Bahan kuliah IF4020 Kriptografi

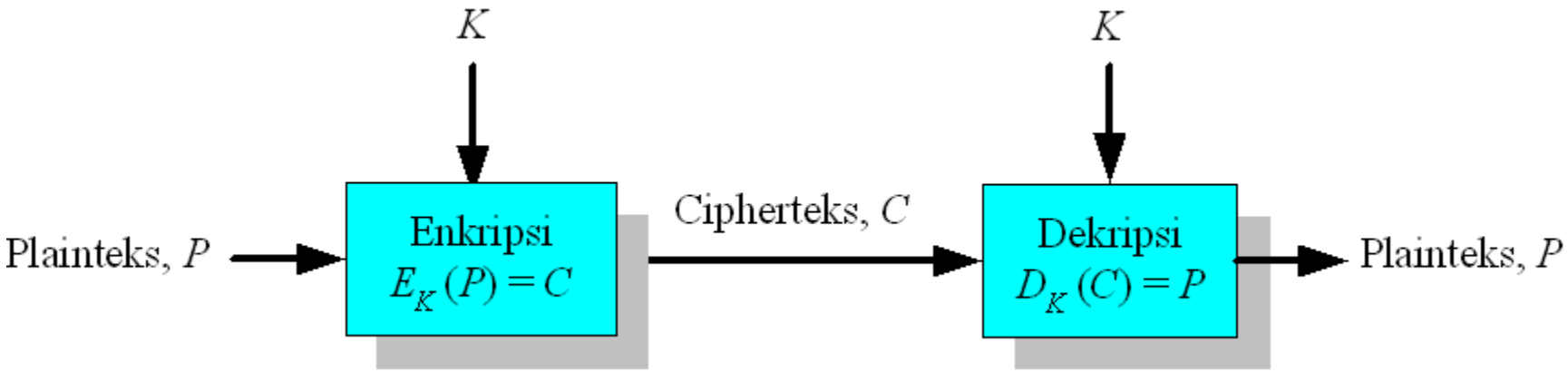
Kriptografi Kunci-Publik

Oleh: Rinaldi Munir

Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2024

Pendahuluan

- Sebelum pertengahan tahun 1970-an, hanya ada sistem kriptografi kunci-simetri.
- Pengirim dan penerima pesan memiliki kunci rahasia (K) yang sama untuk enkripsi dan dekripsi.
- $E_K(P) = C$ dan $D_K(C) = P$



- Satu masalah dalam sistem kriptografi kunci-simetri: bagaimana cara berbagi kunci rahasia K kepada penerima pesan?

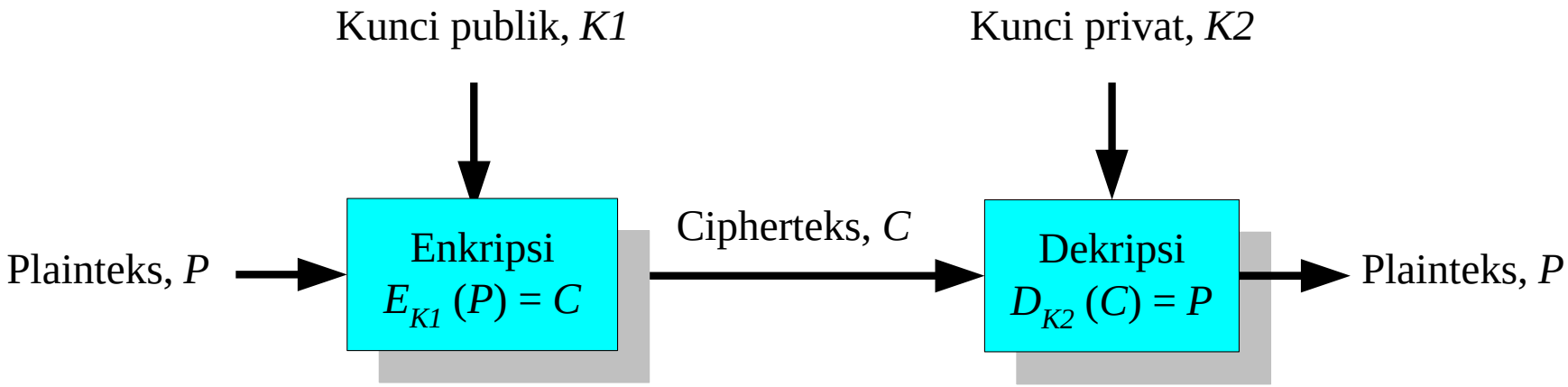
- Mengirim kunci privat pada saluran publik (telepon, internet, pos) sangat tidak aman.

- Oleh karena itu, kunci privat harus dikirim melalui saluran kedua yang benar-benar aman.

- Namun saluran kedua tersebut umumnya lambat dan mahal.

- Ide **kriptografi kunci-publik** (*public-key cryptography*) muncul tahun 1976.

- Pengirim dan penerima mempunyai sepasang kunci:
  1. Kunci publik (K1): untuk mengenkripsi pesan
  2. Kunci privat (K2): untuk mendekripsi pesan.



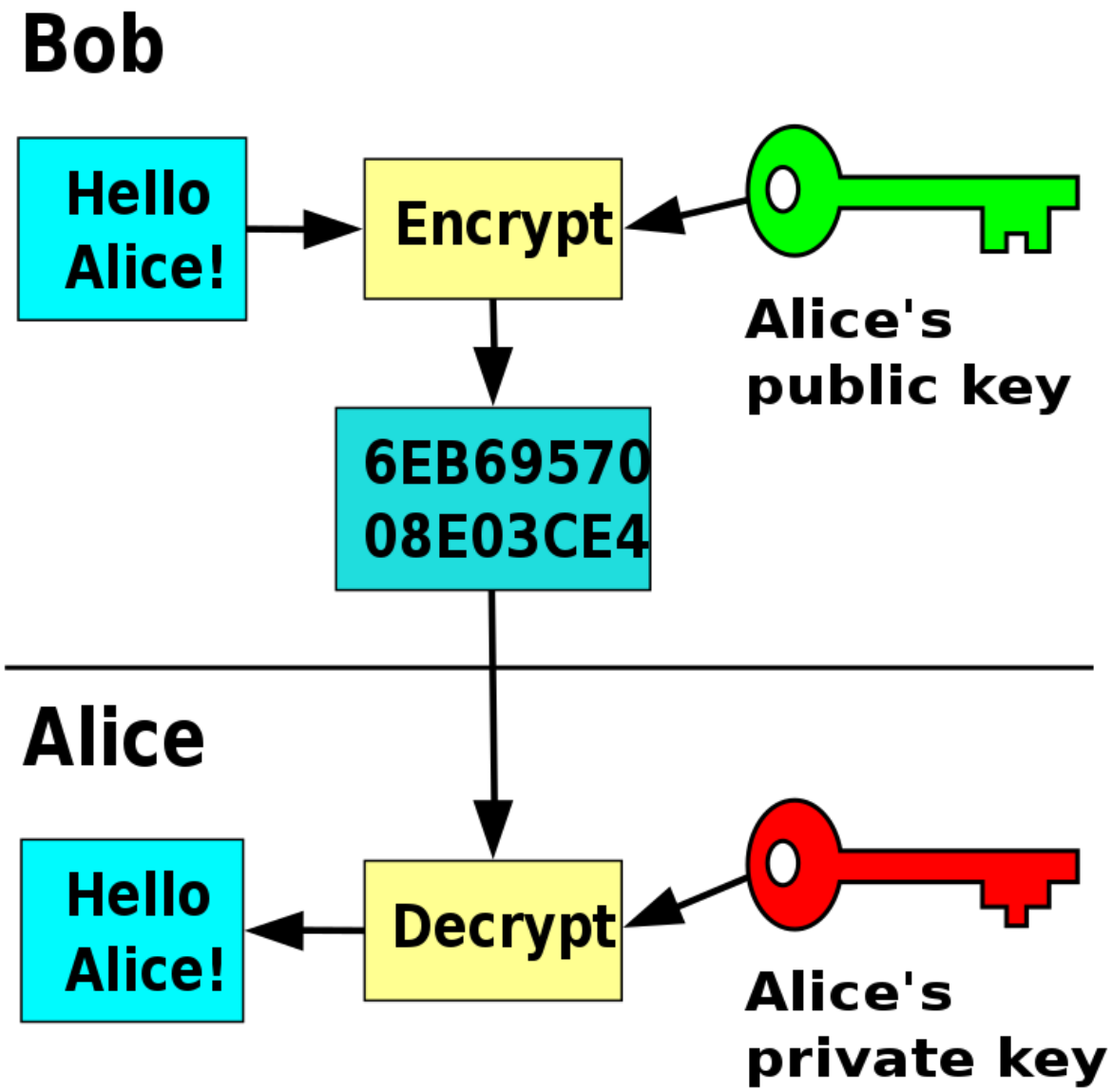
- $E_{K1}(P) = C$ dan $D_{K2}(C) = P$

- Misalkan: Pengirim pesan: Bob
  Penerima pesan: Alice

- Bob mengenkripsi pesan dengan kunci publik Alice
  Alice mendekripsi cipherteks dari Bob dengan kunci privatnya sendiri (kunci privat Alice)

- Jika Alice membalas pesan Bob, maka Alice mengenkripsi pesan dengan kunci publik Bob
  Bob mendekripsi pesan dari Bob dengan kunci privatnya (kunci privat Bob)

- Dengan mekanisme seperti ini, tidak ada kebutuhan mengirim kunci privat masing-masing seperti halnya pada sistem kriptografi kunci-simetri



Sumber gambar: Wikipedia

- Kriptografi kunci-publik disebut juga **kriptografi kunci-nirsimetri** (*asymmetric-key cryptography*) karena kunci enkripsi tidak sama dengan kunci dekripsi.

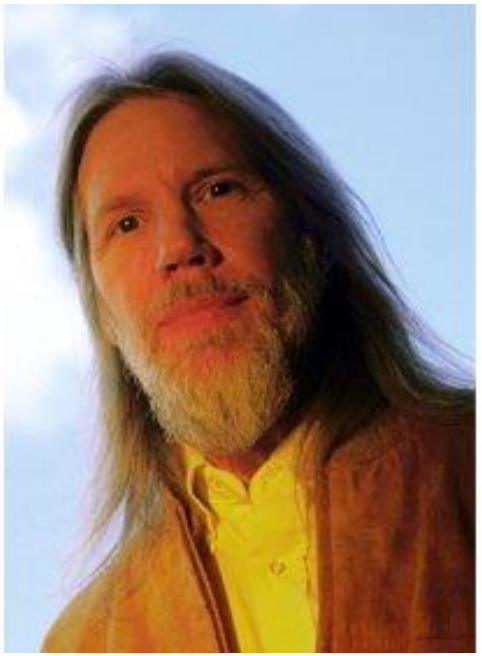
- Istilah “publik” muncul karena kunci untuk enkripsi diumumkan kepada publik (tidak rahasia), misalnya disimpan di dalam repositori yang dapat diakses oleh publik.

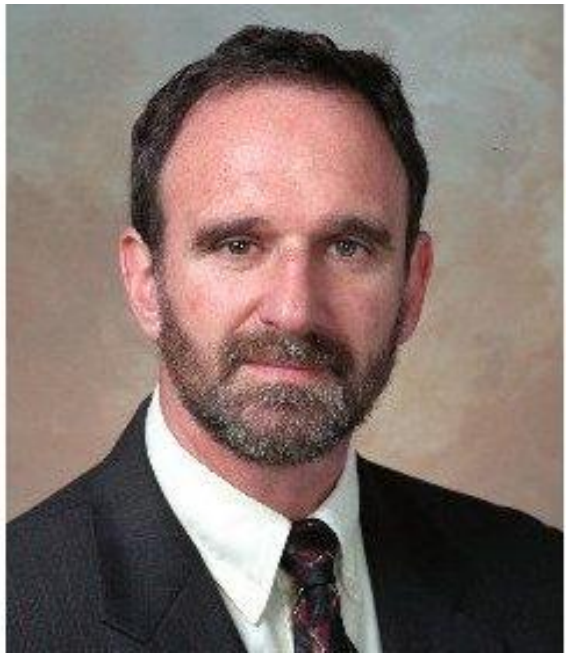
- Hanya kunci privat yang rahasia, hanya pemilik kunci privat yang mengetahui kuncinya sebdiri.

Sejarah Kriptografi Kunci-Publik

- Makalah pertama perihal kriptografi kunci-publik ditulis oleh Whitfield Diffie (kiri) dan Martin E. Hellman (kanan) di IEEE pada tahun 1976.

- Keduanya adalah ilmuwan dari Stanford University dan merupakan penemu konsep kriptografi kunci-publik.





- Judul makalahnya "*New Directions in Cryptography*". Namun di dalam makalah tersebut belum didefinsikan algoritma kriptografi kunci-publik yang sesungguhnya.

New Directions in Cryptography

Invited Paper

Whitfield Diffie and Martin E. Hellman

Abstract Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

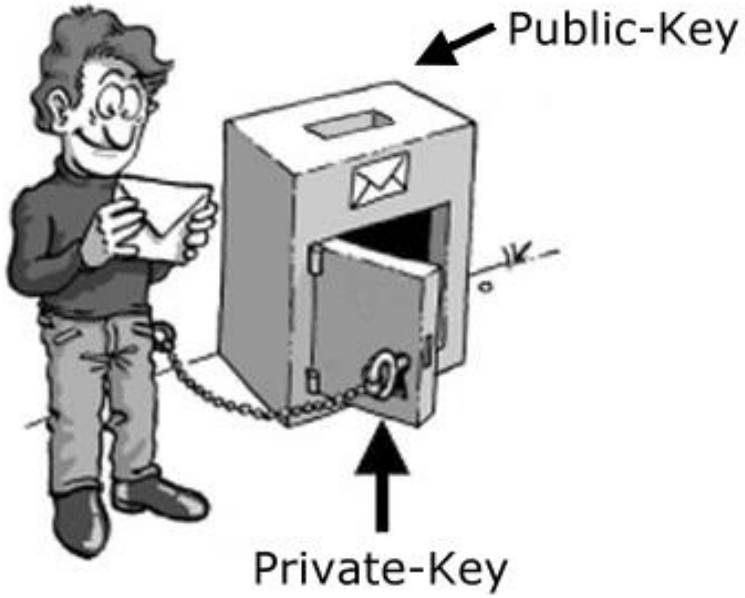
1 INTRODUCTION

We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where

communications over an insecure channel order to use cryptography to insure privacy, however, it currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such a private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channel without compromising the security of the system. In *public key cryptosystem* enciphering and deciphering are governed by distinct keys, *E*

Analogi Kriptografi Kunci-Publik



- Analogi yang lain tentang kriptografi kunci-publik adalah seperti kotak surat di depan rumah atau PO Box di kantor pos, yang dapat dikunci.

- Alamat kotak surat = kunci publik

  Kunci kotak surat = kunci privat

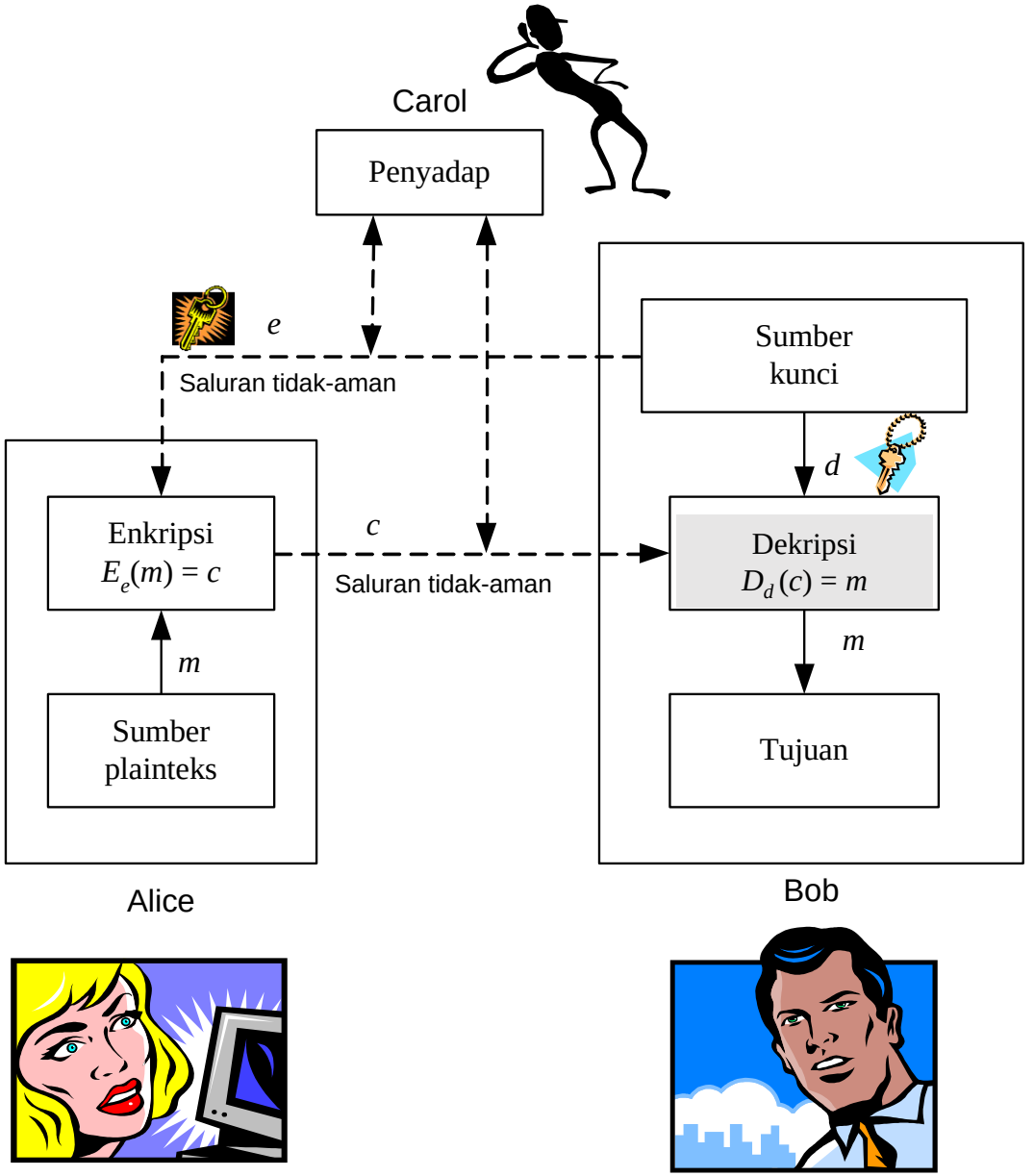
- Siapapun dapat memasukkan surat ke dalam kotak surat atau PO Box. Namun hanya pemilik kotak surat atau PO Box yang dapat membukanya

PO Box

- Kunci publik 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.

- Pihak lawan/kriptanalis dapat menyadap cipherteks dan kunci publik, tetapi tidak dapat mendekripsi cipherteks karena ia tidak mengetahui kunci privat.



- Dua keuntungan kriptografi kunci-publik:
  1. Tidak diperlukan pengiriman kunci privat (kunci rahasia)

     Setiap orang memiliki kunci privat masing-masing
  2. Jumlah kunci dapat ditekan

     Setiap orang hanya perlu memiliki sepasang kunci saja (privat dan publik), kunci publik orang lain dapat diketahui dari repositori publik.

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

- Algoritma kriptografi kunci-publik didasarkan pada beberapa persoalan *integer* klasik yang sulit dipecahkan sebagai berikut:

  1. **Pemfaktoran**

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

     Contoh: $n = 10 = 2 \times 5$

     $n = 60 = 2 \times 2 \times 3 \times 5$

     $n = 252601 = 41 * 61 * 101$

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

  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 $x \equiv {}^3\log 15 \pmod{17} = 6$

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:

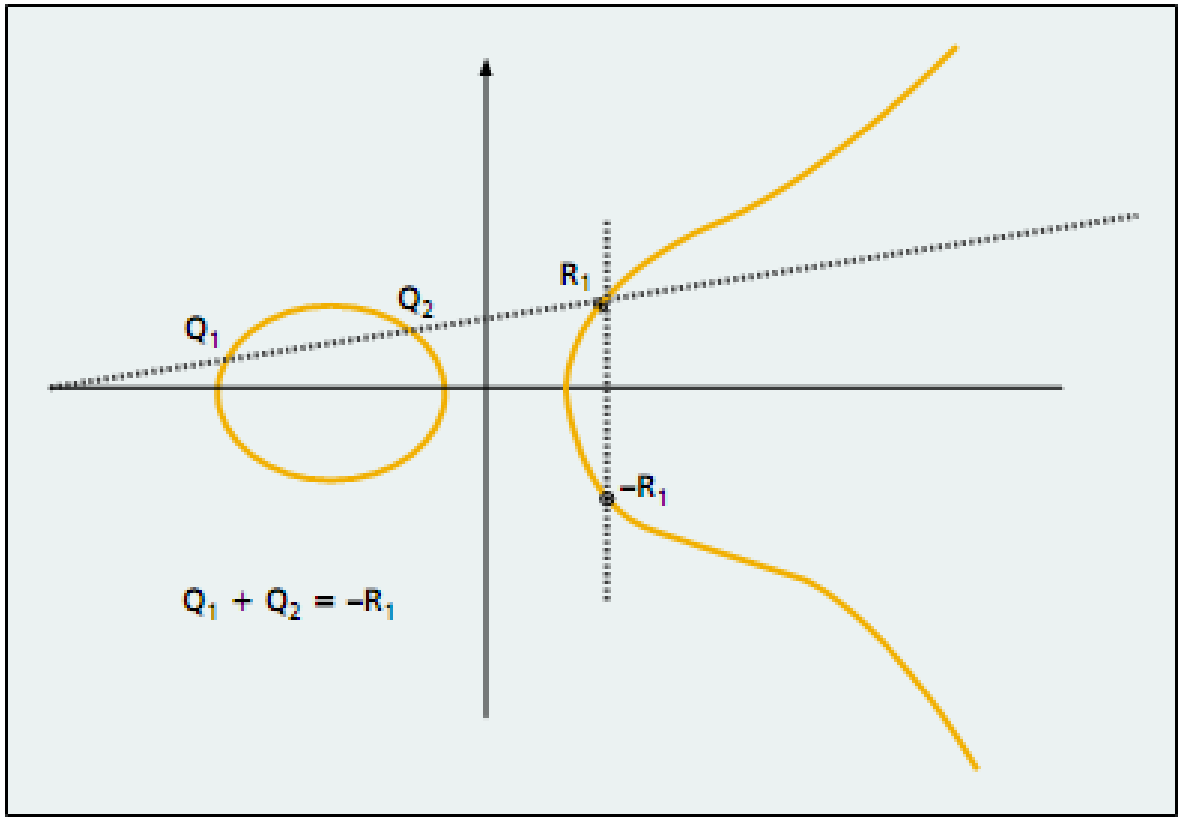
$b = a^x \bmod n$ → perpangkatan modular, b mudah dihitung

$a^x \equiv b \pmod{n}$, x = ? → logaritma diskrit, x sulit 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)



4. *Knapsack problem*

Diberikan bobot *knapsack* adalah M. Diketahui n buah objek yang masing-masing bobotnya adalah $w_1, w_2, \ldots, w_n$. Tentukan nilai b_i sedemikian sehingga

$$M = b_1w_1 + b_2w_2 + \ldots + b_nw_n$$

yang dalam hal ini, b_i bernilai 0 atau 1. Jika $b_i = 1$, berarti objek i dimasukkan ke dalam *knapsack*, sebaliknya jika $b_i = 0$, objek i tidak dimasukkan.

5.* Persamaan *diophantine

Diberikan persamaan *diophantine* linier $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$, tentukan solusi integer non-negatif untuk persamaan tersebut. Untuk sistem persamaan *diophantine* yang berbentuk polinom, persolan tersebut termasuk NP-complete.

Kriptografi Kunci-Simetri *vs* Kriptografi Kunci-publik

Kelebihan kriptografi kunci-simetri:

1. Proses enkripsi/dekripsi membutuhkan waktu yang lebih 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 dan tidak sama dengan saluran untuk pengiriman pesan. 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 setiap entitas yang berkomunikasi. Tidak ada kebutuhan mengirim kunci privat sebagaimana pada kriptografi kunci simetri.

2. Pasangan kunci public dan kunci privat tidak perlu sering 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 pesan umumnya lebih lambat daripada sistem kriptografi 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*, *Knapsack*, *ElGamal* , *Paillier*, *ECEG*

  2. ***Digital signatures***

     Tujuan: membuktikan otentikasi pesan dan pengirim

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

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

     Tujuan: berbagi kunci simetri

     Algoritma: *Diffie-Hellman*

Beberapa algoritma kriptografi kunci-publik:

- RSA (Rivest-Shamir-Adleman)
- ElGamal
- DSA
- Diffie-Hellman Key-Exchange
- Mercke-Hellman Knapsack Algorithm
- Rabin
- EPOC
- Mc Eliece cryptosystem
- XTR
- Paillier
- Kyber
- Cramer-Shoup
- Diophantine cryptosystem
- ECC (*Elliptic Curve Cryptography*)