**Disciplina:** Segurança e Auditoria de Sistemas

**Professora:** Janniele Aparecida Soares Araújo

**Equipe:**

Carlos Henrique Pereira Abreu

Igor Gabriel Souza Silva

Guilherme Augusto Rodrigues de Jesus

Mateus Martins Pereira

**Relatório – RSA e ElGamal**

No presente trabalho foram desenvolvidos dois algoritmos de criptografia assimétrica: RSA e ElGamal. A implementação do RSA foi realizada na linguagem Java, com a IDE Eclipse 2021-09. Por outro lado, a implementação do ElGamal foi realizada na linguagem Python.

A máquina utilizada nos testes possui a seguinte configuração:

* Notebook Avell A60 MUV
* Processador Intel Core i7 9750H 2.60GHz
* Memória RAM 16GB DDR4
* Placa de Vídeo GTX1660Ti

Abaixo são apresentadas as saídas dos testes realizados. Foram abrangidas mensagens de 100, 200, 250, 300 e 1000 caracteres.

**RSA**

------------------------- Teste RSA -------------------------

Variáveis

p: 139673744574529896764356509349369494525590672761401073085848363997471414669109620046585656964834235672332700731303062383109767288665223998642786665362912615872987576906953491741716429312336435862473903552842883339254075124959964807751101129738425655100915696957196116252965880882001940762264267186163980782699

q: 161556956860300649111561137654008992958913282852882423427011483835226437649106627589874463056750992373580374866588555413682265456720451492408294301886017528587053892580492066894030945905302512601644561485624389252403773735124767470850825196858979032011689708858490314995024650691111838777831016159114037976659

n: 22565265126743978373554147850678602670963245925896766473753780050335406952539311803133567218416361380380496717622903919925991220539100912284430744640320326133428845842624243230340468024089827863025894285476690971640644188738062136462147301608001130333073059668234055514889002326140227049387389893420296903235552596009349492229599576138240942020862951760601098594049739244514364412221130113049280447384881071449355521211314655664937949990230053178980947083716144450632010061370748953962150586907041611263028325652915277692937049925337479531899553685237765439211215747570766136358557241033081342676844281384953113022641

z: 22565265126743978373554147850678602670963245925896766473753780050335406952539311803133567218416361380380496717622903919925991220539100912284430744640320326133428845842624243230340468024089827863025894285476690971640644188738062136462147301608001130333073059668234055514889002326140227049387389893420296903235251365307914661683723658491237563533378447804986815097536879396681666559902913865412820327363295843403442445613423037868145917244844377687929866116467214306171968591883303395326403211689402662798909860614448005101279201065252747253297627358640360752098610341755079705110566709459967563136748998039675094263284

e: 11191132097991312017201236737796490244187350334368604702715194040578445551994749855104925512888131495445958518922644258015025263026198921542962422096340767

d: 7670651407086811436236186066660041663755779904234274311199697568951032185392642637758528218602398471688068102645262255770111769416465323423765215979708624506663804550709774658996368672367702523872395080900777441449781605380170790703391768206509090628075431896164524033914512685779259863105307074675570509250038740050406511845008793372574516058977015001168865788555419220171832218058781457891789629688920371154043908789703175438134067576117437200176171057590035522409226323773885475489596820740347243534805926477174016669687897463461099360013936614973708556305247799297099225329297875575700048240018556274517246255467

----------

Tamanho da mensagem: 100 caracteres

Mensagem descriptada com sucesso? true

----------

Tempo para gerar a mensagem: 1ms

Tempo para criar a chave: 345ms

Tempo de encriptar: 3ms

Tempo de decriptar: 9ms

Tempo de execução geral: 358ms

------------------------- Teste RSA -------------------------

Variáveis

p: 138333274800824457949119539597774954513525425943442844278618678336482435882768502734791925106227488431730046801892361909834237268461558911740596999105164196949606118330748312414242737197085223753688125654223544109085847213713546868906507138026689447823262556256054211542458923517412746847063998723783722230051

q: 153732649458207977505880232110890315462567318447950689104346832914766360404131204277156435944824843119851314203470319040930488153824468855588843076328583832952287382489189059838584384037265687435761505289902186034604342663873142487158458654833706968796907173634432916673419439435500126495239735633158967894061

n: 21266340843361101372758176013914622493694900933926837057817031904552712021511109669022827171530731248057923297061564667145916588585838984345115853603932857138484444647921209424115746273243213235444610528160571786937403191437452076501297595858847475298691532467557795627895586908074065767566778314936035052773366665425302072466995082523374559993994558628172266849056976042914166956745675394777077526975919865896142922162731216479214035730333194161874354549727751311697189002720256355341209814431166563620127904783254748728110652151617578832309776062437614039969683353512828721912770553306554623171938063825998038627111

z: 21266340843361101372758176013914622493694900933926837057817031904552712021511109669022827171530731248057923297061564667145916588585838984345115853603932857138484444647921209424115746273243213235444610528160571786937403191437452076501297595858847475298691532467557795627895586908074065767566778314936035052773074599501043040031540082751665894724018465883780873315674010531662918160458775687765129165924867534344561561157368535528449310308047166394544914474294003281795295501900318983088382693196815652430678273839129018584420462274030889476244810269577217623349513623622341593696892190353641749829634329469055348503000

e: 12710832226192620665975981368750000448685417183935310434576222128876109872395740366400174095084282133545113051353787007503401306433207838471714456245799213

d: 9342973475932510217169578693638774155909430635433192421558680232811338241446548738494796963203960089261685001929532026795182646124083196139913517034049440342666794155756054586726162643343849087810437752875715124074345604178401519641931400117250655333064076803572324877365214981181804645389178139599669168676091143971802563169757963357321206878886112009052238061522141983140267006008192749320331712217710808610835186233092227843588161841551508571607001738388911181139776192959862379381256662591821670053797682636627908641970757823397131381062196930450929710099773297610045382279653156874840328368517954893910871577277

----------

Tamanho da mensagem: 200 caracteres

Mensagem descriptada com sucesso? true

----------

Tempo para gerar a mensagem: 0ms

Tempo para criar a chave: 67ms

Tempo de encriptar: 3ms

Tempo de decriptar: 8ms

Tempo de execução geral: 78ms

------------------------- Teste RSA -------------------------

Variáveis

p: 101760059734340420259675056089435742677121488829295762210044080997520542916009345065580127596093653666160831093450169660818513276562880164330440056573186814850083812860766142691545637214693438413177560740265562918811397567358107841703244308500261468183956902148524467140431570575096305081291957976993733891471

q: 94793045252888281657811396696350385257176562497445576328288322844456604406665391045551686313698701650033396969573112142333573840742345278037278560875336356791377619704463622694969133178991527694873764035393521991869346887429274077425337232089814624998364750575195987762502634576231684291328662045830180855377

n: 9646145947333946150607881847300722723281567870106968050964948283369062287240413334194256574137949101738602306534549942263146089921211750673440297454529218867041107207688707136777282953188728026499686599558796878772087229595102059193875561972235022279235325737718334308933576172224529098805078518601769991043108522611449547124124160172497569329185626301431957709032215545701818890139172070415855264433763589227102855136576580285363048643796351638288975251355874968434138578038724457160107968532019257485436415870225964204112122013054131067054982448328485956362236165522428155930244166696062308629463407185509664789567

z: 9646145947333946150607881847300722723281567870106968050964948283369062287240413334194256574137949101738602306534549942263146089921211750673440297454529218867041107207688707136777282953188728026499686599558796878772087229595102059193875561972235022279235325737718334308933576172224529098805078518601769991042911969506462318422206673719711783201251328250105216370493883141859841742816497334304723450523971233910908627073553298482210961526491126195921256633907351796792677145473494691773593198138334291377385091094566879293431377558266749147926400907738409863179914512798707701027309961544734319256842787162685750042720

e: 8678081272663320725078464716241487457645194899126522262721517598239350565314214191732412952049776135695098965444450715256255752203059422670916388728711767

d: 894695601403137083515884352500250054045521257283228564189264877872329583533955720979921121089784489358328386473505043349719236949651199038776184702771970801304613558740384799900373066707820507699253094975104662588619088026377754116394138753068763124526608040542144402087520968445540831772208101034205617897243833652475058717723708567648036401753016021110569958905107284280975743906662295952323691929945527442817512613935160224653425249651947710986743249954614752125676567593743110854373896675545079063044193553865449876896780742931081489536795252469981333965663867031420049880839568380586900359046993381366128472423

----------

Tamanho da mensagem: 250 caracteres

Mensagem descriptada com sucesso? true

----------

Tempo para gerar a mensagem: 0ms

Tempo para criar a chave: 157ms

Tempo de encriptar: 3ms

Tempo de decriptar: 7ms

Tempo de execução geral: 167ms

------------------------- Teste RSA -------------------------

Variáveis

p: 153611513686133728987549925352007201222419807016710648187553188040627142614570378888992970078966983154292129466274580493691363351934042181201805042331646845403961582995424929585351288636755688546931875323574766672992555006406474918941989039629174305693335250245137619035456856164205858985878422124015772732277

q: 173647428182949288638848814159054344985653380005211625473128455784778461502903403369699043524030266141485635702535249837141971870039564832208664895255783638831891414148211092699205576063523924573293274772808097039070720391840917137225075904247043675643171436940463531588505675472387850387075526764813959175761

n: 26674244290887038458352043109589144538050942668983995759575845099200206357546602777597064413770363737855864028933644391946005017967493659443885412034934399717117835174756828002645507186688276251406562545393266386860018751285427639132463905619677581816631283068319822699684038654070516052111302436632012825137261038288102685255876659619417003734850510171336987984485050672804776004774308660147897500548844338863702530626595579343188818954414160967942185429474834817154178151453384455065290026477830285040036431773883658094689597890658697911128235029164400654079209777347156270000833029787195651246425458155685840737797

z: 26674244290887038458352043109589144538050942668983995759575845099200206357546602777597064413770363737855864028933644391946005017967493659443885412034934399717117835174756828002645507186688276251406562545393266386860018751285427639132463905619677581816631283068319822699684038654070516052111302436632012825136933779346233602238250260879905942188642436984315065710824369028979370400656834877889205486945847089567924765457785749012355483732440553954531715491887404332918325154309748432780733161777550671919811281677500794382626322492411305854961170085288182672742703090161555119376870498150601941873471509266856108829760

e: 10411905449633037108149759179295128255603099047999673665069133880867750282136081532872171425109768886340918951321548252425220379862896833794450108416367869

d: 12163743185547781588497156067123132490600495778623590642044876235098397794926210828277336978265869093323936813434065111357754268282636331607148596482725890869962427921556462456497177351638800999413624761957464553957599942432960637339038407856293747854161065901411055857668461743373975890729610749892264566301596185926117013144087681553382433376438244934044450127445681718256057431431605781013217193484951312159422424134485083432447978171777791694431305214403718095365620712877449399870843301386351313128342427129378644334484208145409047514484244218454225321636719333951843437146192738289528284307558505652640472422869

----------

Tamanho da mensagem: 300 caracteres

Mensagem descriptada com sucesso? false

----------

Tempo para gerar a mensagem: 0ms

Tempo para criar a chave: 242ms

Tempo de encriptar: 2ms

Tempo de decriptar: 8ms

Tempo de execução geral: 252ms

------------------------- Teste RSA -------------------------

Variáveis

p: 134798207410535104580003770511574354624594847953844699900086789046301297821868657920991523732608939268183642801963009700733320595307338919250188675221107779571080362138893701144723936183993184099316631753595963086314621946827973153005767169958614790426507873023737686719900476692513369949165532986551920273969

q: 122498040756956087095318096076847337976176920609177459296875002787570484437691723851151909528000829535877947818994054545461268363011886055570863039623630815275714122497634356701096470548685714091514085155203556642408843053137826227926964962336353433763829481790180908414836703943384736788471467666492099787587

n: 16512516305340349291187248904237268240652142978255026377578797964371636956849556701033793617263717992025559525238333056104436243531305331468812171458865211211340864401730720529797603652052512914659506470101506814074932121903162088333537657706487025643926849885219150532531232721584759147533314440228989430877451728556721927530440193744622575802834842406833855339424272834093864189005548391369430464515922806672223143534434478871766894704471423415247684334643143982132806310250577770578043499569687231843491716204342403264535923046832527403320582682314100070464012902946858934065021711163464081542086680721103745422803

z: 16512516305340349291187248904237268240652142978255026377578797964371636956849556701033793617263717992025559525238333056104436243531305331468812171458865211211340864401730720529797603652052512914659506470101506814074932121903162088333537657706487025643926849885219150532531232721584759147533314440228989430877194432308554436338764871878034154110234070638270833180227311042259992406745988009597287031255313037868161552913477414625572305746152198440426632619798405387286011825614049712732223092837008333652660999295542883535812458046866728022387850550019131846273675548132940338930284530527565974804449680068059725361248

e: 8475743814941738544130768912977752709124599711810442011122103793096805995360844277398220016505799907361993803104888027112678642497250163152330897766222611

d: 10699403210121963864017406119665313856814903954175938182241233701539966982542935462122001014524257929341699302915360466951953225946673372366977887931968479365654556842693826663467285046303467106182582295562550753932628569816819134411282886941619216531236859107499741464512620626085574990765467579758819584366988911411629957488737937420577290978294608747838931850622918551118151747652587334394004647719216889882787763732732233751810273134981700636004688824949569746654966404519355783388925984586911101156625964958719912329856654885385686809682617407742270204399559879735240327790843281506990430017768264499957088017339

----------

Tamanho da mensagem: 1000 caracteres

Mensagem descriptada com sucesso? false

----------

Tempo para gerar a mensagem: 1ms

Tempo para criar a chave: 89ms

Tempo de encriptar: 2ms

Tempo de decriptar: 8ms

Tempo de execução geral: 100ms

--------------------------------------------------

Testes falhos: 2

Tempo de execução total: 961ms

**ElGamal**

------------------------- Teste ElGamal -------------------------

Variáveis

p: 131835938162651538543274704420330499270508446530163675494047736221286104878260119678652481945093862601751850639053726380933678927143353617451378464246682544607077563615420990648941564411566803077754680675460674727526956176155330857634441088117576391459344601349664704208434093708250455742861959201634588186767

g: 83477085214525340288435971541423978141855151687087349762693060556561676039828597227392551964899036810150931054014033623921148046404064219156785991164746930853469952834700462412724657143501249858638970387875645711296484976779413567727881153869441136115938562761937773117444661821279860281956884698705854274720

b: 49948679885607620904288263321127111828472578725154155928916041741459860262971600387400126232863771393226177517728180152786648103326850574435707577004730421758997209768827239422097923775489187522591653881399058217601088034363015517596938427046657835058066983135325629167875141201667549724929411550568656410663

chaveB: 61975610787123902048048353976724543055949847567191959468481404952041211810027376465617539988895228024523618714302250748726379967750057935589093232133665445976952119889738129974392696370454657282428767436153536541196032907232437394416131652611532102333494990928925202855423465859823207335010698087637020164348

a: 124760805505994407081810740941954499074134688733439799260015904726718983201776362725371898820235218902693986412338548279190106716237534616172700061313559020933492465408989249887693536915142509862299927271117364580503292222419772070772000400061376782905829252015711839588498030988455591418125315233918351704455

chaveA: 90207777299370328635715213473032187818738932694765618618332445311065013250193386218307258412369553543638544460426971316041367335111223740100641999146344143225061520157153859922048650205228328416165760506363345141287610306919110727160393940611417397720985972402250896905881483736123241329713669444086914938661

----------

Tamanho da mensagem: 100 caracteres

Mensagem descriptada com sucesso? True

----------

Tempo para gerar a mensagem: 0 ms

Tempo para criar as chaves: 127 ms

Tempo para encriptar: 348 ms

Tempo para descriptar: 344 ms

Tempo de execução geral: 819 ms

------------------------- Teste ElGamal -------------------------

Variáveis

p: 137319209167352179018481338023966991133530483455764921711358408742308116226546118272678984454586983049218275061700042160680591597799870564806980636460919207741341264866754071531727686270864750178041384193886518723351183138198111632069330163043423213258471408206008481578205898658864509541821733676808032161673

g: 119969313329602637363520490493947100399094222718723373043318914127390309194584420529390329395848021873237639390270154582936220312800629725630826357317260127972147330383412817826132274718846344855932589821834847902626352672396312077249418267828828265618103045145260698192007107338518918624016176509388358055201

b: 82740678899252664212192197771600232596079891233817539628268890978545027273510916362448825257975557070454331792121839858476042654751862804396651826776594508517925111683327283747859304250730425876317545405170348052661558954608109720820189057717086416425295933907741040408529933017336857205487310099867484503854

chaveB: 83154190519078744583847722371830969798755865473341150624524133106493882166277589864434145001636906442215508182430154846299596691591546757145946767855971733782051518229784340673255974688054243029363444688463975691057417505002207472117152293718806941119658856570764848801264108417000059513261573124830750139866

a: 25760913608521739174295770953419648330256436752661653319389352823544008495583552486006791127379326577021095146787213118047467878640424888671792118785624237125173847727187812323935065416694218489690806606451377696162785907733815441231162979289988248721293177635926030401207741590267177024736160492771355968282

chaveA: 124545310560956191158978858060196188700250136893744260583418515256846458859617745091376273561902947049768983023279694889908666964032087476533874801620911689101590188316842738606376407170850065310668438415319522330816015175101628667928153928986131704015116326031377000645656320948740451644035238802450870688392

----------

Tamanho da mensagem: 200 caracteres

Mensagem descriptada com sucesso? True

----------

Tempo para gerar a mensagem: 0 ms

Tempo para criar as chaves: 552 ms

Tempo para encriptar: 703 ms

Tempo para descriptar: 699 ms

Tempo de execução geral: 1954 ms

------------------------- Teste ElGamal -------------------------

Variáveis

p: 146752805664674426587773706489441500649556933501356722542835664635908565591892220835919139852035553443359757624807371953290777729891371651256700053553153014645106319982073899079217572668575793811258795785487752340646069978716975316311861042860879733407765339315496914830450770792099966934926208807419589681179

g: 69867900124864826107425370068507900974247053775215343639721333254620303922263791704955600040476852179371585566303437806620705381179625916250051209186208870393520206755894296354009489777091621167238420275335062980178680156975881265610130208528343193351161377086042503627412896131552485732137602120918979181255

b: 170446021749295109147339130549173974434568336604946133118731708181705016415908738541054700766837176093765070034518528860167931719704798364459755987007416225714812860572852309912718344390865423233923837873576755642819950235801946608921813294723845203400962436726555526154246867010557547529793786941256535914740

chaveB: 111516316714839044391429944517263171696031020915561451842570104653153283182566470982720686056443721979323066535697242941506349331991229837468371829905735507777914266918565420646267750831155214918562112384539153214303189755578292890961055787807431288379315349338094847750251241264198463939399396824370926157697

a: 134991961296565181917737409798534234652101075057585116840560361398426969887093780252514679205397981227465640383759542733273424465013975064944956024180533502087652372980050306465678067975030029469322277591988563610192729575811039889634603249128140781770106128152573843352063687632552778672294495451200882554934

chaveA: 85747113187713792957384190749228366254743840436672003850464183273842675661406298396017934622653281129853270933485650980000343134407150605359022722873176238969656092585763048931656177581898083057140876767359526356185085059798661274990718682300191992137290877044711689712806206954381698106217077419848826753826

----------

Tamanho da mensagem: 250 caracteres

Mensagem descriptada com sucesso? True

----------

Tempo para gerar a mensagem: 0 ms

Tempo para criar as chaves: 79 ms

Tempo para encriptar: 908 ms

Tempo para descriptar: 898 ms

Tempo de execução geral: 1885 ms

------------------------- Teste ElGamal -------------------------

Variáveis

p: 170619309500430672013643606657954436393285113549266013067774292196673755242536104658611421414089588679582898399889838502404289351246698242181919438846033225760316568977509711404166785656762416400045398078036150874231633693946580632047351221675816573128295331033874236039095878312975050625957465331984421310811

g: 52969476656434108245849385743768932197254643474166313911088111483310995973956117412866432634371799419894594191486712681428995075644365573928749350656251424180376212819362907512158070461164972267872883683184457249508782414832537317658160585244999200960127208160808250410084194965117199789533884147814815812827

b: 8461180780172098743005456763685414371088059970066943755600913101006555321121812722612562661282265828945761226472401176815257702862765484673490115840843532012800066195139347434151648086281769959990433535022870103555877437490744864105845173927173978477931477208602872516338965460931693080038457591715379998223

chaveB: 31603953815626593017806416071582660257873320498383325811340181270545759254197405154807913702410724995519976573441120584425959146727547591567547362815304014155314381526255116679157692805974710260058198165090183052462970520290596154898986274131186995441373998680484168236059825599334177922542128279319541255164

a: 111666053537027936926486502262974174224117450837291944104179466481659649625288288733171748904878486551052975553903617680151969173485294813735298855937061704270488886601219135362403463384629557692600958101534699987997281592128369339415965394230174148176105972962618810535354398411702126645875333405813597061131

chaveA: 3064298193683758648968759198010243575271403967013957711087821808446816710410465145868134730694501562969361933125293687278052207557234446166763312511295093099986541941556458850983980206966772081739133767533022477735285833188574441428390234007449996738327701190767642426800217090804780995969488148289262807638

----------

Tamanho da mensagem: 300 caracteres

Mensagem descriptada com sucesso? True

----------

Tempo para gerar a mensagem: 1 ms

Tempo para criar as chaves: 1110 ms

Tempo para encriptar: 1086 ms

Tempo para descriptar: 1079 ms

Tempo de execução geral: 3276 ms

------------------------- Teste ElGamal -------------------------

Variáveis

p: 153372057541792115820991937971105729897080525884422588876855426638631211687249077692735056389170235218460050382592906298031605196118415071464578025144321968544751873497688640866798962569437572769825923613569664341261485313671900492434167721564225086359586324418561031872095649825165304505528942908276803698259

g: 29332139767936804706850522750268525513876088783986772145445461002843865993236982102591926117928112932666232855915306060206249325204756065543188196477377440441162374059064140623904844474027292024261468732415833215605796527748142066030797720878318776750964348080456383862371356921428862860936206950170781640419

b: 4099661133160659558121614144302884606351215587841421163197724962872192590451576886648252660724654868746649858445682369815240302528737371739453387749570827600868242081673128614489910644097191283846458284298381892531086765137980258644715839135236707618718498409141487216123668459585988039071261800797615364765

chaveB: 31880987176780159514682806072829752282930349916584480369374800291515933144464114200497636967704142934016063586000753587079370240644603281369602390664210500269612290531380323708484821162506534269001947825842800635696198409768175514765702459458851912763815764403779484773249594191835549707987059574577310999614

a: 140714899792838743800310793123954594814438991055834855346229140700902910484099813768922320843435450698736673562416587226607633131868362616965423735759053732335260602873684602621062633482453652050010006560251779427247179628180188065101173369259326783256898873191046243897932152173936598734267297462325504081659

chaveA: 72385798609217254056093958731970811942232143756918347087737117878716401178551691399242156394628077662289577887138874792176936694074766164105695683124754778529433241160580052143261527593412769536134271865940399551009731919452471109703795177420535753113432848350582494986490384136286983841611765999266420684742

----------

Tamanho da mensagem: 1000 caracteres

Mensagem descriptada com sucesso? True

----------

Tempo para gerar a mensagem: 0 ms

Tempo para criar as chaves: 275 ms

Tempo para encriptar: 3656 ms

Tempo para descriptar: 3682 ms

Tempo de execução geral: 7613 ms

--------------------------------------------------

Testes falhos: 0

Tempo de execução total: 15561 ms

De acordo com os testes realizados, percebemos que o RSA possui um tempo de encriptação e decriptação menor do que o ElGamal, ou seja, o RSA é mais eficaz que o ElGamal para encriptar e decriptar. Sobre o tempo de criação de chaves, há variação de qual é mais rápido, ou seja, não há um algoritmo que seja o mais rápido em todas as ocasiões.

A implementação do RSA que desenvolvemos só consegue encriptar e decriptar corretamente mensagens menores (até 256 dígitos) e para esses casos, o RSA é, no geral, mais eficaz que o ElGamal. No entanto, para mensagens maiores (mais do que 256 dígitos) apenas nossa implementação do ElGamal consegue encriptar e decriptar as mensagens corretamente. Essa limitação é particular da nossa implementação, mas tendo em vista nosso caso, podemos dizer que tivemos dificuldade com o RSA para lidar com mensagens maiores.