RSA Algorithm and Encryption

ASCL White Papers can be downloaded from:
www.asianlaws.org/whitepapers
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 \( \phi \) which is the product of \( p-1 \) and \( q-1 \)
  
  i.e. \( \phi = (p-1)(q-1) \).
- Select \( e \) such that \( 1 < e < \phi \) and gcd of \( e \) and \( \phi \) is 1.
- Compute \( d \) such that \( 1 < d < \phi \) and \( ed \equiv 1 \mod \phi \). This means that the value of \( d \) must be such that \( ed-1 \) should be completely divisible by \( \phi \) or \( (ed-1) / \phi \) 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.

\[ c = m^e \mod n. \]

**Step 3:**
**Decryption process**

Decryption is achieved by raising the cipher-text \( e \) obtained in step 2 to the value of \( d \) and finding out its modulo \( n \) i.e.
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 \( \phi \) 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:

\[
\text{Encrypt (123)} = (123^{17}) \mod 3233 \\
= 337587917446653715596592958817679803 \mod 3233 \\
= 855
\]

To decrypt the cipher text value 855:

\[
\text{decrypt(855)} = (855^{2753}) \mod 3233 \\
= 50432888958416068734422899127394466631453878360035509315554967564501 \\
05562861208255997874424542811005438349865428933638493024645144150785 \\
1720917966547826353070963803538732650089668607477182974582295034295 \\
0407903581845940956377938586598936883808360284013250976620766977396 \\
67533250542826093475735137988063256482639334453092594385562429233017 \\
51977190016924916912809150596019178760171349725439279215696701789902 \\
1343071464689712796102771813783945869678289693423652403116932170892 \\
69617643726521315665833158712459759803042503144006837883246101784830
\]
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.

\[ = 123 \]
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

This White Paper is provided for general information only. Neither Asian School of Cyber Laws (ASCL) nor Tech Juris (TJ) makes any warranty, express or implied, to the accuracy of the contents of these White Papers. Although all reasonable care and caution is taken while preparing these White Papers, errors and omissions may occur and neither ASCL not TJ will be liable for any direct, indirect, special, incidental or consequential damages or loss (including damages for loss of business, loss of profits, or the like) arising directly or indirectly from the use of information contained in this White Paper.