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	0000000000000000000000000000000000000000000000000000000000000001
10	7940054983670647866865192393581281283969931522187821803440074589259881077489 5
255	057572222252309379779136279824819201014590105577118771421205603417051897502 67
246	82275284282168475055857616303379456683910113662031432684892442429365393359885

- 2048 bit:
  - All components of a public key: 2^16+1
  - All components of a private key: 43282769669256117678324952820239239303439307742503199645310898604847087704589838138951399249480700027121959838728789453884136657611461239882562804315807213667585126678067256837003526263000389651040456343545297750716345510174132061201969079939326373402544685209561480670825754396060070859230408856341746914351171687849335685579749780259726041856684456139042446248731113942658201 8

	472100874076522731964107163676778399212231574938748192 751859452833865502425841298980530135042159478314706909 251777101281861996647173404034882935120365300587483152 655294980074023363622129498067006084163122767611894411 8731782914130019066081
1	0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000001
10	083907400438883186986390078746591246412178493039652220381570689396 04437060311971618282004407990215179684310137494431551807449203466159 43725905261518949646979500099759543083107961458876732634414984931488 68668933357487200916922941673517210247819610426813297423864613899052 6222695179547848703332930737929214551359831592057084491369939165017 92349804882540785283172490760216736630411980204276650590659685577705 26361142342189544635813179249822161285733479566855833664096752201067 88763520807990090010304395749660960171757828190547396363858052711390 92833224214810129748207726563876195183499714421527734120552332241673 2132
2047	056596805177482856157522237724463496462214436888329349323257086789292 864363928441847588005897834797517576818235075968093186856577080353337 136526943939808318645549941804759880670624304850028563488792450781479 419701974230823020966129942415436628236066846174363923969637345587526 617581263789715407791820207240962215610992751641508071777841215564747 182276871093352240589178758431366661181645430375925344345631127463085 968430743448347852931565854120459246702292115927308318540156391690472 530976564792285849720105704104886036474896959961614218669992929270486 5380612144595180012867032899615432432246161180443998049427850390

2048	10331881482635325161809923103737431588521014905536056177640820595341817493510002745623302793486217283653844397892467324439644407348346347633908250673229073743236038753652430949861417976873746926333304377559454199909144438422738716967561579750445379894328030355815494442883829306848833562324278541933779844921732976840797144017734605996497033424727787188990279082098087547925501839022482136803586933046837356552269657646769507568971977797250468254702833657163511381637075834106964067470281913028544121614402754074102756948331630822636380359593484383828795673025277542596882605477804374903242656074156471838371619137320

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 = 98344254560345685911386562660 9

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

1. Factorized number = 98344254560345685911386562660 9

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 = 120252885822835461978871515277283618578310 4133

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

1. Factorized number =
120252885822835461978871515277283618578310413 3

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:

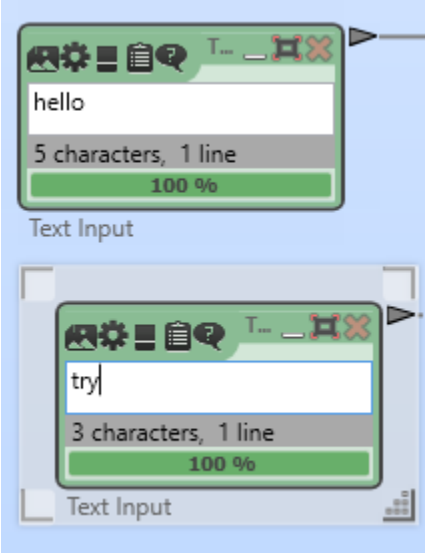
32162930963977948774291 * 37388658999242662601863

Part 3

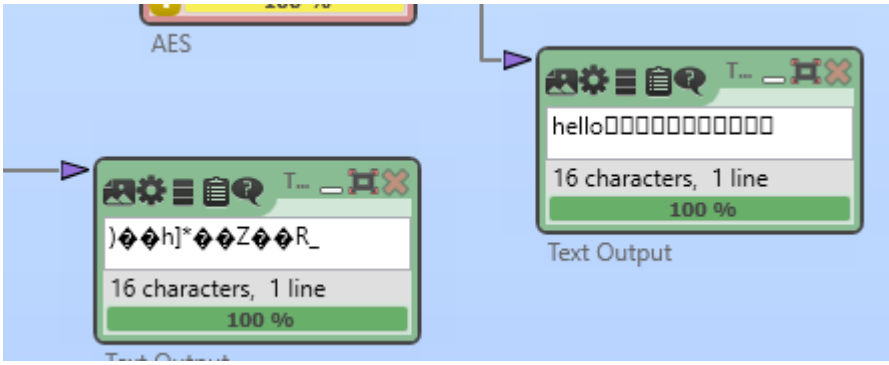
Screenshots:

Sender side.

AES-RSA:

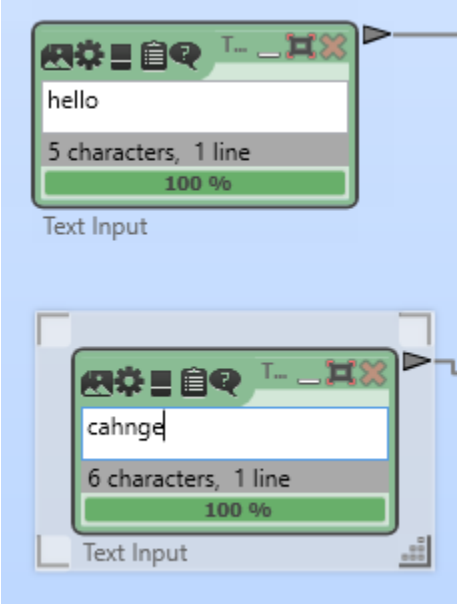


Receiver side:



AES:

Sender side.



Receiver side: