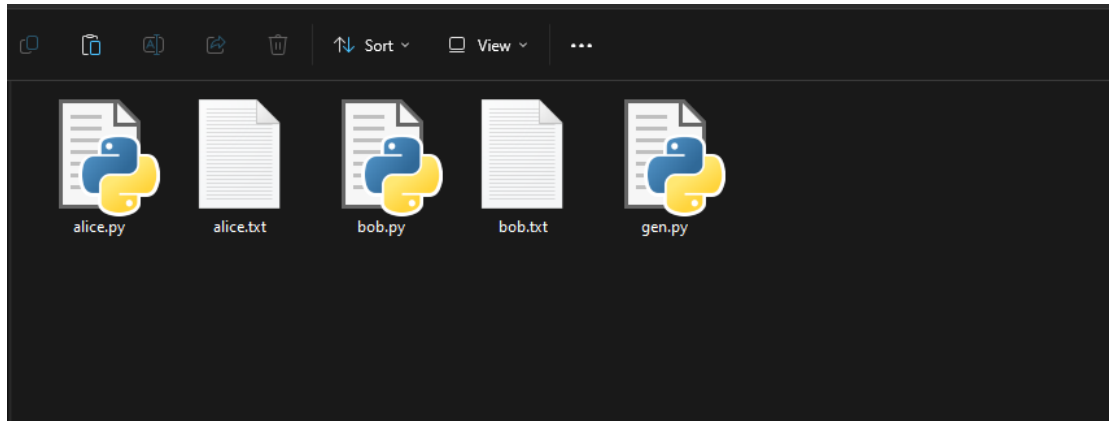


# CSCI368 – Network Security

## Assignment 1 Report



Folder should have:

alice.py (alice program)

bob.py (bob program)

alice.txt (alice IP, Port, PK information)

bob.txt (bob IP, Port, PK information)

gen.py (program to generate P, G, Alice PK & SK, Bob PK & SK)

### Instructions to run Alice.py and Bob.py

Ensure alice.py, alice.txt, bob.py, bob.txt are in the same folder

Open up 2 terminals

Navigate both to path of folder

run `$py alice.py` on the first terminal

Run `$py bob.py` on the second terminal

Alice will be the first sender so type the first message in the Alice terminal, followed by Bob and back to Alice and so on.

## Generation of P, G, Alice PK & SK, Bob PK & SK

(Please zoom in the document to see clearer)

PK =  $G^A SK$  (calculated in gen.py)

```
C:\Bronson\CyberSecurity\CSCI368 - Network Security\Assignment\Assignment 1\py gen.py
Prime Number P: 303872874471546795410288898649025852601795140552222545500544212951262750149398233717365588894515445025654001849346850741695145609607561026835712457879567542132484850267
6085581631310249322945252854482082907422889832857279826603262220151163299941929861832121590721243155928230160463942888307753876996250337237962007438929182836655370036213701089635605821
6588460006167263113055883958693079956764173088786636833741475248349474216382088309952753294167301826462974090310040917134094350618323414478802384160616876169031718056279558719032677489
325456923710039681947242914779981981898601579196507837389712412153895381323408781

Primitive Root G: 6

Secret Key (Alice): 14728160824416020100827132597799318844134754410843995243487047119304500542087603237417112833131942200537840238628292112672338395527337920354833620500866759254621127
2603883195779466396734648169998488804591288559005775644492344826073379720050047383071245910939035736696054614362475239973012287183752586920626470572029380507724652866192956864039752875
3683874057671585101425984439608704300375453743695766526714714064508501754370930874773302412374932980875198098695603825799850751448842022925742621469515114211036086706245821656831086823
353055204593015678516649605324232872402006730310288903208054726976788915851947743339

Secret Key (Bob): 1835983877865125605496397240357738583677499308177951998186700509316664990552167346158362627572766129895268609851849762483301354767264774501609135478049006514608516497
1163053329956192489879776298100196439982361269937331870865900600798561905138837631268970577886079046981250519470743279668954001859947737557358723514676010607744585789380427400626917043
328972895346701320074189856536499613758732297381360293214248331953510809286530719234121571063527994728115513889081334465918519788784276670599754082308404281682652700804155306971772451
9032721208524028279968237293246402729721047002777922016641218753024031461710676037

Public Key (Alice): 20492107684893881731047770451124610380222400310073929619534312926737604929758541155062979333089835911013176784386243629953083066446695055261029071862947398262135300
0877821959793076942955037007924290622149399111915123066704579673076942796805916352306574743992867939251231388501886961394090197950202060502855428977527359497900654444926803299565573421
9476361868844619853498983541570692228152284529472234442696308274232439265777970180073769067181019918677642634936310278773667845268493980681652968314244005090933829184838317933565031427
811912594058124131648360103632349353006034936506382178965578142431024264985516948347

Public Key (Bob): 8005538364173816535484286329561727628305282348627110581557242605175628688961892190588330611508649086633397453839279157510063377587760971982626125532884602585827434117
6375757783941563260166259528230821058872585303816993662027465117419702425216277860088628092167296389367957064571147129335747913244290291323379663730880005373041298636813216720659833232
257216367698005724420810357922893839788542458492219433158067486389646843434110627209517995167787751450970342815603838539225781696863804998867280401414642146350810906539696382990622962
913508126549311951010188028397921526211958781369430212450039910558679197235152355
```

## Checking of TK and LK in Alice.py and Bob.py

First, we got to make sure both LK in Alice and Bob is the same

Secondly, we got to make sure TK in Alice and Bob is the same for that ONE message transmission which is 1 encryption + 1 decryption.

Below, LK stays constant throughout, but TK is always changing per message transmission since r (nonce) is different every time a sender sends a message.

```
Command Prompt - py alice.py

C:\Bronson\CyberSecurity\CSCI368 - Network Security\Assignment\Assignment 1>py alice.py
TK:
707550915406868594456496070256319618425125773810648879117958351174855507404309442772616780608695752812823744810337707697
004208273507876606937085227104963840170398868390895391617375961454612788775564610456018420370441344299421545121716361405
708233727698063902318817431042815836452521859142727346723182700872412147585387659595447466378867869929290942328987254618
523387888221517940447213643932367125405752818007645563140479722274786675583093762281536904464990964795152057084756085510
757371732204273220431408098496822052494426463310468955583327770933482090429893155411589578820940997749741549395893033439
4641337229848815

Alice: network security
LK:
617519062461491655525535856735375298223599875306043439769288588606636499429798047216829716819650622735354631937118450303
257937886200600537057518770232003489137524665923642247134470960176298316284101408137854237479836403168275293787585798510
823508047198262091715217668158844611492122768012933484311827300042126486389489031333300645108908480773658259478406932790
649996893303383542419031469241373415791133837113682661884769652898451025587243724358919810946842396732012121163053924327
999604610091277394241269983893770040798472821584697726478854015747246920927042157560983631331517422551960254808951199589
3264403456393224

Sending: (18992401196528423701014877783728638939299564237620061957779554790219768388326791843191734752546431515709367817
993559462387167159311609566615288358669350909004245328508288632438134606536829074683852429495293487136652096151307037030
523970214647207515103818400274682439150691853829836718315651306591180652827816635189968660691416243310431178099249977621
415444294157583651349235702078959726513778008675557406056334022747267317058057298277914190596644351944924192184782741196
738740437370610650784174452890320730787006601401675273854569221530171147235400843531398645014671897144975838038501386165
558849223215371818394159981,gYqbmICdhM+cioyanYabl==,f0885ed388e74f3fea5677a108254c90d30c47bcfbfa959008dd2d6026e81918)

Command Prompt - py bob.py

C:\Bronson\CyberSecurity\CSCI368 - Network Security\Assignment\Assignment 1>py bob.py
Alice: 18992401196528423701014877783728638939299564237620061957779554790219768388326791843191734752546431515709367817993
559462387167159311609566615288358669350909004245328508288632438134606536829074683852429495293487136652096151307037030523
970214647207515103818400274682439150691853829836718315651306591180652827816635189968660691416243310431178099249977621415
444294157583651349235702078959726513778008675557406056334022747267317058057298277914190596644351944924192184782741196738
740437370610650784174452890320730787006601401675273854569221530171147235400843531398645014671897144975838038501386165558
849223215371818394159981,gYqbmICdhM+cioyanYabl==,f0885ed388e74f3fea5677a108254c90d30c47bcfbfa959008dd2d6026e81918

TK:
707550915406868594456496070256319618425125773810648879117958351174855507404309442772616780608695752812823744810337707697
004208273507876606937085227104963840170398868390895391617375961454612788775564610456018420370441344299421545121716361405
708233727698063902318817431042815836452521859142727346723182700872412147585387659595447466378867869929290942328987254618
523387888221517940447213643932367125405752818007645563140479722274786675583093762281536904464990964795152057084756085510
757371732204273220431408098496822052494426463310468955583327770933482090429893155411589578820940997749741549395893033439
4641337229848815

LK:
617519062461491655525535856735375298223599875306043439769288588606636499429798047216829716819650622735354631937118450303
257937886200600537057518770232003489137524665923642247134470960176298316284101408137854237479836403168275293787585798510
823508047198262091715217668158844611492122768012933484311827300042126486389489031333300645108908480773658259478406932790
649996893303383542419031469241373415791133837113682661884769652898451025587243724358919810946842396732012121163053924327
999604610091277394241269983893770040798472821584697726478854015747246920927042157560983631331517422551960254808951199589
3264403456393224

network security
Bob:
```



ca Command Prompt - py alice.py

Bob: 2365241377464997210705273419086722291369845655853651315956438851681770759218224856556235506690333892030451339050144  
271676627046226068231653738888863496153016196290389051839363223956771608445200298021310205412866075218184306776398045924  
857553953400008758924320109879201734183845461030040500377615501635274472150675754309517590386046674180856162283673946727  
05673414028259332772353551144690836086048271403952772640258592694120226994575512728623521176460015306229755309537503385  
253686501396610647207203135768512156832411408494449549128379300016707557491773944583329171836629867453707628298184275564  
3721177788527439688069,QEtaWUfRV1LTvtcR1pXHx4fHh8=,5aff47db299baee37c5cfd42103a8c348e52a8b10c470d9f23c9914cd18a96f

TK:

157306373617353786324604448165622186455732342478976472409479707336230718203782751806372700832793200601624057544518658922  
023515719022776943463050125326916060093655600468684519433597893787528195217908878743721868410658233335126411530890948392  
812726312623089844948936379655661887846144403204247156836602599683746618786774466402837681426850142181784363744521345075  
499055627742190959359290216053065467335345359485934644575619694645943559483041300619899738218381792563712358765626499888  
860409283296647826572616076630558914551906078692195824539116207842951219684195028778825918580123101467810019503632258171  
82139242541286190

LK:

617519062461491655525535856735375298223599875306043439769288588606636499429798047216829716819650622735354631937118450303  
257937886200600537057518770232003489137524665923642247134470960176298316284101408137854237479836403168275293787585798510  
823508047198262091715217668158844611492122768012933484311827300042126486389489031333300645108908480773658259478406932790  
649996893303383542419031469241373415791133837113682661884769652898451025587243724358919810946842396732012121163053924327  
999604610091277394241269983893770040798472821584697726478854015747246920927042157560983631331517422551960254808951199589  
3264403456393224

networksecurity10101

Alice:

ca Command Prompt - py bob.py

999604610091277394241269983893770040798472821584697726478854015747246920927042157560983631331517422551960254808951199589  
3264403456393224

network security

Bob: networksecurity10101

TK

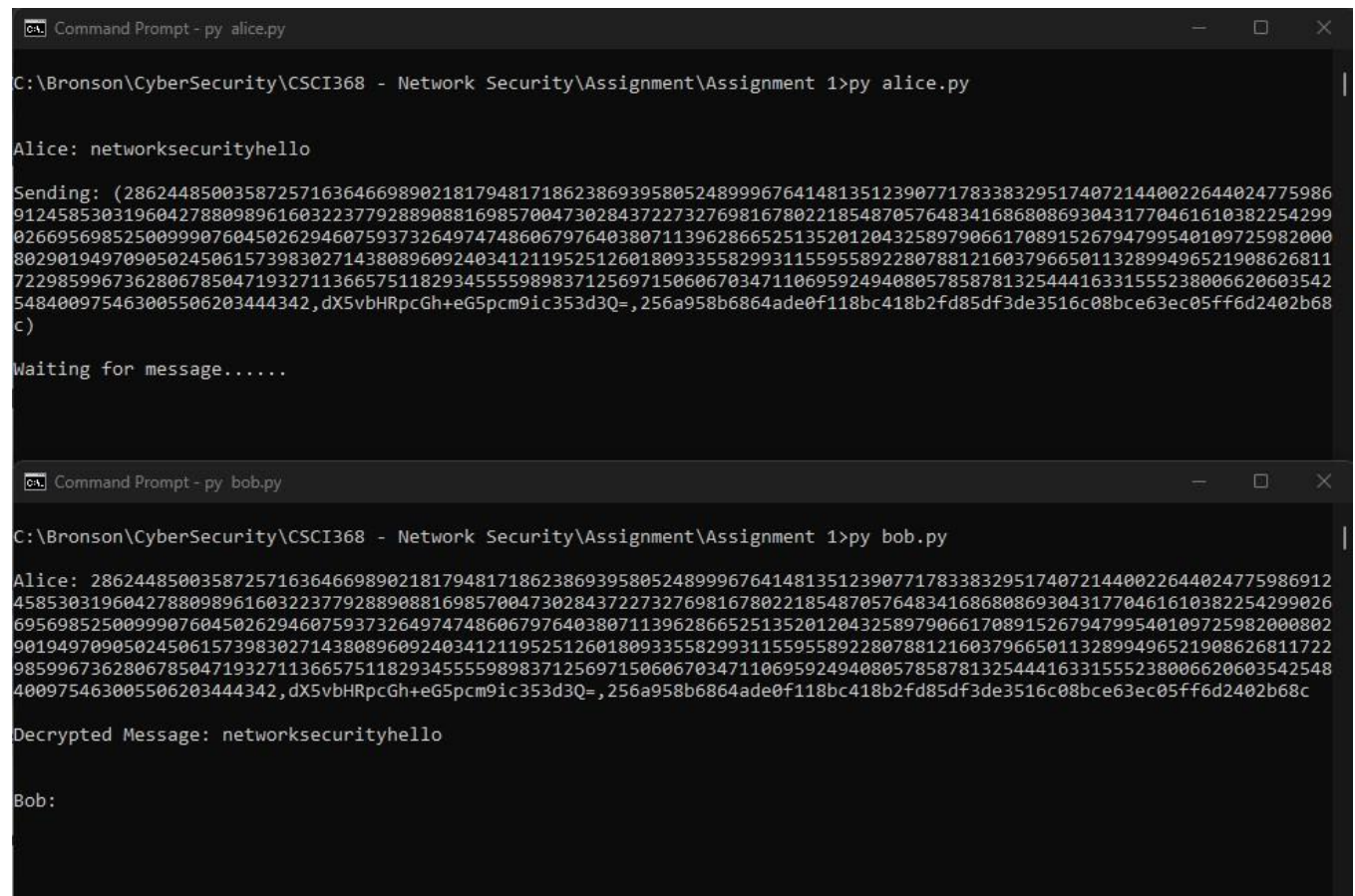
157306373617353786324604448165622186455732342478976472409479707336230718203782751806372700832793200601624057544518658922  
023515719022776943463050125326916060093655600468684519433597893787528195217908878743721868410658233335126411530890948392  
812726312623089844948936379655661887846144403204247156836602599683746618786774466402837681426850142181784363744521345075  
499055627742190959359290216053065467335345359485934644575619694645943559483041300619899738218381792563712358765626499888  
860409283296647826572616076630558914551906078692195824539116207842951219684195028778825918580123101467810019503632258171  
82139242541286190

LK:

617519062461491655525535856735375298223599875306043439769288588606636499429798047216829716819650622735354631937118450303  
257937886200600537057518770232003489137524665923642247134470960176298316284101408137854237479836403168275293787585798510  
823508047198262091715217668158844611492122768012933484311827300042126486389489031333300645108908480773658259478406932790  
649996893303383542419031469241373415791133837113682661884769652898451025587243724358919810946842396732012121163053924327  
999604610091277394241269983893770040798472821584697726478854015747246920927042157560983631331517422551960254808951199589  
3264403456393224

Sending: (23652413774649972107052734190867222913698456558536513159564388516817707592182248565562355066903338920304513390  
501442716766270462260682316537388888634961530161962903890518393632239567716084452002980213102054128660752181843067763980  
459248575539534000087589243201098792017341838454610300405003776155016352744721506757543095175903860466741808561622836739  
46727056734140282593327723535511446908360860482714039527726402585926941202269945755127286235211764600153062297553095375  
033852536865013966106472072031357685121568324114084944495491283793000167075574917739445833291718366298674537076282981842  
755643721177788527439688069,QEtaWUfRV1LTvtcR1pXHx4fHh8=,5aff47db299baee37c5cfd42103a8c348e52a8b10c470d9f23c9914cd18a96  
f)

## Running of Alice.py and Bob.py



```
Command Prompt - py alice.py

C:\Bronson\CyberSecurity\CSCI368 - Network Security\Assignment\Assignment 1>py alice.py

Alice: networksecurityhello

Sending: (28624485003587257163646698902181794817186238693958052489996764148135123907717833832951740721440022644024775986
912458530319604278809896160322377928890881698570047302843722732769816780221854870576483416868086930431770461610382254299
026695698525009990760450262946075937326497474860679764038071139628665251352012043258979066170891526794799540109725982000
802901949709050245061573983027143808960924034121195251260180933558299311559558922807881216037966501132899496521908626811
722985996736280678504719327113665751182934555598983712569715060670347110695924940805785878132544416331555238006620603542
548400975463005506203444342,dX5vbHRpcGh+eG5pcm9ic353d3Q=,256a958b6864ade0f118bc418b2fd85df3de3516c08bce63ec05ff6d2402b68
c)

Waiting for message.....

Command Prompt - py bob.py

C:\Bronson\CyberSecurity\CSCI368 - Network Security\Assignment\Assignment 1>py bob.py

Alice: 28624485003587257163646698902181794817186238693958052489996764148135123907717833832951740721440022644024775986912
458530319604278809896160322377928890881698570047302843722732769816780221854870576483416868086930431770461610382254299026
695698525009990760450262946075937326497474860679764038071139628665251352012043258979066170891526794799540109725982000802
901949709050245061573983027143808960924034121195251260180933558299311559558922807881216037966501132899496521908626811722
985996736280678504719327113665751182934555598983712569715060670347110695924940805785878132544416331555238006620603542548
400975463005506203444342,dX5vbHRpcGh+eG5pcm9ic353d3Q=,256a958b6864ade0f118bc418b2fd85df3de3516c08bce63ec05ff6d2402b68c

Decrypted Message: networksecurityhello

Bob:
```

First, Alice sent a message to Bob.

Both sender and receiver will have ( $G^r$ , C, MAC) displayed.

Receiver will decrypt and display message.



Next, Bob will send back to Alice.

```
Select Command Prompt - py alice.py

C:\Bronson\CyberSecurity\CSCI368 - Network Security\Assignment\Assignment 1>py alice.py

Alice: networksecurityhello

Sending: (28624485003587257163646698902181794817186238693958052489996764148135123907717833832951740721440022644024775986
91245830319604278809896160322377928890881698570047302843722732769816780221854870576483416868086930431770461610382254299
026695698525009990760450262946075937326497474860679764038071139628665251352012043258979066170891526794799540109725982000
802901949709050245061573983027143808960924034121195251260180933558299311559558922807881216037966501132899496521908626811
722985996736280678504719327113665751182934555598983712569715060670347110695924940805785878132544416331555238006620603542
548400975463005506203444342, dX5vbHRpcGh+eG5pcm9ic353d3Q=, 256a958b6864ade0f118bc418b2fd85df3de3516c08bce63ec05ff6d2402b68
c)

Waiting for message.....

Bob: 1603232633648717107730135733752772515394000743386098170472678942385734715277047568839316825053589697453266025959002
621773708114204634948110379148278331202784702735889459361970578483130509558241646676947654340453414230480210436989466291
022125710583363786317838281160428064090997664257644515289139254425003029980889599273364407362763046084872679975997123694
435635598552064503424446844044281765676307018126973525680032234488680504367631526088831423995721473963748795982990924963
092905915863172817420723746795041323765392239832329116316062924183252909884617172645663698091199353087704311279974723913
1530952663786672018844, q6Cxsqq3rragprC3rLG8p7ygoKA=, a5624a95863704da05824aaae5465d8c35c07b4532c2c7da02cdebb293d0dc05

Decrypted Message: networksecuritybyeee

Alice:

C:\Bronson\CyberSecurity\CSCI368 - Network Security\Assignment\Assignment 1>py bob.py

Alice: 28624485003587257163646698902181794817186238693958052489996764148135123907717833832951740721440022644024775986912
458530319604278809896160322377928890881698570047302843722732769816780221854870576483416868086930431770461610382254299026
695698525009990760450262946075937326497474860679764038071139628665251352012043258979066170891526794799540109725982000802
901949709050245061573983027143808960924034121195251260180933558299311559558922807881216037966501132899496521908626811722
985996736280678504719327113665751182934555598983712569715060670347110695924940805785878132544416331555238006620603542548
400975463005506203444342, dX5vbHRpcGh+eG5pcm9ic353d3Q=, 256a958b6864ade0f118bc418b2fd85df3de3516c08bce63ec05ff6d2402b68c

Decrypted Message: networksecurityhello

Bob: networksecuritybyeee

Sending: (16032326336487171077301357337527725153940007433860981704726789423857347152770475688393168250535896974532660259
590026217737081142046349481103791482783312027847027358894593619705784831305095582416466769476543404534142304802104369894
662910221257105833637863178382811604280640909976642576445152891392544250030299808895992733644073627630460848726799759971
236944356355985520645034244468440442817656763070181269735256800322344886805043676315260888314239957214739637487959829909
249630929059158631728174207237467950413237653922398323291163160629241832529098846171726456636980911993530877043112799747
239131530952663786672018844, q6Cxsqq3rragprC3rLG8p7ygoKA=, a5624a95863704da05824aaae5465d8c35c07b4532c2c7da02cdebb293d0dc0
5)

Waiting for message.....
```

Similarly, both sender and receiver will have (G<sup>r</sup>, C, MAC) displayed.  
Receiver will decrypt and display message.