RFC RSA

Public key

n RSA modulus (> 0)
e RSA public component

$n = \prod r_i \quad i = 1 \ldots v \quad r_i$ odd prime
$v \geq 2$

$e = 3 \ldots n-1$ s.t.

$$GCD(e, \lambda(n)) = 1$$

$$\lambda(n) = LCM(r_1 - 1, \ldots r_v - 1)$$

Private key

Either:

Rep1
1) n modulus (positive integer)
2) d private exponent > 0

or:

Rep2
p first factor > 0
q second factor
dP First factor CRT Exponent > 0
dQ second " "
$qInv$ first CRT exponent > 0
r_i ith factor > 0
d_i ith factor CRT exponent > 0
t_i ith factor CRT coefficient > 0

Rep1 private(n) = public(n)

$n > e$ s.t.

$$e * d = 1 \pmod{\lambda(n)}$$

(e.g. $\frac{e*d}{\lambda(n)} = x$ Remainder 1)

Rep2 $p, q = r_1, r_2$ (from public(n))

$e * dP = 1 \pmod{(p-1)}$ $\quad \frac{e*dP}{(p-1)} = \ldots R1$
$e * dQ = 1 \pmod{(q-1)}$ $\quad \frac{e*dQ}{(q-1)} = \ldots R1$
$q * qInv = 1 \pmod{p}$

$\forall r_i \; i \geq 3 \; \exists (r_i \; d_i \; t_i)$
s.t. $e * d_i = 1 \pmod{r_i - 1}$
$(r_{i-1} r_{i-2} \cdots r_2 r_1) * t_i = 1 \pmod{r_i}$

Data conversions

Integer to octet string (I2OSP)

Octet string to Integer (OS2IP)

octet string = (10100001)(01000110)....
sequence of 8 bit bytes

I2OSP (x, xLen) = Octet string

1. If $x \geq 256^{xlen}$ => too large error
2. $x = x_{xlen-1} 256^{xlen-1} + x_{xlen-2} 256^{xlen-2} \ldots x_1 256 + x_0$

$0 \leq x_i < 256$

(think $12345 = 1\times10^4 + 2\times10^3 + 3\times10^2 + 4\times10^1 + 5\times10^0$)

3. OS = $x_{xlen-1} x_{xlen-2} \ldots x_0$

OS2IP (X) = x

↑
octet string

1. Let $x = x_{xlen-1} 256^{xlen} \ldots + x_0$