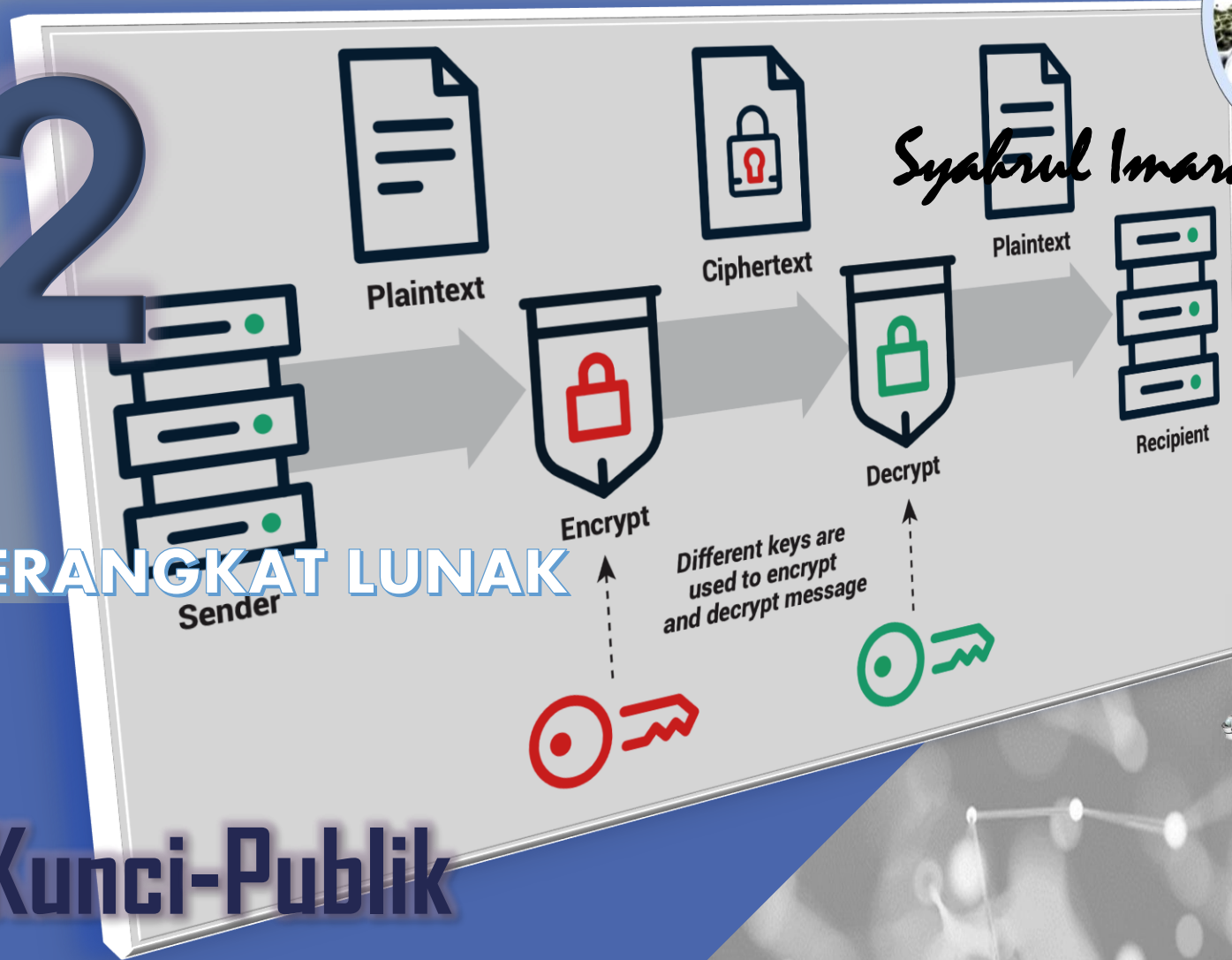


# #22

MATAKULIAH  
KEAMANAN PERANGKAT LUNAK

## Kriptografi Kunci-Publik



*Syahrul Imardi, MT*





P22



STMIK  
Amik Riau

# MATAKULIAH **KEAMANAN PERANGKAT LUNAK**

*Syahrul Imardi, MT*

*Public Key Cryptography*

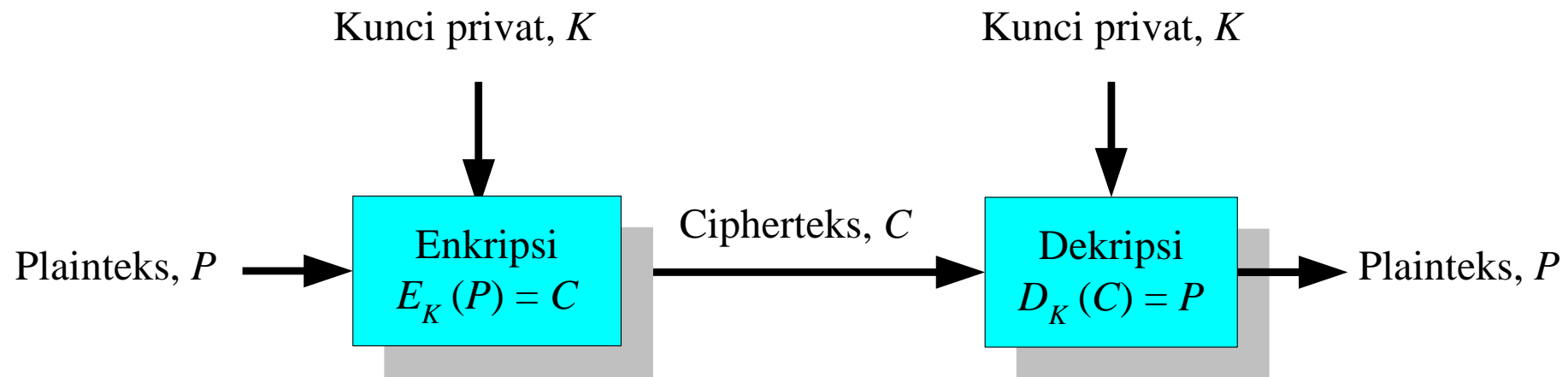
P22 : **Kriptografi Kunci-Publik**



# Kriptografi Kunci-Publik

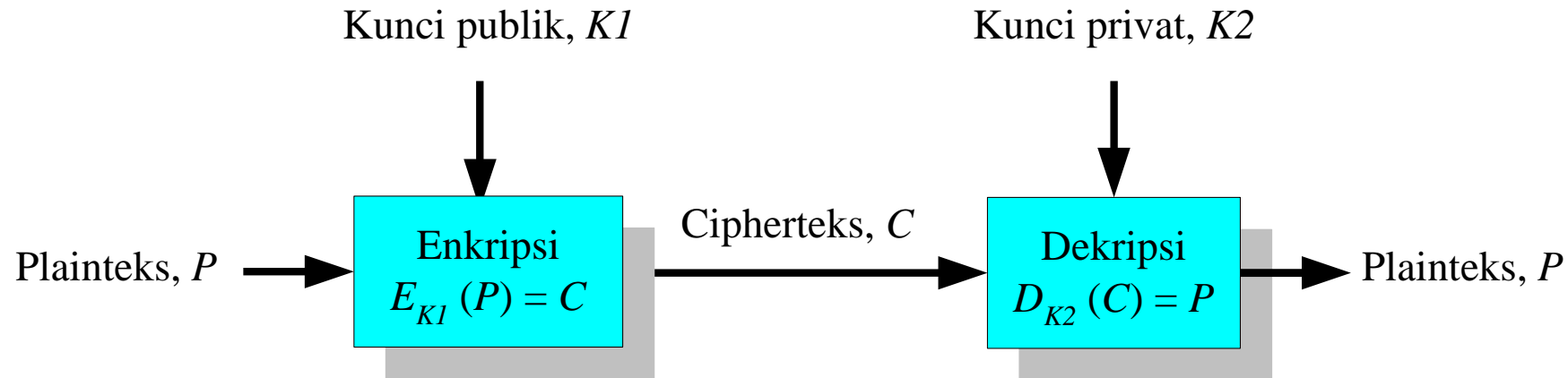
# Pendahuluan

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



- Satu masalah dalam sistem kriptografi kunci-simetri: bagaimana cara mengirim kunci rahasia (kunci privat) 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.



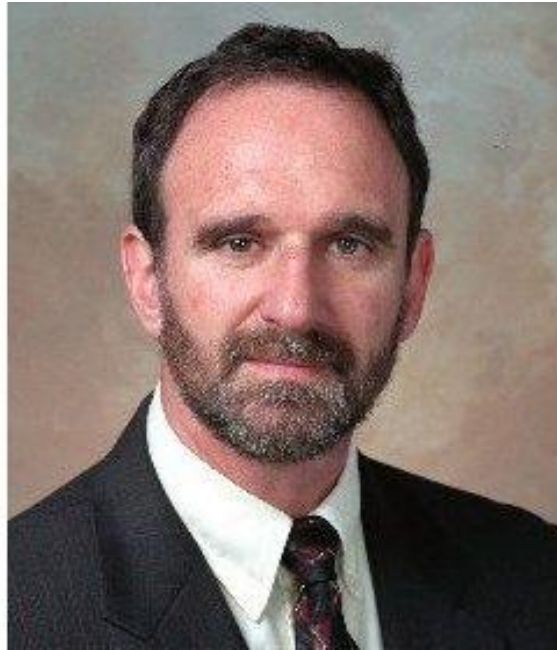
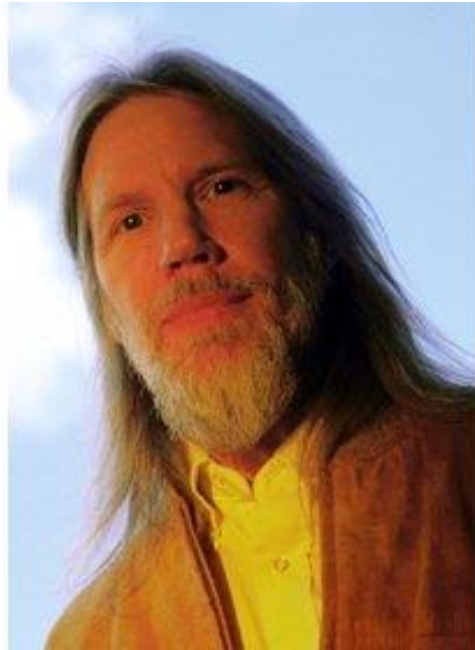
- $E_{K1}(P) = C$  dan  $D_{K2}(C) = P$

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

- 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 sendiri.



- 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 kriptografi kunci-publik.



- Judul makalahnya “*New Directions in Cryptography*”.
- Namun di dalam makalah tersebut belum didefinisikan algoritma kriptografi kunci-public 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 is 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 as 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) channels without compromising the security of the system. In *public key cryptosystems* enciphering and deciphering are governed by distinct keys,  $E$

- Ide kriptografi kunci-publik 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 mengirim kotak surat dengan gembok dalam keadaan terbuka kepada Bob. 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 = surat terenkripsi

Kotak digembok dengan kunci publik Alice

Bob mengirim kotak surat tersebut kembali kepada ALice

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



Kunci gembok = kunci privat Alice

Membuka kotak surat dengan kunci = mendekripsi surat

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

- Bob mengirim kotak surat dengan gembok dalam keadaan terbuka kepada Alice. 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 = surat terenkripsi

Kotak digembok dengan kunci publik Bob

Alice mengirim kotak surat tersebut kembali kepada Bob.

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



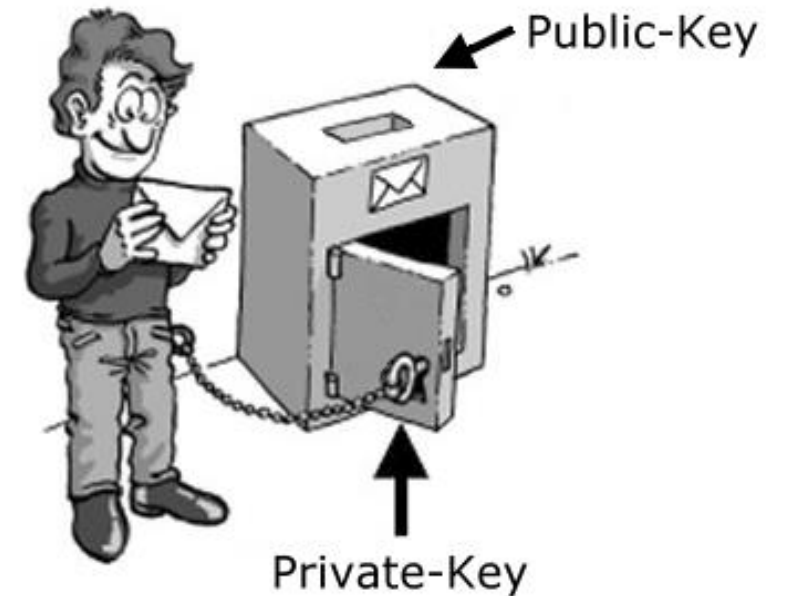
Kunci gembok = kunci privat Bob

Membuka kotak surat dengan kunci = mendekripsi surat

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



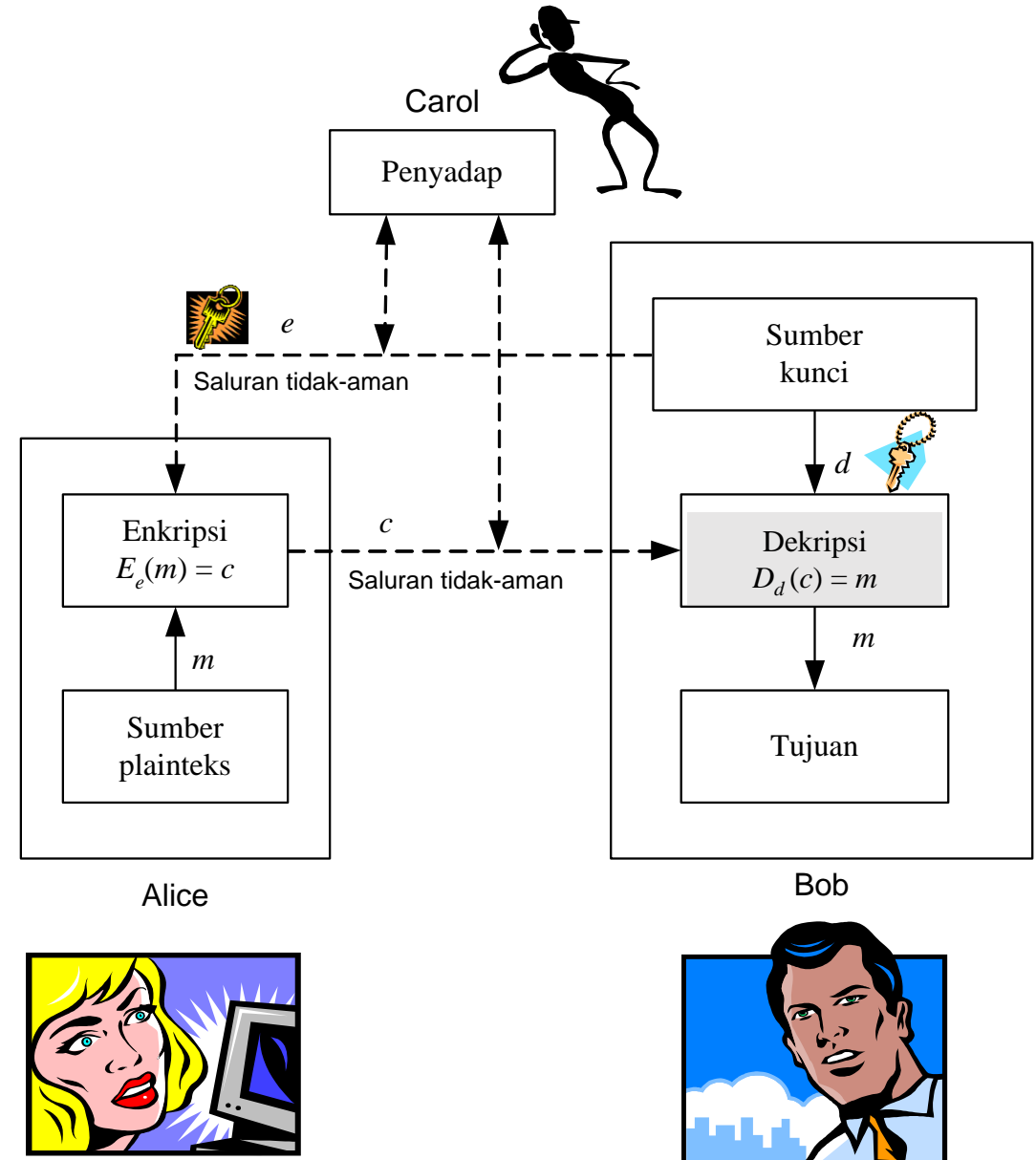
- Analogi yang lain tentang kriptografi kunci-publik adalah seperti kotak surat di depan rumah atau PO Box di kantor pos, yang dapat dikunci.
- Alamat kotak surat = kunci publik  
Kunci kotak surat = kunci privat
- Siapapun dapat memasukkan surat ke dalam kotak surat atau PO Box. Namun hanya pemilik 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  
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 persoalan *integer* klasik sebagai berikut:

## 1. Pemfaktoran

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

Contoh:  $n = 10 = 2 * 5$

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

$$n = 252601 = 41 * 61 * 101$$

$$n = 2^{13} - 1 = 3391 * 23279 * 65993 * 1868569 * \\ 1066818132868207$$

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:

$$b = a^x \pmod{n}$$

→ perpangkatan modular,  $b$  mudah dihitung

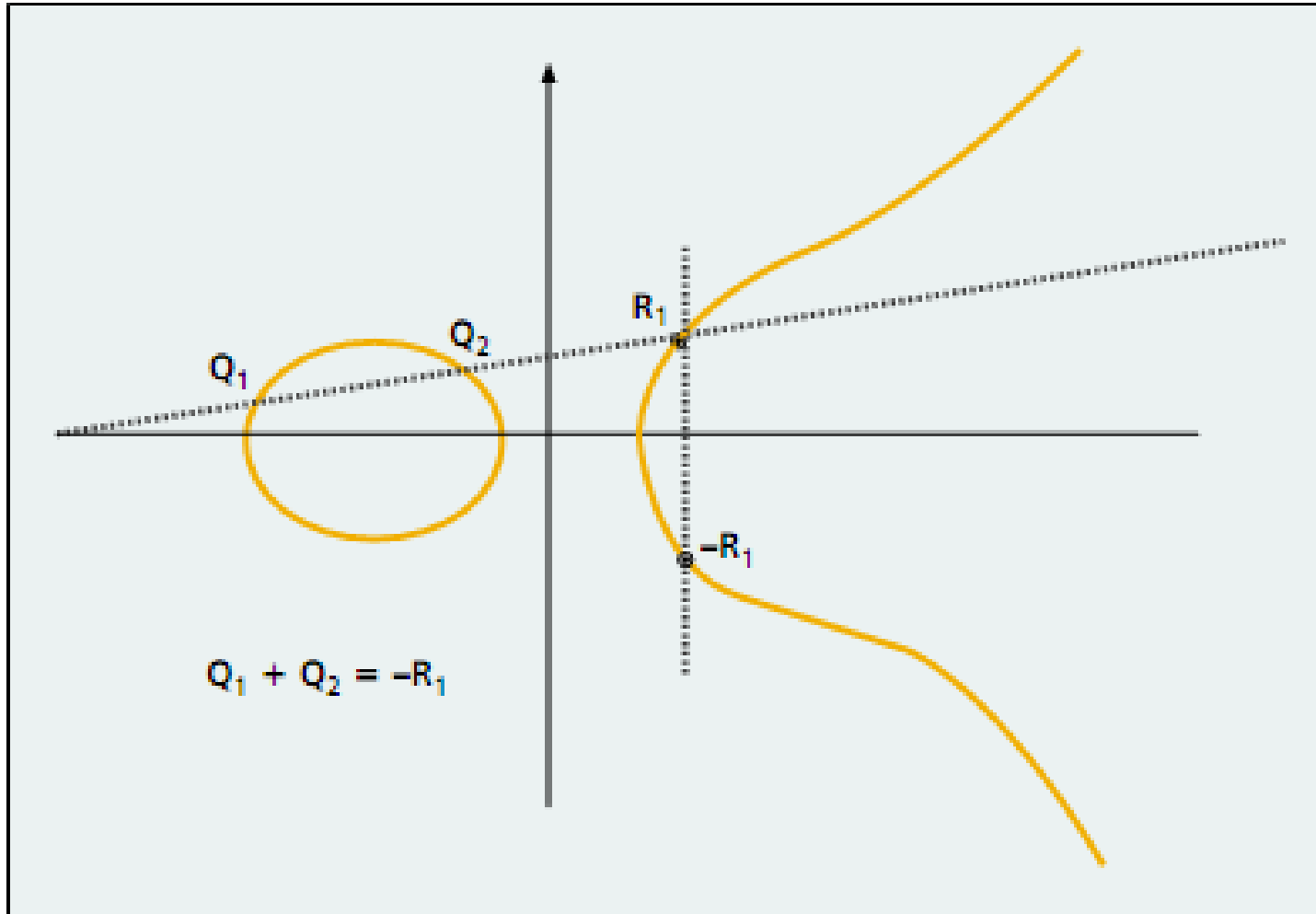
$$a^x \equiv b \pmod{n}, x = ?$$

→ 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)



# 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 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, 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

## ***Referensi utama :***

>> Michael Felderer , Riccardo Scandariato (editor) - Exploring Security in Software Architecture and Design, 2018.

>> Nancy R. Mead, Carol Woody - Cyber Security Engineering\_ A Practical Approach for Systems and Software Assurance-Addison-Wesley Professional (2016)

>> James Helfrich - Security for Software Engineers-CRC Press (2019)

>> Pete Loshin - Simple Steps to Data Encryption\_ A Practical Guide to Secure Computing-Syngress (2013)

>> Tefvik Bultan,Fang Yu,Muath Alkhalaf,Abdulbaki Aydin (auth.) - String Analysis for Software Verification and Security (2017)



Ada pertanyaan?

