Practice07

Friday, April 21, 2023 1:55 PM

RSA in practice

p, q are large prime numbers

$n = p \cdot q$ $1 < e < \varphi(n)$ s.t. $\gcd(e, \varphi(n)) = 1$

↓

Euler's φ (totient)

Number of coprimes to n

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

(n, e) public key of RSA

$ed \equiv 1 \pmod{\varphi(n)}$

$\varphi(n) \mid ed - 1 \Rightarrow ed - 1 = k \cdot \varphi(n)$

$ed - k \cdot \varphi(n) = 1 = \gcd(e, \varphi(n))$

$XGCD(e, \varphi(n)) = (1, d, -k)$

Encrypt:

$1 < m < n$: $c = m^e \bmod n$

Decrypt $m = c^d \bmod n$

Private key (p, q, d)

$x \in \mathbb{Z}$

$$100 \leq x < 1000$$

$$10^2 \leq x < 10^3 \quad / \log_{10}$$

$$2 \leq \log_{10} x < 3$$

number of digit require to store x in base 10 $\lfloor \log_{10} x \rfloor + 1$

$x = 100, 101, 110, 111$

$4 \quad 5 \quad 6 \quad 7$

$$2^2 \leq x < 2^3 \quad / \log_2$$

$2^2 \downarrow 4$ $\quad 2^3 \downarrow 8$

$0 < x \in \mathbb{Z}$, $\lfloor \log_2 x \rfloor + 1$ bits

a, b

$$\log(ab) = \log(a) + \log(b)$$

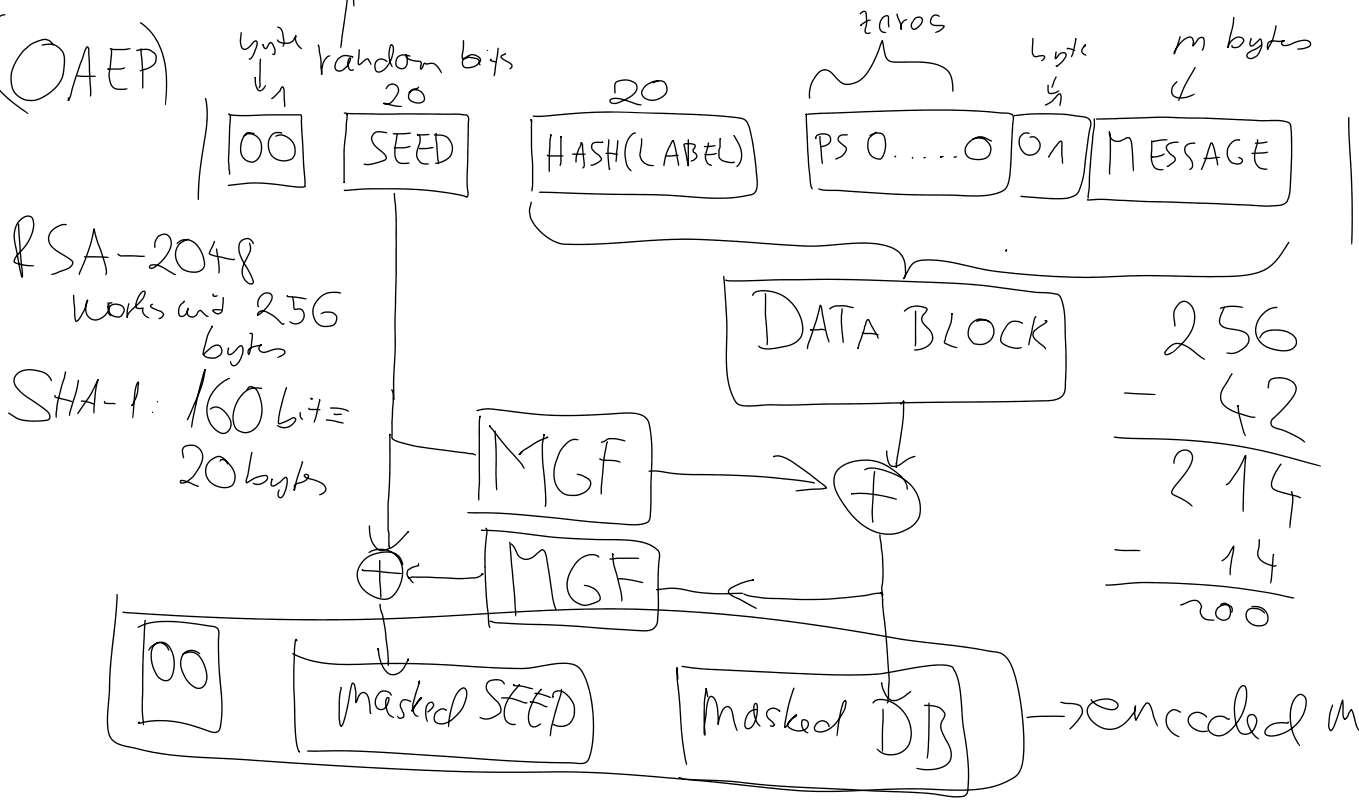
In practice

if $m < 2^{2048} \leq n = pq$ 256-bytes

$p, q \in [2^{1023}, 2^{1024})$

$m' = r \| m$

(OAEP)



RSA-2048 works and 256 bytes

SHA-1: 160 bit = 20 bytes

256
- 42
214
- 14
200

```
MGF(s: byte, l: int, H: hash fn)
    T = []
    counter = 0
    while (len(T) < l):
        T += hash(seed||counter)
```

T += hash(seed || bytes(counter))

return T[:length]