Cryptography Mathematics and Basic Implementation

Christian Chinchole

July 1, 2023

1 RSA

The RSA algorithm is asymmetric, meaning it works with two keys: the public for encryption and the private for decryption.
Important variables are as follows:

- P,Q: are the primes.
- N: $p.q$
- e: Encryption Exponent
- d: Decryption Exponent
- N,e pair: form the public key
- N,d pair: form the private key

1.1 How are the keys generated?

1. First find the LCM of $(p-1)(q-1)$
2. $d = e^{-1} \mod \text{LCM}$
3. $n = p.q$
4. $dP = d \mod (p-1)$
   $dQ = d \mod (q-1)$
   $qInv = q^{-1} \mod p$

1.2 Pairwise Testing

The pairwise consistency test is used to check that the public and private exponent are suitable for encryption/decryption.

For k between $1 < k < (n-1$:

$$k = (k^e)^d \mod n$$

1.3 Encryption

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

1.4 Decryption

The standard method: $m = c^d \mod n$
An exponentially faster method is to use the Chinese Remainder Theorem components:

$$m_1 = c^{dP} \mod p$$

$$m_2 = c^{dQ} \mod q$$

$$h = (qInv)(m_1 - m_2) \mod p$$

$$m = m_2 + h.q$$