RSA

procedure, correctness and security

Jingqi Chen

May 18, 2021

Contents

What is RSA

- RSA is a public-key cryptosystem.
- It was invented in 1977 by Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman; they won 2002 Turing Award.
- An equivalent system was developed secretly in 1973 at GCHQ, by Clifford Cocks.

Where are we using RSA

- Almost everywhere if encrypting / signing is needed.
- TLS, SSH, etc...

Create Keys

- Generate 2 distinct primes, p and q; they must be kept hidden, and they are commonly hundreds of digits long.
- $n = pq$
- Select $e \in [0..n), e \in \mathbb{Z}$ such that $\gcd(e, (p-1)(q-1)) = 1$.
- **Public key** is the pair (e, n), which should be distributed widely.
- **Private key** is $d \in [0..n]$, which is the inverse of e in the ring $\mathbb{Z}_{(p-1)(q-1)}$.

Encode and Decode

encode:

$$\widehat{m} ::= m^e(\mathbb{Z}_n)$$

decode:

$$m = \widehat{m}^d(\mathbb{Z}_n)$$

Euler's

$$\phi(n) = |\{k \in [0..n) | \gcd(k, n) = 1\}|$$

Euler's Theroem: $k^{\phi(n)} \equiv 1 \mod n, \quad \gcd(k, n) = 1$

Fermat's Little Theroem: $k^{p-1} \equiv 1 \mod p, \quad p \text{ is prime} \wedge p \nmid k$

Proof of Euler's Theroem

let: $\mathbb{Z}_n^* = \{k \in [0..n) | \gcd(k, n) = 1\}$

then: Euler's Theroem $\iff \forall k \in \mathbb{Z}_n^*, k^{\phi(n)} \equiv 1 \mod (\mathbb{Z}_n)$

lemma: $\forall k \in \mathbb{Z}_n, S \subset \mathbb{Z}_n; |S| = |kS|$

hint: k is cancellable in $\mathbb{Z}_n$

then: $k\mathbb{Z}_n^* = \mathbb{Z}_n^*$

then: $k^i\mathbb{Z}_n^* = \mathbb{Z}_n^*, i \in \mathbb{Z}_+$

let: $P = \prod_{i=1}^{\phi(n)} k_i(\mathbb{Z}_n), k \in \mathbb{Z}_n$

Proof of Euler's Theroem – continue

$$
\begin{aligned}
Q &= \prod_{i=1}^{\phi(n)} k \cdot k_i(\mathbb{Z}_n), k \in \mathbb{Z}_n \\
&= k^{\phi(n)} P(\mathbb{Z}_n) \\
&= P(\mathbb{Z}_n) \\
&\rightarrow k^{\phi(n)} \equiv 1 \mod n
\end{aligned}
$$

Lemma

- n is a product of distinct primes.
- $a \equiv 1 \mod \phi(n), a \in \mathbb{N}$
- **then:**
- $m^a \equiv m \mod n$

Lemma Proof - if n is prime p

- $p|m$, the trivial case, both sides are 0.
- $a \equiv 1 \mod p-1$
- $$\begin{aligned} m^a &= m^{1+k(p-1)} \mod n \\ &= m \cdot (m^{p-1})^k \mod n \\ &= m \cdot 1^k \mod n \end{aligned}$$

Lemma Proof - another lemma

- n is a product of distinct primes.
- and $a \equiv b \mod p_i$, p_i are all the prime factors of n
- then $a \equiv b \mod n$

Lemma Proof - finally

- n is a product of distinct primes p_i.
- $\phi(n) = \prod_i (p_i - 1)$
- $a \equiv 1 \mod \phi(n) \iff a = 1 + k\phi(n) \to a = 1 + k'(p_i - 1)$
- $a \equiv 1 \mod p_i - 1 \to m^a = m \mod p_i$
- $m^a = m \mod n$

Proof

- RSA correctness can be easily proved as it is just a special case of the previous lemma!
- $m^{de} = m \mod n$
- n is a product of p, q
- $de \equiv 1 \mod \phi(n)$