1 [45 Points] The following *cipherText* was constructed using RSA public key. Obtain the English plaintext message using the Chinese Remainder Theorem.

$e = 65537$

$p =$ 7469181024937916359781935619257215213890320520601121720754594442483716371258826591087017882797039
3712943346042198037094659327501111947882748795213050859549466713296250934606644417362993354203461134913
2729498512285514869231727208183265338605340411960790972742728885257977066110281623786504277111054699 74
7668456174867028332364030451993361284089242098108499736626018067145520647791382979567015725736517345 29
7306479248652120085656466600881681678035081582004476300131682223318774988658917112388215733308839256 67
3501016259069353604606540133360794698476384663487179611639958217070406763048499763816256524655278730 65
1091492314170933158314561231004171637119685133858964390153837653827908733987022572957525349989965831 79
4749802811336568467784771900582854306507238819017517071766552772338666361848365082108932880437540006 5
9732233400293574882398932424305229587531606575416301714322656146957677265337724306301590162303692483 66
6592651972266692818751757096729783781031999073866892013399951394514165264109501711761272184025806482 09
5011671635653680943413779839006874988423781196093743374175964832137015652413165268863282344071038282 86
3394844425480147459674891496726790950042204895309203853856530895002485129408715778745357320039080568 10
1120364796859939938519293354295128271906529662631276834008744302913479026316878542848844163598209040 02
0116759735317163393228715170620167292292874311206479708928163196412811174477980713767458059567482537 49
8230121182149988200443703014669816288234001851573923200344847170984565738271780119616382171765503256 47
6644544671368938634392447728160744718335516492436132126757796123696049578028399628866336302033019013 38
5376918311203600842379304976766438732625914489991675309694891355707915795844633512877890515632065538 68
2171125821688958141760785459126800719748642723134513402703435086878557727795890764307011993074559396 19
9092233734561833951564228092639718239603991920539686390940547224458676434267925850404495656547142640 18
7392579457648913839138679403215733590558836021840347776069605841618611651039281714012001433576965268 18
6144553584571143871643745158176175392135412101310685176723808315957748570789800057800329559001274560 89
2241984164584503758916017371076490580229670475173417957189483504391961921078800989970598964830398089 21
0068531688599561443586922402389232457393533781071121579897302122325897025851177431962566609399012004 09
4295813147763334804852329327707215523882343996040392207194190476936200228833265292045370473223193273 47
7675830986726306087447 7
$q =$ 1019368383220082033812320071753804562181490082201026772967927544232545804882102607865081646959397
2776941330406260217328268200567553058616016191391734279589850920767982219986072321623245196459103092 64
8623077369636171766450509433635660127525613378825957576651415718274442564860060642432575972048381421 46
5145111743161121817396948143586170324318029467722472341742986104517344821901147536629930562572310925 42
9466590969218590242017651484086647395628852547770740041675345412647820358565666523763698430112714082 71
5575404461721178593588490523794842719776570861610050590837620508240574849716680031113380685367376759 96
3689587818628366993200282023943400274862748282008260397945994818339371749320990629091192994532516793 27
1700689587347179905422979500661508099856479125390076276155248683153522175961621384007049309344950690 2
2883278545514521881776552276881849656554983507576715472749143218893620236273062068917882219701913523 94
2089490926835557007018200625221842598595087188548714215398481638695147069814555192291088776118291501 74
9938133636691116664226921725147035882723282870624419086145431367816476661740808164679259631104020315 24
6590022721365268452986505451784965727795693334979593209108212626689038681099440532086406343737537632 12
8342739557170883839926840259242330679700473397772092000235274416328363805585270802852633085711861815 60
9346623636513599971930533484337102345790336488827626324440403845045377997304508683672938982009733183 50
6630257232297993382843940936918075444812632848324158282633184529872836460147046431243651310045119164 31
9539659065226294253379161112191423009343499477558847175909318437643442810228887679616654074420641756 09
2728502118617784624463882015954558003601633522689665819511409967015115837071076198187050429747538509 64
9374729551511755686483806077373066296569063895408176378408646498292103678857174395229718686543618414 71
3385305053156151911946499227659204734760188098614573556934551088287072926146729214750439223682362772 38
7597735693385513735636484763276091347561565081002212982704143494945209766787881221107481817355936808 29
8634225512666560487542060013459530813142090379464690688530308500379418651645096333456530617837892181 82
1118264880867101368744211388119726746505297761792938853525145531298870075210859648952097595860810322 321
2466369802643423209455460124755378789903336904831743028033176248804059004742797430212028974576150802 32

582392378077813744626494617853128444314169063119687560470773673998161414803814743349462786003448195478
607193782012031548381701
$cipherText$ = 334389536006277477386291102358666999529020843408514311830770604844772610085717202858094 3
623647582508912425820356660440701053985371828071626793878505493013365321422460599088630807423611873422
950357919905572430749734771324870345392406585303418569506148517694464657726474300003229747552005334813
621749073911844217977711373738919321659314513490154701711853031417928868776265109985608737269307263649
421185857337601720467967257423549583546185492697735217667763774048144478281731903877248981405626267299
819444906801632534161670218913061156845833482639052263694701958654082088718828359489408472315509797845
889626027383418536851829133628117511586828847220442923482574607491346726957600989818068436074513291125
225787927481361442950926992414013322051591816945095728191376443486741413769615143921327348828477046435
947897833432545772357800960358290603671331470838883463363518941204438065725114506673844523618433117657
829936646963673661517409451008885504312182767270613707018094503793014203573026187825426525784509384161
897375738656328622852443048864717384615121960668499254650380739032386240978955021061805404800859078962
637421029022161693433189469018772819287000323800565920095170527445767949990390514137514530457160935957
601736977038858715081527129149827433203728780646736323399212691756936362201856292587906376234823926680
767552957321281351053514567435630487033870926715141019853499185945627272876961195892977250697219526065
531506897750544672153370597674415779666506051351929415673257376083291203337517626875832669460679871864
361620970637539385247733907756089989948317707398299199800278575036251954203979924580935484678680140714
675727256682208574483596354029723730494299398737622030974851515955617480464495803469345399371981945010
842279052771606522104401974370002310652977949840640123461341658663811190455785493035897056937254348731
075110725682132684096479179804297250093868291501754802439469111527262323358425302759534128823515420954
627050457540573700935139843082093609352079522021220460721895985778008465716715352989354380033684958414
738503567391695195975213129975339037876265936606366996539333995512260229118718483664044570618222067980
090011913833340394609684599704808682978439808074624730481694574772953823444914091340757508987451006808
424503553394307371033195125057398502158604646708837212480608464756624169135846625270041572047453251761
013381670876438725681058061472916236896359425797927911894685715375233095105624473332753142073189313089
567069158616853939162157006350568482980358894244620688120703102536528588464950560061224312660281282260
711352953270310833517251963570531581910351625271381405976920776515935110380949533957703701531216831655
373934771975905597961752307848912807482659322301886331339639698106971527830628983179902870938931350209
534060005441709613235135023923080934998048750770035203779759924492786637984426897258677323193581982603
008837618269623888101109890933795010123589894285953322921820818306134536385207980074699716345520913393
484966786310643023880195181589830745481017425874682746620008803235704878721429726195359171764180849187
297381487710978881156202284633080354486015825986406771351106594975349966038490120258742596707481997383
643444173154177417514627021869776542263892518543996849822446416616968010598863521481370886474063020650
429087188401691187476642246129008115048944561971905641715550702708778985005484960986593718082442261716
168304734241436675890606560236734833457469965342582693427939199222281967653432502973398128205180579524
733151702462713274253931733144592549424397535810810946213806610174798444235700796746466574694440185151
120834155781580689631821620192307337467825648002988458126199342934801677264185889336119700596713612503
862139862656817159055289837723439485784699897174139572179487005554865380216003545095194528572175738896
772975325917335743853134407593914348279087272413868730374981267312870487883721322110400018482495136257
638876073329530295078493282429241195344465095493664555205303801510059463446679007666180765773280103323
719547395555982541825934541452430272928626079643780676177480787155817684350741005617659508480909586 56
105324506170591758031745155749876249181625310408930900295019882398162632616406474194758274132487394020
255191487349950251679552101413546298742436187832595139975607836868528236499714743775479330162840692758
906614616125702205338008779442425241684816109503656937391140799577902720122580326603609619044704654533
082590354821502270071231136104115318951123033823867325209536107790411095340050106281160192140397170265
246989092127022755844820103341242570375756217432279845883858085051156710430445258874781527330072631796
709980705245943911165416623080806706612623238211394403563089854594773823389321615692778000893811207904
580755215027523551622001790891622224006692985354076117730833760443266675237664022360711183333809633420
753082704430191403427730245072040606192473850198003473281463852760563490432587492318212807546587806533
308185227923220481931234804722363388381260923649 97

The plaintext is shown below:

> Alan Turing , in full Alan Mathison Turing, (born June 23, 1912, London, England-died June 7, 1954, Wilmslow, Cheshire), British mathematician and logician, who made major contributions to mathematics, cryptanalysis, logic, philosophy, and mathematical biology and also to the new areas later named computer science, cognitive science, artificial intelligence, and artificial life.

2 [45 Points] Digital Signature Algorith (DSA)

2.1 Generate a DSA Key pair such that $p \geq 1024$ bits and $q \geq 160$ bits. Hint: find a prime $q \geq 160$ bits, then find a random number $tmp \geq$ (1024-160) bits and conduct primality testing of $q \cdot tmp + 1$ to find p.

$p =$ 10001853143778494232202384602024313642094805653096823084366069837121916875673318144392481824754571591019914647954148235839918474041737917834153304906130842531340642759985605323885600376783743504011699153274291543243383894693653825201821761398821608472804320233 9
$q =$ 1020075474687528267148368281341911216071243953321

2.2 Identify Public Key parameters

The public key parameters include p and q, shown above. The other public parameters are the generator
$\alpha =$ 70440476158060150391144015467375696885003960565135892705855086799105799975832380893112928918137437429918484483320867314998786798170650386021240447799421970267729080139044688181082082748070329147143610544032074233752112468299815726640604586730154256433204644050
$\beta =$ 28868565430922019260273536154542033165691642253684781128220334958079416225855590879250670937820327158741157629854344645824096075192444762327829721402032415913486090823611412441878261444329952625008602068719970588284018296874802225004304701231907598704800003714

2.3 Generate Signature for MD5-Hash = 120654484320263588514608261628026439285

The signature for the hash above is calculated using the following equation:[1]

1. Choose an ephemeral key $0 < k_e < q$
2. Compute $r \equiv (\alpha^{k_e} \mod p) \mod q$
3. Compute $s \equiv (h(x) + d \cdot r) \cdot k_e^{-1} \mod q$

This gave the following value for s:
$s =$ 23538244294866186141158117962251670271593807 60

2.4 Verify the Digital Signature Generated in 2.3

The signature verification is calculated as follows:

1. Calculate $w \equiv s^{-1} \mod q$
2. Calculate $u_1 \equiv w \cdot H(x) \mod q$
3. Calculate $u_2 \equiv w \cdot r \mod q$
4. Compute $v \equiv (\alpha^{u_1} \cdot \beta^{u_2} \mod p) \mod q$

The signature is accepted if $v \equiv r \mod q$.
$v =$ 84689259942807986803896349113501100163269881 8035
$r =$ 84689259942807986803896349113501100163269881 8035

[1] Private key $d =$ 40219232304995875563757721009517283934859227339 4

3 [10 Points] Determine which of the following are prime numbers:

a. 1798758724805508496502821597814073869874527469062680029407582127634855549890892589223
Composite

b. 1590185219871957542493116114600499667909712644341208146306088343203153786078500704513
Prime

c. 1558300851914478563667041381534759830705314746936787434965724391346205826745658837071
Prime

d. 1114877723960165303086266262246739999351736545842688547890178051251754046778209265277
Composite

e. 1701649747274389836328758796469387963534468348605280671300393693087386178552597581769
Prime

f. 1117051982972964176255977546560314971353934122161907626868626575920914731369490827133
Composite

g. 1611569730562977142991554343582160703829926902359468746732249403748667962099955153711
Composite

h. 1006744242693144138991183226283715627966199890221950842268830665672999172760980350997
Prime

i. 1478334445679686145289703414648978484686846953084162826560705697383514195532048498801
Prime

j. 1551284045384578966055927057771184821750749160366773302510856670260232043818664801937
Prime