http://world.std.com/~franl/crypto/rsa-guts.html

The Mathematical Guts of RSA Encryption

The RSA algorithm was invented in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman.

Here's the relatively easy to understand math behind RSA public key encryption.

1. Find *P* and *Q*, two large (e.g., 1024-bit) prime numbers.
2. Choose *E* such that *E* is greater than 1, *E* is less than *PQ*, and *E* and *(P-1)(Q-1)* are *relatively prime*, which means they have no prime factors in common. *E* does not have to be prime, but it must be odd. *(P-1)(Q-1)* can't be prime because it's an even number.
3. Compute *D* such that *(DE - 1)* is evenly divisible by *(P-1)(Q-1)*. Mathematicians write this as *DE = 1 (mod (P-1)(Q-1))*, and they call *D* the *multiplicative inverse* of *E*. This is easy to do -- simply find an integer X which causes *D = (X(P-1)(Q-1) + 1)/E* to be an integer, then use that value of *D*.
4. The encryption function is *C = (T^E) mod PQ*, where *C* is the ciphertext (a positive integer), *T* is the plaintext (a positive integer), and ^ indicates exponentiation. The message being encrypted, *T*, must be less than the modulus, *PQ*.
5. The decryption function is *T = (C^D) mod PQ*, where *C* is the ciphertext (a positive integer), *T* is the plaintext (a positive integer), and ^ indicates exponentiation.

Your *public key* is the pair *(PQ, E)*. Your *private key* is the number *D* (reveal it to no one). The product *PQ* is the *modulus* (often called N in the literature). *E* is the *public exponent*. *D* is the *secret exponent*.

You can publish your public key freely, because there are no known easy methods of calculating *D*, *P*, or *Q* given only *(PQ, E)* (your public key). If *P* and *Q* are each 1024 bits long, the sun will burn out before the most powerful computers presently in existence can factor your modulus into *P* and *Q*.

Here is an example of RSA encryption.

Caveats

> Though it is widely suspected to be true, it is not yet proven that no easy methods of factoring exist. It is not yet proven that the only way to crack RSA is to factor the modulus.

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
        =
5043288895841606873442289912739446663145387836003550931555496756450105562861208255997874424542811005438349865428933638493024645144150785172091796654782635307099638035387326500896686074771829745822950342950407903581845940956377938586598936883808360284013250976862076697739667534325054282609347573513798806325648263933445309259438556242923301751977190016924916912809150596019178760171349725439279215696701789902134307146468971279610277181378394586967728986934236524031169321708926961764372652131566583315871245975980304250314400683788324610178483071758547454725206968892599589254436670143220546954317400228550092386369424448559733330630516073853028632193029135037454719467577767135795496520291979050578153287155839207030315958593749366328354860209083063550704455658896319318011934122017826923344101330116480696334024075046952588669876586690062240241020884665075302639538705266319335847348109487615622712603732759736037523738836414808894843809615775704538008107946980066734877795883758289985132793070353355127509043994817897905489933812173294585354474132680569810872633482854638168850488243465889783933466254454006619645218766694795528023088412465948239275105770491133290256843065052292561427303898320890070515110552506189941712317795157979429711795475296301837843862913977877661298207389072796767202350113992715819642730764074189891904868607481245493157953743771244160143876506914586819640227602776686953090395131496831909732450545234594477256587887692693353918692354818518542420923064996406822184490119135710885424428521120773712238311054554312653073940759278908226060431711333957522660344516452597631618427745904320191345289329932161307440532227470572894812143586831978415597276496357090901215131304
```

157569209798518321041155969357848833665315951327344675243940875769777890849012691532284208094963079297247130442219424390659030814289393029158483087368745078977086921845296741146321155667865528338164806795455941891006950919658990854567980723923708463025535456869192355462995715735879062274586195721721110788286575638597094190776320509783239571346411902500470208485604082175094910771655311765297473803176765820587673140288910328834318508844721164427193903740413155649869959137365162108451137402243351859957665775396936281254253900685526245456141925880943740212888666974410972184534221817198089911953707545542033911964539366461792968165342652234639936742330970183533904623677693670380534264482173582384219251590438148524738896864244370318665419961537791396964900303958760654915244945043600135939277133952101251928572092597887511601959629615690271164318946373426500236310045557180036935860552649100009072451837866895644171649072783562810097085452413546966084481161338780654854515176167308605108065782936524108723263667228054003879410864348226750090778265121013728195831653139698309088731741747453598868429855980718519221597004650810606844559536480892249440542763296745923088984848684358654798505115428440164623526969317993778443021785701919709875162965466513027800996658005217820813931723237901323249468260920081998103768484716787498919369499791482471634506093712565412250195379516689760185508759931336779779395278222732333752958026312266535894820556651528946636903208328768043239061154935095459093406676402258670848337605369986794102620470905715674470565311124286290735488849298998356099963609214112849774586146960402870296707014781794902482829074841600836804586668550760461922520943498047157452688181318508591501948527635965034581536416565493160130613304074344579651083803040622402788980428251890947162922668980166844809636451980905109057965130757037924595807447975237126676101147387874214414915481359174392794969564156538668838917154463056118053697283434702192063489995319176401611039249043917980339897549176539592360851180765318470647331891764016110392490439179803398975491765395923608511807653184706473318

01578207412764787592739087492955716853665185912666373831235945891267

87095838000224515094244575648744840868775308453955217306366938917023

94037184780362774643171470855830491959895146776294392143100245613061

11429937000557751339717282549110056008940898419671319709118165542908

76109008324997831338240786961578492341986299168008677495934077593066

02207814943807854996798945399364063685722697422361858411425048372451

24465580270859179795591086523099756519838277952945756996574245578688

38354442368572236813990212613637440821314784832035636156113462870198

51423901842909741638620232051039712184983355286308685184282634615027

44187358639504042281512399505995983653792227285847422071677836679451

34363807086579774219853595393166279988789721695963455346336497949221

13017661316207477266113107012321403713882270221723233085472679533015

07998062253835458948024820043144726191596190526034069061930939290724

10284948700167172969517703467909979440975063764929635675558007116218

27727603182921790350290486090976266285396627024392536890256337101471

68327404504583060228676314215815990079164262770005461232291921929971

69907690169025946468104141214204472402661658275680524166861473393322

65959127006456304474160852916721870070451446497932266687321463467490

41185886760836840306190695786990096521390675205019744076776510438851

51941619318479919134924388152822038464729269446084915299958818598855

19514906630731177723813226751694588259363878610724302565980914901032

78384821401136556784934102431512482864529170314100400120163648299853

25166349056053794585089424403855252455477792240104614890752745163425

13992163738356814149047932037426337301987825405699619163520193896982

54478631309773749154478427634532593998741700138163198116645377208944

00285485000269685982644562183794116702151847721909339232185087775790

95933267631141312961939849592613898790166971088102766386231676940572

95932538078643444100512138025081797622723797210352196773268441946486

16402961059899027710532570457016332613431076417700043237152474626393

99011899727845362949303636914900881060531231630009010150839331880116

68215163893104666659513782749892374556051100401647771682271626727078

37012242465512648784549235041852167426383189733332434674449039780017

84689726405462148024124125833843501704885320601475687862318094090012

63241969092252022679880113408073012216264404133887392600523096072386

15855496515800103474611979213076722454380367188325370860671331132581

99227975522771848648475326124302804177943090938992370938053652046462

55147267884961527773274119265709116613580084145421487687310394441054

79639308530896880365608504772144592172500126500717068969428154627563

70458838904219177398190648731908014828739058159462227867277418610111

02763247972904122211994117388204526335701759090678628159281519982214

57652796853892517218720090070389138562840007332258507590485348046564

54349837073287625935891427854318266587294608072389652291599021738887

95773647738726574610400822551124182720096168188828493894678810468847

31265541726209789056784581096517975300873063154649030211213352818084

76122990409576427857316364124880930949770739567588422963171158464569

84202455109029882398517953684125891446352791897307683834073696131409

74522985638668272691043357517677128894527881368623965066654089894394

95161912002160777898876864736481837825324846699168307281220310791935

64666840159148582699993374427677252275403853322196852298590851548110

40229657916338257385513314823459591633281445819843614596306024993617

53097925561238039014690665163673718859582772525683119989984646027216

46279764077057074816406450769779869955106180046471937808223250148934

07851137833251073753823403466269553292608813843895784099804170410417

77608463062862610614059615207066695243018438575031762939543026312673

77406936404705896083462601885911184367532529845888040849710922999195

65539701911191919188327308603766775339607722455632113506572191067587

51186812786344197572392195263333856538388240057190102564949233944519

65959203992392217400247234147190970964562108299547746193228981181286

05556588093851898811812905614274085809168765711911224763288658712755

38928438126611991937924624112632990739867854558756652453056197509891

$$145781147357712836075540017742686609650933051721027230666357394623 34$$

$$136380459142377599652203094185588800394967558297112583616218901403 59$$

$$542349304247490536939927761142617964071001276432804287060835315945 82$$

$$= 123$$