Kriptografi Kunci-Publik

Bahan Kuliah

IF4020 Kriptografi

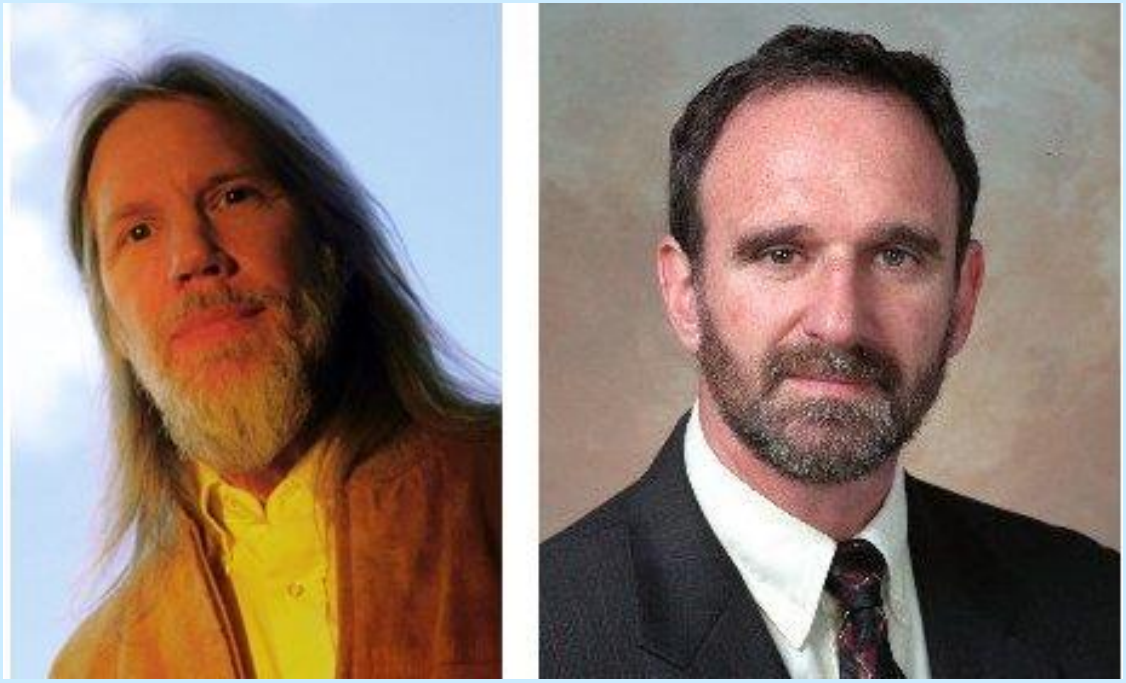
Pendahuluan

- 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.

- Ide kriptografi kunci-nirsimetri (*asymmetric-key cryptography*) muncul pada tahun 1976.

- Makalah pertama perihal kriptografi kunci-publik ditulis oleh Diffie-Hellman (ilmuwan dari Stanford University) di IEEE
- Judul makalahnya "*New Directions in Cryptography*".

- Namun pada saat itu belum ditemukan algoritma kriptografi kunci-nirsimetri yang sesungguhnya.

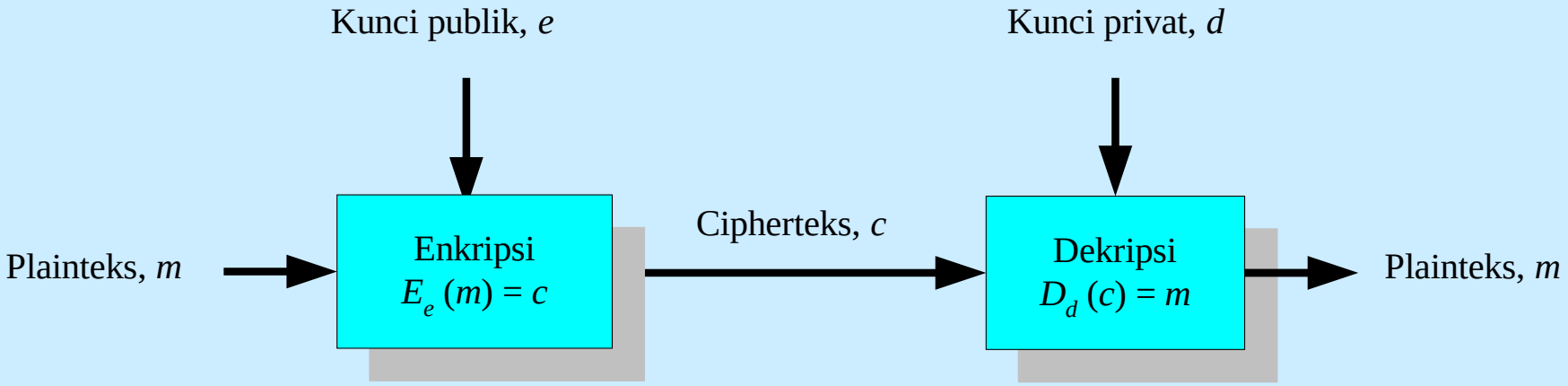


Gambar Whitfield Diffie dan Martin Hellman, penemu kriptografi kunci-publik

- Kriptografi kunci-nirsimetri disebut juga kriptografi kunci-public jika kunci untuk enkripsi dibuat public.
- Pada kriptografi kunci-publik, masing-masing pengirim dan penerima mempunyai sepasang kunci:

  1. Kunci publik: untuk mengenkripsi pesan

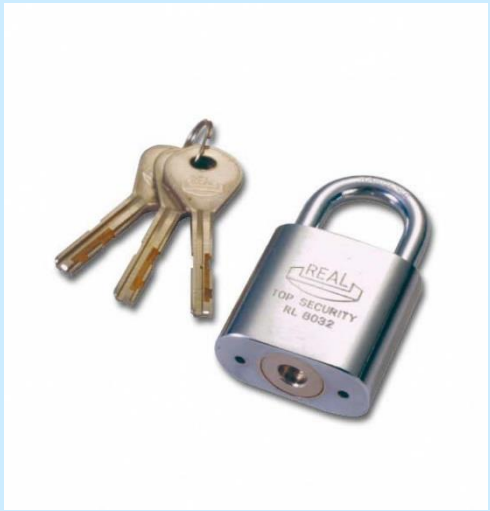
  2. Kunci privat: untuk mendekripsi pesan.
- $E_e(m) = c$ dan $D_d(c) = m$



- 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

- Idenya mirip dengan mengirim surat menggunakan kotak yang dapat dikunci dengan gembok.



- Misalkan Alice dan Bob akan berkirim surat dengan sistem kriptografi kunci publik. Analoginya adalah sbb:

- Alice mengirimkan kotak surat dengan gembok dalam keadaan terbuka. Kunci gembok dipegang oleh Alice.

Gembok terbuka = kunci publik Alice

Kunci gembok = kunci privat Alice

- Bob memasukkan surat ke dalam kotak, lalu menekan gembok sehingga terkunci.

  Surat di dalam kotak = mengenkripsi surat

  Kotak digembok dengan kunci publik Alice

- Alice menerima kotak surat yang telah terkunci dari Bob.
- Alice membuka kotak surat dengan kunci yang dimilikinya.

Kunci gembok = kunci privat Alice

Membuak kotak surat dengan kunci = mendekripsi surat

- Hal yang sama dilakukan Bob jika membalas/mengirim surat kepada Alice.

- Bob mengirimkan kotak surat dengan gembok dalam keadaan terbuka. Kunci gembok dipegang oleh Bob.

Gembok terbuka = kunci publik Bob

Kunci gembok = kunci privat Bob

- Alice memasukkan surat ke dalam kotak, lalu menekan gembok sehingga terkunci.

  Surat di dalam kotak = mengenkripsi surat

  Kotak digembok dengan kunci publik Bob

- Bob menerima kotak surat yang telah terkunci dari Alice.
- Bob membuka kotak surat dengan kunci yang dimilikinya.

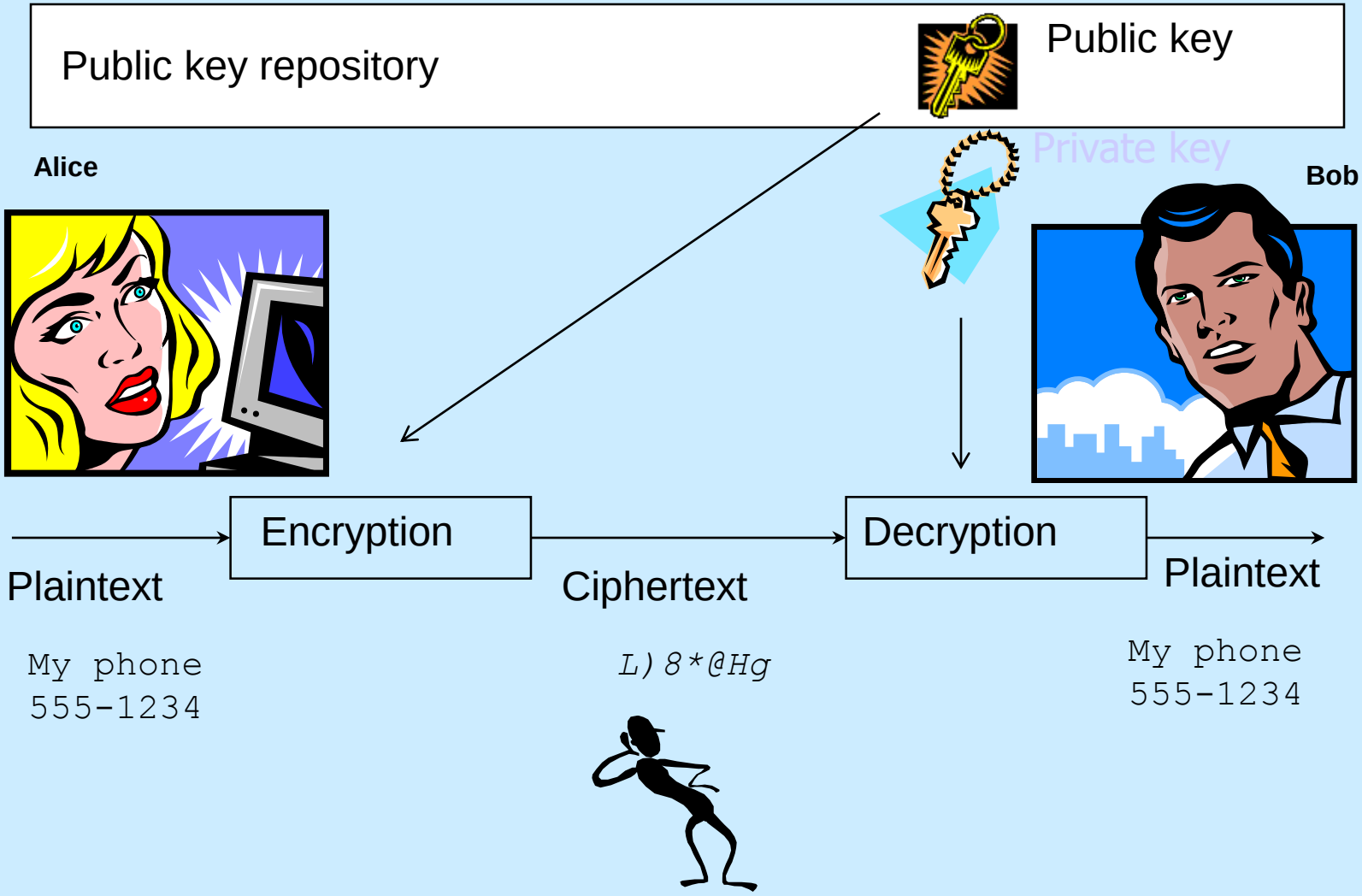
Kunci gembok = kunci privat Bob

Membuka kotak surat dengan kunci = mendekripsi surat

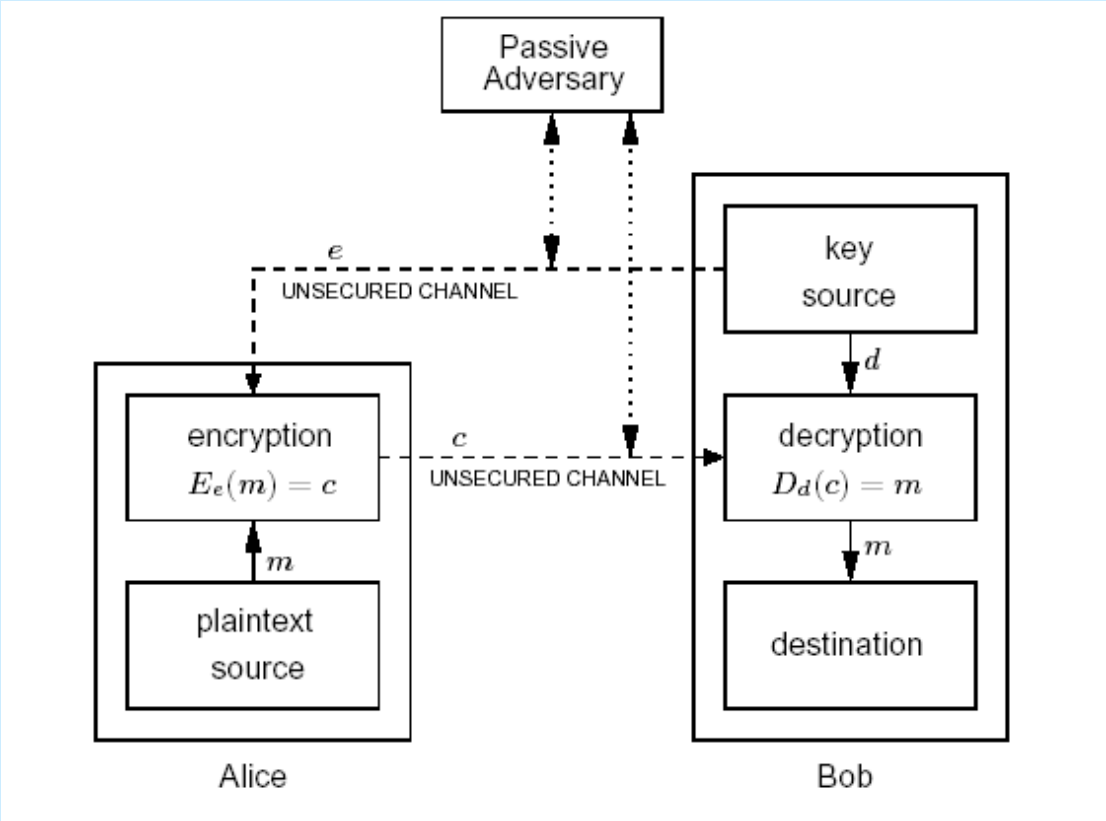
- Alice dan Bob sudah berkomunikasi dengan system kriptografi kunci-publik.

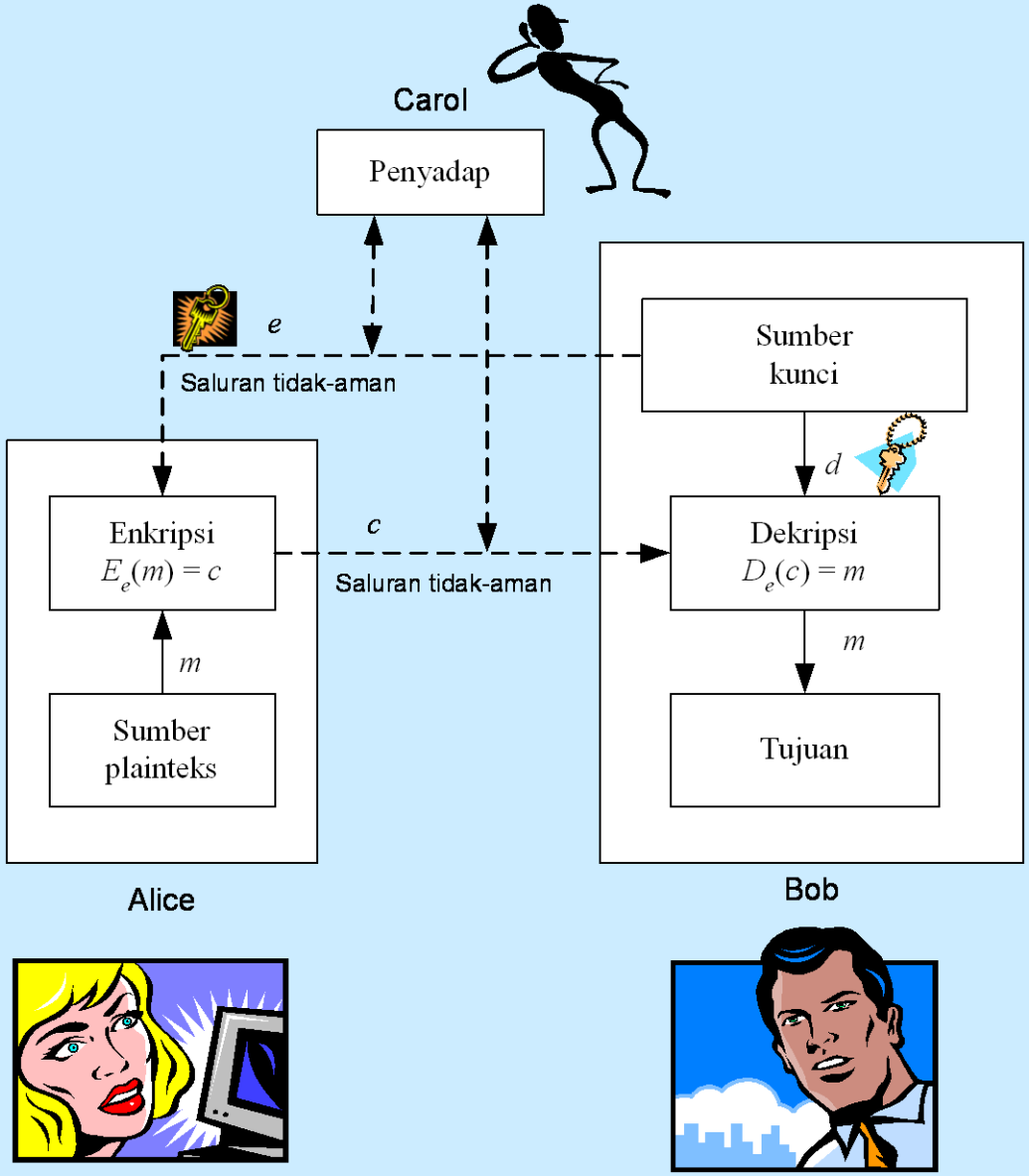
Kriptografi Kunci-publik

(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 factor-faktor primanya

     Contoh: $n = 10 = 2 * 5$

     $n = 60 = 2 * 2 * 3 * 5$

     $n = 252601 = 41 * 61 * 101$

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

  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*

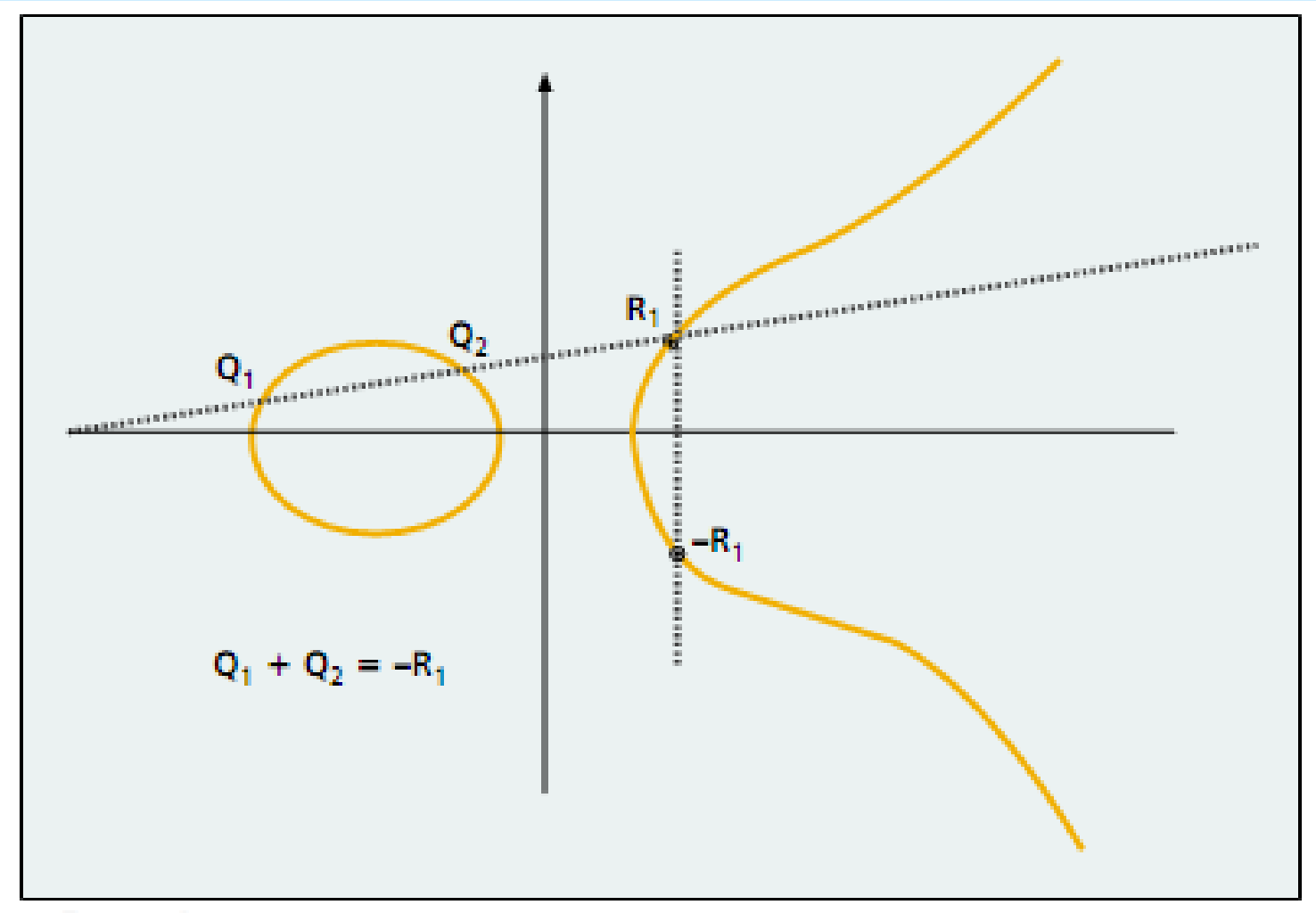
Catatan: Persoalan logaritma diskrit adalah kebalikan dari persoalan perpangkatan modular:

$a^x \bmod n$ → mudah dihitung

3. ***Elliptic Curve Discrete Logarithm Problem (ECDLP)***

Diberikan P dan Q adalah dua buah titik di kurva eliptik, carilah integer n sedemikian sehingga $P = n\,Q$

Algoritma yang menggunakan prinsip ini: *Elliptic Curve Cryptography* (ECC)


Q_1
Q_2
R_1
$-R_1$
$Q_1 + Q_2 = -R_1$

- 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 (akan dijelaskan pada materi kuliah selanjutnya)

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* , *ECC*

  2. ***Digital signatures***

     Tujuan: membuktikan otentikasi pesan/pengirim

     Algoritma: *RSA*, *ElGamal*, *DSA*, *ECC*

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

     Tujuan: mempertukarkan kunci simetri

     Algoritma: Diffie-Hellman