An Example of the RSA Algorithm

```
P  = 61    <- first prime number (destroy this after computing E and D)
Q  = 53    <- second prime number (destroy this after computing E and D)
PQ = 3233  <- modulus (give this to others)
E  = 17    <- public exponent (give this to others)
D  = 2753  <- private exponent (keep this secret!)

Your public key is (E,PQ).
Your private key is D.

The encryption function is:

        encrypt(T) = (T^E) mod PQ
                   = (T^17) mod 3233

The decryption function is:

        decrypt(C) = (C^D) mod PQ
                   = (C^2753) mod 3233

To encrypt the plaintext value 123, do this:

        encrypt(123) = (123^17) mod 3233
                     = 337587917446653715596592958817679803 mod 3233
                     = 855

To decrypt the ciphertext value 855, do this:

        decrypt(855) = (855^2753) mod 3233
                     = 123

One way to compute the value of 855^2753 mod 3233 is like this:

2753 = 101011000001 base 2, therefore

        2753 = 1 + 2^6 + 2^7 + 2^9 + 2^11
             = 1 + 64  + 128 + 512 + 2048

Consider this table of powers of 855:

        855^1 = 855 (mod 3233)
        855^2 = 367 (mod 3233)
        855^4 = 367^2 (mod 3233) = 2136 (mod 3233)
        855^8 = 2136^2 (mod 3233) = 733 (mod 3233)
        855^16 = 733^2 (mod 3233) = 611 (mod 3233)
        855^32 = 611^2 (mod 3233) = 1526 (mod 3233)
```

```
        855^64 = 1526^2 (mod 3233) = 916 (mod 3233)
        855^128 = 916^2 (mod 3233) = 1709 (mod 3233)
        855^256 = 1709^2 (mod 3233) = 1282 (mod 3233)
        855^512 = 1282^2 (mod 3233) = 1160 (mod 3233)
        855^1024 = 1160^2 (mod 3233) = 672 (mod 3233)
        855^2048 = 672^2 (mod 3233) = 2197 (mod 3233)

Given the above, we know this:

        855^2753 (mod 3233)
        = 855^(1 + 64  + 128 + 512 + 2048) (mod 3233)
        = 855^1 * 855^64 * 855^128 * 855^512 * 855^2048 (mod 3233)
        = 855 * 916 * 1709 * 1160 * 2197 (mod 3233)
        = 794 * 1709 * 1160 * 2197 (mod 3233)
        = 2319 * 1160 * 2197 (mod 3233)
        = 184 * 2197 (mod 3233)
        = 123 (mod 3233)
        = 123

If you have a computer program (such as the "bc" utility that comes with Linux),
you can compute 855^2753 mod 3233 directly, like this:

        855^2753 mod 3233
        = 50432888958416068734422899127394466631453878360035509315554967564501
          05562861208255997874424542811005438349865428933638493024645144150785
          17209179665478263530709963803538732650089668607477182974582295034295
          04079035818459409563779385865989368838083602840132509768620766977396
          67533250542826093475735137988063256482639334453092594385562429233017
          51977190016924916912809150596019178760171349725439279215696701789902
          13430714646897127961027718137839458696772898693423652403116932170892
          69617643726521315665833158712459759803042503144006837883246101784830
          71758547454725206968892599589254436670143220546954317400228550092386
          36942444855973333063051607385302863219302913503745471946757776713579
          54965202919790505781532871558392070303159585937493663283548602090830
          63550704455658896319318011934122017826923344101330116480696334024075
          04695258866987658669006224024102088466507530263953870526631933584734
          81094876156227126037327597360375237388364148088948438096157757045380
          08107946980066734877795883758289985132793070353355127509043994817897
          90548993381217329458535447413268056981087263348285463816885048824346
          58897839333466254454006619645218766694795528023088412465948239275105
          77049113329025684306505229256142730389832089007051511055250618994171
          23177795157979429711795475296301837843862913977877661298207389072796
          76720235011399271581964273076407418989190486860748124549315795374377
          12441601438765069145868196402276027766869530903951314968319097324505
          45234594477256587887692693353918692354818518542420923064996406822184
          49011913571088542442852112077371223831105455431265307394075927890822
          60604317113339575226603445164525976316184277459043201913452893299321
          61307440532227470572894812143586831978415597276496357090901215131304
          15756920979851832104115596935784883366531595132734467524394087576977
```

```
78908490126915322842080949630792972471304422194243906590308142893930
29158483087368745078977086921845296741146321155667865528338164806795
45594189100695091965899085456798072392370846302553545686919235546299
57157358790622745861957217211107882865756385970941907763205097832395
71346411902500470208485604082175094910771655311765297473803176765820
58767314028891032883431850884472116442719390374041315564986995913736
51621084511374022433518599576657753969362812542539006855262454561419
25880943740212888666974410972184534221817198089911953707545542033911
96453936646179296816534265223463993674233097018353390462367769367038
05342644821735823842192515904381485247388968642443703186654199615377
91396964900303958760654915244945043600135939277133952101251928572092
59788751160195962961569027116431894637342650023631004555718003693586
05526491000090724518378668956441716490727835628100970854524135469660
84481161338780654854515176167308605108065782936524108723263667228054
00387941086434822675009077826512101372819583165313969830908873174174
74535988684298559807185192215970046508106068445595364808922494405427
66329674592308898484868435865479850511542844016462352696931799377844
30217857019197098751629654665130278009966580052178208139317232379013
23249468260920081998103768484716787498919369499791482471634506093712
56541225019537951668976018550875993133677977939527822273233375295802
63122665358948205566515289466369032083287680432390611549350954590934
06676402258670848337605369986794102620470905715674470565311124286290
73548884929899835609996360921411284977458614696040287029670701478179
49024828290748416008368045866685507604619225209434980471574526881813
18508591501948527635965034581536416565493160130613304074344579651083
80304062240278898042825189094716292266898016684480963645198090510905
79651307570379245958074479752371266761011473878742144149154813591743
92799496956415653866883891715446305611805369728343470219206348999531
91764016110392490439179803398975491765395923608511807653184706473318
01578207412764787592739087492955716853665185912666373831235945891267
87095838000224515094244575648744840868775308453955217306366938917023
94037184780362774643171470855830491959895146776294392143100245613061
11429937000557751339717282549110056008940898419671319709118165542908
76109008324997831338240786961578492341986299168008677495934077593066
02207814943807854996798945399364063685722697422361858411425048372451
24465580270859179795591086523099756519838277952945756996574245578688
38354442368572236813990212613637440821314784832035636156113462870198
51423901842909741638620232051039712184983355286308685184282634615027
44187358639504042281512399505995983653792227285847422071677836679451
34363807086579774219853595393166279988789721695963455346336497949221
13017661316207477266113107012321403713882270221723233085472679533015
07998062253835458948024820043144726191596190526034069061930939290724
10284948700167172969517703467909979440975063764929635675558007116218
27727603182921790350290486090976266285396627024392536890256337101471
68327404504583060228676314215815990079164262770005461232291921929971
69907690169025946468104141214204472402661658275680524166861473393322
65959127006456304474160852916721870070451446497932266687321463467490
41185886760836840306190695786990096521390675205019744076776510438851
51941619318479919134924388152822038464729269446084915299588185988558
```

```
  1951490663073117772381322675169458825936387861072430256598091490103278384821401136556784934102431512482864529170314100400120163648299853251663490560537945850894244038552524554777922401046148907527451634251399216373835681414904793203742633730198782540569961916352019389698254478631309773749154478427634532593998741700138163198116645377208944002854850002696859826445621837941167021518477219093392321850877757909593326763114131296193984959261389879016697108810276638623167694057295932538078643444100512138025081797622723797210352196773268441946486164029610598990277105325704570163326134310764177000432371524746263939901189972784536294930363691490088106053123163000901015083933188011668215163893104666659513782749892374556051100401647771682271626727078370122424655126487845492350418521674263831897333324346744490397800178468972640546214802412412583384350170488532060147568786231809409001263241969092252022679880113408073012216264404133887392600523096072386158554965158001034746119792130767224543803671883253708606713311325819922797552277184864847532612430280417794309093899237093805365204646255147267884961527773274119265709116613580084145421487687310394441054796393085308968803656085047721445921725001265007170689694281546275637045883890421917739819064873190801482873905815946222786727741861011102763247972904122211994117388204526335701759090678628159281519982214576527968538925172187200900703891385628400073322585075904853480465645434983707328762593589142785431826658729460807238965229159902173888795773647738726574610400822551124182720096168188828493894678810468473126554172620978905678458109651797530087306315464903021121335281808476122990409576427857316364124880930949770739567588422963171158464569842024551090298823985179536841258914463527918973076838340736961314097452298563866827269104335751767712889452788136862396506665408989439495161912002160777898876864736481837825324846699168307281220310791935646668401591485826999933744276772522754038533221968522985908515481104022965791633825738551331482345959163328144581984361459630602499361753097925561238039014690665163673718859582772525683119989984646027216462797640770570748164064507697798699551061800464719378082232501489340785113783325107375382340346626955329260881384389578409980417041041777608463062862610614059615207066695243018438575031762939543026312673774069364047058960834626018859111843675325298458880408497109229991956553970191111919191883273086037667753396077224556321135065721910675875118681278634419757239219526333385653838824005719010256494923394451965959203992392217400247234147190970964562108299547746193228981181286055565880938518988118129056142740858091687657119112247632886587127553892843812661199193792462411263299073986785455875665245305619750989114578114735771283607554001774268660965093305172102723066635739462334136380459142377599652203094185588800394967558297112583616218901403595423493042474905369399277611426179640710012764328042870608353159458230596463268278612702033569803461432456970214843752 mod 3233
= 123
```