**TRƯỜNG ĐẠI HỌC BÁCH KHOA TP HỒ CHÍ MINH**

**KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH**



*BÁO CÁO LAB 2 – MẬT MÃ VÀ AN NINH MẠNG*

*GVHD: Nguyễn Hữu Hiếu*

*Sinh viên: Nguyễn Thị Thu Hà 1411010*

Part 1

* 16 bíts:
* All components of a public key: 2^16+1
* All components of a private key: 19073
* Ciphertext

|  |  |
| --- | --- |
| 1 | 00001 |
| 10 | 28579 |
| 15 | 38303 |
| 6 | 40353 |

* 256 bits:
* All components of a public key: 2^16+1
* All components of a private key: 52738157418252485211371653756350856811438729262467531927178372427919298984641

Ciphertext

|  |  |
| --- | --- |
| 1 | 00000000000000000000000000000000000000000000000000000000000000000000000000001 |
| 10 | 79400549836706478668651923935812812839699315221878218034400745892598810774895 |
| 255 | 05757222225230937977913627982481920101459010557711877142120560341705189750267 |
| 246 | 82275284282168475055857616303379456683910113662031432684892442429365393359885 |

* 2048 bit:
* All components of a public key: 2^16+1
* All components of a private key: 4328276966925611767832495282023923930343930774250319964531089860484708770458983813895139924948070002712195983872878945388413665761146123988256280431580721366758512667806725683700352626300038965104045634354529775071634551017413206120196907993932637340254468520956148067082575439606007085923040885634174691435117168784933568557974978025972604185668445613904244624873111394265820184721008740765227319641071636767783992122315749387481927518594528338655024258412989805301350421594783147069092517771012818619966471734040348829351203653005874831526552949800740233636221294980670060841631227676118944118731782914130019066081

|  |  |
| --- | --- |
| 1 | 000000000000000000000000000000000000000000000000000000000000000000  000000000000000000000000000000000000000000000000000000000000000000  000000000000000000000000000000000000000000000000000000000000000000  000000000000000000000000000000000000000000000000000000000000000000  000000000000000000000000000000000000000000000000000000000000000000  00000000000000000000000000000000000000000000000000000000000000000  00000000000000000000000000000000000000000000000000000000000000000  00000000000000000000000000000000000000000000000000000000000000000  00000000000000000000000000000000000000000000000000000000000000000  00000000000000000000000001 |
| 10 | 08390740043888318698639007874659124641217849303965222038157068989396  04437060311971618282004407990215179684310137494431551807449203466159  43725905261518949646979500099759543083107961458876732634414984931488  68668933357487200916922941673517210247819610426813297423864613899052  62226951795478487033332930737929214551359831592057084491369939165017  92349804882540785283172490760216736630411980204276650590659685577705  26361142342189544635813179249822161285733479566855833664096752201067  88763520807990090010304395749660960171757828190547396363858052711390  92833224214810129748207726563876195183499714421527734120552332241673  2132 |
| 2047 | 056596805177482856157522237724463496462214436888329349323257086789292  864363928441847588005897834797517576818235075968093186856577080353337  136526943939808318645549941804759880670624304850028563488792450781479  419701974230823020966129942415436628236066846174363923969637345587526  617581263789715407791820207240962215610992751641508071777841215564747  182276871093352240589178758431366661181645430375925344345631127463085  968430743448347852931565854120459246702292115927308318540156391690472  530976564792285849720105704104886036474896959961614218669992929270486  5380612144595180012867032899615432432246161180443998049427850390 |
| 2048 | 103318814826353251618099231037374315885210149055360561776408205953418  174935100027456233027934862172836538443978924673244396444073483463476  339082506732290737432360387536524309498614179768737469263333043775594  541999091444384227387169675615797504453798943280303558154944428838293  068488335623242785419337798449217329768407971440177346059964970334247  277871889902790820980875479255018390224821368035869330468373565522696  576467695075689719777972504682547028336571635113816370758341069640674  702819130285441216144027540741027569483316308226363803595934843838287  95673025277542596882605477804374903242656074156471838371619137320 |

**Part 2**

**50 bit.**

Details for the factorization of the

Input number = 753059083286911

The respective next composite factor will be factorized into two factors:

1. Factorized number = 753059083286911

Bit length = 50

Method: Quadratic sieve. Time: 0.306 seconds.

- First factor = 25086049

Bit length = 25, prime number.

- Second factor = 30019039

Bit length = 25, prime number.

Found 2 factors in 0.306 seconds.

The input integer has been factorized into the following factors:

25086049 \* 30019039

**100 bit:**

Input number = 983442545603456859113865626609

The respective next composite factor will be factorized into two factors:

1. Factorized number = 983442545603456859113865626609

Bit length = 100

Method: Quadratic sieve. Time: 0.083 seconds.

- First factor = 893133386213581

Bit length = 50, prime number.

- Second factor = 1101114974295989

Bit length = 50, prime number.

Found 2 factors in 0.083 seconds.

The input integer has been factorized into the following factors:

893133386213581 \* 1101114974295989

**150 bit:**

Details for the factorization of the

Input number = 1202528858228354619788715152772836185783104133

The respective next composite factor will be factorized into two factors:

1. Factorized number = 1202528858228354619788715152772836185783104133

Bit length = 150

Method: Quadratic sieve. Time: 5.950 seconds.

- First factor = 32162930963977948774291

Bit length = 75, prime number.

- Second factor = 37388658999242662601863

Bit length = 75, prime number.

Found 2 factors in 5.950 seconds.

The input integer has been factorized into the following factors:

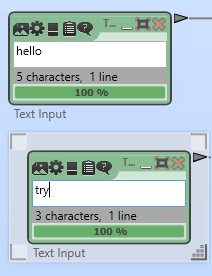
32162930963977948774291 \* 37388658999242662601863

**Part 3**

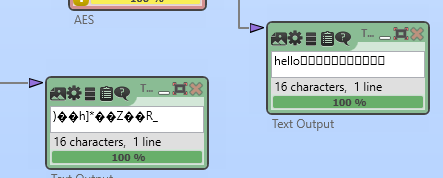
Screenshots:

Sender side.

AES-RSA:

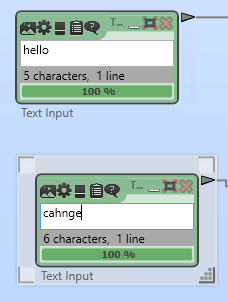


Receiver side:



AES:

Sender side.



Receiver side:

