kit-rsa Explanation

Jakub Juszczakiewicz (Krypto-IT)

April 27, 2024

RSA key generation:

$$p = rand\_prime(),\ q = rand\_prime() \tag{1}$$

$$n = p * q \tag{2}$$

$$x = \lambda(n) = \frac{|p * q|}{gcd(p, q)} \tag{3}$$

$$e = rand(1, x), gcd(e, x) = 1 \tag{4}$$

$$d \to d \equiv e^{-1} (mod\ x) \tag{5}$$

$$keys \to (e, n), (d, n) \tag{6}$$

kit-RSA variant **b**-bits key generation:

$$p = rand\_prime(0.45 * b),\ q = rand\_prime(0.55 * b), m = rand\_prime(b) \tag{7}$$

$$n = p * q \tag{8}$$

$$x = \lambda(n) = \frac{|p * q|}{gcd(p, q)} \tag{9}$$

$$eu = \lambda(n * m) \tag{10}$$

$$e = rand(1, eu),\ gcd(e, eu) = 1,\ e > x \tag{11}$$

$$d \to d \equiv e^{-1} (mod\ eu) \tag{12}$$

$$keys \to (e, n), (d, n) \tag{13}$$

$$eu \to FORGET! \tag{14}$$