Practice08

Friday, April 28, 2023 2:03 PM

4 assignments - 8 point

4 point grade 2

6 points grad 3

RSA in practice

$n \geq 2^{2048}$

RSA-2048

This can encrypt 256 bytes at once

m is not this long since OAEP

p, q primes $n = pq$

$\varphi(n) = (p-1)(q-1)$

$ed \equiv 1 \mod \varphi(n)$

$e = 2^{16} + 1$

Public key (n, e) Enc $c = m^e \mod n$

Private key (p, q, d) Dec $m = c^d \mod n$ $O(n^2 \log_2 d)$

$$m = c^{d} \bmod n \quad O(\ldots \log_2 d)$$

$$m = c^{d} \bmod n \overset{CRT}{\iff} \boxed{\begin{array}{l} m \equiv c^{d} \bmod p \\ m \equiv c^{d} \bmod q \end{array}} \quad O(p^{2}\log_2 d)$$

Euler-Fermat's Theorem

$$a^{\varphi(b)} \equiv 1 \pmod b \qquad \varphi(p) = p-1$$

$$c^{d} \bmod p = c$$

$$d = \underbrace{\left\lfloor \frac{d}{p-1} \right\rfloor}_{\text{quotient}}^{q} (p-1) + \underbrace{d \bmod p-1}_{\text{remainder}} \quad \text{(Euclid division)}$$

$$c^{d} = c^{q \cdot (p-1) + d \bmod p-1} = \left(c^{p-1}\right)^{q} \cdot c^{d \bmod p-1} \equiv$$

$$\cancel{1^{q}} \cdot c^{d \bmod p-1} \pmod{p-1}$$

The system to solve is

$$m \equiv c^{d_p} \pmod p \qquad d_p = d \bmod p-1$$

$m \equiv c^{d_p} \pmod{p}$ $\quad d_p = d \bmod p-1$

$m \equiv c^{d_q}\ (\text{mod}\ \ )$ $\quad d_q = d \bmod q-1$

From Garner's algorithm

$q_{inv} = q^{-1} \bmod p \quad$ (EEA)

$m_1 = c^{d_p} \bmod p$

$m_2 = c^{d_q} \bmod q \quad , \quad h = q_{inv}(m_1 - m_2) \bmod p$

$$\boxed{m = m_2 + qh}$$

$m = c^d \bmod n$

Public key (n, e)

Private key $(p, q, d, d_p, d_q, q_{inv})$

<u>Digital signature RSA</u>

1° Integrity

2° Authenticity

2° Authenticity

$m \| \sigma$

$$H : X^* \longrightarrow X^n$$

Instead of „decrypting" m, we will

„decrypt" $H(m)$

$$H(m)^d \bmod n = \sigma \quad \longrightarrow m \| \sigma$$

To check the signature

We $\sigma^e \bmod n \stackrel{?}{=} H(m)$

Assignment

You are given

$\overline{m}$, H, RSA length

bytes, SHA1, 2048 bits

1° Generate the key for RSA

2° Hash the message $\overline{H(\overline{m})}$

3° ... $\overline{H(\overline{m})}$ ...

3° Convert $H(\bar{m})$ to an integer

4° Calculate σ

5° Convert the σ to $\bar{\sigma}$

Send $\bar{m} \| \bar{\sigma}$

For checking the signature

1° Extract $\bar{\sigma}$, convert it to σ

2° Calculate $H(\bar{m})$ and convert to int

3° Check if $H(\bar{m}) \stackrel{?}{=} \sigma^{e} \bmod n$