Name: Ali Aqeel Zafar

Neptune ID: AAFZDE

Key1:

Weiner Attack:  
p multiply by q is equal to n  
d: 337887397732849885042432719442904467090957623265839363457260197851078514008747054316084864266932128947509064943078622999045604526784729902554400670933673  
p: 128722120298891516680849108211505059970684911348260528052479414328384022122957801434486189807460443685722058827513709747673889238930116914135307935650318831517748716912179316086829620881991741566746407258036285814770215812039169913160740933036972568174490227113227591761773123921996685177815391205082415921353  
q: 170803660617699844386851179371474599914120074391670623284230456231340632216235823594317544657111290128163195498458345559009440054300896480626166775773958533737983722600643663176159640550714443040373686666386121518654700746808579670287028757522251425593880869139343315951714659486171542531688632207952963104791  
message: 12  
RSA Correctness holds

Key3:

Weiner Attack:  
p multiply by q is equal to n  
d: 3283673933017227189356662861009948751731057023614561068589169926421280053886822588048872053844292452859471708815679948895771162933579992353411290305859401  
p: 95122153533143958793575101382023276292294088612808646584559115629973211280738149214016120593922299186514612223346211491263572324852175448915457225508096896362901324234244231924977769204685214503684267913869526354710811942804195997771308503824094090937857949260676491972273802606178562579168486321151594762139  
q: 120944773863804188714015975666717756816301519446824647999863115102065605973878912340045856162474408383121543730374527851500410213142615410104178185658269191089284023710242150649963959085226126429577122756017131077884270991667145752904575367675415498756316235742886894465243502530825987252280113337729269733789  
message: 12  
RSA Correctness holds

Key2:

pollard p-1:  
d: 780587068912554756413173066311130169345596139808870398856262209763469477472629980430738372785956255482859401410817936236542606353197574831027111596363639575300220703628598303712968776789949996771012571470549036787528627813991408807747375673479340026887832283356791239012519443551857107176688062068817978784669607526663726323245423276314584317217315992033034083735236555489957069738582443946071453764078701519927382155185276065138461758134988986245111737667354296398321110291819427964655531232263194549387668093844087509402757959163625489419727046419019319500851929770942328600520014245919612017638891008132810473473  
p: 201802338323822247762976091312398953585365203464182021987954259021442074856059725386336671167057110186239586246391430373219782265224062444199720355929977151162091729083826303862872370046603937645608706305315346136611803579780695403143292373193235079862482776555201550917056154776371200000000000000000000000001  
q: 121061217819736895841873936884083089330870560881680370467822468395190538367714840920450445114510967689554869749779971895880113238102014149285468820060945341075560185498026002399515443707709686559585850444389100313511190304311929000630644099804294564031108902176528627092011505496232835614585976098809592350027  
p multiply by q is equal to n  
message: 12  
RSA Correctness holds

Key 4:

pollard p-1:  
d: 3972964852288108561261876403219585552893047414641819851768320009916410845289927168362187475109880758575817294437589040073251711217079294845309046319170574861404064645467893098094477425267171819956800547314206824144907044802511148556448698865427673322171475605610214780662495841015095488999151188101330692654965842769741486976173591170580693037597326713926402355909472853661447047067211600106745185220449903746204954601509044925082401776004062332239463390182449730237223948593882724785446309101895218929544759576287335865756276829382267488382128228608539999117156398324836674957669821065722748017638891008132810473473  
p: 289808331960851737771759803525087737335855755367096019474685543005145912741210826243913523913735837567991589842550928695116960878879769477359746539719590978358151867193191260774291907964146799773722581429252590602423600156461241891433764242585143412511606610899753360453071807137080934400000000000000000000001  
q: 75881989831787878698795302444385080712072005550233655066040851486716894141246390304315061621635456367692593343879429999810482859770450442899238266385213650364434396147195322667439244566369802803433781209508750613775711707572576311641175510832168423380380974519970597965509109264841945100269715051661053097943  
p multiply by q is equal to n  
message: 12  
RSA Correctness holds