LAB REPORT

**Lab 3**

**Course name:** Network Security

**Class:** CNBU006.N31.ATBC

|  |  |  |
| --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** |
| 1 | Trần Thanh Trực | 21521746 |

|  |
| --- |
| **Grade** |
|  |

Content

[**1** Hardware Resources 2](#_Toc141108034)

[**2** Computation Performance 2](#_Toc141108035)

[2.1 Set of different input sizes 2](#_Toc141108036)

[2.2 Summarize the results. 3](#_Toc141108037)

[2.3 Comparison 3](#_Toc141108038)

[2.3.1 Signing a message. 3](#_Toc141108039)

[2.3.2 Verify a message. 3](#_Toc141108040)

# Hardware Resources

* CPU: Intel(R) Core(TM) i5-8300H
* Ram: 24GB
* GPU: NVIDIA GeForce GTX 1050
* OS: Windows 11, Kali

# Computation Performance

## Set of different input sizes

* Test case 1: 39 bytes
* Test case 2: 445 bytes
* Test case 3: 1221 bytes ~ 1.19KB
* Test case 4: 3335 bytes ~ 3.25KB
* Test case 5: 79MB
* Test case 6: 316MB

## Summarize the results.

* Curve: secp256k1
* SHA512

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Operating System | Windows | | | | | | Kali | | | | | |
| Keys generate time | 308 milliseconds | | | | | | 358 milliseconds | | | | | |
| Input Size | 39B | 445 B | 1.19 KB | 3.25 KB | 79 MB | 316 MB | 39B | 445 B | 1.19 KB | 3.25 KB | 79 MB | 316 MB |
| Signing time (milliseconds) | 1133 | 1427 | 1570 | 1643 | 2488 | 3666 | 1023 | 1063 | 1799 | 1690 | 2522 | 5235 |
| Verify time (milliseconds) | 775 | 1006 | 1725 | 1156 | 1684 | 2720 | 619 | 696 | 839 | 607 | 1126 | 4393 |

## Comparison

### Signing a message.

* The results show that with the small input size, Windows is better than Kali.
* With the large input size, Kali takes more time to load the message to sign.

### Verify a message.

* Overall, the computation of a small input size to verify a message is better at Kali.
* Verifying and signing a message in Kali has the same problem of taking more time than Windows when calculating a large input size.