Algoritma RSA

Budi Rahardjo

2024

Algoritma RSA

Key Generation

- **Kunci publik**
  - Ambil 2 bilangan prima p dan q yang besar
  - $n = p \,.\, q$
  - $\Phi(n) = (p - 1) \,.\, (q - 1)$
  - Cari bilangan e yang relatif prima terhadap $\Phi(n)$
- **Kunci rahasia**
  - d = e^{-1} mod $\Phi(n)$

Encryption & Decryption

- m = message
- c = ciphered text

- **Enkripsi**
  - c = m^e mod n
- **Dekripsi**
  - m = c^d mod n

Contoh RSA

- **Kunci Publik:**
  - Pilih bil. prima p = 7 dan q = 11, n = 7.11 =77
  - $\Phi(n)$=(p-1).(q-1)=6.10= 60 artinya
  - Pilih e dalam {x|gcd(x, 60)=1}, misalnya e=17
  - Hapus p dan q dan Kunci Publik **n=77, e=17**
- **Kunci Rahasia:**
  - d = e^{-1} mod $\Phi(n)$, d .e = 1 mod 60, d =53
  - 53 . 17 mod 60 = 901 mod 60 = 1 mod 60

Contoh RSA (lanjutan 1)

- M = “BUDI”, ASCII value of the text: m = 66, **85**, 68, 73
- Enkripsi: $c = m^e \bmod n$
  - Gunakan Wolfram Alpha
  - $c_1 = 66^{17} \bmod 77 = 33$
  - $c_2 = 85^{17} \bmod 77 = 57$
  - $c_3 = 68^{17} \bmod 77 = 73$
  - $c_4 = 73^{17} \bmod 77 = 61$
- c = 33 57 73 61

Contoh RSA (lanjutan 2)

- c = 33 57 73 61
- Dekripsi: m = c^d mod n
  - m_1 = 33^{53} mod 77 = 66
  - m_2 = 57^{53} mod 77 = 8 => 85
  - m_3 = 73^{53} mod 77 = 68
  - m_4 = 61^{53} mod 77 = 73
- m = 66, 85, 68, 73 = BUDI

Bagaimana Menghitung?

- 66^{17} mod 77
- 66^{17} = **855552971876131706920300353945 6**
- How to implement this in coding?
    - In many languages, integer is usually 32 or 64-bits
    - This number is more than 64 bits
    - Must use special library (such as BIGNUM library)
    - Time consuming to calculate

Contoh RSA 512 bit ≈ $1{,}3.10^{154}$

- 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

Fast Exponentiation

$$c = 6^{73} \ mod\ 100$$

$73 = 1 + 2^3 + 2^6$

Successive squares of 6, $6^2 = 36$

6^{2^2} mod 100 $= 36^2$ mod 100 = 96 mod 100 = - 4 mod 100,
6^{2^3} mod 100 = 16 mod 100,
6^{2^4} mod 100 = 16^2 mod 100 = 56 mod 100,
6^{2^5}mod 100 = 56^2 mod 100 = 36 mod 100,
6^{2^6} mod 100 = - 4 mod 100

Fast Exponentiation (2)

$6^{73} = 6 * 6^{2^3} * 6^{2^6}$

6^{73} mod 100 = 6 * 16 * (-4) mod 100 = 16 mod 100