Tech Juris

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

```
3048 0241 00C0 324
68E1 9E52 7EB1 E8F
84BF D79D 1106 56F
6512 C8FE E421 1A3
2AC4 B955 FCD2 0F0
458C B195 4C4F 6C3
CA00 B0FF CADC AFA
```

RSA Algorithm and Digital Signatures

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

Tech Juris
The Technology Lawyers
www.techjuris.com

ASCL-WP-IS-Tec-Algo-02

The RSA Algorithm is named after Ronald Rivest, Adi Shamir and Leonard Adleman, who first published the algorithm in April 1977. It is probably the most commonly used public key algorithm. It can be used both for encryption and for digital signatures. The security of RSA is generally considered equivalent to factoring, although this has not been proved.

Encryption techniques typically use mathematical operations to transform a message (represented as a number or a series of numbers) into an encrypted form known as cipher text. One-way functions are suitable for this. A one-way function is one which is comparatively easy to do in one direction but difficult to do in reverse.

Let us take a simple example. It is comparatively easy to square a three-digit number e.g. 297. On the other hand, calculating the square root of the number 88209 is much more difficult.

This outline below presents a simplified explanation of how the RSA algorithm works. We will see how the algorithm is used to generate a public and private key pair and a message is signed that is verified by the receiver of the message.

1. At the onset, two large prime numbers, **p** and **q** are chosen.
   (A prime is such a number that is not divisible by any other number than itself and *1*. Thus the integers *2,3,5,7,11,...* and so on are primes. There are infinitely many primes, and the biggest prime number currently known is $2^{69,72,593} –1$.)

2. Then **n** is computed, which is the product of **p** and **q**

   $$\mathbf{n} = \mathbf{p} * \mathbf{q}$$

3. The next step is to compute a number ϕ. This number is the product of (p-1) and (q-1).

   $$\phi = (\mathbf{p}\text{-}1) * (\mathbf{q}\text{-}1)$$

4. He now calculates a number that has the following properties:

   a. it lies between 1 and ϕ
   b. it is relatively prime to ϕ

   Two numbers are said to be relatively prime or coprime if the only number that they are both divisible by is 1 e.g. 22 and 33 are not coprime as they are divisible by 1 and 11. However 51 and 52 are coprime as the only number that they are both divisible by is 1.

   In other words, if two numbers are coprime then their greatest common divisor (gcd) is 1.

   Let us call this number **e**.

As we have discussed, e has the following properties:

a. $1 < \mathbf{e} < \phi$
b. gcd (e, ϕ) = 1

5. Now a number **d** is calculated that satisfies the following properties:

   a. $1 < \mathbf{d} < \phi$
   b. $\mathbf{ed} \equiv 1 \bmod \phi$

   When we say that $\mathbf{ed} \equiv 1 \bmod \phi$ (i.e. **ed** is congruent to 1 mod ϕ), what it means is that (**ed** – 1) is divisible by ϕ.

6. The generation of the key pair is now complete:

   The public key is = (**n, e**)
   The private key is = (**d**)

7. To sign a message (**m**), a person will use his private key to generate his signature (**s**). This will be accomplished as under:

$$\mathbf{s} = \mathbf{m}^{\mathbf{d}} \bmod \mathbf{n}$$

   The message is first raised to the power of **d** (i.e. multiplied by itself **d** times) to yield $\mathbf{m}^{\mathbf{d}}$. The remainder after dividing $\mathbf{m}^{\mathbf{d}}$ by **n** is taken as the signature of the person for the message **m**.

8. The receiver of the message will need the public key of the signer (i.e. the person above who signs), the signature and the message. He will then compute $\mathbf{m}^{\mathbf{1}}$ as follows:

$$\mathbf{m}^{\mathbf{1}} = \mathbf{s}^{\mathbf{e}} \bmod \mathbf{n}$$

   If $\mathbf{m} = \mathbf{m}^{\mathbf{1}}$, the signature is verified. If however, $\mathbf{m} \neq \mathbf{m}^{\mathbf{1}}$, it means that either the message has been altered or that the person's private key was not used to sign the message.

Illustration 1: (Key pair generation)

Let us take an illustration with artificially small prime numbers.

Let p = 11 and q = 5

n = p * q = 55

ϕ = (p-1) * (q-1) = 40

Let us take e = 3

Now, (ed – 1) should be divisible by 40.

Therefore, d will be 27

The public key will be = (55, 3) and
The private key will be = (27)

Illustration 2: (Digital Signature creation and verification)

Let us use the key pair generated in Illustration 1 above.
If the message is 3, the signature will be

$s = 3^{27} \bmod 55$

i.e. s = 42

The receiver of the message will receive the public key (55, 3) and the signature (42). He will then compute

$m = 42^3 \bmod 55$

i.e. m = 3

Weaknesses of the RSA algorithm

The RSA algorithm suffers from the following weaknesses:

(i) Multiplicative property of RSA

The RSA signature scheme has the following multiplicative property, sometimes referred to as the homomorphic property.

If $s_1 = m_1^d \bmod n$

and $s_2 = m_2^d \bmod n$

are the signatures on messages m_1 and m_2 then

$$s_1 s_2 \bmod n = (m_1 m_2)^d \bmod n$$

On getting two different signed messages from a person it maybe computationally feasible to forge a person's signature.

(ii) Integer factorization

If an adversary is able to factor the public modulus n of some one then the adversary can compute ϕ and then, using the extended Euclidean algorithm, deduce the private key d from ϕ and the public exponent e by solving

$$ed \equiv 1 \bmod \phi$$

This constitutes a total break of the system. To guard against this p and q must be sufficiently large numbers so that factoring n is a computationally infeasible task.

However, with the rapid enhancement in computational power of modern computers it would be difficult to guarantee the computational infeasibility of factorization of large numbers.

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