Tên: Lâm Thanh Ngân

MSSV: 19521884

REPORT LAB4

ECC-based Digital signature with cryptoPP

Required:

+) Algorith:ECDSA

+) Separation the signing function and the verify function (using switch case)

+) signing function; verify function

- May adopt from library or direct compute from formulas. Deploy driectly from formulas will get 10/100 bonus points.

+) Message to sign:

- Input from file

- Support Vietnamese (using UTF-16)

+) ECC curve: should select from standard curves

+) Secret key/public key

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

- The public key: >= 256 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 từ file message.txt : Chủ tịch Quốc hội Vương Đình Huệ

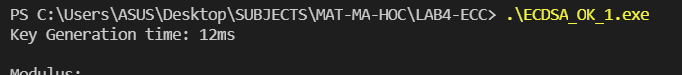
\* Key length : 256 bits

TABLE 1

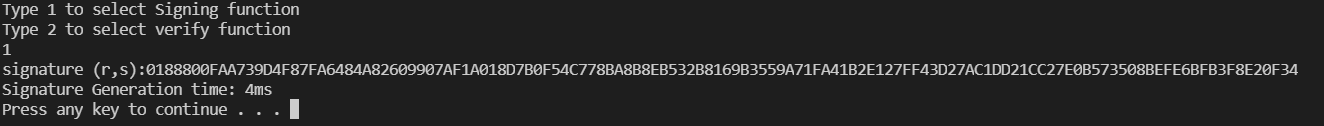
|  |  |  |
| --- | --- | --- |
| ECDSA | Time (ms) | |
| Windown | Linux |
| Key Generation | 12 | 10.19 |
| Signature Generation | 4 | 1.583 |
| Signature Verification | 8 | 7.387 |

Window:

Key Generation



Signature Generation

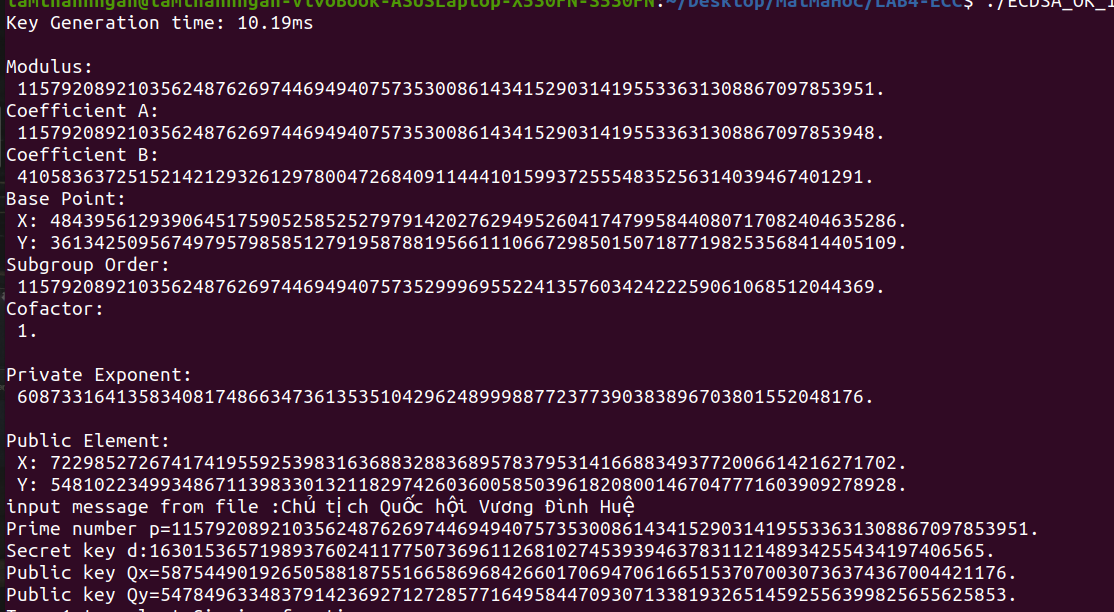


Signature Verification



Linux

Key Generation



Signature Generation



Signature Verification

