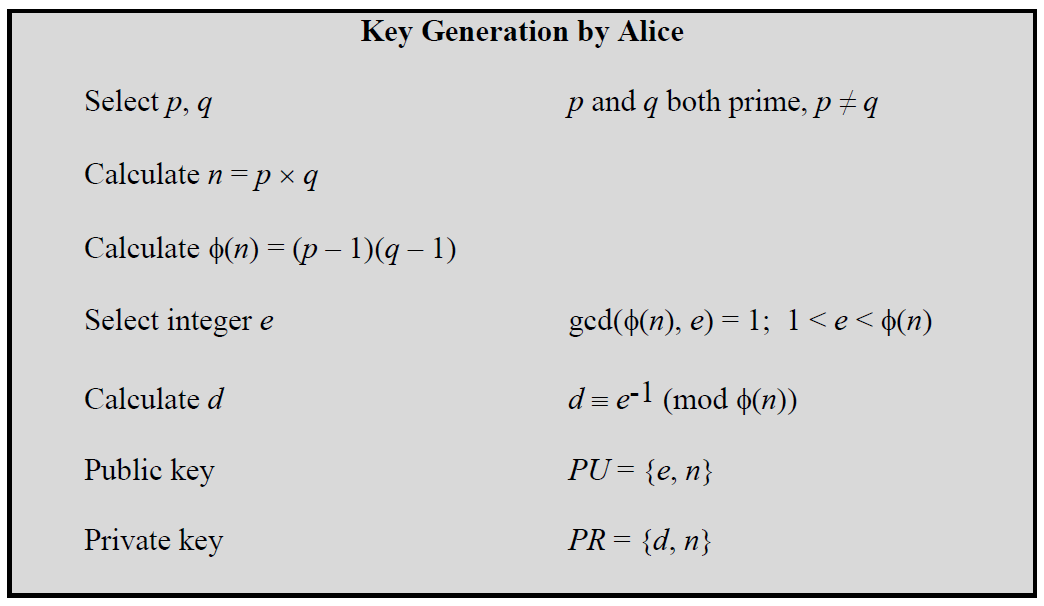


**SUMMER SEMESTER 2024**

**APT3090 CRYPTOGRAPHY AND NETWORK SECURITY**

Write a program using any Object oriented programming language to show implementation of RSA. The input p and q should be generated by randomly (15 Marks)



To encrypt a message, M, with the public key, create the ciphertext, C, using the equation: C = Me mod n

The receiver then decrypts the ciphertext with the private key using the equation: M = Cd mod n

**Evaluation Criteria**

1. Correctness of code
2. Random number Generation of p, q
3. Generation of multiple pairs of PU ( e,n) and PR Keys (d,n)
4. Encryption and Decryption of input message
5. A lab report showing your code , sample outputs and code explanation
6. import random
7. from sympy import isprime, mod\_inverse
8. def generate\_prime\_candidate(length):
9. """ Generate an odd integer randomly """
10. p = random.getrandbits(length)
11. # ensure p is odd
12. p |= (1 << length - 1) | 1
13. return p
14. def generate\_prime\_number(length=1024):
15. """ Generate a prime number of length bits """
16. p = 4
17. # keep generating while the number is not prime
18. while not isprime(p):
19. p = generate\_prime\_candidate(length)
20. return p
21. def generate\_keypair(bits=1024):
22. p = generate\_prime\_number(bits)
23. q = generate\_prime\_number(bits)
24. n = p \* q
25. phi = (p - 1) \* (q - 1)
26. e = random.randrange(1, phi)
27. # Ensure e is coprime with phi
28. g = gcd(e, phi)
29. while g != 1:
30. e = random.randrange(1, phi)
31. g = gcd(e, phi)
32. d = mod\_inverse(e, phi)
33. return ((e, n), (d, n))
34. def gcd(a, b):
35. while b != 0:
36. a, b = b, a % b
37. return a
38. def encrypt(pk, plaintext):
39. key, n = pk
40. cipher = [pow(ord(char), key, n) for char in plaintext]
41. return cipher
42. def decrypt(pk, ciphertext):
43. key, n = pk
44. plain = [chr(pow(char, key, n)) for char in ciphertext]
45. return ''.join(plain)
46. if \_\_name\_\_ == '\_\_main\_\_':
47. message = "This is the message!"
48. print("Generating keypair...")
49. public, private = generate\_keypair(1024)
50. print("Public key:", public)
51. print("Private key:", private)
53. encrypted\_msg = encrypt(public, message)
54. print("Encrypted message:", ''.join(map(lambda x: str(x), encrypted\_msg)))
56. decrypted\_msg = decrypt(private, encrypted\_msg)
57. print("Decrypted message:", decrypted\_msg)

output

[Running] python -u "c:\Users\smute\Downloads\rsa.py"

Generating keypair...

Public key: (2853353715139667262846884568827099313896261378929355134609598556169384162251035940884050586694143222327142412113448832307508548513102097966869221561488811258400847132912732336980422743695704073153993702203430820439388508092318029755205982786187556843111468574592626618706716617619604968702514828182938925619422095177624291004416965056498424867053418297667662883895916249589565552895424033266459100603402138531626084733787872046747097378134205350885295382107966001748220557629825209943823460629639562685103927704249596236610035643099955403068712279077355162122240895876293073762318166030471590488372132937874509194839, 17002418259786815659712503776709783065740260306520985610772141708361047749092280627637575530519535221738650223120651137512568838401893209882384529685466831222923912037837708633661849016350497240268278758510307306283034142923448912292581967115247272604145817244532274790326603004998531374044857701442060341291793253594172511588331774677778239912663107224488707935117405417001710705370779978873836590001375020925747675506981688745947095100946436274481684840554142029531850898279715952535055117387557634490286927154334480995065730453817720173624855964951796630680452192574409244624614014185696846249704585401829615514807)

Private key: (5499129978088859890640002482398148844473781719030962584339658473699984137055313063267056947617069834213692478851989303422281819044942841047801961426430819156159833136957869644497506318052567048162987654231065774984470213763377845725240714263811071978412484180826157468129697104430469007025802762776651538606216925506049133183952508922744705077030304215954974234990417292158910584825992296964348592856055122237612623214674998101574188506012957904427663266697665330560635317046856561320611739257884493962027344412505901260273155348351754752585564292411056665492585657906749484084492246026116412752456844877579258842759, 17002418259786815659712503776709783065740260306520985610772141708361047749092280627637575530519535221738650223120651137512568838401893209882384529685466831222923912037837708633661849016350497240268278758510307306283034142923448912292581967115247272604145817244532274790326603004998531374044857701442060341291793253594172511588331774677778239912663107224488707935117405417001710705370779978873836590001375020925747675506981688745947095100946436274481684840554142029531850898279715952535055117387557634490286927154334480995065730453817720173624855964951796630680452192574409244624614014185696846249704585401829615514807)

Encrypted message: 14829972509653626984825292745033691726548780499731701205842865646652275919797938327879668408789598802142894367364351005038294037657751597179721194650096060806558679625266463530323937014464480899788347974026541563468198969262344448930901940492489049485590752427006018143568254206164247316441606669893206789645996640551128476037053119906739880416908293984911921176553282299581957023677538956805665435996833711105924625144742851251391017622641474611855566408337146073169767126119683043595058473138684385139842611741084923572299715051837193428208257590232486711420037032149441617610321468053166337403487082481744409900925254411307512424265360645123775500134947037420639201321401241036785904148160258713134875756934119965253645480143481980955369371781545324967612600815727230910425154146254782419448258255747866158055801857053067559442602773520492456022238924945926492591899621262464675343413509899303180335415844496466446887368720322855849213373874779198244043836694312377016606850630523412277011126129223946088412122992982144354765360316838048009576096692845014982871502744139833102529789653184400181004181857506897793881399480597834958093547530579320464339457463226055774998169286802628613976423059501914109909786631656567748652613942113410799948484795667229342959485893395331735840257720564614484457871594223666735738183377084791088854474917727929936822833331815743241983221431101838886275791038013673853112251723993153510794306596688572324998907224006022433001211058709522986718395056464389162104939799915750105616579461437398634480654262468779589916490947544302801089262502728311432393585120453618106088540444531146103268506461935593007987522464090856798504119697287172230273223607202700712940345714786440858459585459702501489068100301065328697337154569291795400983774996484249908070685689717587939770250732469381496661822647356897583605768885330661609847365052828617749170297664245980171040832502286312148687052726136331654218777690079672260575780955749065871251946257374426218736013896592435321946516559899392152134469033780049132787991282039155040691209646621501431762125469963141623302157822243642274956554807862450935752786602033367802627107436634734817942195415119844581595160939009248718243610773210637453128555848525485223345437661200730827020966463586229684180547414647227393582000081269492521852052329689454443463100439300730480009343090546112843089122127631765782088687944657096293133927979128063854725608217519226781409711765615779774364142249500711404842353394886541721293748789018580301544420596861003945885627413902907930112830489373751951937804424659914642904124851456184504166939784632603754380948428383142491390540940246833044965880338388668448494584893716742933160065738971729887379876627728579220100952710345103916620259022924213081306843501186142991760399192444834411509819716269539282541895319435841553330682471921064710602104661637946712712642970837565520585929950545455764816929873432889185877836925466733616918434110911614341610882686519482972783237250860123355463162327956218826036555921656140129705193792912594603105328557258604146425529916513393057215041134107999484847956672293429594858933953317358402577205646144844578715942236667357381833770847910888544749177279299368228333318157432419832214311018388862757910380136738531122517239931535107943065966885723249989072240060224330012110587095229867183950564643891621049397999157501056165794614373986344806542624687795899164909475443028010892625027283114323935851204536181060885404445311461032685064619355930079875224640908567985041196972871722302732236072027007129403457147864408584595854597025014890681003010653286973371545692917954009837749964842499080706856897175879397702507324693814966618226473568975836057688853306616098473650528286177491702976642459801710408325022863121486870527261363316542187776900796722605757809557490658712519462573744262187360138965924353219465165598993921521344690337800491327879912820391550406912096466215014317621254699631416233021578222436422749565548078624509357527866020333678026271074366347348179421954151198445815951609390092487182436107732106374531285558485254852233454376612007308270209664635862296841805474146472273935820000812694925218520523296894544434631004393007304800093430905461128430891221276317657820886879446570962931339279791280638547256082175192267814097117656157797743641422495007114048423533948865417212937487890185803015444205968610039458856274139029079301128304893737519519378044246599146429041248514561845041669397846326037543809484283831424913905409402468330449658803383886684484945848937167429331600657389717298873798766277285792201009527103451039166202590229242130813068435011861429917603991924448344115098197162695392825418953194358415533306824719210647106021046616379467127126429708375655205859299505454557648169298734328891858778369254667336169184341109116143416108826865194829727832372508601233554631623279562188260365559216561401297051937929125946031053285572586041464255299165133930572150442980214944886770029098351758749620158451776437679929013676981401168136873886299524706421856857593295970272396027870938486448385031846872923176881437188917456494201645858004328934045633486043887027295939043965868733040635102189994924106155050163315388422400297033893637446750948218656981830723659002570991168233824095010097448481002117566425810440926375323890653724690191152541461944949042129922118726361715588878104406645393995177440015043309026740283408286154130178186736458009065268630439757089963127791566612650552505713953613172134093022502086007646222818215030758871812653689972314944890218093288633306580807902544113075124242653606451237755001349470374206392013214012410367859041481602587131348757569341199652536454801434819809553693717815453249676126008157272309104251541462547824194482582557478661580558018570530675594426027735204924560222389249459264925918996212624646753434135098993031803354158444964664468873687203228558492133738747791982440438366943123770166068506305234122770111261292239460884121229929821443547653603168380480095760966928450149828715027441398331025297896531844001810041818575068977938813994805978349580935475305793204643394574632260557749981692868026286139764230595019141099097866316565677486526139424536703137616200568460727235619561993467843650045870910405508639584743835621092274203812726553705728766251512901699175465409501027825435207344840601900597423787939894014510722738699828029966027956169852081571663331736779445593434452387494202461574499003581912283583812666951948037839632897498607654764554584842992788825782720011848662170319155195995070109488152325577151263322225346057195835577909386954602051757870841159796817960687323788429236485126372659108193390695626525940921913435100483305257783175975452654107827997586575212151965484992249352708603067837028584684062538147213023615646023345039517968226140536423533948865417212937487890185803015444205968610039458856274139029079301128304893737519519378044246599146429041248514561845041669397846326037543809484283831424913905409402468330449658803383886684484945848937167429331600657389717298873798766277285792201009527103451039166202590229242130813068435011861429917603991924448344115098197162695392825418953194358415533306824719210647106021046616379467127126429708375655205859299505454557648169298734328891858778369254667336169184341109116143416108826865194829727832372508601233554631623279562188260365559216561401297051937929125946031053285572586041464255299165133930572150484478828449321020835223717280790869080032525341946005172658978337331839979897851571914743265298112220130731828414069938900187098937923271236212406426108812442699424677112704944465774595265288249910371595724900881269098896294645727169985017471963704103238165926981497172644238649491380995443026126451171874468976056093507286833662961338421133849507810496690705990389238976885082516465966262230079411375927960212537112358642817506516952029922720790764316786411847179752730150937425276173787547649648052168576434621298667857349072763526629704271541154264200109469901984284622235731328127976535239132537630562462653543364536703137616200568460727235619561993467843650045870910405508639584743835621092274203812726553705728766251512901699175465409501027825435207344840601900597423787939894014510722738699828029966027956169852081571663331736779445593434452387494202461574499003581912283583812666951948037839632897498607654764554584842992788825782720011848662170319155195995070109488152325577151263322225346057195835577909386954602051757870841159796817960687323788429236485126372659108193390695626525940921913435100483305257783175975452654107827997586575212151965484992249352708603067837028584684062538147213023615646023345039517968226140536160984736505282861774917029766424598017104083250228631214868705272613633165421877769007967226057578095574906587125194625737442621873601389659243532194651655989939215213446903378004913278799128203915504069120964662150143176212546996314162330215782224364227495655480786245093575278660203336780262710743663473481794219541511984458159516093900924871824361077321063745312855584852548522334543766120073082702096646358622968418054741464722739358200008126949252185205232968945444346310043930073048000934309054611284308912212763176578208868794465709629313392797912806385472560821751922678140971176561577977436414224950071140481609847365052828617749170297664245980171040832502286312148687052726136331654218777690079672260575780955749065871251946257374426218736013896592435321946516559899392152134469033780049132787991282039155040691209646621501431762125469963141623302157822243642274956554807862450935752786602033367802627107436634734817942195415119844581595160939009248718243610773210637453128555848525485223345437661200730827020966463586229684180547414647227393582000081269492521852052329689454443463100439300730480009343090546112843089122127631765782088687944657096293133927979128063854725608217519226781409711765615779774364142249500711404815915979569164295038298804212986254240892952031581782721917429300815387842242223233862869649706861833086490444910447330193542333595718236714889255979011640794263289646605742037461451668533811773186460697060721071490333881819282317637239489866672068440716031901092180077079278963377178642259378462160573773446786964805187941324580121807944218799001774045883044012909717955169748215321776308884982216355219804456101758689566732562969602081922358945396834520255051631931029144511364053021874302696176572503769167643373968512023431502660942983472292561941278328212447499674533303075341209096711642844092370154922906692100361339930467459275677598180483437611126176775045326696062606774373338487809159891809993251320103167606176832548963891484222791064181062981412435117615300895040725090411760805374623940411980263424352095311409600009493534987613361153376457489292875848736182302969060851684067153617863794573401075119320605647405198191605955406188193868935082166204145579226164038314652487822127935969178323291522318495820044364336294551766172280383472035247122926926580959890554834618667561530022913890279716555479217089872673041719092459703358120874136980900051862792400439203447728029010732029316165542513507490856488614390548644747045367031376162005684607272356195619934678436500458709104055086395847438356210922742038127265537057287662515129016991754654095010278254352073448406019005974237879398940145107227386998280299660279561698520815716633317367794455934344523874942024615744990035819122835838126669519480378396328974986076547645545848429927888257827200118486621703191551959950701094881523255771512633222253460571958355779093869546020517578708411597968179606873237884292364851263726591081933906956265259409219134351004833052577831759754526541078279975865752121519654849922493527086030678370285846840625381472130236156460233450395179682261405369654375244617843691367616754122353766171494775681944690712615312770401703101017996196578919077414993633911658075896612341582668733527364012469705075720232702851225701798695904398294494246629083409927954643937023000906140145405689804863064350664183865285207253257377750973799605879853921286799750073229981386650680696333304538703062153693360751683487761660207711369409055166069871704779417390764957610361041631447173173657126060101612805604957108720310888192847622029508028057325214269801417535441375675689182655898151541056438378603928666381556970682318809674969179273251151568835270607731311937200653969979422152684

Decrypted message: This is the message!

[Done] exited with code=0 in 6.453 seconds