Final Year B.Tech. (CSE) – VII [2024-25]

6CS451: Cryptography and Network Security Lab (C&NS Lab)

Date: 26/08/2024

Assignment 7

PRN: 21510042 **Name:** Omkar Rajesh Auti

---

1. Implementation of RSA Algorithm

Ans:

The RSA algorithm is one of the first public-key cryptosystems and is widely used for secure data transmission. It is an asymmetric cryptographic algorithm, meaning it uses a pair of keys: a public key for encryption and a private key for decryption. It relies on the mathematical properties of prime numbers.

How RSA Works:

1. **Key Generation:**
   - Choose two large prime numbers p and q.
   - Compute n = p * q.
   - Compute the totient $\phi(n) = (p-1) * (q-1)$.
   - Choose an encryption key e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. The integer e is the public key exponent.
   - Calculate the decryption key d such that $d * e \equiv 1 \pmod{\phi(n)}$. The integer d is the private key exponent.
2. **Encryption:**
   - The public key is (n, e).
   - Given a plaintext message M, the ciphertext C is computed as:

     C = M^ e mod n.
3. **Decryption:**

- The private key is (n, d).
- Given a ciphertext C, the plaintext M is recovered as:

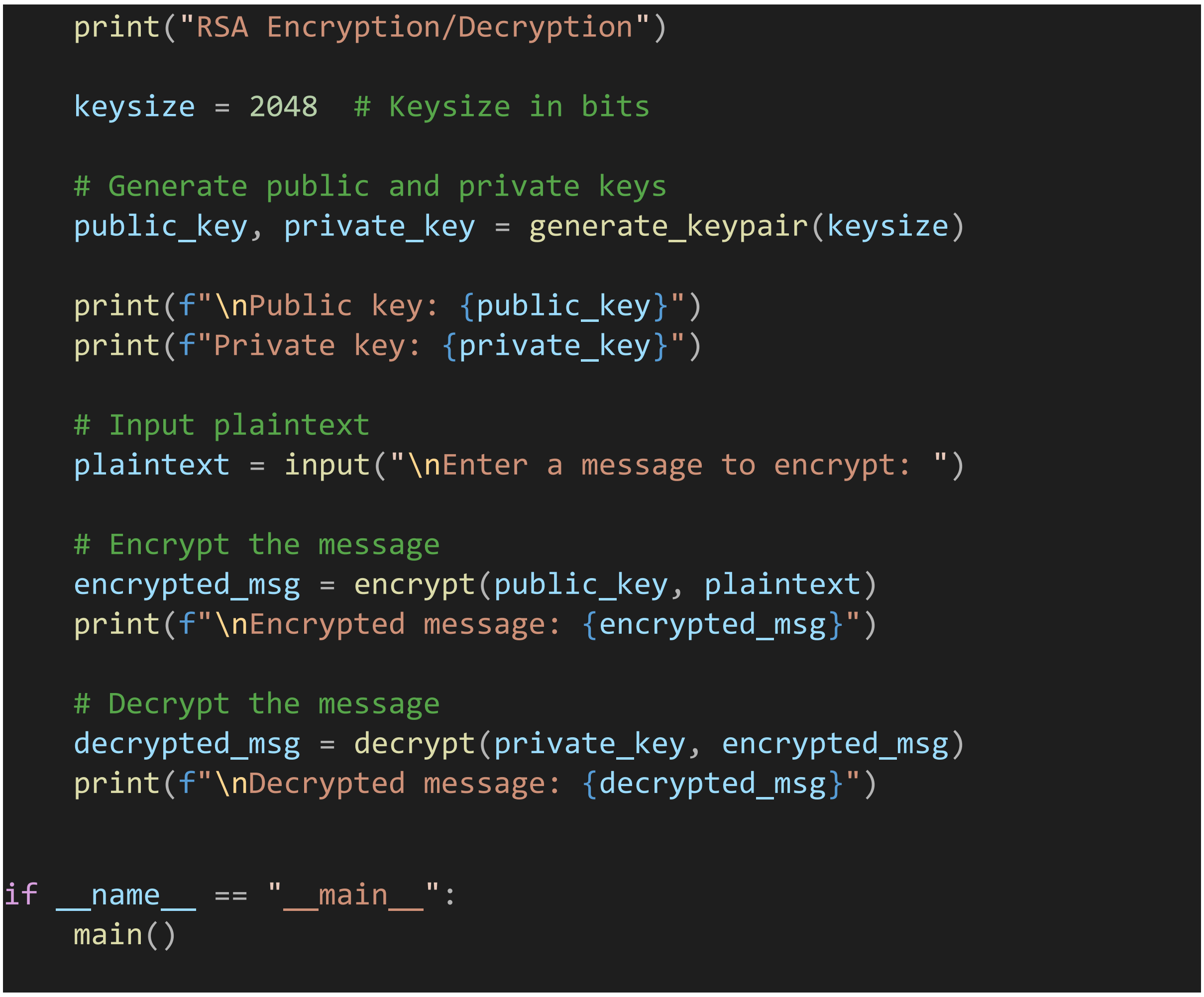
  M = C^d mod n

To implement the RSA algorithm **using large prime numbers with 2048 bits** and converting plaintext into numbers, we'll use the **Crypto library in Python**, which provides the **necessary tools to handle such large prime numbers and perform RSA encryption and decryption.**

The large primes and the strong key sizes make RSA secure against most attacks when implemented correctly.

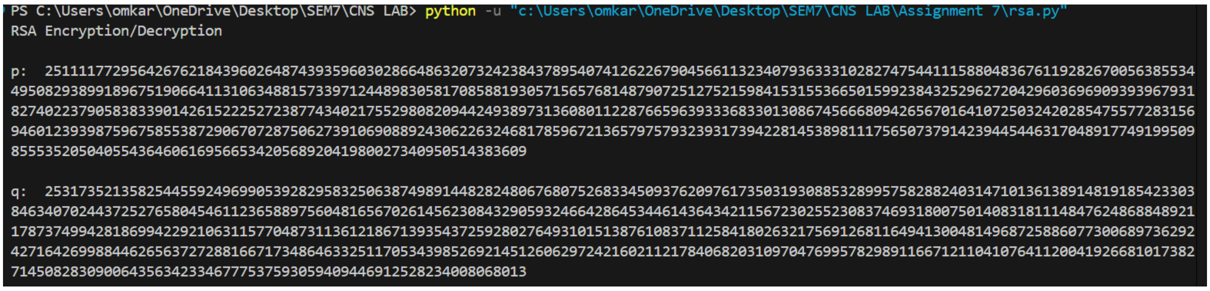
Python Code:

```python
import random
from sympy import isprime, mod_inverse

def generate_prime_candidate(length):
    """Generate an odd integer randomly."""
    p = random.getrandbits(length)
    # Ensure p is odd
    p |= (1 << length - 1) | 1
    return p


def generate_prime_number(length):
    """Generate a prime number."""
    p = 4
    while not isprime(p):
        p = generate_prime_candidate(length)
    return p


def generate_keypair(keysize):
    """Generate RSA public and private keys."""
    # Generate two large primes p and q
    p = generate_prime_number(keysize)
    q = generate_prime_number(keysize)

    print("\np: ", p)
    print("\nq: ", q)

    # Compute n = p * q
    n = p * q

    # Compute Euler's Totient ϕ(n) = (p-1)*(q-1)
    phi = (p - 1) * (q - 1)

    # Choose an integer e such that 1 < e < phi(n) and gcd(e, phi(n)) = 1
    e = random.randrange(2, phi)
    g = gcd(e, phi)
    while g != 1:
        e = random.randrange(2, phi)
        g = gcd(e, phi)

    # Compute d, the modular inverse of e
    d = mod_inverse(e, phi)

    # Public key (e, n) and Private key (d, n)
    return ((e, n), (d, n))


def gcd(a, b):
    """Compute the greatest common divisor using Euclid's algorithm."""
    while b != 0:
        a, b = b, a % b
    return a


def encrypt(public_key, plaintext):
    """Encrypt plaintext using the public key."""
    e, n = public_key
    cipher = [pow(ord(char), e, n) for char in plaintext]
    return cipher


def decrypt(private_key, ciphertext):
    """Decrypt ciphertext using the private key."""
    d, n = private_key
    plain = [chr(pow(char, d, n)) for char in ciphertext]
    return ''.join(plain)


def main():
    """Run RSA algorithm."""
```

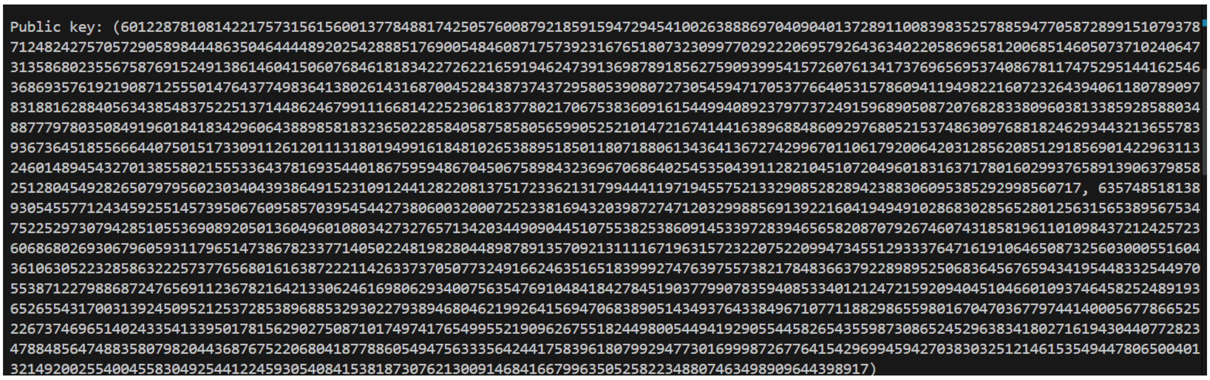


```
    print("RSA Encryption/Decryption")

    keysize = 2048  # Keysize in bits

    # Generate public and private keys
    public_key, private_key = generate_keypair(keysize)

    print(f"\nPublic key: {public_key}")
    print(f"Private key: {private_key}")

    # Input plaintext
    plaintext = input("\nEnter a message to encrypt: ")

    # Encrypt the message
    encrypted_msg = encrypt(public_key, plaintext)
    print(f"\nEncrypted message: {encrypted_msg}")

    # Decrypt the message
    decrypted_msg = decrypt(private_key, encrypted_msg)
    print(f"\nDecrypted message: {decrypted_msg}")


if __name__ == "__main__":
    main()
```

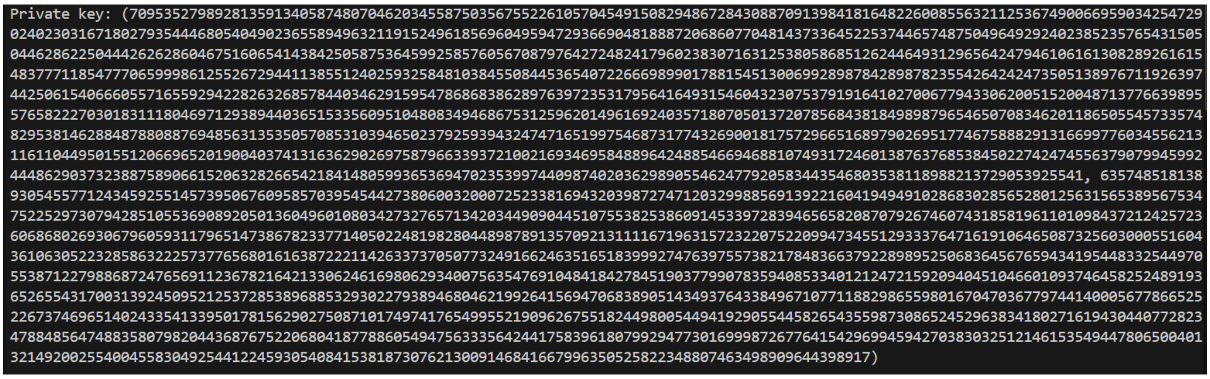
Output:



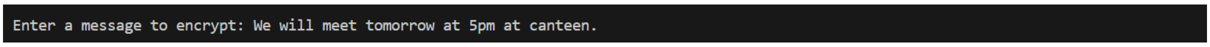
```
PS C:\Users\omkar\OneDrive\Desktop\SEM7\CNS LAB> python -u "c:\Users\omkar\OneDrive\Desktop\SEM7\CNS LAB\Assignment 7\rsa.py"
RSA Encryption/Decryption

p:  25111177295642676218439602648743935960302866486320732423843789540741262226790456611323407936333102827475441115880483676119282670056385534
4950829389918967519066411310634881573397124489830581708588193057156576814879072512752159841531553665015992384325296272042960369690939396793l
827402237905838339014261522252723877434021755298082094424938973136080112287665963933368330130867456668094265670164107250324202854755772831S6
946012393987596758553872906707287506273910690889243062263246817859672136579757932393173942281453898111756507379142394454463170489177491995O9
8555352050405543646061695665342056892041980027340950514383609

q:  25317352135825445592496990539282958325063874989144828248067680752683345093762097617350319308853289957582882403147101361389148191854233O3
846340702443725276580454611236588975604816567026145623084329059324664286453446143643421156723025523083746931800750140831811148476248688489Z1
17873749942818699422921063115770487311361218671393543725928027649310151387610837112584180263217569126811649413004814968725886077300689736292
42716426998844626563727288166717348646332511705343985269214512606297242160211217840682031097047699578298911667121104107641120041926681017382
71450828309006435634233467775375930594094469125282340O8068013
```



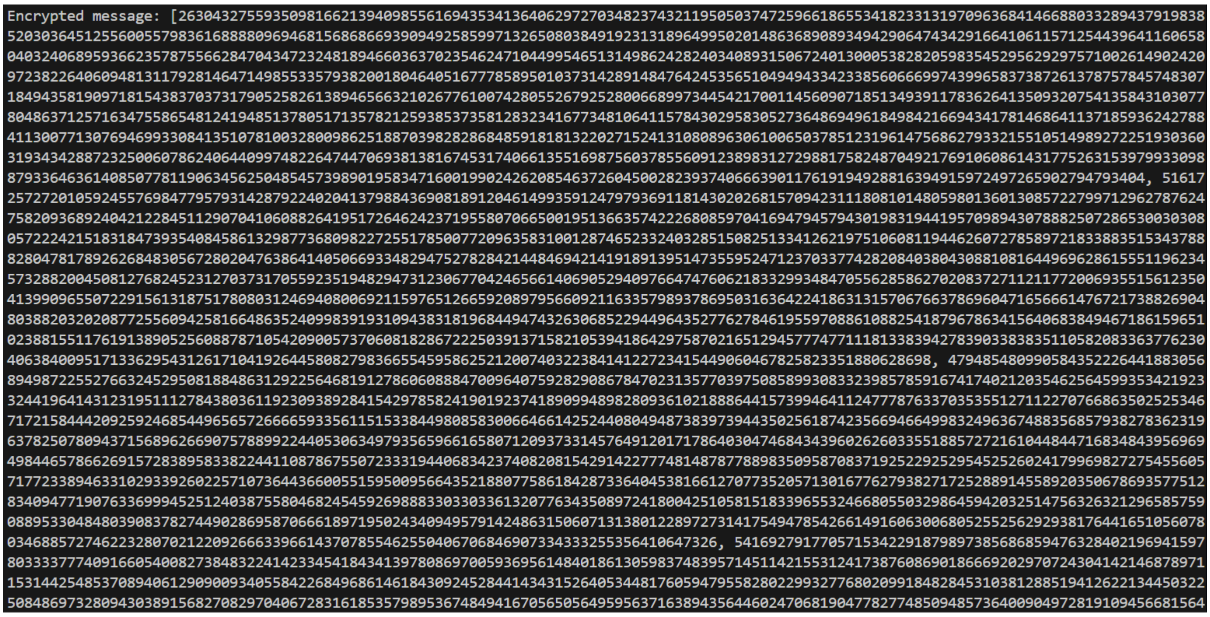
```
Public key: (6012287810814221757315615600137784881742505760087921859159472945410026388869704090401372891100839835257885947705872899151079378
71248242757057290589844486350464444892025428885176900548460871757392316765180732309977029222069579264363402205869658120068514605073710240647
31358680235567587691524913861460415060768461818342272622165919462473913698789185627590939954157260761341737696569537408678117475295144162546
36869357619219087125550147643774983641380261431687004528438737437295805390807273054594717053776640531578609411949822160723264394061180789097
83188162884056343854837522513714486246799111668142252306183778021706753836091615449940892379773724915968905087207682833809603813385928588034
88777978035084919601841834296064388985818323650228584058758580565990525210147216741441638968848609297680521537486309768818246293443213655783
93673645185566644075015173309112612011131801949916184810265388951850118071880613436413672742996701106179200642031285620851291856901422963113
24601489454327013855802155533643781693544018675959486704506758984323696706864025453504391128210451072049601831637178016029937658913906379858
25128045492826507979560230340439386491523109124412822081375172336213179944411971945575213329085282894238830609538529299856O717, 635748518138
93054557712434592551457395067609585703954544273806003200072523381694320398727471203299885691392216041949491028683028565280125631565389567534
75225297307942851055369089205013604960108034273276571342034490904451075538253860914533972839465658208707926746074318581961101098437212425723
60686802693067960593117965147386782337714050224819828044898789135709213111167196315723220752209947345512933376471619106465087325603000551604
36106305223285863222573776568016163872221142633737050773249166246351651839992747639755738217848366379228989525068364567659434195448332544970
55387122798868724765691123678216421330624616980629340075635476910484184278451903779907835940853340121247215920940451046601093746458252489193
65265543170031392450952125372853896885329302279389468046219926415694706838905143493764338496710771188298655980167047036779744140005677866525
22673746965140243354133950178156290275087101749741765499552190962675518244980054494192905544582654355987308652452963834180271619430440772823
47884856474883580798204436876752206804187788605494756333564244175839618079929477301699987267764154296994594270383032512146153549447806500401
321492002554004558304925441224593054084153818730762130091468416679963505258223488074634989O9644398917)
```



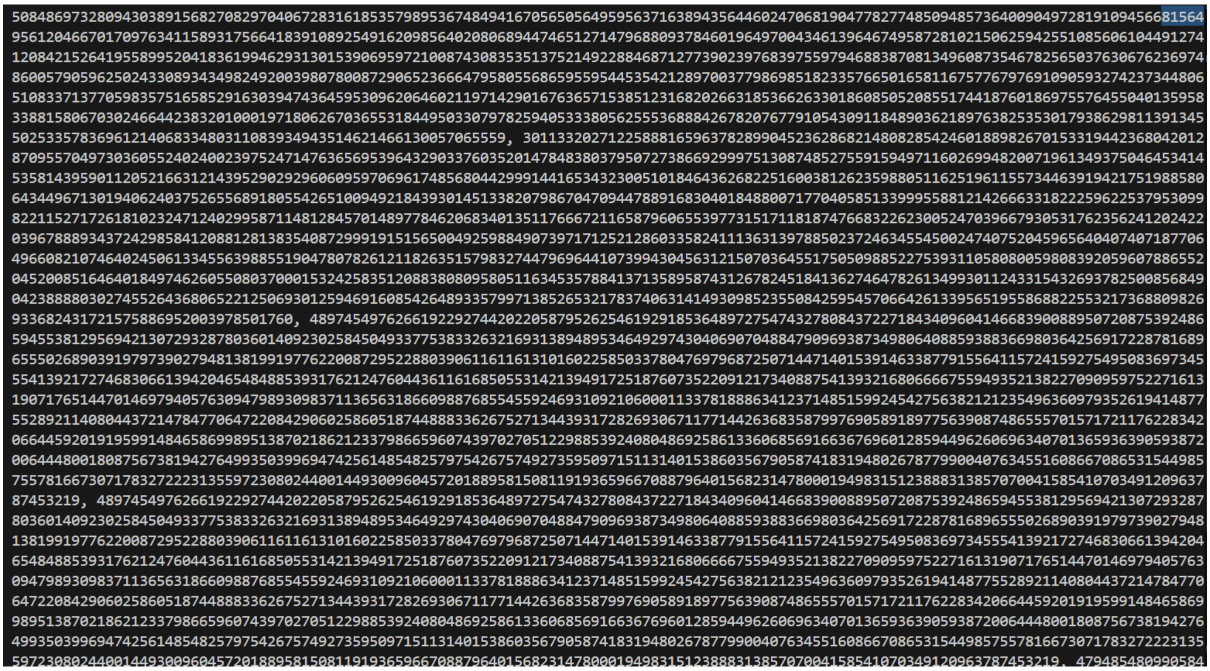
```
Private key: (709535279892813591340587480704620345587503567552261057045491508294867284308870913984181648226008556321125367490066959034254729
02402303167180279354446805404902365589496321191524961856960495947293669048188872068607704814373364522537446574875049649292402385235765431505
04462862250444262628604675160654143842505875364599258576056708797642724824179602383071631253805868512624464931296564247946106161308289261615
48377711854777065999861255267294411385512402593258481038455084453654072266698990178815451300699289878428987823554264242473505138976711926397
44250615406660557165592942282632685784403462915954786868386289763972353179564164931546043230753791916410270067794330620051520048713776639895
57658222703018311180469712938944036515335609510480834946867531259620149616924035718070501372078568438184989879654650708346201186505545733574
82953814628848788088769485631353505708531039465023792593943247471651997546873177432690018175729665168979026951774675888291316699776034556213
11611044950155120669652019004037413163629026975879663393721002169346958488964248854669468810749317246013876376853845022742474556379079945992
444862903732388758906615206328266542184148059936536947023539974409874020362989055462477920583443546803538118988213729053925541, 635748518138
93054557712434592551457395067609585703954544273806003200072523381694320398727471203299885691392216041949491028683028565280125631565389567534
75225297307942851055369089205013604960108034273276571342034490904451075538253860914533972839465658208707926746074318581961101098437212425723
60686802693067960593117965147386782337714050224819828044898789135709213111167196315723220752209947345512933376471619106465087325603000551604
36106305223285863222573776568016163872221142633737050773249166246351651839992747639755738217848366379228989525068364567659434195448332544970
55387122798868724765691123678216421330624616980629340075635476910484184278451903779907835940853340121247215920940451046601093746458252489193
65265543170031392450952125372853896885329302279389468046219926415694706838905143493764338496710771188298655980167047036779744140005677866525
22673746965140243354133950178156290275087101749741765499552190962675518244980054494192905544582654355987308652452963834180271619430440772823
47884856474883580798204436876752206804187788605494756333564244175839618079929477301699987267764154296994594270383032512146153549447806500401
32149200255400455830492544122459305408415381873076213009146841667996350525822348807463498909644398917)
```



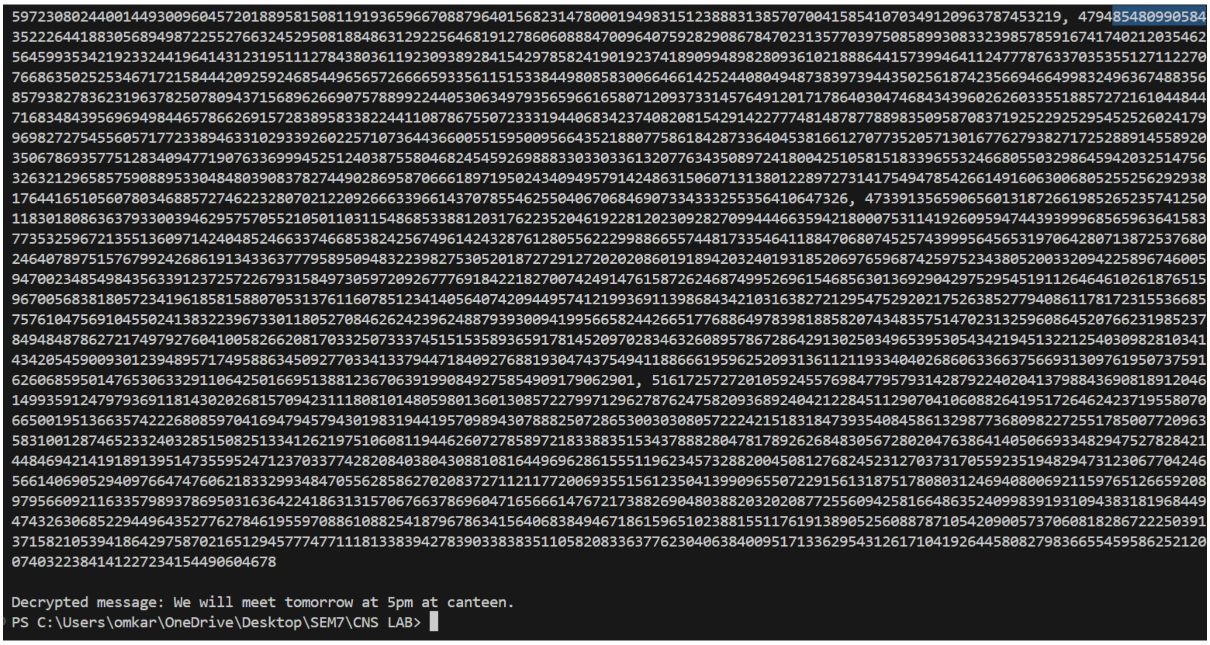
```
Enter a message to encrypt: We will meet tomorrow at 5pm at canteen.
```



```
Encrypted message: [263043275593509816621394098556169435341364062972703482374321195050374725966186553418233131970963684146688033289437919838
52030364512556005579836168888096946815686866939094925859971326508038491923131896499502014863689089349429064743429166410611571254439641160658
04032406895936623578755662847043472324818946603637023546247104499546513149862428240340893150672401300053828205983545295629297571002614902420
97238226406094813117928146471498553357938200180464051677785895010373142891484764245356510494943342338560666997439965837387261378757845748307
18494358190971815438370373179052582613894656632102677610074280552679252800668997344542170011456090718513493911783626413509320754135843103077
80486371257163475586548124194851378051713578212593853735812832341677348106411578430295830527364869496184984216694341781468641137185936242788
41130077130769469933084135107810032800986251887039828286848591818132202715241310808963061006503785123196147568627933215510514989272251930360
31934342887232500607862406440997482264744706938138167453174066135516987560378556091238983127298817582487049217691060861431775263153979933098
8793364636140850778119063456250485457398901958347160019902426208546372604500282393740666390117619194928816394915972497265902794793404, 51617
25727201059245576984779579314287922402041379884369081891204614993591247979369118143020268157094231118081014805980136013085722799712962787624
75820936892404212284511290704106088264195172646242371955807066500195136635742226808597041694794579430198319441957098943078882507286530030308
05722242151831847393540845861329877368098227255178500772096358310012874652332403285150825133412621975106081194462607278589721833883515343788
82804781789262684830567280204763864140506693348294752782842144846942141918913951473559524712370337742820840380430881081644969628615551196234
57328820045081276824523127037317055923519482947312306770424656614069052940976647476062183329934847055628586270208372711211772006935515612350
41399096550722915613187517808031246940800692115976512665920897956609211633579893786950316364224186313157067663786960471656661476721738826904
80388203202087725560942581664863524099839193109438318196844947432630685229449643527762784619559708861088254187967863415640683849467186159651
02388155117619138905256088787105420900573706081828672225039137158210539418642975870216512945777477111813383942783903383835110582083363776230
406384009517133629543126171041926445808279836655459586252120074032238414122723415449060467825823351880628698, 479485480990584352226441883056
89498722552766324529508188486312922564681912786060888470096407592829086784702313577039750858993083323985785916741740212035462564599353421923
32441964143123195111278438036119230938928415429785824190192374189099489828093610218886441573994641124777876337035355127112270766863502525346
71721584442092592468544965657266665933561151533844980858300664661425244080494873839739443502561874235669466499832496367488356857938278362319
63782507809437156896266907578899224405306349793565966165807120937331457649120171786403047468434396026260335518857272161044844716834843956969
49844657866269157283895833822441108786755072333194406834237408208154291422777481487877889835095870837192522925295452526024179969827275455605
71772338946331029339260225710736443660055159500956643521880775861842873364045381661270773520571301677627938271725288914558920350678693577512
83409477190763369994525124038755804682454592698883303303361320776343508972418004251058151833965532466805503298645942032514756326321296585759
08895330484803908378274490286958706661897195024340949579142486315060713138012289727314175494785426614916063006805255256292938176441651056078
03468857274622328070212209266633966143707855462550406706846907334333255356410647326, 5416927917705715342291879897385686859476328402196941597
80333377740916605400827384832241423345418434139780869700593695614840186130598374839571451142155312417387608690186669202970724304142146878971
15314425485370894061290900934055842268496861461843092452844143431526405344817605947955828022993277680209918482845310381288519412622134450322
50848697328094303891568270829704067283161853579895367484941670565056495956371638943564460247068190477827748509485736400904972819109456681564
```



```
50848697328094303891568270829704067283161853579895367484941670565056495956371638943564460247068190477827748509485736400904972819109456681564
95612046670170976341158931756641839108925491620985640208068944746512714796880937846019649700434613964674958728102150625942551085606104491274
12084215264195589952041836199462931301539069597210087430835351375214922884687127739023976839755979468838708134960873546782565037630676236974
86005790596250243308934349824920039807800872906523666479580556865955954453542128970037798698518233576650165811675776797691090593274237344806
51083371377059835751658529163039474364595309620646021197142901676365715385123168202663185366263301860850520855174418760186975576455040135958
33881580670302466442383201000197180626703655318449503307978259405333805625553688842678207677910543091184890362189763825353017938629811391345
5025335783696121406833480311083934943514621466130057065559, 30113320271225888165963782899045236286821480828542460188982670153319442368042012
87095570497303605524024002397524714763656953964329033760352014784838037950727386692999751308748527559159497116026994820071961349375046453414
53581439590112052166312143952902929606095970696174856804429991441653432300510184643626822516003812623598805116251961155734463919421751988580
64344967130194062403752655689180554265100949218439301451338207986704709447889168304018488007177040585133999558812142666331822259622537953099
82211527172618102324712402995871148128457014897784620683401351176667211658796065539773151711818747668322623005247039667930531762356241202422
03967888934372429858412088128138354087299919151565004925988490739717125212860335824111363139788502372463455450024740752045965640407407187706
49660821074640245061334556398855190478078261211826351579832744796964410739943045631215070364551750509885227539311058080059808392059607886552
04520085164640184974626055080370001532425835120883808095805116345357884137135895874312678245184136274647826134993011243315432693782500856849
04238888030274552643680652212506930125946916085426489335799713852653217837406314149309852355084259545706642613395651955868822553217368809826
933682431721575886952003978501760, 489745497626619229274420220587952625461929185364897275474327808437227184340960414668390088950720875392486
59455381295694213072932878036014092302584504933775383326321693138948953464929743040690704884790969387349806408859388366980364256917228781689
65550268903919797390279481381991977622008729522880390611611613101602258503378047697968725071447140153914633877915564115724159275495083697345
55413921727468306613942046548488539317621247604436116168505531421394917251876073522091217340887541393216806666755949352138227090959752271613
19071765144701469794057630947989309837113656318660988768554559246931092106000113378188863412371485159924542756382121235496360979352619414877
55289211408044372147847706472208429060258605187448883362675271344393172826930671177144263683587997690589189775639087486555701571721176228342
06644592019195991484658699895138702186212337986659607439702705122988539240804869258613360685691663676960128594496260696340701365936390593872
00644480018087567381942764993503996947425614854825797542675749273595097151131401538603567905874183194802678779900407634551608667086531544985
75578166730717832722231355972308024400144930096045720188958150811919365966708879640156823147800019498315123888313857070041585410703491209637
87453219, 4897454976266192292744202205879526254619291853648972754743278084372271843409604146683900889507208753924865945538129569421307293287
80360140923025845049337753833263216931389489534649297430406907048847909693873498064088593883669803642569172287816896555026890391979739027948
13819919776220087295228803906116116131016022585033780476979687250714471401539146338779155641157241592754950836973455541392172746830661394204
65484885393176212476044361161685055314213949172518760735220912173408875413932168066667559493521382270909597522716131907176514470146979405763
09479893098371136563186609887685545592469310921060001133781888634123714851599245427563821212354963609793526194148775528921140804437214784770
64722084290602586051874488833626752713443931728269306711771442636835879976905891897756390874865557015717211762283420664459201919599148465869
98951387021862123379866596074397027051229885392408048692586133606856916636769601285944962606963407013659363905938720064448001808756738194276
49935039969474256148548257975426757492735950971511314015386035679058741831948026787799004076345516086670865315449857557816673071783272223135
597230802440014493009604572018895815081191936596670887964015682314780001949831512388831385707004158541070349120963787453219, 479485480990584
```



```
597230802440014493009604572018895815081191936596670887964015682314780001949831512388831385707004158541070349120963787453219, 479485480990584
35222644188305689498722552766324529508188486312922564681912786060888470096407592829086784702313577039750858993083323985785916741740212035462
56459935342192332441964143123195111278438036119230938928415429785824190192374189099489828093610218886441573994641124777876337035355127112270
76686350252534671721584442092592468544965657266665933561151533844980858300664661425244080494873839739443502561874235669466499832496367488356
85793827836231963782507809437156896266907578899224405306349793565966165807120937331457649120171786403047468434396026260335518857272161044844
71683484395696949844657866269157283895833822441108786755072333194406834237408208154291422777481487877889835095870837192522925295452526024179
96982727545560571772338946331029339260225710736443660055159500956643521880775861842873364045381661270773520571301677627938271725288914558920
35067869357751283409477190763369994525124038755804682454592698883303303361320776343508972418004251058151833965532466805503298645942032514756
32632129658575908895330484803908378274490286958706661897195024340949579142486315060713138012289727314175494785426614916063006805255256292938
17644165105607803468857274622328070212209266633966143707855462550406706846907334333255356410647326, 4733913565906560131872661985265235741250
11830180863637933003946295757055210501103115486853388120317622352046192281202309282709944466359421800075311419260959474439399968565963641583
77353259672135513609714240485246633746685382425674961424328761280556222998866557448173354641188470680745257439995645653197064280713872537680
24640789751576799242686191343363777958950948322398275305201872729127202020860191894203240193185206976596874259752343805200332094225896746005
94700234854984356339123725722679315849730597209267776918422182700742491476158726246874995269615468563013692904297529545191126464610261876515
96700568381805723419618581588070531376116078512341405640742094495741219936911398684342103163827212954752920217526385277940861178172315536685
75761047569104550241383223967330118052708462624239624887939300941995665824426651776886497839818858207434835751470231325960864520766231985237
84948487862721749792760410058266208170332507333745151535893659178145209702834632608957867286429130250349653953054342194513221254030982810341
43420545900930123948957174958863450927703341337944718409276881930474375494118866619596252093136112119334040268606336637566931309761950737591
6260685950147653063329110642501669513881236706391990849275854909179062901, 51617257272010592455769847795793142879224020413798843690818912046
14993591247979369118143020268157094231118081014805980136013085722799712962787624758209368924042122845112907041060882641951726462423719558070
66500195136635742226808597041694794579430198319441957098943078882507286530030308057222421518318473935408458613298773680982272551785007720963
58310012874652332403285150825133412621975106081194462607278589721833883515343788828047817892626848305672802047638641405066933482947527828421
44846942141918913951473559524712370337742820840380430881081644969628615551196234573288200450812768245231270373170559235194829473123067704246
56614069052940976647476062183329934847055628586270208372711211772006935515612350413990965507229156131875178080312469408006921159765126659208
97956609211633579893786950316364224186313157067663786960471656661476721738826904803882032020877255609425816648635240998391931094383181968449
47432630685229449643527762784619559708861088254187967863415640683849467186159651023881551176191389052560887871054209005737060818286722250391
37158210539418642975870216512945777477111813383942783903383835110582083363776230406384009517133629543126171041926445808279836655459586252120
0740322384141227234154490604678

Decrypted message: We will meet tomorrow at 5pm at canteen.
PS C:\Users\omkar\OneDrive\Desktop\SEM7\CNS LAB> 
```

Practical Applications of RSA

- **Secure Communication**: Encrypting emails and messages.
- **Digital Signatures:** Verifying the authenticity of a message or document.
- **Key Exchange**: Securely exchanging keys for symmetric encryption algorithms.

RSA is widely used in various security protocols, including SSL/TLS for secure internet communications.

RSA ensures security through the difficulty of factoring large numbers. It is commonly used for securing sensitive data, digital signatures, and in SSL/TLS protocols.