Kripsografi Kunci Publik

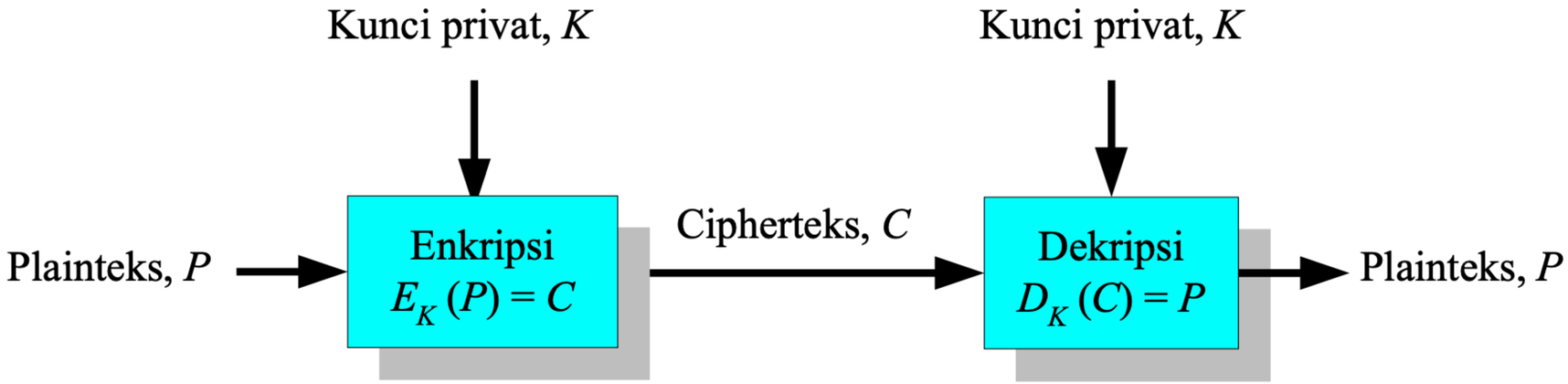
Bahan Kuliah Keamanan Data

Sevi **Nurafni**

Fakultas Sains dan Teknologi
Universitas Koperasi Indonesia 2025

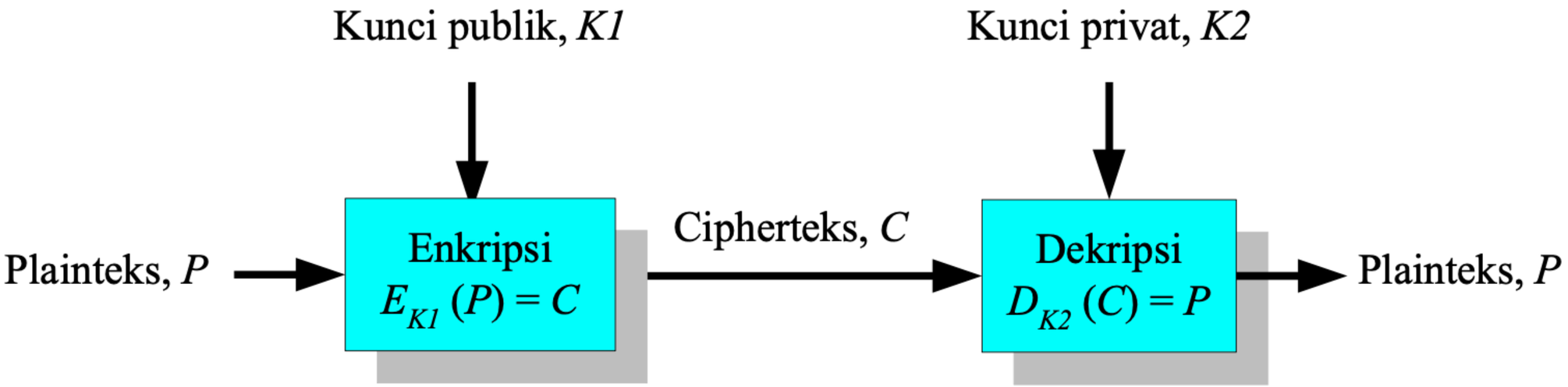
Get to Know

- Sebelum pertengahan tahun 1970-an, 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 berbagi 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.

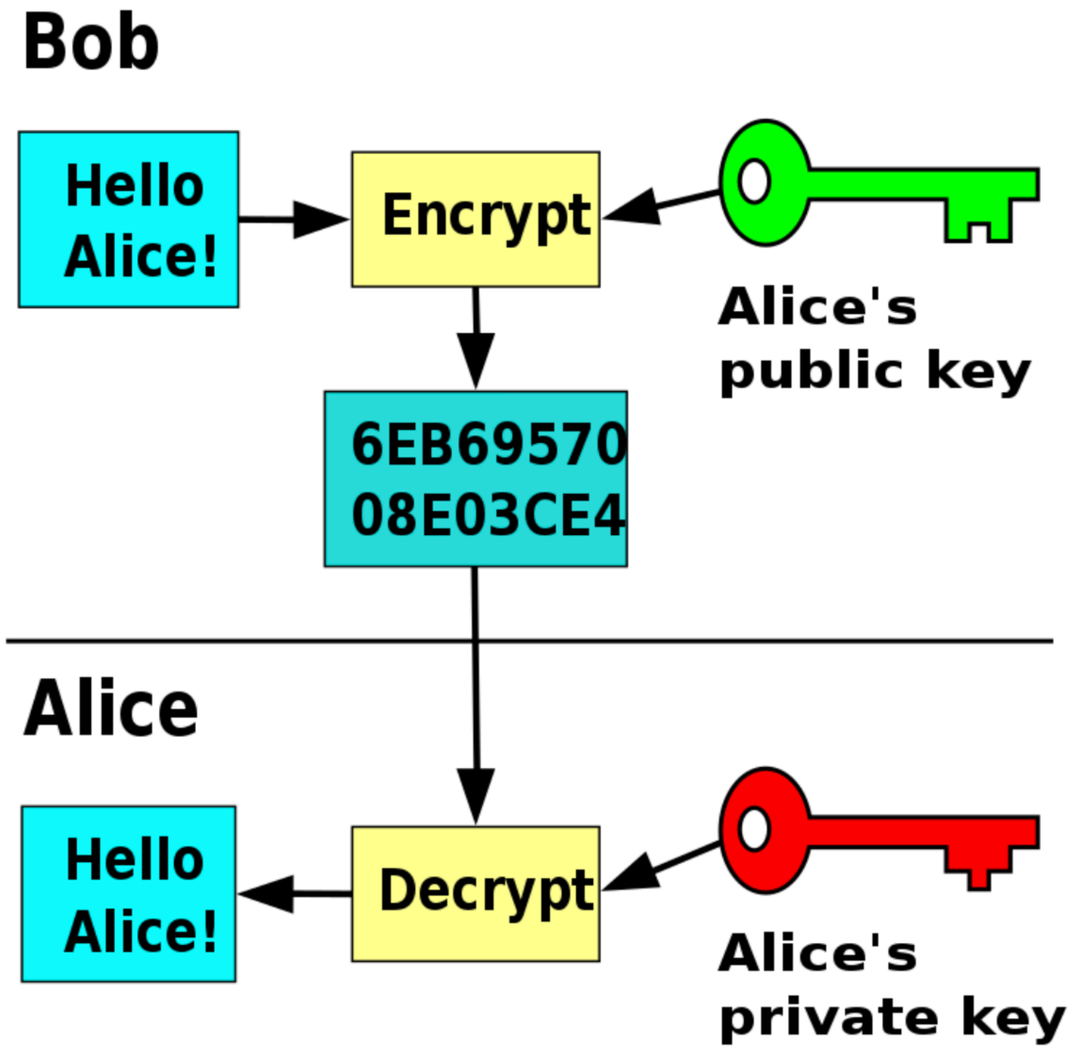
- Ide **kriptografi kunci-publik** (*public-key cryptography*) muncul tahun 1976.
- Pengirim dan penerima masing-masing mempunyai sepasang kunci:
    1. Kunci publik (K1): untuk mengenkripsi pesan
    2. Kunci privat (K2): untuk mendekripsi pesan.
- Pengirim mengenkripsi pesan dengan kunci publik si penerima pesan, $E_{K1}(P) = C$
- Penerima pesan mendekripsi cipherteks dengan kunci privatnya, $D_{K2}(C) = P$
- Kunci publik $\rightarrow$ *K1,* Kunci privat $\rightarrow$ *K2*


Kunci publik, K1
Kunci privat, K2
Plainteks, P
Enkripsi
$E_{K1}(P) = C$
Cipherteks, C
Dekripsi
$D_{K2}(C) = P$
Plainteks, 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



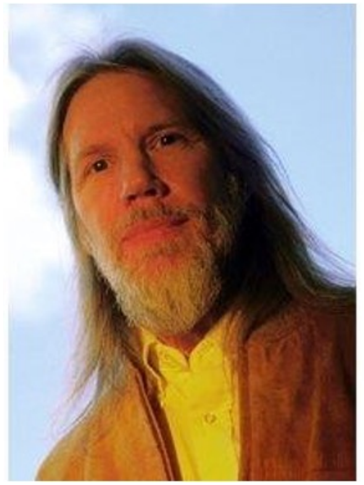
Contoh kunci publik: 45A0FB7C2

Contoh kunci privat: D12BC0FF4

Sumber gambar: Wikipedia

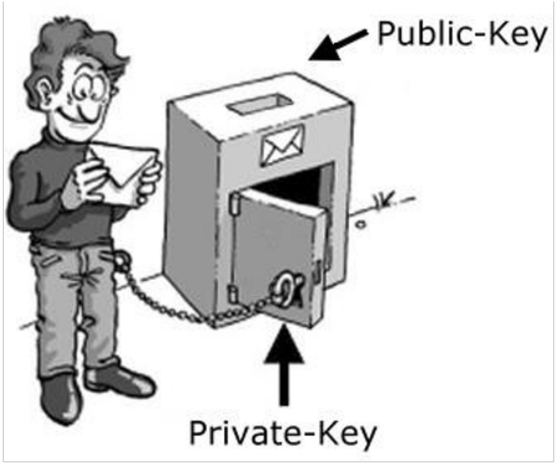
- Kriptografi kunci-publik disebut juga kriptografi kunci-nirsimetri (*asymmetric-key cryptography*) karena kunci enkripsi tidak sama dengan kunci dekripsi.
- Istilah “publik” muncul karena kunci untuk enkripsi diumumkan kepada publik (tidak rahasia), misalnya disimpan di dalam repositori yang dapat diakses oleh publik.
- Hanya kunci privat yang rahasia, hanya pemilik kunci privat yang mengetahui kuncinya 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 konsep kriptografi kunci-publik.
- Judul makalahnya “*New Directions in Cryptography*”. Namun di dalam makalah tersebut belum didefinsikan algoritma kriptografi kunci-publik yang sesungguhnya.

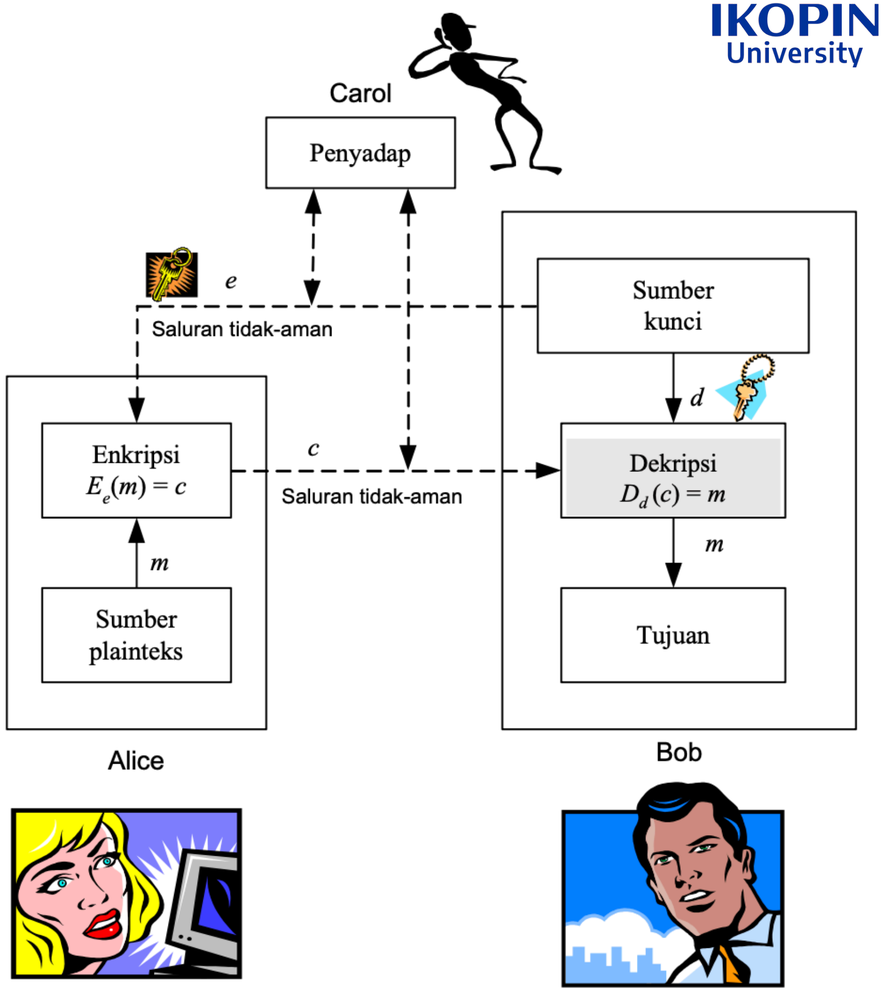


Analogi Kriptografi Kunci-Publik

- Analogi 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



- 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.



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

Pemfaktoran

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

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

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

$$n = 252601 = 41 \times 61 \times 101$$

Semakin besar n, semakin sulit memfaktorkan (butuh waktu sangat lama).

Algoritma yang menggunakan prinsip ini: *RSA*

Logaritma Diskrit

Temukan x sedemikian sehingga $a^x \equiv b(\bmod n)$

$\rightarrow$ sulit dihitung

Contoh: jika $3^x \equiv 15(\bmod 17)$ maka $x \equiv {}^3\log 15(\bmod 17) = 6$

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

Algoritma yang menggunakan prinsip ini: ElGamal, Diffie-Hellman, DSA

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

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

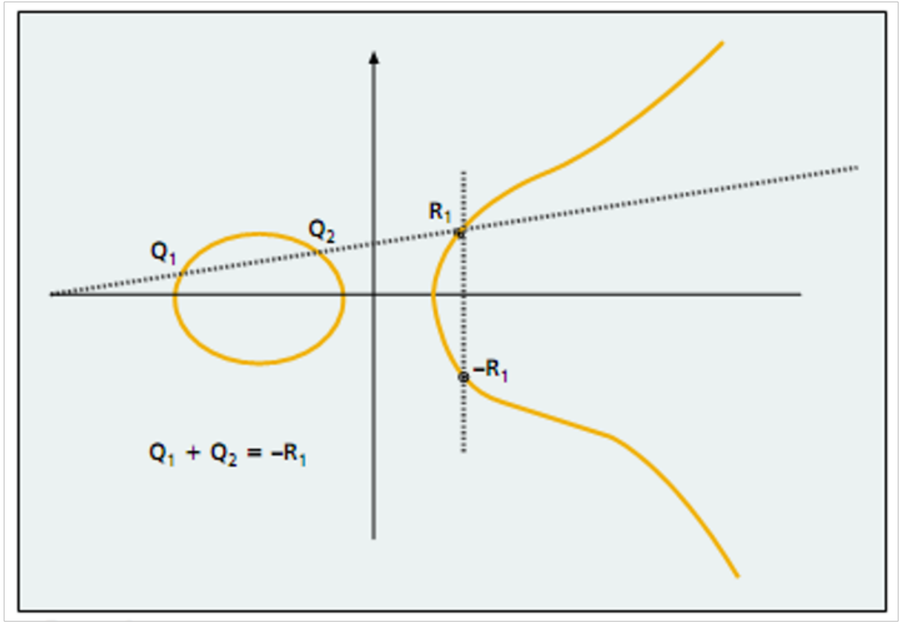
$a^x \equiv b(\bmod n), x = ?$ $\rightarrow$ logaritma diskrit, x sulit dihitung

Elliptic Curve Discrete Logarithm Problem

Diberikan *P* dan *Q* adalah dua buah titik di kurva eliptik,

carilah integer n sedemikian sehingga $P = nQ$

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



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

$$M = b_1 w_1 + b_2 w_2 + \ldots + b_n w_n$$

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.

Kriptografi Kunci-Simetri vs Kriptografi Kunci-Publik

Kelebihan Kriptografi Kunci-Simetri

- Proses enkripsi/dekripsi membutuhkan waktu yang lebih singkat.
- Ukuran kunci simetri relatif pendek
- 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 (hybrid cryptography).
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).
6. 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

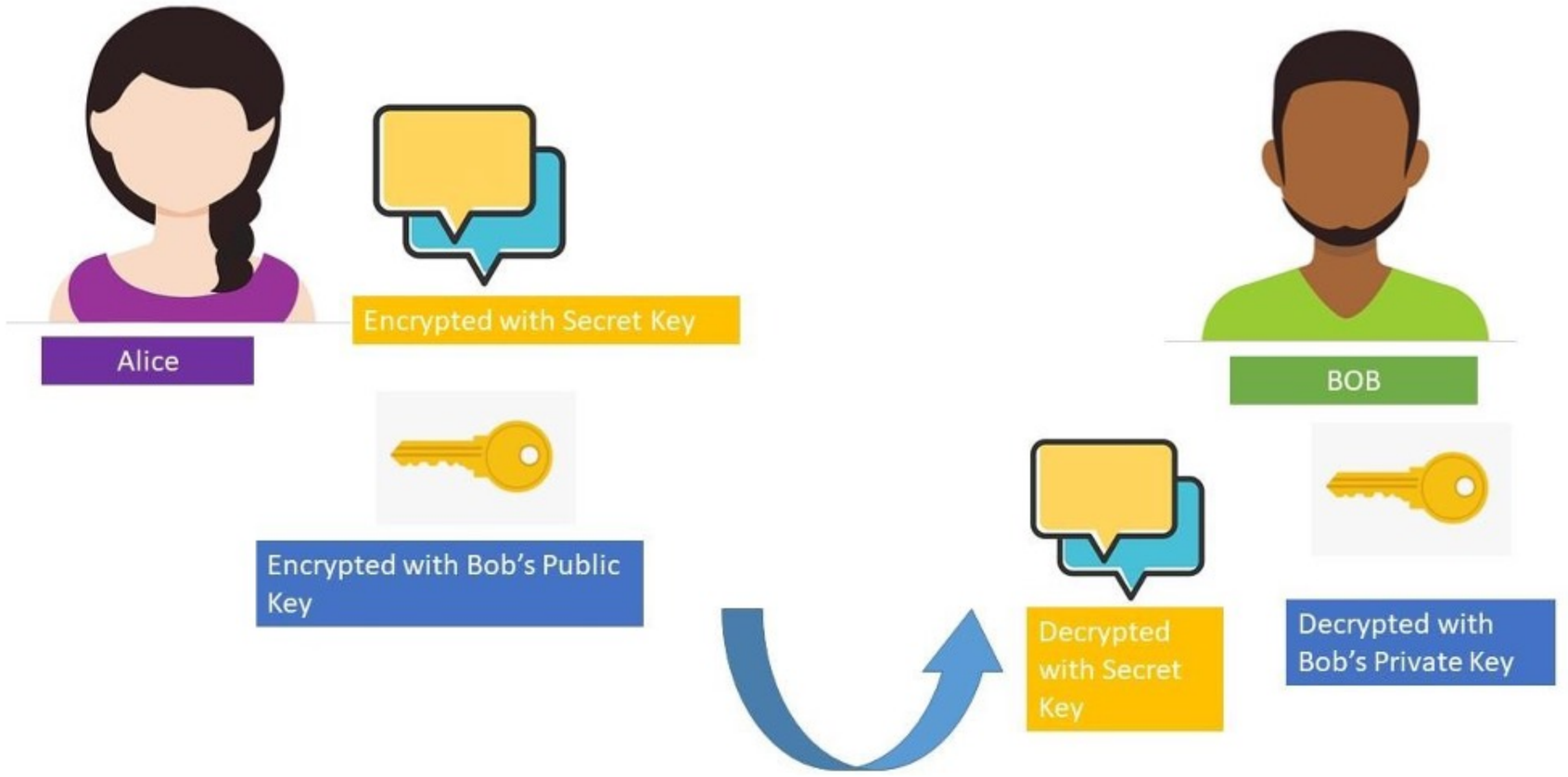
2. Digital signatures

   Tujuan: membuktikan otentikasi pesan dan pengirim Algoritma: RSA, ElGamal, DSA, ECC

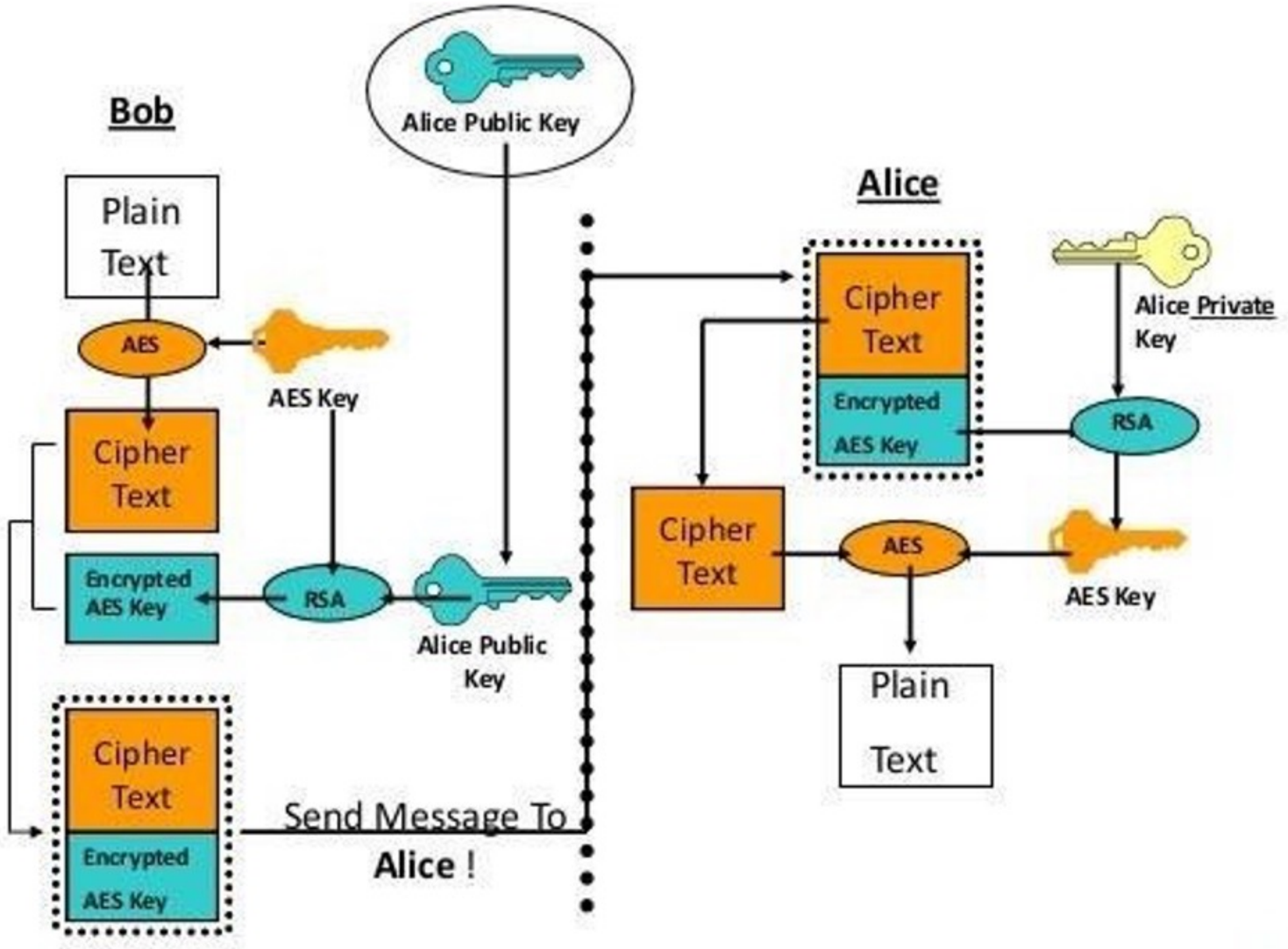
3. Pertukaran kunci (key exchange)

   Tujuan: berbagi kunci simetri Algoritma: Diffie-Hellman

Hybrid Kriptografi



Hybrid Kriptografi



SELAMAT BELAJAR