CH 9 - RSA Public-Key Encryption Scheme

Luke Lu • 2025-12-17

Implementing RSA Scheme

🐳 **Info — RSA**

Setting up RSA

1. Randomly choose two large, distinct primes p and q and let $n = pq$.
2. Select an arbitrary integer e so that $\gcd(e, (p-1)(q-1)) = 1$ and $1 < e < (p-1)(q-1)$
3. Solve the congruence

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

   for an integer d where $1 < d < (p-1)(q-1)$
4. Publish the public key (e, n)
5. Keep secret of the private key (d, n), and the primes p and q

Encryption of RSA

1. Obtain a copy of public key (e, n)
2. Construct the plain text message M where $0 \leq M < n$
3. Encrypt M as the ciphertext C given by

$$C \equiv M^e \pmod{n}$$

   where $0 \leq C < n$
4. Send C

Decryption of RSA

1. Use the private key (d, n) to decrypt the ciphertext C as the received message R, given by

$$R \equiv C^d \pmod{n}$$

   where $0 \leq R < n$
2. Claim: $R = M$

Examples:

1. If $p = 2, q = 11, e = 3$, compute n and d

   $n = pq = 2 \cdot 11 = 22$, e is already prime, thus coprime to any other number.

   $1 \leq 3 < 10$

   Solve $3d \equiv 1 \pmod{10} \implies d \equiv 7 \pmod{10}$

   ANS: the public key is $(3, 22)$ and private key is $(7, 22)$

2. If $M = 8$, from (1), compute C

   Given public key is $(3, 22)$ and $0 \leq 8 < 22$

   $C \equiv 8^3 \equiv 512 \equiv 6 \pmod{22} \implies C = 6$

3. If $C = 6$, from (2), compute R

   $R \equiv C^d \equiv 6^7 \pmod{22}$

   $R \equiv 6^7 \pmod{2} \land R \equiv 6^7 \pmod{11}$ by Splitting Modulus Theorem

   $R \equiv 0 \pmod{2} \land R \equiv \left(6^2\right)^3 \cdot 6 \equiv 3^3 \cdot 6 \equiv 81 \cdot 2 \equiv 4 \cdot 2 \equiv 8 \pmod{11} \implies R = 8$

   $R = M = 8$

4. Given $p = 11, q = 13, e = 23$ find public and private keys
   Public Key: (47, 143)
   Private Key: (23, 143)

5. From (4), find C if $M = 25$
   $C = 38$

6. Find R from (4) and (5)
   $R = 25$

Why RSA Works

Info – RSA Works

For all integers p, q, n, e, d, M, C, R if

1. p, q are distinct
2. $n = pq$
3. e and d are positive integers s.t. $ed \equiv 1 \pmod{(p-1)(q-1)}$ and $1 < e, d < (p-1)(q-1)$
4. $0 \leq M < n$
5. $M^c \equiv C \pmod{n}$ where $0 \leq C < n$
6. $C^c \equiv R \pmod{n}$ where $0 \leq R < n$

then $R = M$