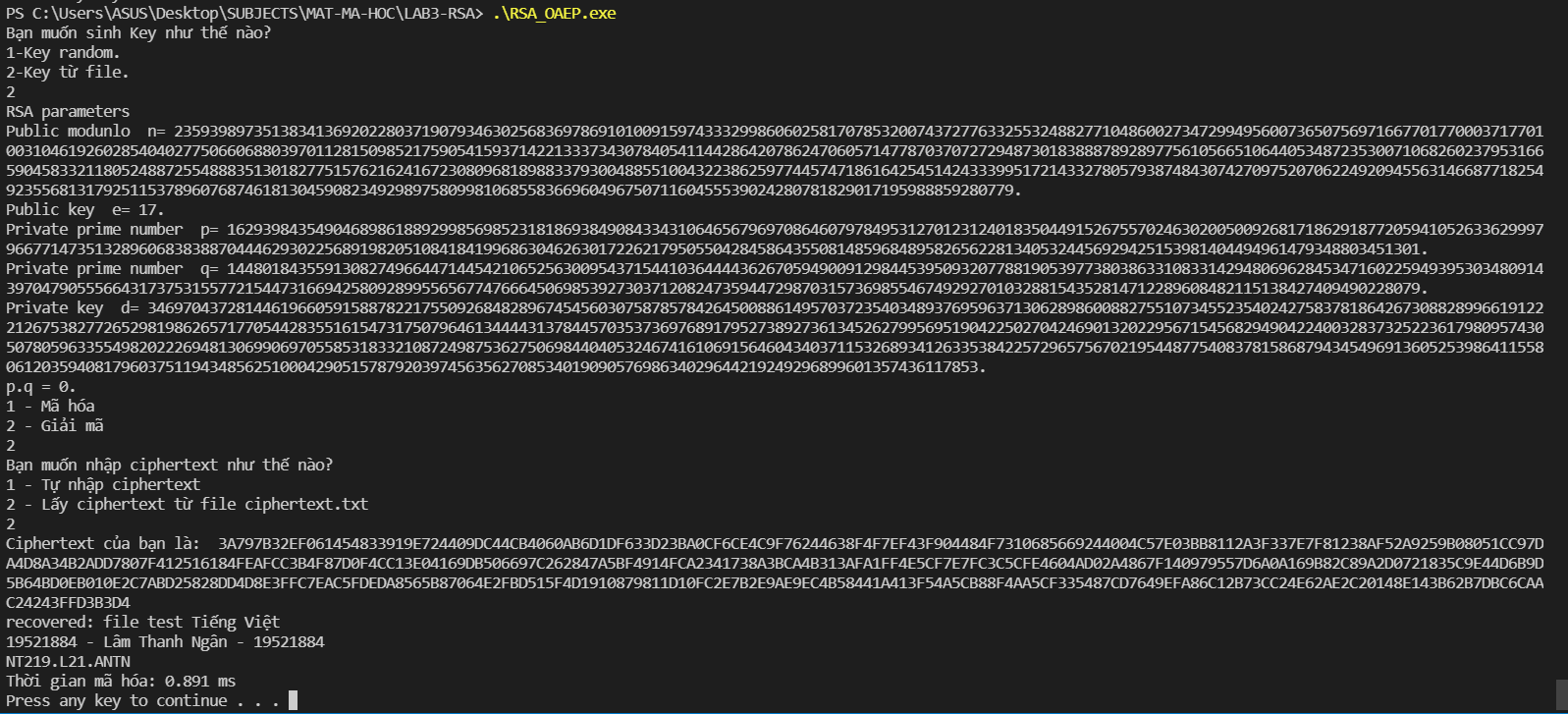
Cho phép chọn mã hóa hoặc giải mã.

Windows:

\*Mã hóa

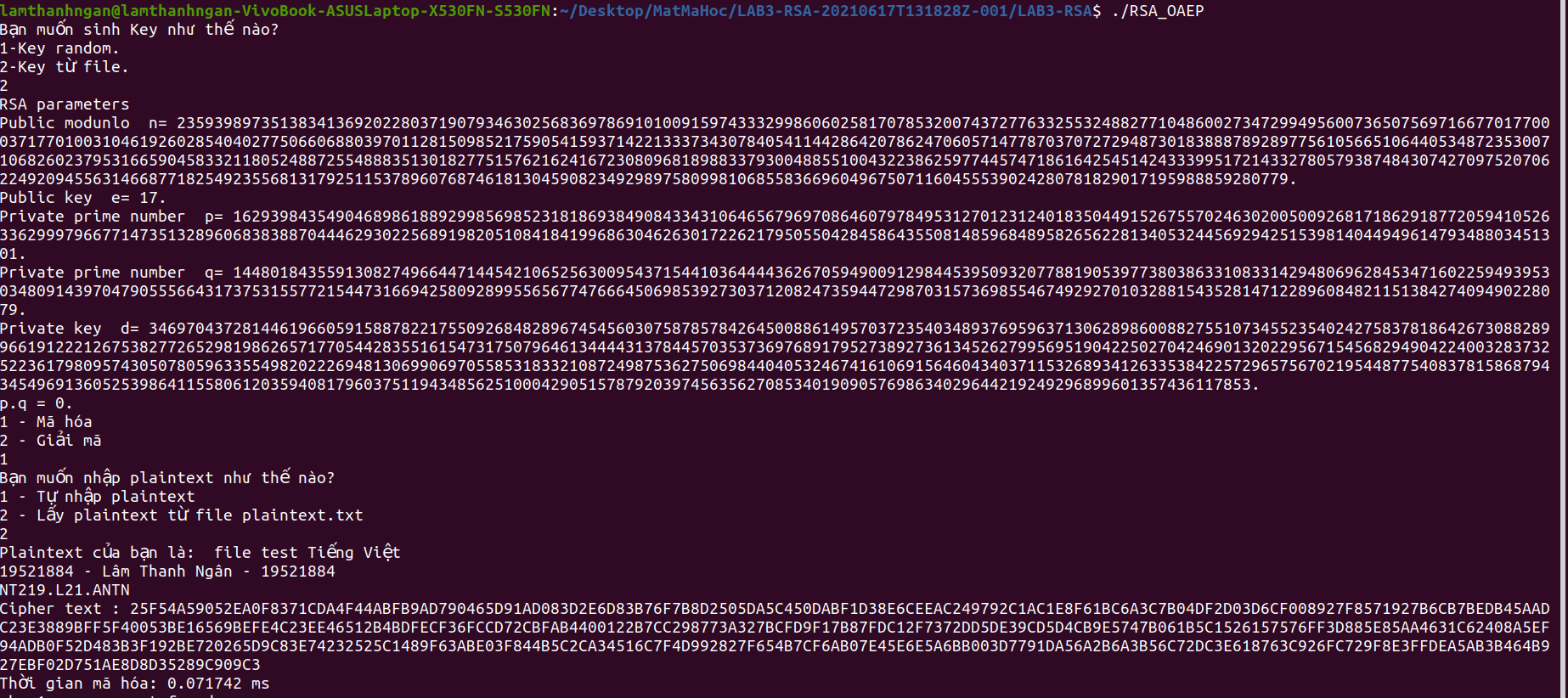


\* Giải mã



Linux

\* Mã hóa:



\* Giải mã :

