COMP0147 RSA

pick large prime. $n = p \times q$.

$\phi(n) = (p-1) \times (q-1)$

secret.

choose e in $[2, \phi(n))$ $\gcd(e, \phi(n)) = 1$.

compute $e^{-1} \pmod{\phi(n)} = d$.

Public key $n = p \times q$. e

Private key $n = p \times q$, d.

$Enc(m)$ $m_{sec} \Rightarrow m^e \bmod n$.

$Dec(m_{sec})$ $m_{sec} \Rightarrow m_{sec}^d \bmod (n)$

$p=7$ $q=11$ $\phi(n) = 10 \times 6 = 60$

$e = 17$, $d = e^{-1} \pmod{60}$

$d = 53 \pmod{60}$

$n = 77$.

Public $(77, 17)$

$m = 69$ $69^{17} \pmod{77} = 20$.

$d = 20^{53} \pmod{77} = 69$.

$p = 11$ $q = 17$. $n = 11 \times 17 = 187$.

$\phi(n) = (11-1) \times (17-1) = 16 \times 10 = 160$.

secret

public $a = 7$

$7^{-1} = 23 \pmod{160}$

private $b = 23$

(n, a)

160		1	0
7	22	0	1
6	1	1	-22
1	6	-1	23
0			

$23 \times 7 - 160 = 1$.

$M = 15$

$M_{sec} = 15^7 \pmod{187} = 64$

$64^{23} \pmod{187} = 15.$

$p = \sim \quad q = \sim \quad n = p \times q$

$\phi(n) = (p-1) \times (q-1)$

$\gcd(a, \phi(n))$

$b = a^{-1} \pmod{\phi(n)}$

(n, a) — $M^a \pmod n$

(n, b) — $M_{sec}^b \pmod n$

$x^3 = 1 \pmod{11}$

$x = 1^{7^{-1}} \pmod{11}$

$3 = 7^{-1} \pmod{10}$

$x = 3 \pmod{11}$