Criptografia com RSA

A implementação do trabalho prático dois demandou uma pequena revisão da implementação do primeiro trabalho. Inclui novamente o código do primeiro TP na forma da biblioteca Primos.java, cujos métodos são usados no arquivo da classe principal Crypt.java.

Os métodos específicos do segundo TP estão na classe RSA.java, nela estão inclusos os métodos para cálculo dos números E, D, do fi de N, e os algoritmos de codificação e decodificação. Os métodos estão claramente comentados no código, portanto vou abreviar a descrição.

O programa roda primeiramente as mesmas etapas do TP1, gerando duas chaves privadas e uma pública, porém não tenta quebrar a chave pública dessa vez. Em seguida, são geradas as chaves de codificação (E) e decodificação (D), e todos esses números são impressos pra saída.

O próximo passo é a leitura e quebra do texto. Para fazê-lo, o programa conta a quantidade de caracteres do texto e faz uma estimativa, baseada na codificação do Unicode UTF-8, assumindo 3 como a constante CHARMAX - representando a quantidade máxima de dígitos que cada caractere pode possuir, que pode ser alterada. A estimativa de 3 baseia-se no fato de que estamos usando apenas caracteres ASCII nos textos de teste, portanto são apenas 256 caracteres possíveis. Para usar textos de outros idiomas, basta aumentar o valor de CHARMAX.

O programa então calcula o tamanho do bloco como o nímero máximo de dígitos que vários caracteres agrupados podem formar, tendo esse número que ser menor que a quantidade de dígitos da chave pública. Os blocos são divididos e encriptados usando a chave de decodificação E. São impressos organizados numa tabela todos os blocos gerados pela codificação, bem como o texto codificado gerado.

Para rodar o programa, existe um script chamado rodatp.sh, que rodará em qualquer estação Linux com o shell BASH instalado, basicamente o que ele faz é limpar as saídas, compilar o programa e executar três testes, com os textos enviados junto com o trabalho. As saídas possuem a mesma númeração de cada teste:

- texto0.txt -> saida0
- texto1.txt -> saida1
- texto2.txt -> saida2

O primeiro texto trata-se de uma sequencia de caracteres digitados aleatoreamente. O segundo de um bloco de Lorem Ipsum gerado no site www.lipsum.org, e o terceiro um capítulo, em inglês, do livro “Assim Falou Zaratustra”, de Friederich Nietszche.

O programa também pode ser compilado e rodado “na mão”, bastando para isso compilar os módulos na ordem: Primos.java, RSA.java, Crypt.java, e rodá-lo com o comando:

java Crypt arquivo_de_entrada

A saída será impressa na saída padrão.

Nos arquivos de saída estão incluídos também os tempos de execução, gerados com o auxílio do comando 'time', do Linux.

Teste 2

Texto

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Nunc convallis faucibus velit. Morbi risus. Duis eu neque at dolor pellentesque ultrices. Sed tempus suscipit quam. Duis in lacus. Donec quis nulla. Cras commodo, metus sed vulputate lobortis, enim elit luctus metus, a scelerisque risus lectus sit amet enim. Phasellus vestibulum elit eget eros. Nullam aliquam venenatis est. Quisque et leo. Cras laoreet. Praesent et elit id nulla rhoncus condimentum.

Morbi suscipit lectus nec dui. In aliquet. Pellentesque adipiscing ligula vel urna. Ut lectus. Praesent porta felis cursus augue. Aliquam erat volutpat. Praesent suscipit. Praesent dignissim cursus leo. Donec arcu augue, sodales eu, cursus at, luctus sed, augue. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Pellentesque at risus ut sem consectetuer varius. Praesent accumsan erat id augue. Phasellus mi est, elementum quis, porta ut, porttitor non, sapien. Quisque posuere. Maecenas adipiscing, erat quis iaculis porttitor, neque mi consequat metus, et egestas nisi leo sed nulla. Nulla venenatis. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Mauris lacus. In iaculis adipiscing nisl.

Quisque rhoncus porttitor eros. Proin tortor magna, tincidunt id, porta non, cursus blandit, nulla. Maecenas gravida. Proin massa odio, varius vitae, ultricies a, porta ut, risus. Nam lobortis tortor ut libero. Praesent nisl orci, scelerisque eu, laoreet et, porttitor quis, quam. Pellentesque nisi leo, imperdiet sed, ornare et, aliquam sed, justo. Nullam fringilla urna sed diam. Pellentesque eu turpis. Morbi tincidunt congue enim. Quisque volutpat libero ut arcu. Duis ultricies sem in sem. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Maecenas dictum mollis tellus. Praesent libero dolor, rutrum a, consequat at, dapibus eget, quam. Curabitur in enim eu leo ullamcorper pellentesque. Phasellus metus.

Vivamus non nisi. Etiam neque. Praesent varius mollis sapien. Sed blandit convallis massa. Cras quis metus ac ipsum vehicula adipiscing. Pellentesque sagittis feugiat nibh. Mauris volutpat ante vitae erat. Suspendisse eleifend consectetuer nisl. Suspendisse ut nunc. Quisque interdum.

Chaves

Chave Privada = 12553
Chave Privada = 7643807
Chave Publica = 95952709271
Numero E = 3
Numero D = 53346009660

Blocos

```
:    76111114::    10110932::   105112115::    11710932::   100111108:
:    11111432::   115105116::     3297109::    10111644::     3299111:
:   110115101::    99116101::   116117101::     1143297::   100105112:
:    10511599::   105110103::    32101108::    10511646::     3278117:
:     1109932::    99111110::    11897108::   108105115::     3210297:
:    11799105::    98117115::    32118101::   108105116::      463277:
:    11111498::    10532114::   105115117::     1154632::    68117105:
:    11532101::    11732110::   101113117::     1013297::    11632100:
:   111108111::    11432112::   101108108::   101110116::   101115113:
:    11710132::   117108116::    11410599::    10111546::     3283101:
:    10032116::   101109112::    11711532::   115117115::    99105112:
:    10511632::    11311797::     1094632::    68117105::    11532105:
:    11032108::     9799117::     1154632::    68111110::     1019932:
:   113117105::    11532110::   117108108::      974632::     6711497:
:     1153299::   111109109::   111100111::     4432109::   101116117:
:    11532115::    10110032::   118117108::   112117116::    97116101:
:    32108111::    98111114::   116105115::     4432101::   110105109:
:    32101108::    10511632::    10811799::   116117115::    32109101:
:   116117115::      443297::     3211599::   101108101::   114105115:
:   113117101::    32114105::   115117115::    32108101::    99116117:
:    11532115::    10511632::    97109101::    11632101::   110105109:
:      463280::    10497115::   101108108::    11711532::   118101115:
:    11610598::   117108117::    10932101::   108105116::    32101103:
:    10111632::   101114111::     1154632::    78117108::    10897109:
:     3297108::   105113117::     9710932::   118101110::    10111097:
:   116105115::    32101115::     1164632::    81117105::   115113117:
:    10132101::    11632108::    10111146::     3267114::     9711532:
:    10897111::   114101101::     1164632::     8011497::   101115101:
:    11011632::    10111632::   101108105::    11632105::    10032110:
:   117108108::     9732114::   104111110::    99117115::     3299111:
:   110100105::   109101110::   116117109::      461010::    77111114:
:     9810532::   115117115::    99105112::    10511632::    10810199:
:   116117115::    32110101::     9932100::    11710546::     3273110:
:     3297108::   105113117::    10111646::     3280101::   108108101:
:   110116101::   115113117::     1013297::   100105112::    10511599:
:   105110103::    32108105::   103117108::     9732118::    10110832:
:   117114110::      974632::     8511632::    10810199::   116117115:
:      463280::    11497101::   115101110::    11632112::   111114116:
:     9732102::   101108105::     1153299::   117114115::    11711532:
:    97117103::    11710146::     3265108::   105113117::     9710932:
:    10111497::    11632118::   111108117::    11611297::     1164632:
:     8011497::   101115101::    11011632::   115117115::    99105112:
:    10511646::     3280114::    97101115::   101110116::    32100105:
:   103110105::   115115105::     1093299::   117114115::    11711532:
:   108101111::      463268::   111110101::      993297::    11499117:
:     3297117::   103117101::     4432115::    11110097::   108101115:
:    32101117::      443299::   117114115::    11711532::     9711644:
:    32108117::    99116117::    11532115::    10110044::     3297117:
:   103117101::      463280::   101108108::   101110116::   101115113:
:    11710132::     1049798::    10511697::    11011632::   109111114:
:     9810532::   116114105::   115116105::   113117101::    32115101:
:    11010199::   116117115::    32101116::    32110101::   116117115:
:    32101116::     3210997::   108101115::    11797100::     9732102:
```

```
:    97109101::     1153297::     9932116::   117114112::    10511532:
:   101103101::    11511697::     1154632::    80101108::   108101110:
:   116101115::   113117101::     3297116::    32114105::   115117115:
:    32117116::    32115101::     1093299::   111110115::    10199116:
:   101116117::    10111432::    11897114::   105117115::      463280:
:    11497101::   115101110::     1163297::     9999117::    10911597:
:    11032101::    11497116::    32105100::     3297117::   103117101:
:      463280::    10497115::   101108108::    11711532::    10910532:
:   101115116::     4432101::   108101109::   101110116::    11710932:
:   113117105::     1154432::   112111114::     1169732::    11711644:
:    32112111::   114116116::   105116111::    11432110::    11111044:
:     3211597::   112105101::     1104632::    81117105::   115113117:
:    10132112::   111115117::   101114101::      463277::     9710199:
:    10111097::     1153297::   100105112::    10511599::   105110103:
:     4432101::    11497116::    32113117::    10511532::     1059799:
:   117108105::    11532112::   111114116::   116105116::    11111444:
:    32110101::   113117101::    32109105::     3299111::   110115101:
:    11311797::    11632109::   101116117::     1154432::    10111632:
:   101103101::    11511697::    11532110::   105115105::    32108101:
:    11132115::    10110032::   110117108::     1089746::     3278117:
:    10810897::    32118101::   110101110::    97116105::     1154632:
:    76111114::    10110932::   105112115::    11710932::   100111108:
:    11111432::   115105116::     3297109::    10111644::     3299111:
:   110115101::    99116101::   116117101::     1143297::   100105112:
:    10511599::   105110103::    32101108::    10511646::      327797:
:   117114105::    11532108::     9799117::     1154632::     7311032:
:     1059799::   117108105::     1153297::   100105112::    10511599:
:   105110103::    32110105::    11510846::      101081::   117105115:
:   113117101::    32114104::    11111099::    11711532::   112111114:
:   116116105::   116111114::    32101114::    11111546::     3280114:
:   111105110::    32116111::   114116111::    11432109::    97103110:
:      974432::   116105110::    99105100::   117110116::    32105100:
:     4432112::   111114116::     9732110::    11111044::     3299117:
:   114115117::     1153298::    10897110::   100105116::     4432110:
:   117108108::      974632::     7797101::    99101110::     9711532:
:    10311497::   118105100::      974632::    80114111::    10511032:
:    10997115::     1159732::   111100105::     1114432::    11897114:
:   105117115::    32118105::    11697101::     4432117::   108116114:
:    10599105::    10111532::      974432::   112111114::     1169732:
:    11711644::    32114105::   115117115::      463278::     9710932:
:    10811198::   111114116::    10511532::   116111114::   116111114:
:    32117116::    32108105::    98101114::     1114632::     8011497:
:   101115101::    11011632::   110105115::    10832111::    11499105:
:     4432115::    99101108::   101114105::   115113117::    10132101:
:     1174432::    10897111::   114101101::    11632101::     1164432:
:   112111114::   116116105::   116111114::    32113117::    10511544:
:    32113117::     9710946::     3280101::   108108101::   110116101:
:   115113117::    10132110::   105115105::    32108101::     1114432:
:   105109112::   101114100::   105101116::    32115101::     1004432:
:   111114110::    97114101::    32101116::      443297::   108105113:
:    11797109::    32115101::     1004432::   106117115::    11611146:
:     3278117::    10810897::    10932102::   114105110::   103105108:
:     1089732::   117114110::     9732115::    10110032::    10010597:
:     1094632::    80101108::   108101110::   116101115::   113117101:
:    32101117::    32116117::   114112105::     1154632::    77111114:
```

```
:     9810532::   116105110::    99105100::   117110116::     3299111:
:   110103117::    10132101::   110105109::      463281::   117105115:
:   113117101::    32118111::   108117116::    11297116::    32108105:
:    98101114::    11132117::     1163297::    11499117::      463268:
:   117105115::    32117108::   116114105::    99105101::    11532115:
:    10110932::    10511032::   115101109::      463267::    11710932:
:    11511199::   105105115::     3211097::   116111113::    11710132:
:   112101110::    97116105::    98117115::    32101116::     3210997:
:   103110105::    11532100::    10511532::    11297114::   116117114:
:   105101110::    11632109::   111110116::    10111544::     3211097:
:    11599101::   116117114::    32114105::    10010599::   117108117:
:    11532109::    11711546::      327797::    10199101::    11097115:
:    32100105::    99116117::    10932109::   111108108::    10511532:
:   116101108::   108117115::      463280::    11497101::   115101110:
:    11632108::    10598101::    11411132::   100111108::    11111444:
:    32114117::   116114117::     1093297::      443299::   111110115:
:   101113117::     9711632::     9711644::     3210097::    11210598:
:    11711532::   101103101::     1164432::    11311797::     1094632:
:    67117114::     9798105::   116117114::    32105110::    32101110:
:    10510932::    10111732::   108101111::    32117108::    10897109:
:    99111114::   112101114::    32112101::   108108101::   110116101:
:   115113117::     1014632::     8010497::   115101108::   108117115:
:    32109101::   116117115::      461010::    86105118::    97109117:
:    11532110::    11111032::   110105115::     1054632::    69116105:
:     9710932::   110101113::    11710146::     3280114::    97101115:
:   101110116::     3211897::   114105117::    11532109::   111108108:
:    10511532::    11597112::   105101110::      463283::    10110032:
:     9810897::   110100105::     1163299::   111110118::    97108108:
:    10511532::    10997115::     1159746::     3267114::     9711532:
:   113117105::    11532109::   101116117::     1153297::     9932105:
:   112115117::    10932118::   101104105::    99117108::      973297:
:   100105112::    10511599::   105110103::      463280::   101108108:
:   101110116::   101115113::    11710132::    11597103::   105116116:
:    10511532::   102101117::    10310597::    11632110::    10598104:
:      463277::    97117114::    10511532::   118111108::   117116112:
:     9711632::    97110116::    10132118::    10511697::    10132101:
:    11497116::      463283::   117115112::   101110100::   105115115:
:    10132101::   108101105::   102101110::     1003299::   111110115:
:    10199116::   101116117::    10111432::   110105115::     1084632:
:    83117115::   112101110::   100105115::    11510132::    11711632:
:   110117110::      994632::    81117105::   115113117::    10132105:
:   110116101::   114100117::     1094610:
```

Texto Codificado

```
289356150921378768985739721606024508584360108154676063144725252298675609168837381961064915543359536084868692064567465077395924490727961257906930896431934954195121348538283805967216402017634714489723200374397400673164771827408235054155595139869973467931752407904401772753495423040852740479045042944005741941930368223533020519127861199478136202689425887243428986066800583452112692956841616488697951787316017765188986152557709548362792691315089205327748263034085460981004628896111549970621317679276472594807444499235743788585234496557643930173614665742801433636253127463834438023758534880156442880771138469668014491859107177407040640805211269295671496284921547331509553854090923460668005834299492805003312297286289526422175722141420655408446096108661006582924500357029670593723126453512191953177288345 1
```

36681095328310553644676359991732862343548294491297253556770344361952405312022177
07997674633514036610223693154837847907377208845376347144897469668014451735486805
56388905843771933258655638890584324280131406873939048332399004048512758043475892
99767597858493595078534880156463110328544812298380224467635999146966801447183261
07925001127613737720884531589058355948404552856546098100468344380237523910481164
14572391401271029261769283348132619303682235755741968441540513076852731737734606
68005834678462367129289801056584967380472175850054937797829303322274735488276863
36463661022369366328209701569866987818148471363942290254489488868168723785629012
04329373420535636827788077143963011707672187002364167569866987819479927917311899
59459958320876275154051307681043210010379049984346653366449205540844609625194248
44663715201887171772323286084868692049946980700812531188486332857495093899171648
63277386518364650695853488015644288077113846966801443591794032056388905843728421
07018299585277399433669354267759051686849673804721758500549348071602602446444226
88396365157216653784786042290254489152557709549541951213485382838059672164020143
64312183828932595586343349829391399551530330419292573108661006587727401608235917
94032056388905843158905835592906431262928505287387563816135262677010469733777410
95104321001032967059372364210383218344380237577010822002587346715298570484300317
58500549377978293033775630004079450361510886317611379676549979556986698781947992
79173118995945995832087627585348801564428807711382320037439748550031848472711413
09288961115495957632690263866733278764964298892809197967864210383218344380237573
65216300616392673424969987479119468245343461588167768130233738414499314470445050
67306536002176833203046932351491587012519263209806421038321834438023757761854479
73735771736812298380224467635999146099413191813023373841449931447015890583559546
09810046288961115499706213176792764725942503607976778631127186583208762756117043
53501836465069555413789232619394016938929976759780525479534335763156925638890584
31083724037372842107018563889058431083724037358973729565320304693234524204488133
77741095718326107913167802390588959327954741042671270379114641118164357790163672
51606680058345554472439426808597042311523982138929976759792291845807858493595078
53488015642912203756280525479534280919796785148436483655725114813283105536931526
91153931638049195052628717315890583559290643126292850528738758652619665946557900
17281178878989312632517182337629663173608006081302337384144993144701589058355948
40455285654609810046834438023754658685272346796584988154837847904690058444428896
11154950858436010895264221760014365219433664408576838854373595838449020201571613
95463600480626633818116413949680928813285882090721103002743566148432954708054981
48471363942290254489127907883022374261520834505783378330205191252051059045827686
33646131678023909541951213485382838059672164020115483784790823376296631046743330
11270379114645434237758455070588595199581449826770104697417695803442928580385272
84210701889299767597607109169916084868692064567465077918591071773826281388832831
05536600143652191540513076841118164357790163672515722141420681442528887631103285
44727051355357328623435430660658457935420288364006731647783313523296944005741945
21988858525824066212260668005834289356150921378768985739721606024508584360108154
67606314472525229867560916883738196106491554335953608486869206456746507739592449
07279612579069308964319349541951213485382838059672164020176347144897232003743974
12242197067198466332562723784554385409092346066800583434591909053454342377584550
70588591316780239095419512134853828380596721640201593684959769036651243242821630
66889698194228929976759737883582870328481019908344380237543366440857803945837884
72658424502605907644893757732535485500318488396399761214105093303950493706542478
21894277725303868846433046727212629006688732193193923858204732173608006092677561
81226770104697169877968978813285882040173685520182091689216939209279861474852313
56571195165609570486725540844609610866100658276248831494836118419578807714396552
86531138812775449731086610065829515587232136799283277455488929045118409114180336
35564797065567893163804919505262871739908636537917116793257649150725658403282584
39190647542867674334094643304672743366440857683885437359583844902085849359507853
48801564714639223057797829303341440434572267701046971270379114647265842450472658
42450291220375624364312183814085337288522271622219479927917311899594599583208762

```
751167182660631732718759208200836944505067306594903836149208757507542290254489488
886816872776932375523011707672187002364167250011276135509190246143366440857803948
583788472658424501046743330120661478257104674333014016799766344644422688396365158
721665378478604229025448971144410194814425288876311032854479706556786503494807693
359157893775966166058805254795348351313617543671209752195726391261083724037324288
013140658595751306764080492798052547953483513136175675493180304379111781640067316
647783313523296500885545061195823095469569583706166924387173041929257351380020348
673286234354674528928174070406408055544724394268085970423115239821389299767597514
915870123444783622448205088383606680058346327738651836465069521262900668873219319
193923858204732608486869208618132976148886816872737720884538406079297489698194228
929976759732881052978666155992416624569758743643121838140853372887920081929458626
526196654615881677661639267342896981942294680208733554137892328383501476446763599
991137876898571367992832791846163139894579025705085843601010130421353379415813447
833607303885526869097792764725949253487554458240662122404790450421083724037358917
737295656386673327887500971386127037911462002174081539811642459253740509233826287
138882234295865111320499478336073038634817387673981164245985849359507425779708627
710292617659938003053806028645412242197067685553162186534948701595763269028122983
380224056878805184427468644127037911464146531062767233459861158905835592906431267
292850528738737856290153674790131146340229781546760631292858038524799117110918117
872316527420741775192632098051484364836177651889868733365838777618544797138934137
189803655101668344380237541118164357550919024619185910717740704064080400168277067
771498624173981164245930847401516588140287586359289776070977201772736521630094680
020873392898010565282274570615471524559132837020820396365157216653784786042290254
448933886719426273724209635992493627467233459861771933258655638890584393899171647
897133069514352017246857221414206397651245821167182660767311111717612068981077977
829303335799737875873467152948550031848472711413092889611154969207854768754420088
834599380030538442746864412703791146123248869792537405092328504132326732862343541
853535542649946980700222457524566201283764627386989936127037911467455488929018743
670262320535636827788077143968952642217599380030533283105536131678023904312991727
732263678097946759289595123974538048355747434987371591008954195121348538283805967
216402011589058355954609810046288961115499706213176792764725943424335077328568716
932127037911461442332206777314874277621685752969872024709330205191281788985943127
037911461556397300218438917127873336583878755380265531094365488786311271864888
681687282337629663285041323267091078260409451821933227445854488868168723780189126
166045310887745079226645148436483655725114813283105536931526911531167182660347660
876164507015359192534875544893705056965317011523469483093935902663783311972703201
181484713639422902544892618691782766537847860159874326852485768041 6
```

Tempos

3.07 user, 0.06 system, 3.15 real