UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTER NETWORK AND COMMUNICATION

Logo, company name

Description automatically generated

**REPORT**

Subject: Cryptography

Semester II (2021 – 2022)

**Report Lab 3 – 4**

Student: Võ Anh Kiệt

Student ID Number: 20520605

Class: NT219.M21.ANTN

University of Information Technology

Lecturer: Nguyễn Ngọc Tự

**Hồ Chí Minh City, March 2022**

Report Lab 3 – 4

**Student Information**

Full Name: Võ Anh Kiệt

Student ID Number: 20520605

Class: ANTN2020

**Device Information**

CPU: Intel core i5 – 8250U @ 1.60 GHz

Ram: 16 GB DDR3L

SSD M2 SATA: 500GB

HDD: 1000GB

Display chip name: UHD 620

**RSA**

|  |  |
| --- | --- |
| Plaintext | Võ Anh Kiệt - 20520605 - ANTN2020 (testcase1) |
| Keysize | 3072 bits |
| Modulo N | 3094342908147763265590132917572861112257549816812479067601342865572889463289538257247593117370325293671119369173971986423507336456732032972709068500292121699523269209494382227759250496533363019948600531748288470312209930571295538470592342639324144825782946516054208698359346263814786690547035723084124072998512707954186806748239631423700541521042342254469633139373379451028788081026596856503260342125446971303480711513676222484647271202365554164437636849626816058357173789943433543782101098873505528660705086582348885285108979966471162212821617885029202225791420722437712127343998979641827704841989418050846531570190643042130078888089899962698928805899860314219433648540823838126392734130750786217693908357564796054125208637900868904995133597700842906041852469026705837059852412401640420144736573775893395655905131985917693004183530710384179756293264662014253291089968196788450497825826240042357555084494195971554581191153369. |
| Prime1 P | 1760307012405166607648281054357973805201847707677833046009507921450573521399234693264912873612346556842132931571737717174938484296856606155312711721418613717869724955110643271900864968025702149151503612290135965228477668354433942834112938729626371824862008751043718783099754095524991510290423356974241441865858799864945321972061200688446441466127822056859748897659752515906852388473566623134227053509212680689183381933609267000225358128417607100014479949489904379. |
| Prime2 Q | 1757842743533617239498600533345498045774787945184480118901181551960888931411344988365384306906857902439663554061502259040449412905184641366189278162142052276546603016525045742760639542054940136128304615935201802291219861422514706407868052620749392329742726577908925599370711789138405455054306972360051747638023717045242865478691561461543256892478586053641510025581042026842956035197836291746930000120797112890692029760146445737826040642970922391670932315893738811. |
| PublicExponen E | 17. |
| PrivateExponen D | 30336695177919247701864048211498638355466174674632147721581792799734210424407237816152873699709071506579601658568352808073601337811098362477539887257765899014934011857788061056463240162091794313221573840669494806982450299718583710496003359209060243390028887412296163709405355527595947946539565912589451696063850077982223595570976778663730799225905316220290520974248818147341059617907812318659415118876931091210595210918394338084777168650642687886643498525753098576853176803967153888580583442843467428275190526667016866415877515245183425512175845634627663790068249418051240138274732982881671596085704868126045568720829888488255953454910640207788418875074265043247111992186826651263362325314721021928456450801967073033234114561338102299306362101018407463838462105230552286052308845229931072470337488099951343622519818477046762386166548633095647891081860596639212363531123695225870628138367666578027291136908865550414860857943. |

**Deploy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TimeCounter mili seconds | Encrypt (Window) | Decrypt (Window) | Encrypt (Linux) | Decrypt (Linux) |
| Testcase1 | 0.0709 | 5.7614 | 0.0686 | 5.645 |
| 100 Char | 0.0621 | 5.0323 | 0.0737 | 6.315 |
| 200 Char | 0.0619 | 5.0437 | 0.0720 | 5.865 |
| 300 Char | 0.0628 | 5.0689 | 0.0702 | 5.293 |

**ECDSA**

|  |  |
| --- | --- |
| Message | FullName: Võ Anh Kiệt  Student ID: 20520605  Class: ANTN2020  University of Information Technology  Vietnam National University  (testcase1) |
| Modulus | 115792089210356248762697446949407573530086143415290314195533631308867097853951. |
| Coefficient A | 115792089210356248762697446949407573530086143415290314195533631308867097853948. |
| Coefficient B | 41058363725152142129326129780047268409114441015993725554835256314039467401291. |
| BasePoint X | 48439561293906451759052585252797914202762949526041747995844080717082404635286. |
| BasePoint Y | 36134250956749795798585127919587881956611106672985015071877198253568414405109. |
| Subgroup Order | 115792089210356248762697446949407573529996955224135760342422259061068512044369. |
| Cofactor | 1. |
| Private Exponent | 33360757757844613763231249822967924308599330557752078721666064976586396684777. |
| Public Element X | 65334450998399388256013006099864013326337659815457080538154222401125433814626. |
| Public Element Y | 113169335534755752670278067102842238523333018363659333838364281765647202300982. |

**Deploy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TimeCounter  Mili seconds | Sign (Window) | Verify (Window) | Sign (Linux) | Verify (Linux) |
| Testcase1 | 0.7075 | 2.0228 | 0.5684 | 2.0983 |
| 20 KB | 0.7924 | 2.0403 | 0.7064 | 2.2743 |
| 50 KB | 0.9019 | 2.1926 | 0.8227 | 2.3838 |
| 100 KB | 1.0742 | 2.3690 | 0.9537 | 2.7144 |
| 200 KB | 1.0726 | 2.4089 | 0.9786 | 2.5635 |
| 1 MB | 0.8282 | 2.1171 | 0.7741 | 2.3401 |
| 5 MB | 0.8293 | 2.1237 | 0.5684 | 2.0983 |