CPU: Intel(R) Core(TM) i5-2410M CPU @ 2.30GHz

Memory: 7829MiB

SSD:250GB

Dùng thư viện có sẵn ECDSA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Input length** | **Sign** | | **Verify** | |
| Windows (10) | Linux (xubuntu) | Windows (10) | Linux (xubuntu) |
| 780B | 0.288 | 1.24 | 6.26 | 4.685 |
| 415KB | 0.357 | 5.856 | 6.621 | 7.314 |
| 16.2MB | 0.435 | 101.864 | 6.654 | 114.639 |

Tự viết theo công thức ECDSA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Input length** | **Sign** | | **Verify** | |
| Windows (10) | Linux (xubuntu) | Windows (10) | Linux (xubuntu) |
| 780B | 0.288 | 1.016 | 6.26 | 2.289 |
| 415KB | 0.357 | 6.343 | 6.621 | 1.435 |
| 16.2MB | 0.435 | 104.3 | 6.654 | 1.43 |

Dùng thư viện có sẵn RSA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Input length** | **Encryption** | | **Decryption** | |
| Windows (10) | Linux (xubuntu) | Windows (10) | Linux (xubuntu) |
| 10B | 0.288 | 0.18 | 6.26 | 12.59 |
| 100B | 0.357 | 0.262 | 6.621 | 9.89 |
| 16.2MB | 0.435 | 0.197 | 6.654 | 12.503 |