RSA Mechanism

References:

- Wikipedia - RSA cryptosystem ⭐

Background

RSA (Rivest–Shamir–Adleman) is a **public-key cryptosystem**.

An RSA user creates a pair of keys, keeps the private key secret, and publishes the public key. Messages can be encrypted by anyone via the public key, but can only be decrypted by someone who knows the private key.

The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers. There are no published methods to defeat the system if a large enough key is used.

Key generation

The keys for the RSA algorithm are generated in the following way:

1. Choose two large prime numbers p and q.
   - p and q should be kept secret.
2. Compute $n = pq$.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
   - n is released as part of the public key.
3. Compute $\lambda(n)$.
   - λ is Carmichael's totient function. In this case, $\lambda(n) = \operatorname{lcm}(p-1, q-1)$.
   - lcm stands for least common multiple.
   - $\lambda(n)$ is kept secret.
4. Choose an integer e.
   - $1 < e < \lambda(n)$
   - e and $\lambda(n)$ are coprime.
   - e is released as part of the public key.
5. Determine d.
   - $d \equiv e^{-1} \mod \lambda(n)$. This means, solve $de \equiv 1 \mod \lambda(n)$ for d
   - d is kept secret as the private key exponent.
6. Get keys.
   - The public key: (n, e)
   - The private key: d

Operation

- Denote the original message as m, the ciphered message as c, both in integer expression.
- Encryption:

$$c \equiv m^e \mod n$$

- Decryption:

$$m \equiv c^d \mod n$$

Example

1. Choose two prime numbers $p = 61$ and $q = 53$.

2. Compute $n = pq = 3233$.
3. Compute $\lambda(n) = \operatorname{lcm}(p-1, q-1) = \operatorname{lcm}(60, 52) = 780$.
4. Choose an integer $e = 17$.
   - $1 < e < \lambda(n)$
   - e and $\lambda(n)$ are coprime.
5. Determine $d = 413$.
   - solve $de \equiv 1 \mod \lambda(n)$, we get $d = 413$.
6. Get keys.
   - The public key: $(n = 3233, e = 17)$
   - The private key: $d = 413$
7. Operation.
   - Original message: $m = 65$
   - Encrypted message:

$$c = m^e \mod n = 65^{17} \mod 3233 = 2790$$

   - Decrypted message:

$$m = c^d \mod n = 2790^{413} \mod 3233 = 65$$