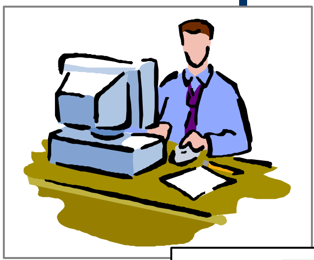
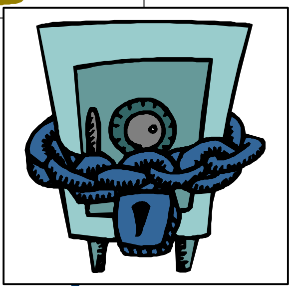
A White Paper prepared for
Asian School of Cyber Laws
www.asianlaws.org





RSA Algorithm and Encryption

ASCL White Papers can be downloaded from:
www.asianlaws.org/whitepapers

Tech Juris
The Technology Lawyers
www.techjuris.com

ASCL-WP-IS-Tec-Algo-01

The RSA public-key encryption algorithm works in the following manner:

1. Generation of a public-private key pair.
2. Encryption of a message (plain text) with the public key generated in step 1 to get the cipher-text.
3. Decryption of the cipher-text by using the private key of the corresponding public key generated in step 1.

Step 1:
Generation of a key pair

- Select two large integer primes **p** and **q**.

- Multiply p and q to get a number **n**,

  i.e., **pq** = **n**.

- Obtain ϕ which is the product of **p**-1 and **q**-1

  i.e. $\phi = (\mathbf{p}-1)(\mathbf{q}-1)$.

- Select **e** such that $1<\mathbf{e}<\phi$ and gcd of **e** and ϕ is 1.

- Compute d such that $1<\mathbf{d}<\phi$ and $\mathbf{ed} \equiv 1 \bmod \phi$. This means that the value of **d** must be such that **ed**-1 should be completely divisible by ϕ or $(\mathbf{ed}-1) / \phi$ should be an integer.

The public-key is (**n**, **e**) and the corresponding private key is (**d**, **n**).

Step 2:
Encryption process

Suppose the message to be encrypted is **m**.

The cipher-text **c** is obtained by raising the message to the value of **e** and finding out its modulo **n** i.e.

$$\mathbf{c} = \mathbf{m}^{\mathbf{e}} \bmod \mathbf{n}.$$

Step 3:
Decryption process

Decryption is achieved by raising the cipher-text **c** obtained in step 2 to the value of **d** and finding out its modulo **n** i.e.

$\mathbf{m} = \mathbf{c}^{\mathbf{d}} \bmod \mathbf{n}$.

The security of the RSA cryptosystem is based on the integer factorization problem. Any adversary who wishes to decipher the cipher-text **c** must do so by using the publicly available information (**n**, **e**).

One possible method is to first factor **n**, and then compute ϕ and **d** just as was done in the above mentioned steps. The factoring of n is currently computationally infeasible and therein lies the strength of the RSA cryptosystem.

An Example of the RSA Algorithm

Note this example uses artificially small numbers. In reality **p** and **q** are likely to be at least 100 digits each.

Let us take **p** = 61 and **q** = 53

pq = 3233

Let us choose **e** = 17

Therefore **d** = 2753

The public key is (3233, 17)

The private key is 2753.

To encrypt the plaintext value 123:

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

To decrypt the cipher text value 855:

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

= 50432888958416068734422899127394466631453878360035509315554967564501
0556286120825599787442454281100543834986542893363849302464514415078
5172091796654782635307099638035387326500896686074771829745822950342
9504079035818459409563779385865989368838083602840132509768620766977
3966753325054282609347573513798806325648263933445309259438556242923
3017519771900169249169128091505960191787601713497254392792156967017
8990213430714646897127961027718137839458696772898693423652403116932
1708926961764372652131566583315871245975980304250314400683788324610
1784830

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
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
51186812786344197572392195263338565383882400571901025649492339444519
65959203992392217400247234147190970964562108299547746193228981181286
05556588093851898811812905614274085809168765711911224763288658712755
38928438126611991937924624112632990739867854558756652453056197509891
14578114735771283607554001774268660965093305172102723066635739462334
13638045914237759965220309418558880039496755829711258361621890140359
54234930424749053693992776114261796407100127643280428706083531594582
305946326827861270203356980346143245697021484375 **mod** 3233

= 123

While it is widely believed that breaking the RSA encryption scheme is as difficult as factoring the modulus n, no such equivalence has been proven. The Rabin public-key encryption scheme was the first example of a *provably secure* public-key encryption scheme – the problem faced by a passive adversary of recovering plaintext from some given cipher text is computationally equivalent to factoring.

Asian School of Cyber Laws

Pune | Bangalore | Kolkata | Nagpur

OUR SERVICES

Information Security

- Training
- Consultancy
- White papers
- Workshops

Technology Law

We provide training, consultancy, workshops, and white papers in the following areas of law:

- Media Laws
- Semi-conductor Law
- Intellectual Property Law
- PKI Law
- Cyber Law
- Drafting
- Software valuation
- Audits
- Arbitration
- E-contracts

In addition, we conduct a Diploma course in Information Technology Law.

Cyber Crime Investigation

- Training
- Consultancy
- Search and seizure operations
- White papers
- Certified Courses

CONTACT US

Regd. Office

6, Rajas, Above IDBI, Pashan Road, Pune 411008
Ph: 91 20 5890894 / 95
Fax: 91 20 5675600

Email: info@asianlaws.org
URL: www.asianlaws.org