**ab 4: Hash function**

TimeCounter: mili second

Window 11

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Hash function | 1MB | 10MB | 50MB | 100MB | 1000MB |
| SHA224 | 1.42 | 12.06 | 66.89 | 125.57 | 1734.67 |
| SHA256 | 1.22 | 12.93 | 76.13 | 117.98 | 1551.27 |
| SHA384 | 1.94 | 23.03 | 117.52 | 218.71 | 2026.76 |
| SHA512 | 1.99 | 19.83 | 100.16 | 210.90 | 1991.28 |
| SHA3-224 | 2.70 | 32.72 | 148.71 | 415.95 | 2935.61 |
| SHA3-256 | 2.74 | 30.91 | 167.38 | 327.86 | 3044.60 |
| SHA3-384 | 4.55 | 37.08 | 192.49 | 365.60 | 3798.19 |
| SHA3-512 | 5.49 | 52.88 | 250.12 | 528.39 | 6663.68 |
| SHAKE128 | 2.5 | 25.62 | 124.78 | 264.04 | 3749.73 |
| SHAKE256 | 2.73 | 31.64 | 165.59 | 319.68 | 3752.67 |

Ubuntu 22.04

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Hash function | 1MB | 10MB | 50MB | 100MB | 1000MB |
| SHA224 | 0. 788311 | 7.1848 | 30. 2826 | 60.9747 | 605.985 |
| SHA256 | 0.649772 | 6.83955 | 31.3967 | 61.5561 | 607.117 |
| SHA384 | 1.51447 | 14.0291 | 68.9668 | 138.205 | 1370.05 |
| SHA512 | 1.4882 | 14.082 | 68.9973 | 137.608 | 1369.09 |
| SHA3-224 | 2.38281 | 21.4823 | 105.774 | 211.16 | 2108.34 |
| SHA3-256 | 2.45782 | 23.0742 | 112.867 | 225.468 | 2252.18 |
| SHA3-384 | 3.13962 | 29.6363 | 147.123 | 293.206 | 2932.3 |
| SHA3-512 | 4. 41077 | 41.9686 | 208.239 | 416.219 | 4163.59 |
| SHAKE128 | 2.01453 | 18.5726 | 91.0495 | 184.23 | 1813.99 |
| SHAKE256 | 2.4694 | 23.3074 | 113.109 | 231.785 | 2253.2 |

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Task4.3: MD5 Collision attack:

**PKI and digital certificate**

Create cert

A screenshot of a computer

Description automatically generated

Check cert

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Task 4.4: Length extension attacks on MAC  in form: H(k||m), k is secret keyA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated