

Kripto Kunci Publik RSA

Sarwono Sutikno

Lab. Elektronika & Komponen

Teknik Elektro ITB

Algoritma RSA

- Kunci Publik:
 - $n = p \cdot q$, p & q bil. Prima besar dan dirahasiakan
 - e relatif prima terhadap $\Phi(n) = (p-1) \cdot (q-1)$
- Kunci Rahasia:
 - $d = e^{-1} \pmod{\Phi(n)}$
- Enkripsi:
 - $c = m^e \pmod{n}$
- Dekripsi:
 - $m = c^d \pmod{n}$

Contoh RSA

- Kunci Publik:
 - Pilih bil. prima $p = 7$ dan $q = 11$, $n = 7 \cdot 11 = 77$
 - $\Phi(n) = (p-1) \cdot (q-1) = 6 \cdot 10 = 60$ artinya
 $\Phi(n) = \{1, 2, 3, 4, 6, 8, \dots, 76\} = \{x \mid \gcd(x, n) = 1\}$
 - Pilih e dalam $\{x \mid \gcd(x, 60) = 1\}$, misalnya $e = 17$
 - Hapus p dan q dan Kunci Publik $n = 77, e = 17$
- Kunci Rahasia:
 - $d = e^{-1} \pmod{\Phi(n)}$, $d \cdot e = 1 \pmod{60}$, $d = 53$
 - $53 \cdot 17 \pmod{60} = 901 \pmod{60} = 1 \pmod{60}$

Contoh RSA (lanjutan 1)

- $M = \text{“PESAN”}$, $m = 16\ 5\ 19\ 1\ 14$
- Enkripsi: $c = m^e \bmod n$
 - $c_1 = 16^{17} \bmod 77 = 25$
 - $c_2 = 5^{17} \bmod 77 = 3$
 - $c_3 = 19^{17} \bmod 77 = 24$
 - $c_4 = 1^{17} \bmod 77 = 1$
 - $c_5 = 14^{17} \bmod 77 = 42$
- $c = 25\ 03\ 24\ 01\ 42$, $C = \text{“YCXAp”}$

Contoh RSA (lanjutan 2)

- $C = \text{“YCXAp”}$, $c = 25\ 03\ 24\ 01\ 42$
- Dekripsi: $m = c^d \bmod n$
 - $m_1 = 25^{53} \bmod 77 = 16$
 - $m_2 = 3^{53} \bmod 77 = 5$
 - $m_3 = 24^{53} \bmod 77 = 19$
 - $m_4 = 1^{53} \bmod 77 = 1$
 - $m_5 = 42^{53} \bmod 77 = 14$

Contoh RSA 512 bit $\approx 1,3 \cdot 10^{154}$

- Modulus $n =$ 81 5a d0 b9 0a ac 9f 4c da cc 57 6e ca a7 6a
c3 46 92 a7 81 68 ec 08 ec 77 dd 40 c2 ec 97 52 cb 3b 34
2c b6 a6 e2 76 3a ed 42 84 fa 55 ac 0d 6c 10 39 a2 7e a3
09 be 40 35 38 04 7d 06 43 1f 6f
- Sec exp $e =$ 29 40 70 02 50 db 19 6b b1 f4 8a a7 b4 59 6c
4b 66 b5 94 f6 15 ae e4 69 44 95 23 f3 d0 fc ea 84 19 7c
55 e0 27 40 2d 19 18 15 08 05 51 ac f5 98 91 f0 98 5f c4
17 05 eb 3b e8 a3 04 32 d4 20 2f
- Pub exp $d =$ 59 f1 2f 29 73 d0 bc 8e 13 6e 2a 21 53 2c b7
4d 69 82 c9 54 92 6c 64 43 0d 69 15 83 e9 44 a6 de 5e 30
e9 ae 48 f9 c8 84 a4 16 44 4d df 50 f2 0e 96 3e 24 df a4 f4
ec 3d c6 db 61 a7 e6 dc ea cf