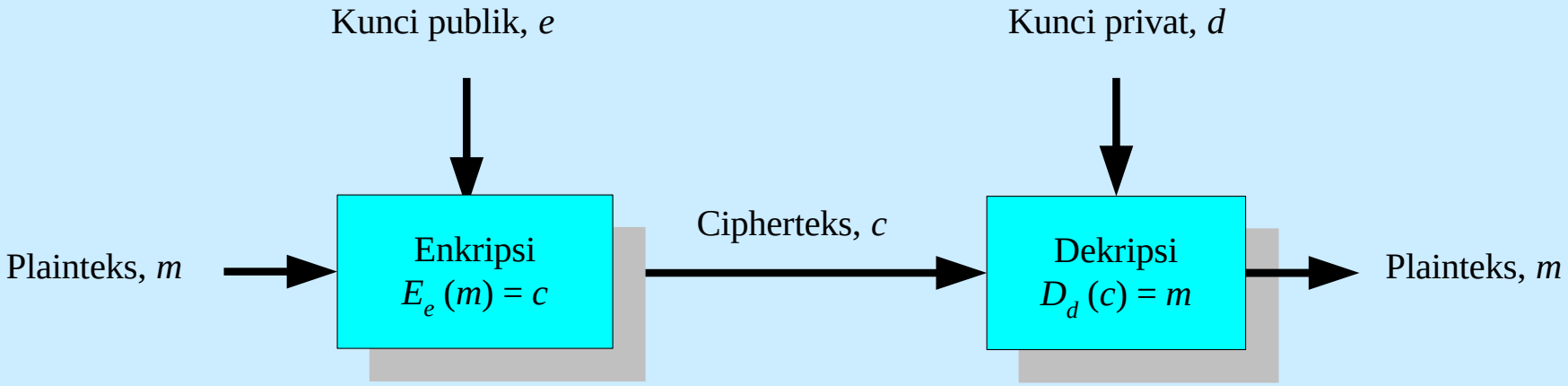
Kriptografi Kunci-Publik

Pendahuluan

- Sampai akhir tahun 1970, hanya ada sistem kriptografi kunci-simetri.
- Satu masalah besar dalam sistem kriptografi: bagaimana mengirimkan kunci rahasia kepada penerima?
- Mengirim kunci rahasia pada saluran publik (telepon, internet, pos) sangat tidak aman.
- Oleh karena itu, kunci harus dikirim melalui saluran kedua yang benar-benar aman.
- Saluran kedua tersebut umumnya lambat dan mahal.

- Kriptografi kunci-Asimetri disebut juga kriptografi kunci-publik
- Pada kriptografi kunci-publik, masing-masing pengirim dan penerima mempunyai sepasang kunci:

  1. Kunci publik: untuk mengenkripsi pesan
  2. Kunci privat: untuk mendekripsi pesan.
- $E_e(m) = c$ dan $D_d(c) = m$

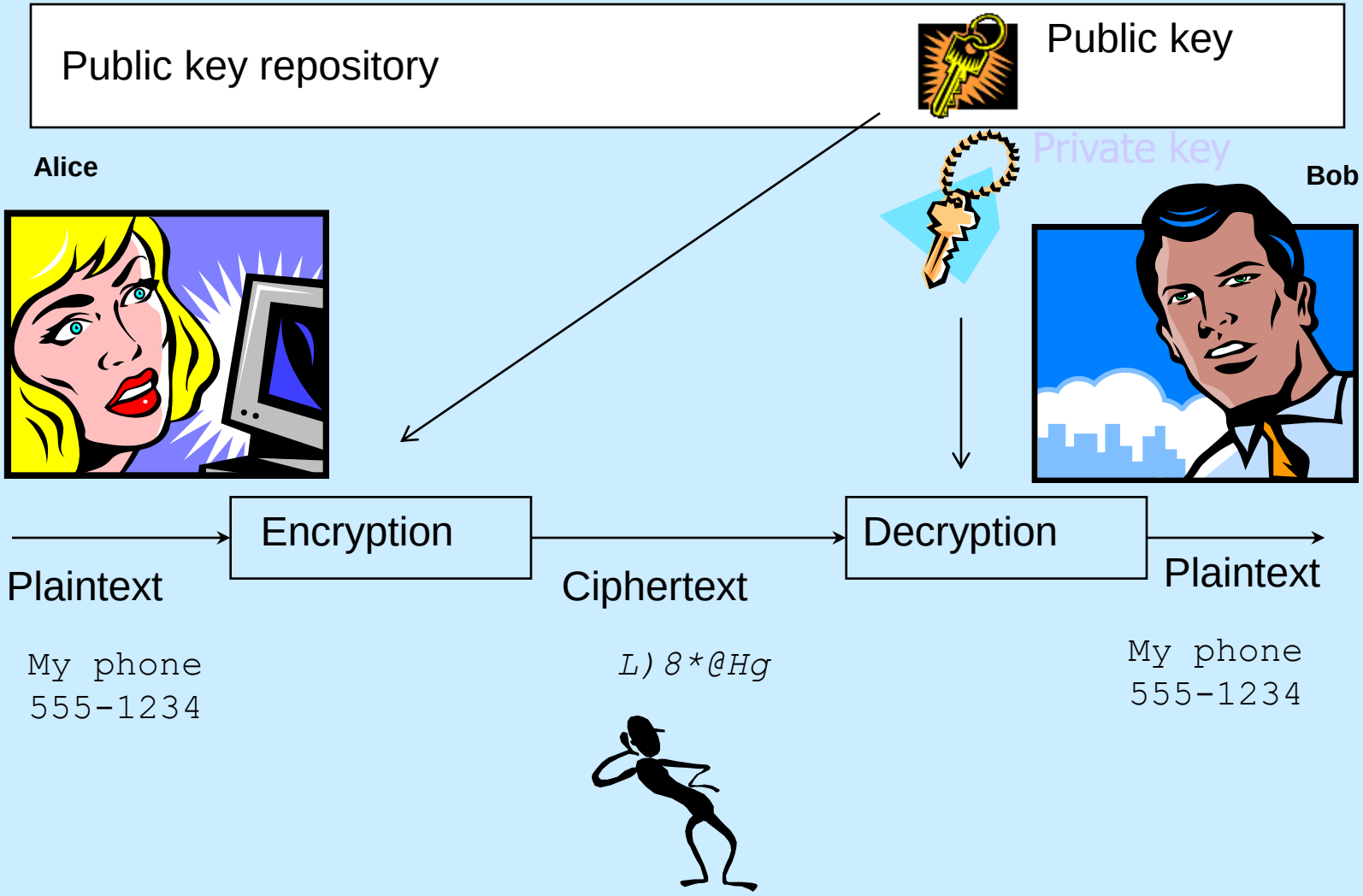


- Misalkan: Pengirim pesan: Alice

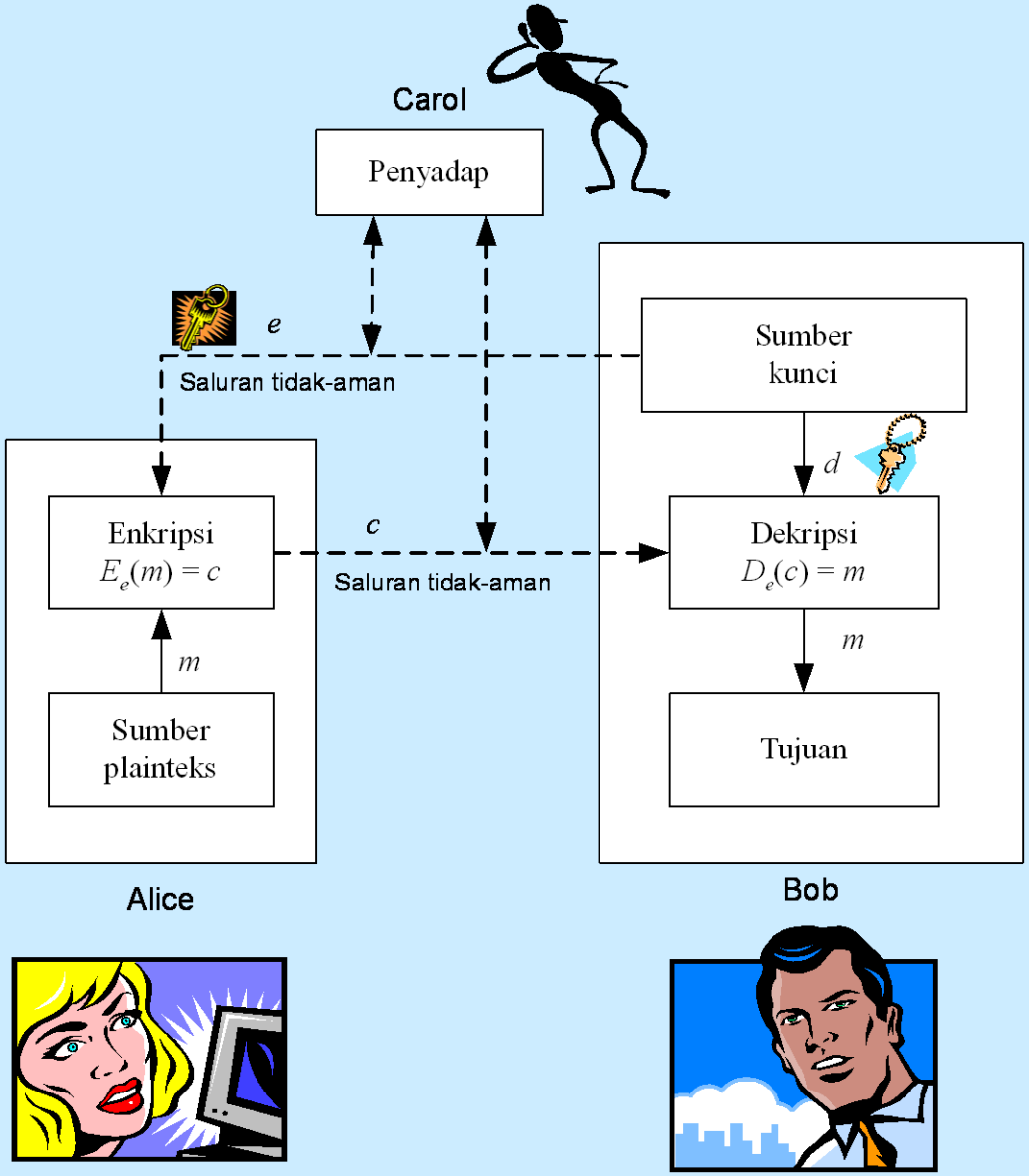
  Penerima pesan: Bob
- Alice mengenkripsi pesan dengan kunci publik Bob
- Bob mendekripsi pesan dengan kunci privatnya (kunci privat Bob)
- Sebaliknya, Bob mengenkripsi pesan dengan kunci publik Alice
- Alice mendekripsi pesan dengan kunci privatnya (kunci privat Alice)
- Dengan mekanisme seperti ini, tidak ada kebutuhan mengirimkan kunci rahasia (seperti halnya pada sistem kriptografi simetri

Kriptografi Kunci-publik

(http://budi.insan.co.id/courses/ec7010)



- Kunci enkripsi dapat dikirim melalui saluran yang tidak perlu aman (*unsecure channel*).
- Saluran yang tidak perlu aman ini mungkin sama dengan saluran yang digunakan untuk mengirim cipherteks.


Carol
Penyadap
e
Saluran tidak-aman
Sumber kunci
d
Enkripsi
$E_e(m) = c$
c
Saluran tidak-aman
Dekripsi
$D_e(c) = m$
m
m
Sumber plainteks
Tujuan
Alice
Bob

Dua keuntungan kriptografi kunci-publik:

1. Tidak diperlukan pengiriman kunci rahasia
2. Jumlah kunci dapat ditekan

- Kriptografi kunci-publik didasarkan pada fakta:
  1. Komputasi untuk enkripsi/dekripsi pesan mudah dilakukan.
  2. Secara komputasi hampir tidak mungkin (*infeasible*) menurunkan kunci privat, *d*, bila diketahui kunci publik, *e*.

- Pembangkitan sepasang kunci pada kriptografi kunci-publik didasarkan pada persoalan *integer* klasik sebagai berikut:

  1. **Pemfaktoran**

     Diberikan bilangan bulat *n*. Faktorkan *n* menjadi faktor primanya

     Contoh: 31 x 47 = 1457

     1457 = ? x ?

     10 = 2 * 5

     60 = 2 * 2 * 3 * 5

     252601 = 41 * 61 * 101

     $2^{13} - 1$ = 3391 * 23279 * 65993 * 1868569 * 106681813286820 7

  Semakin besar *n*, semakin sulit memfaktorkan (butuh waktu sangat lama). Algoritma yang menggunakan prinsip ini: *RSA*

2. **Logaritma diskrit**

Temukan x sedemikian sehingga

$a^x \equiv b \pmod{n}$ → sulit dihitung

Contoh: jika $3^x \equiv 15 \pmod{17}$ maka x = 6

Semakin besar a, b, dan n semakin sulit memfaktorkan (butuh waktu lama).

Algoritma yang menggunakan prinsip ini: ElGamal, *DSA*

Catatan: Persoalan logaritma diskrit adalah kebalikan dari persoalan perpangkatan modular:

$a^x \bmod n$ → mudah dihitung

- Analogi kriptografi kunci-simetri dan kriptografi kunci-publik dengan kotak surat yang dapat dikunci dengan gembok.
- Kriptografi kunci-simetri: Alice dan Bob memiliki kunci gembok yang sama
- Kriptografi kunci-publik: Bob mengirimi Alice gembok dalam keadaan tidak terkunci (gembok = kunci publik Bob, kunci gembok = kunci privat Bob).

Kriptografi Kunci-Simetri *vs* Kriptografi Kunci-publik

Kelebihan kriptografi kunci-simetri:

1. Proses enkripsi/dekripsi membutuhkan waktu yang singkat.
2. Ukuran kunci simetri relatif pendek
3. Otentikasi pengirim pesan langsung diketahui dari cipherteks yang diterima, karena kunci hanya diketahui oleh pengirim dan penerima pesan saja.

Kelemahan kriptografi kunci-simetri:

1. Kunci simetri harus dikirim melalui saluran yang aman. Kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci ini.
2. Kunci harus sering diubah, mungkin pada setiap sesi komunikasi.

Kelebihan kriptografi kunci-publik:

1. Hanya kunci privat yang perlu dijaga kerahasiaannya oleh seiap entitas yang berkomuniaksi. Tidak ada kebutuhan mengirim kunci kunci privat sebagaimana pada sistem simetri.
2. Pasangan kunci publik/kunci privat tidak perlu diubah, bahkan dalam periode waktu yang panjang.
3. Dapat digunakan untuk mengamankan pengiriman kunci simetri.
4. Beberapa algoritma kunci-publik dapat digunakan untuk memberi tanda tangan digital pada pesan

Kelemahan kriptografi kunci-publik:

1. Enkripsi dan dekripsi data umumnya lebih lambat daripada sistem simetri, karena enkripsi dan dekripsi menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar.

2. Ukuran cipherteks lebih besar daripada plainteks (bisa dua sampai empat kali ukuran plainteks).

3. Ukuran kunci relatif lebih besar daripada ukuran kunci simetri.

4. Karena kunci publik diketahui secara luas dan dapat digunakan setiap orang, maka cipherteks tidak memberikan informasi mengenai otentikasi pengirim.

5. Tidak ada algoritma kunci-publik yang terbukti aman (sama seperti *block cipher*).

   Kebanyakan algoritma mendasarkan keamanannya pada sulitnya memecahkan persoalan-persoalan aritmetik (pemfaktoran, logaritmik, dsb) yang menjadi dasar pembangkitan kunci.

Aplikasi Kriptografi Kunci-Publik

- Meskipun masih berusia relatif muda (dibandingkan dengan algoritma simetri), tetapi algoritma kunci-publik mempunyai aplikasi yang sangat luas:

  1. **Enkripsi/dekripsi pesan**

     Algoritma: *RSA*, *Rabin*, *ElGamal*

  2. ***Digital signatures***

     Tujuan: membuktikan otentikasi pesan/pengirim

     Algoritma: *RSA*, *ElGamal*, *DSA*, *GOST*

  3. **Pertukaran kunci (*key exchange*)**

     Tujuan: mempertukarkan kunci simetri

     Algoritma: Diffie-Hellman

Algoritma RSA

Pendahuluan

- Algoritma kunci-publik yang paling terkenal dan paling banyak aplikasinya.
- Ditemukan oleh tiga peneliti dari *MIT* (*Massachussets Institute of Technology*), yaitu Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976.
- Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.

Properti Algoritma RSA

1. p dan q bilangan prima (rahasia)
2. $n = p \cdot q$ (tidak rahasia)
3. $\phi(n) = (p - 1)(q - 1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)

   Syarat: PBB(e, $\phi(n)$) = 1
5. d (kunci dekripsi) (rahasia)

   d dihitung dari $d \equiv e^{-1} \bmod (\phi(n))$
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

Enkripsi

1. Nyatakan pesan menjadi blok-blok plainteks: m_1, m_2, m_3, … (syarat: $0 < m_i < n - 1$)

2. Hitung blok cipherteks c_i untuk blok plainteks p_i dengan persamaan

$$c_i = m_i^e \textbf{ mod } n$$

yang dalam hal ini, e adalah kunci publik.

Dekripsi

Proses dekripsi dilakukan dengan menggunakan persamaan

$$m_i = c_i^d \textbf{ mod } n,$$

yang dalam hal ini, d adalah kunci privat.

Contoh:

- Misalkan dipilih $p = 47$ dan $q = 71$ (keduanya prima), maka dapat dihitung:

  $n = p \times q = 3337$

  $\phi(n) = (p - 1) \times (q - 1) = 3220.$

- Pilih kunci publik $e = 79$ (yang relatif prima dengan 3220 karena pembagi bersama terbesarnya adalah 1).

- Nilai e dan n dapat dipublikasikan ke umum.

- Selanjutnya akan dihitung kunci privat d dengan kekongruenan:

$$e \times d \equiv 1 \pmod{\phi(n)}$$

atau

$$d = \frac{1 + (k \times 3220)}{79}$$

Dengan mencoba nilai-nilai k = 1, 2, 3, …, diperoleh nilai d yang bulat adalah 1019. Ini adalah kunci privat (untuk dekripsi).

- Misalkan plainteks M = ‘HARI INI’
  atau dalam ASCII: 726582732737873

  Pecah M menjadi blok yang 3 digit:

  $m_1 = 726$ $\quad\quad$ $m_4 = 273$

  $m_2 = 582$ $\quad\quad$ $m_5 = 787$

  $m_3 = 733$ $\quad\quad$ $m_6 = 003$

  (Perhatikan, m_i masih terletak antara 0 sampai $n - 1 = 3337$)

- *Enkripsi setiap blok:*

  $c_1 = 726^{79} \bmod 3337 = 215$

  $c_2 = 582^{79} \bmod 3337 = 776$

  dst

  Hasil: C = 215 776 1743 933 1731 158.

- *Dekripsi (menggunakan kunci privat d = 1019)*

  $m_1 = 215^{1019} \bmod 3337 = 726$

  $m_2 = 776^{1019} \bmod 3337 = 582$

  dst untuk sisi blok lainnya

  Plainteks M = 726582733273873

  yang dalam ASCII adalah ‘HARI INI’.