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:
225652651267439783735541478506786026709632459258967664737537800503354069525393118031335672184163613803804967176229039199259912205391009122844307446403203261334288458426242432303404680240898278630258942854766909716406441887380621364621473016080011303330730596682340555148890023261402270493873898934202969032355525960093494922295995761382409420208629517606010985940497392445143644122211301130492804473848810714493555212113146556649379499902300531789809470837161444506320100613707489539621505869070416112630283256529152776929370499253374795318995536852377654392112157475707661363585572410330813426768442813849531130226419
z:
225652651267439783735541478506786026709632459258967664737537800503354069525393118031335672184163613803804967176229039199259912205391009122844307446403203261334288458426242432303404680240898278630258942854766909716406441887380621364621473016080011303330730596682340555148890023261402270493873898934202969032355136530791466168372365849123756353337844780498681509753687939668166655990291386541282032736329584340344244561342303786814591724484437768792986611646721430617196859188330339532640321168940266279890986061444800510127920106525274725329762735864036075209861034175507970511056670945996756313674899803967509426328
e:
111911320979913120172012367377964902441873503343686047027151940405784455519947498551049255128881314954459585189226442580150252630261989215429624220963407667
d:
767065140708681143623618606666004166375577990423427431119969756895103218539264263775852821860239847168806810264526225577011176941646532342376521597970862450666380455070977465899636867236770252387239508090077744144978160538017079070339176820650909062807543189616452403391451268577925986310530707467557050925003874005040651184500879337257451605897701500116886578555419220171832218058781457891789629688920371154043908789703175438134067576117437200176171057590035522409226323773885475489596820740347243534805926477174016669687897463461099360013936614973708556305247799297099225329297875575700048240018556274517246255467
----------
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:
138333274800824457949119539597774954513525425943442844278618678336482435882768502734791925106227488431730046801892361909834237268461558911740596999105164196949606118330748312414242737197085223753688125654223544109085847213713546868906507138026689447823262556256056421154245892351741274684706399872378372223005
1
q:
153732649458207977505880232110890315462567318447950689104346832914766360404131204277156435944824843119851314203470319040930488153824468855588843076328583832952287382489189059838584384037265687435761505289902186034604342663873142487158458654833706968796907173634432916673419439435500126495239735633158967894061
n:
212663408433611013727581760139146224936949009339268370578170319045527120215111096690228271715307312480579232970615646671459165885858389843451158536039328571384844446479212094241157462732432132354446105281605717869374031914374520765012975958588474752986915324675577956278955869080740657675667783149360350527733666654253020724669950825233745599939945586281722668490569760429141669567456753947770775269759198658961429221627312164792140357303331941618743545497277513116971890027202563553412098144311665636201279047832547487281106521516175788323097760624376140399696833535128287219127705533065546231719380638259980386271111
z:
212663408433611013727581760139146224936949009339268370578170319045527120215111096690228271715307312480579232970615646671459165885858389843451158536039328571384844446479212094241157462732432132354446105281605717869374031914374520765012975958588474752986915324675577956278955869080740657675667783149360350527733745995010430400315400827516658947240184658837808733156740105316629181604587756877651291659248675343445615611573685355284493103080471663945449144742940032817952955019003189830883826931968156524306782738391290185844204622740308894762448102695772176233495136236223415936968921903536417498296343294690553485030000
e:
127108322261926206659759813687500004486854171839353104345762221288761098723957403664001740950842821335451130513537870075034013064332078384717144562457992133
d:
934297347593251021716957869363877415590943063543319242155868023281133824144654873849479696320396008926168500192953202679518264612408319613991351703404944034266679415575605458672616264334384908781043775287571512407434560417840151964193140011725065533306407680357232487736521498118180464538917813959966916867609114397180256316975796335732120687888611200905223806152214198314026700600819274932033171221771080861083518623309222784358816184155150857160700173838891118113977619295986237938125666259182167005379768263662790864197075782339713138106219693045092971009977329761004538227965315687484032836851795489391087157727710
----------
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:
947930452528882816578113966963503852571765624974455763282883228444566044066653910455516863136987016500333969695731121423335738407423452780372785608753363567913776197044636226949691331789915276948737640353935219918693468874292740774253372320898146249983647505751959877625026345762316842913286620458301808553771
n:
964614594733394615060788184730072272328156787010696805096494828336906228724041333419425657413794910173860230653454994226314608992121175067344029745452921886704110720768870713677728295318872802649968659955879687877208722959510205919387556197223502227923532573771833430893357617222452909880507851860176999104310852261144954712412416017249756932918562630143195770903221554570181889013917207041585526443376358922710285513657658028536304864379635163828897525135587496843413857803872445716010796853201925748543641587022596420411212201305413106705498244832848595636223616552242815593024416669606230862946340718550966478956
z:
964614594733394615060788184730072272328156787010696805096494828336906228724041333419425657413794910173860230653454994226314608992121175067344029745452921886704110720768870713677728295318872802649968659955879687877208722959510205919387556197223502227923532573771833430893357617222452909880507851860176999104291196950646231842220667371971178320125132825010521637049388314185984174281649733430472345052397123391090862707355329848221096152649112619592125663390735179679267714547349469177359319813833429137738509109456687929343137755826674914792640090773840986317991451279870770102730996154473431925684278716268575004272 0e:
867808127266332072507846471624148745764519489912652226272151759823935056531421419173241295204977613569509896544445071525625575220305942267091638872871176 7d:
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:
173647428182949288638848814159054344985653380005211625473128455784778461502903403369690435240302661414856357025352498371419718700395648322086648952557836388318914141482110926992055760635239245732932747728080970390707203918401971372250759042470436756431714369404635315885056754723878503870755267648139591757761
n:
266742442908870384583520431095891445380509426689839957595758450992002063575466027775970644137703637378558640289336443919460050179674936594438854120349343997171178351747568280026455071866882762514065625453932663868600187512854276391324639056196775818166312830683198226996840386540705160521113024366320128251372610382881026852558766596194170037348505101713369879844850506728047760047743086601478975005488443388637025306265955793431888189544141609679421854294748348171541781514533844550652900264778302850400364317738836580946895978906586979111282350291644006540792097773471562700008330297871956512464254581556858407377977
z:
266742442908870384583520431095891445380509426689839957595758450992002063575466027775970644137703637378558640289336443919460050179674936594438854120349343997171178351747568280026455071866882762514065625453932663868600187512854276391324639056196775818166312830683198226996840386540705160521113024366320128251369337793462336022382502608799059421886424369843150657108243690289793704006568348778892054869458470895679247654577857490123554837324405539545317154918874043329183251543097484327807331617775506719198112816775007943826263224924113058549611700852881826727427030901615551193768704981506019418734715092668561088297609
e:
104119054496330371081497591792951282556030990479996736650691338808677502821360815328721714251097688863409189513215482524252203798628968337944501084163678669
d:
121637431855477815884971560671231324906004957786235906420448762350983977949262108282773369782658690933239368134340651113577542682826336331607148596482725890869962427921556462456497177351638800999413624761957464553957599942432960637339038407856293747854161065901411055857668461743373975890729610749892264566301596185926117013144087681553382433376438244934044450127445681718256057431431605781013217193484951312159422424134485083432447978171777791694431305214403718095365620712877449399870843301386351313128342427129378644334484208145409047514484244218454225321636719333951843437146192738289528284307558505652640472422869
----------
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:
13479820741053510458000377051157435462459484795384469990008678904630129782186
86579209915237326089392681836428019630097007333205953073389192501886752211077
79571080362138893701144723936183993184099316631753595963086314621946827973153
00576716995861479042650787302373768671990047669251336994916553298655192027396
9
q:
12249804075695608709531809607684733797617692060917745929687500278757048443769
17238511519095280008295358779478189940545454612683630118860555708630396236308
15275714122497634356701096470548685714091514085155203556642408843053137826227
92696496233635343376382948179018090841483670394338473678847146766649209978758
7
n:
16512516305340349291187248904237268240652142978255026377578797964371636956849
55670103379361726371799202555952523833305610443624353130533146881217145886521
12113408644017307205297976036520525129146595064701015068140749321219031620883
33537657706487025643926849885219150532531232721584759147533314440228989430877
45172855672192753044019374462257580283484240683385533942427283409386418900554
83913694304645159228066722231435344344788717668947044714234152476843346431439
82132806310250577770578043499569687231843491716204342403264535923046832527403
32058268231410007046401290294685893406502171116346408154208668072110374542280
3
z:
16512516305340349291187248904237268240652142978255026377578797964371636956849
55670103379361726371799202555952523833305610443624353130533146881217145886521
12113408644017307205297976036520525129146595064701015068140749321219031620883
33537657706487025643926849885219150532531232721584759147533314440228989430877
19443230855443633876487187803415411023407063827083318022731104225999240674598
80095972870312553130378681615529134774146255723057461521984404266326197984053
87286011825614049712732223092837008333652660999295542883535812458046866728022
38785055001913184627367554813294033893028453052756597480444968006805972536124
8
e:
84757438149417385441307689129777527091245997118104420111221037930968059953608
44277398220016505799907361993803104888027112678642497250163152330897766222611
d:
10699403210121963864017406119665313856814903954175938182241233701539966982542
93546212200101452425792934169930291536046695195322594667337236697788793196847
93656545568426938266634672850463034671061825822955625507539326285698168191344
11282886941619216531236859107499741464512620626085574990765467579758819584366
98891141162995748873793742057729097829460874783893185062291855111815174765258
73343940046477192168898827877637327322337518102731349817006360046888249495697
46654966404519355783388925984586911101156625964958719912329856654885385686809
68261740774227020439955987973524032779084328150699043001776826449995708801733
9
----------
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:
834770852145253402884359715414239781418551516870873497626930605565616760398285972273925519648990368101509310540140336239211480464040642191567859911647469308534699528347004624127246571435012498586389703878756457112964849767794135677278811538694411361159385627619377731174446618212798602819568846987058542747204b:
499486798856076209042882633211271118284725787251541559289160417414598602629716003874001262328637713932261775177281801527866481033268505744357075770047304217589972097688272394220979237754891875225916538813990582176010880343630155175969384270466578350580669831353256291678751412016675497249294115505686564106634chaveB:
619756107871239020480483539767245430559498475671919594684814049520412118100273764656175399888952280245236187143022507487263799677500579355890932321336654459769521198897381299743926963704546572824287674361535365411960329072324373944161316526115321023334949909289252028554234658598232073350106980876370201643484a:
124760805505994407081810740941954499074134688733439799260015904726718983201776362725371898820235218902693986412338548279190106716237534616172700061313559020933492465408989249887693536915142509862299927271117364580503292222419772070772000400061376782905829252015711839588498030988455591418125315233918351704455chaveA:
902077772993703286357152134730321878187389326947656186183324453110650132501933862183072584123695535436385444604269713160413673351112237401006419991463441432250615201571538599220486502052283284161657605063633451412876103069191107271603939406114173977209859724022508969058814837361232413297136694440869149386614----------
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:
137319209167352179018481338023966991133530483455764921711358408742308116226546
118272678984454586983049218275061700042160680591597799870564806980636460919207
774134126486675407153172768627086475017804138419388651872335118313819811163206
933016304342321325847140820600848157820589865886450954182173367680803216167
3
g:
119969313329602637363520490493947100399094222718723373043318914127390309194584
420529390329395848021873237639390270154582936220312800629725630826357317260127
979721473303834128178261322747188463448559325898218348479026263526723963120772
494182678288282656181030451452606981920071073385189186240161765093883580552012
1
b:
827406788992526642121921977716002325960798912338175396282688909785450272735109
163624488252579755570704543317921218398584760426547518628043966518267765945085
179251116833272837478593042507304258763175454051703480526615589546081097208201
890577170864164252959339077410404085299330173368572054873100998674845038541
chaveB:
831541905190787445838477223718309697987558654733411506245241331064938821662775
898644341450016369064422155081824301548462995966915915467571459467678559717337
820515182297843406732559746880542430293634446884639756910574175050022074721171
522937188069411196588565707648488012641084170000595132615731248307501398661
a:
257609136085217391742957709534196483302564367526616533193893528235440084955835
524860067911273793265770210951467872131180474678786404248886717921187856242371
251738477271878123239350654166942184896908066064513776961627859077338154412311
629792899882487212931776359260304012077415902671770247361604927713559682821
chaveA:
124545310560956191158978858060196188700250136893744260583418515256846458859617
745091376273561902947049768983023279694889908666964032087476533874801620911689
101590188316842738606376407170850065310668438415319522330816015175101628667928
153928986131704015116326031377000645656320948740451644035238802450870688392
----------
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:
698679001248648261074253700685079009742470537752153436397213332546203039222637917049556000404768521793715855663034378066207053811796259162500512091862088703935202067558942963540094897770916211672384202753350629801786801569758812656101302085283431933511613770860425036274128961315524857321376021209189791812559
b:
170446021749295109147339130549173974434568336604946133118731708181705016415908738541054700766837176093765070034518528860167931719704798364459755987007416225714812860572852309912718344390865423233923837873576755642819950235801946608921813294723845203400962436726555526154246867010557547529793786941256535914740
chaveB:
111516316714839044391429944517263171696031020915561451842570104653153283182566470982720686056443721979323066535697242941506349331991229837468371829905735507777914266918565420646267750831155214918562112384539153214303189755578292890961055787807431288379315349338094847750251241264198463939399396824370926157697
a:
134991961296565181917737409798534234652101075057585116840560361398426969887093780252514679205397981227465640383759542733273424465013975064944956024180533502087652372980050306465678067975030029469322277591988563610192729575811039889634603249128140781770106128152573843352063687632552778672294495451200882554934
chaveA:
857471131877137929573841907492283662547438404366720038504641832738426756614062983960179346226532811298532709334856509800003431344071506053590227228731762389696560925857630489316561775818980830571408767673595263561850850597986612749907186823001919921372908770447116897128062069543816981062170774198488267538260
----------
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:
529694766564341082458493857437689321972546434741663139110881114833109959739561174128664326343717994198945941914867126814289950756443655739287493506562514241803762128193629075121580704611649722678728836831844572495087824148325373176581605852449992009601272081608082504100841949651171997895338841478148158128276
b:
846118078017209874300545676368541437108805997006694375560091310100655532112181272261256266128226582894576122647240117681525770286276548467349011584084353201280006619513934743415164808628176995999043353502287010355587743749074486410584517392717397847793147720860287251633896546093169308003845759171537999822 3
chaveB:
316039538156265930178064160715826602578733204983833258113401812705457592541974051548079137024107249955199765734411205844259591467275475915675473628153040141553143815262551166791576928059747102600581981650901830524629705202905961548989862741311869954413739986804841682360598255993341779225421282793195412551646
a:
111666053537027936926486502262974174224117450837291944104179466481659649625288288733171748904878486551052975553903617680151969173485294813735298855937061704270488886601219135362403463384629557692600958101534699987997281592128369339415965394230174148176105972962618810535354398411702126645875333405813597061131
chaveA:
306429819368375864896875919801024357527140396701395771108782180844681671041046514586813473069450156296936193312529368727805220755723444616676331251129509309998654194155645885098398020696677208173913376753302247773528583318857444142839023400744999673832770119076764242680021709080478099596948814828926280763 8
----------
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:
293321397679368047068505227502685255138760887839867721454454610028438659932369821025919261179281129326662328559153060602062493252047560655431881964773774404411623740590641406239048444740272920242614687324158332156057965277481420660307977208783187767509643480804563838623713569214288628609362069501707816404199
b:
409966113316065955812161414430288460635121558784142116319772496287219259045157688664825266072465486874664985844568236981524030252873737173945338774957082760086824208167312861448991064409719128384645828429838189253108676513798025864471583913523670761871849840914148721612366845958598803907126180079761536476 5
chaveB:
318809871767801595146828060728297522829303499165844803693748002915159331444641142004976369677041429340160635860007535870793702406446032813696023906642105002696122905313803237084848211625065342690019478258428006356961984097681755147657024594588519127638157644037794847732495941918355497079870595745773109996144
a:
140714899792838743800310793123954594814438991055834855346229140700902910484099813768922320843435450698736673562416587226607633131868362616965423735759053732335260602873684602621062633482453652050010006560251779427247179628180188065101173369259326783256898873191046243897932152173936598734267297462325504081659
chaveA:
723857986092172540560939587319708119422321437569183470877371178787164011785516913992421563946280776622895778871388747921769366940747661641056956831247547785294332411605800521432615275934127695361342718659403995510097319194524711097037951774205357531134328483505824949864903841362869838416117659992664206847424----------
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.