Cryptography

Muhammad Zen S. Hadi, ST. MSc.

Overview

- Seni menulis pesan rahasia
- Create text yang hanya bisa dibaca oleh orang yang berhak
- Teknik yang digunakan untuk mengubah informasi ke dalam format alternatif dan diubah kembali ke format semula

Terminology

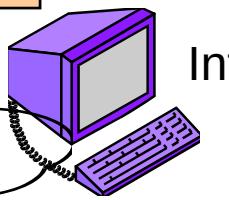
Encryption Key

Note:
Interceptor(MITM) tdk dpt membaca ciphertext tanpa kunci dekripsi

Plaintext "Hello"

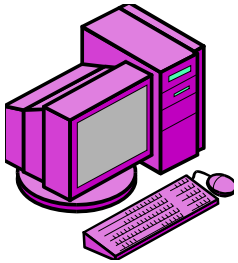
Encryption Method & Key

Ciphertext "11011101"

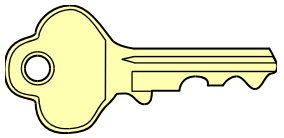


Interceptor

Network



Party A

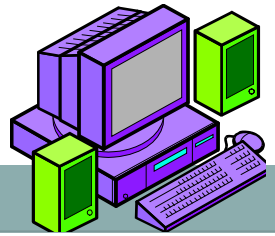


Decryption Key

Ciphertext "11011101"

Decryption Method & Key

Plaintext "Hello"



Party B

Tujuan Kriptografi

- Confidentiality (kerahasiaan)

  Tujuan : agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.

- Data Integrity

  Layanan yang menjamin bahwa pesan masih utuh/asli atau belum pernah dimanipulasi selama pengiriman.

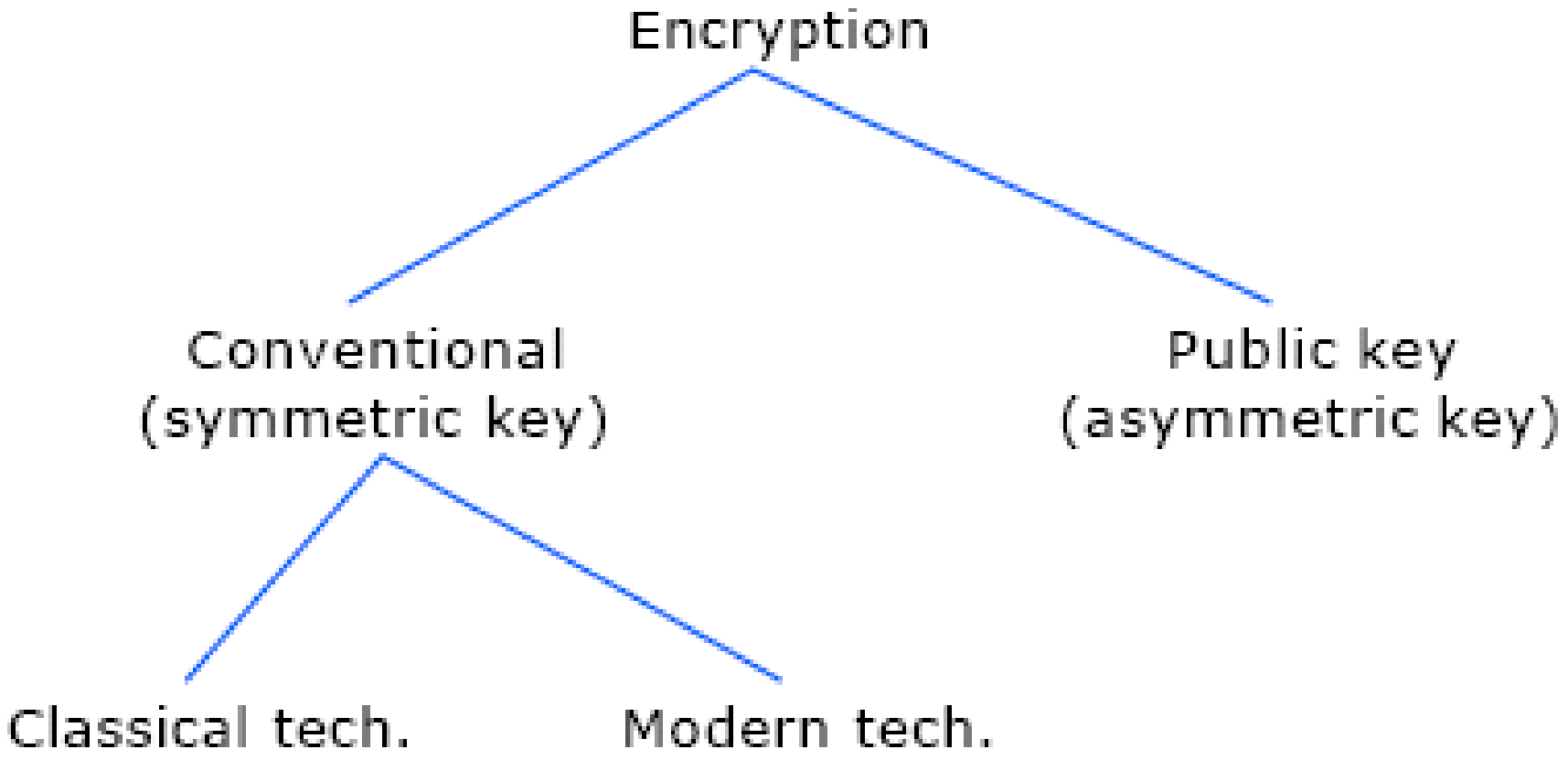
- Authentication

  Untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi

- Non-repudiation

  Layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan.

Pembagian Cryptography



Algoritma Kriptografi

- Algoritma Kriptografi Klasik

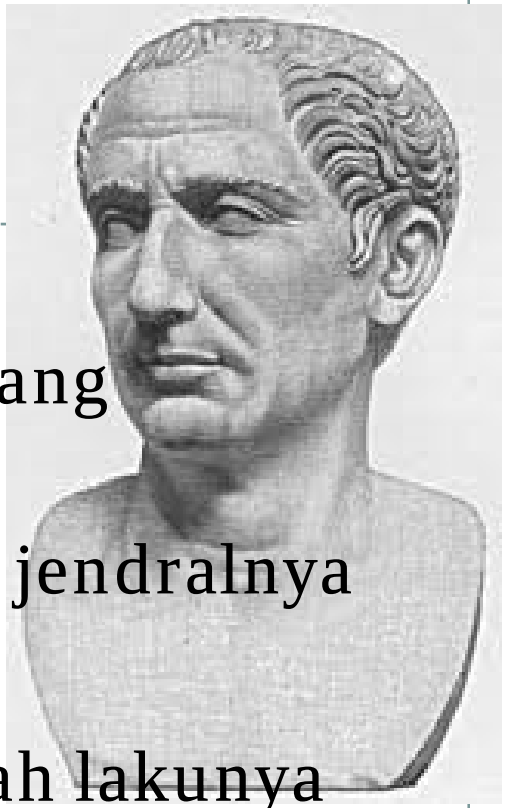
  Contoh : Cipher substitusi (Caesar Cipher), Cipher transposisi, Super enkripsi (penggabungan), Vigenere Cipher, Enigma Cipher

- Algoritma Kriptografi Modern

  a. Symmetric algorithm

  b. Asymmetric algorithm

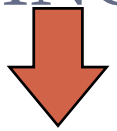
Caesar Cryptography



- Julius Caesar dianggap orang pertama yang menerapkan
- Dipakai untuk pesan rahasia untuk para jendralnya
- Menggunakan metode substitusi
- Kurang aman karena bisa diamati tingkah lakunya

Caesar Cryptography (Cont..)

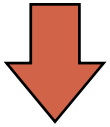
ABCDEFGHIJKLMNOPQRSTUVWXYZ



rotate 13 positions

NOPQRSTUVWXYZABCDEFGHIJKLM

THE GOTHS COMETH — *Plaintext*

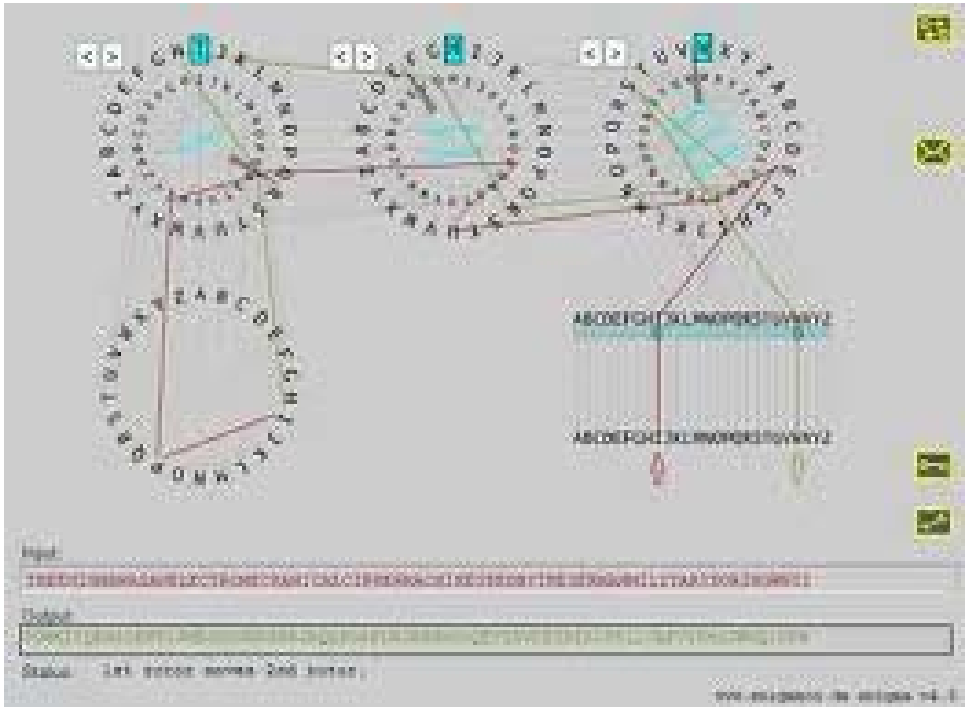


13 — *Key*

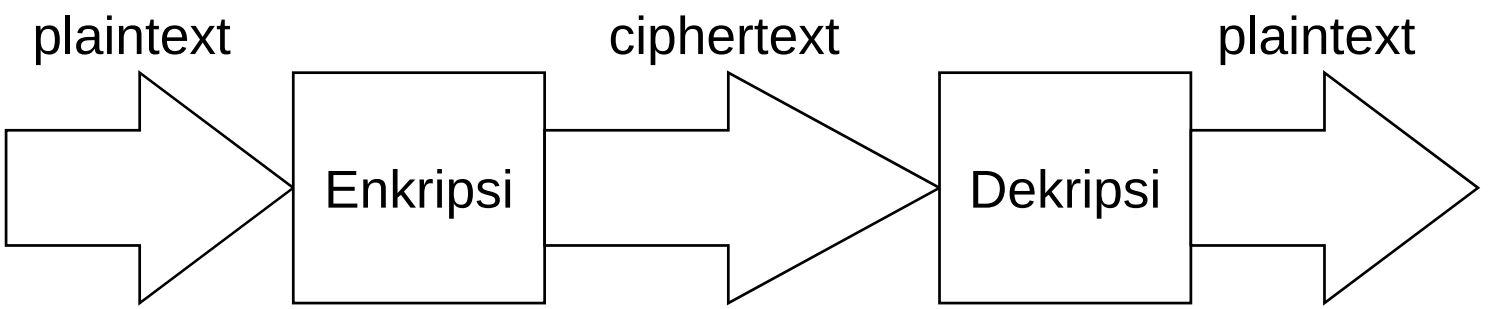
FUR TAFUE PAYRFU — *Ciphertext*

Enigma Cipher

- Digunakan selama PD II oleh tentara Jerman.



Mekanisme Enkripsi



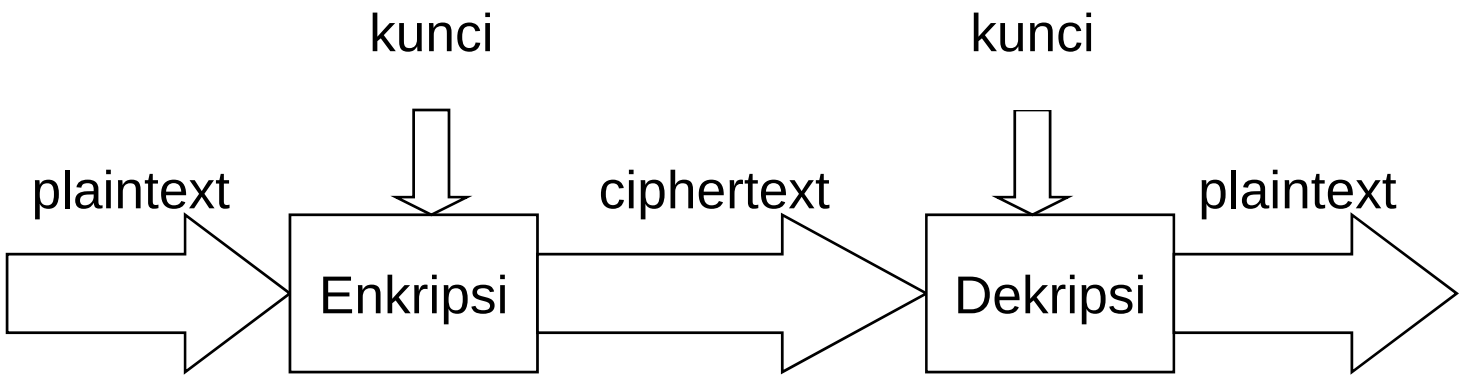
Mekanisme Enkripsi

- Plaintext (m) akan dilewatkan pada proses enkripsi (E) sehingga menghasilkan suatu ciphertext (c).
- Untuk memperoleh kembali plaintext, maka ciphertext (c) melalui proses dekripsi (D) yang akan menghasilkan kembali plaintext (m).
- Secara matematis :
  - $E(m) = c$
  - $D(c) = m$

Cryptography Modern

- Kriptografi modern selain memanfaatkan algoritma juga menggunakan kunci (*key*) untuk memecahkan masalah tersebut.
- Proses enkripsi dan dekripsi dilakukan dengan menggunakan kunci ini.
- Setiap anggota memiliki kuncinya masing-masing yang digunakan untuk proses enkripsi dan dekripsi yang akan dilakukannya

Cryptography Modern



Cryptography Modern (cont..)

- $Ee(m) = c$
- $Dd(c) = m$
- $Dd(Ee(m)) = m$

  - e = kunci enkripsi
  - d = kunci dekripsi

Komponen Cryptography

- Cypertext → Format Alternatif disebut juga text rahasia
- Plaint Text → Informasi/Pesan
- Key → Variable tambahan yang disuntikkan untuk merubah Plaintext ke Cypertext dan sebaliknya
- Algoritma Crypto → Rumus matematika yang diterapkan pada informasi yang ingin dienkripsi

Jenis Kunci Cryptography

- Kriptografi simetrik
- Kriptografi Asimetrik
- Perbedaan utama di antara keduanya terletak pada sama dan tidaknya kunci yang digunakan dalam proses enkripsi dengan kunci yang digunakan pada proses dekripsi

Symmetric Cryptography

- Kriptografi simetrik (*symmetric cryptography*) atau dikenal pula sebagai kriptografi kunci rahasia (*secret-key cryptography*)
- Merupakan kriptografi yang menggunakan kunci yang sama baik untuk proses enkripsi maupun dekripsi.
- Kriptografi simetrik sangat menekankan pada kerahasiaan kunci yang digunakan untuk proses enkripsi dan dekripsi. Oleh karena itulah kriptografi ini dinamakan pula sebagai kriptografi kunci rahasia
- Contoh algoritma simetrik adalah : OTP, DES (Data Encryption Standard), RC2, RC4 (Ron's Code), Rc5, RC6, IDEA (International Data Encryption Algorithm), Twofish, Magenta, Rijndael (AES-Advanced Encryption Standard), Blowfish, GOST, dan lain – lain.

Kategori Symmetric Crytography

- Stream Cipher
  - Setiap bit data akan dienkripsi secara berurutan menggunakan satu bit key
  - Contoh : RC4, A5
- Block Cipher
  - Enkripsi dilakukan terhadap sekelompok data
  - Contoh : IDEA, AES, DES

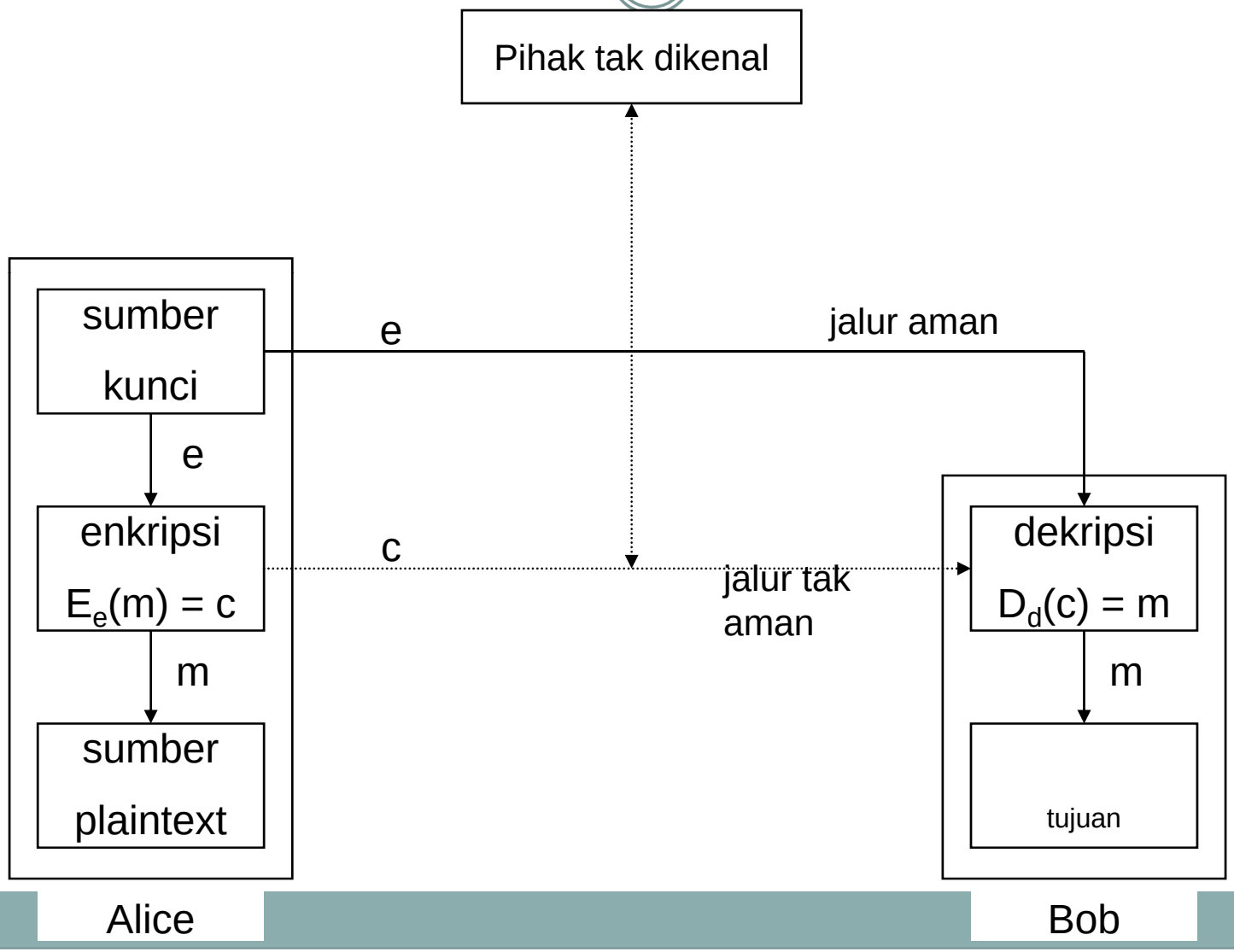
Symmetric Cryptography

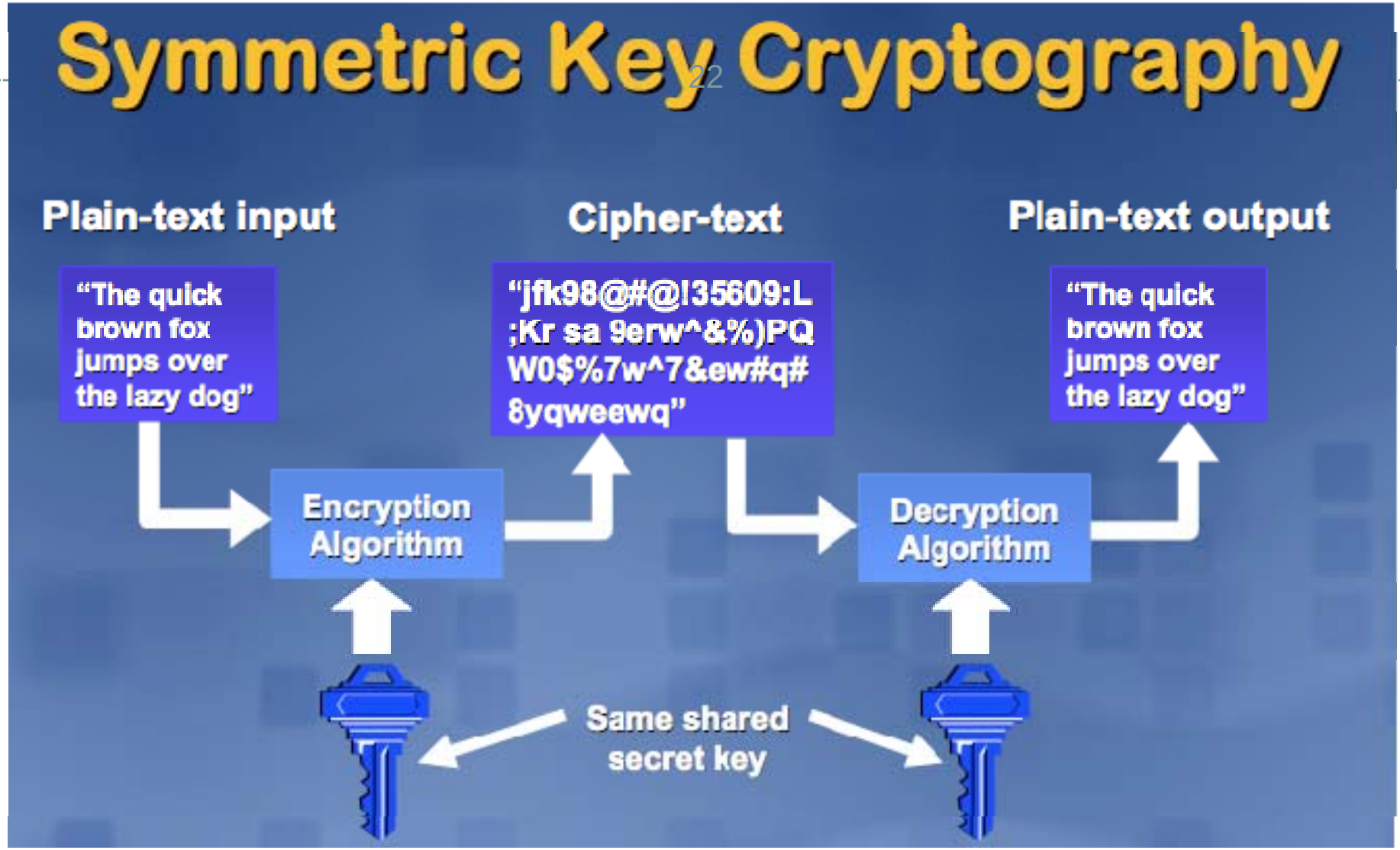
- $e = d = k$
- $Ek(m) = c$
- $Dk(c) = m$

Mekanisme Kerja Symmetric Cryptography

- Alice dan Bob menyetujui algoritma simetrik yang akan digunakan.
- Alice dan Bob menyetujui kunci yang akan dipakai.
- Alice membuat pesan plaintext yang akan dikirimkan kepada Bob, lalu melakukan proses enkripsi dengan menggunakan kunci dan algoritma yang telah disepakati sehingga menghasilkan ciphertext.
- Alice mengirimkan ciphertext tersebut kepada Bob.
- Bob menerima ciphertext, lalu melakukan dekripsi dengan menggunakan kunci dan algoritma yang sama sehingga dapat memperoleh plaintext tersebut.

Mekanisme Kerja Symmetric Cryptography




Symmetric Key Cryptography
Plain-text input
"The quick brown fox jumps over the lazy dog"
Encryption Algorithm
Cipher-text
"jfk98@#@!35609:L ;Kr sa 9erw^&%)PQ W0$%7w^7&ew#q# 8yqweewq"
Decryption Algorithm
Plain-text output
"The quick brown fox jumps over the lazy dog"
Same shared secret key

Kelemahan Symmetric Cryptography

- harus ada jalur aman (*secure channel*) dahulu yang memungkinkan Bob dan Alice melakukan transaksi kunci.
- Hal ini menjadi masalah karena jika jalur itu memang ada, tentunya kriptografi tidak diperlukan lagi dalam hal ini. Masalah ini dikenal sebagai masalah persebaran kunci (*key distribution problem*).
- Kelemahan lainnya adalah bahwa untuk tiap pasang pelaku sistem informasi diperlukan sebuah kunci yang berbeda. Dengan demikian bila terdapat n pelaku sistem informasi, maka agar tiap pasang dapat melakukan komunikasi diperlukan kunci sejumlah total n (n – 1) / 2 kunci. Untuk jumlah n yang sangat besar, penyediaan kunci ini akan menjadi masalah, yang dikenal sebagai masalah manajemen kunci (*key management problem*).

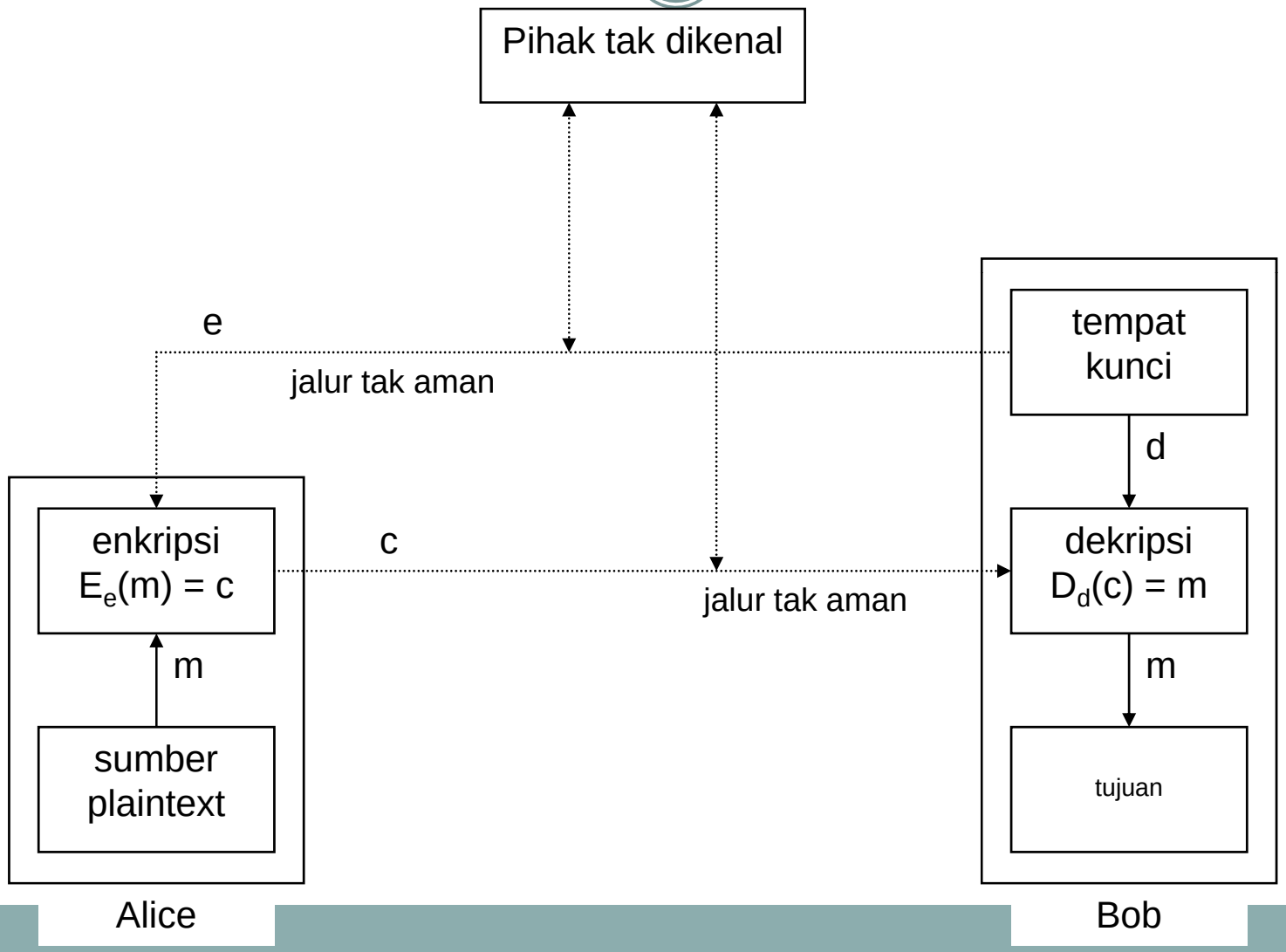
Keuntungan Symmetric Cryptography

- Dibandingkan dengan kriptografi asimetrik, kriptografi simetrik memiliki kecepatan operasi yang jauh lebih cepat.

Asymetric Cryptography

- menggunakan kunci enkripsi dan kunci dekripsi yang berbeda.
- Kunci enkripsi dapat disebarkan kepada umum dan dinamakan sebagai kunci publik (*public key*) sedangkan kunci dekripsi disimpan untuk digunakan sendiri dan dinamakan sebagai kunci pribadi (*private key*).
- Oleh karena itulah, kriptografi ini dikenal pula dengan nama kriptografi kunci publik (*public key cryptography*).
- Pada kriptosistem asimetrik, setiap pelaku sistem informasi memiliki sepasang kunci, yaitu kunci publik dan kunci pribadi.
- Kunci publik didistribusikan kepada umum, sedangkan kunci pribadi disimpan untuk diri sendiri.
- Contoh algoritma asimetrik adalah : RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm), Diffie Hellman, ElGamal, dan lain – lain.

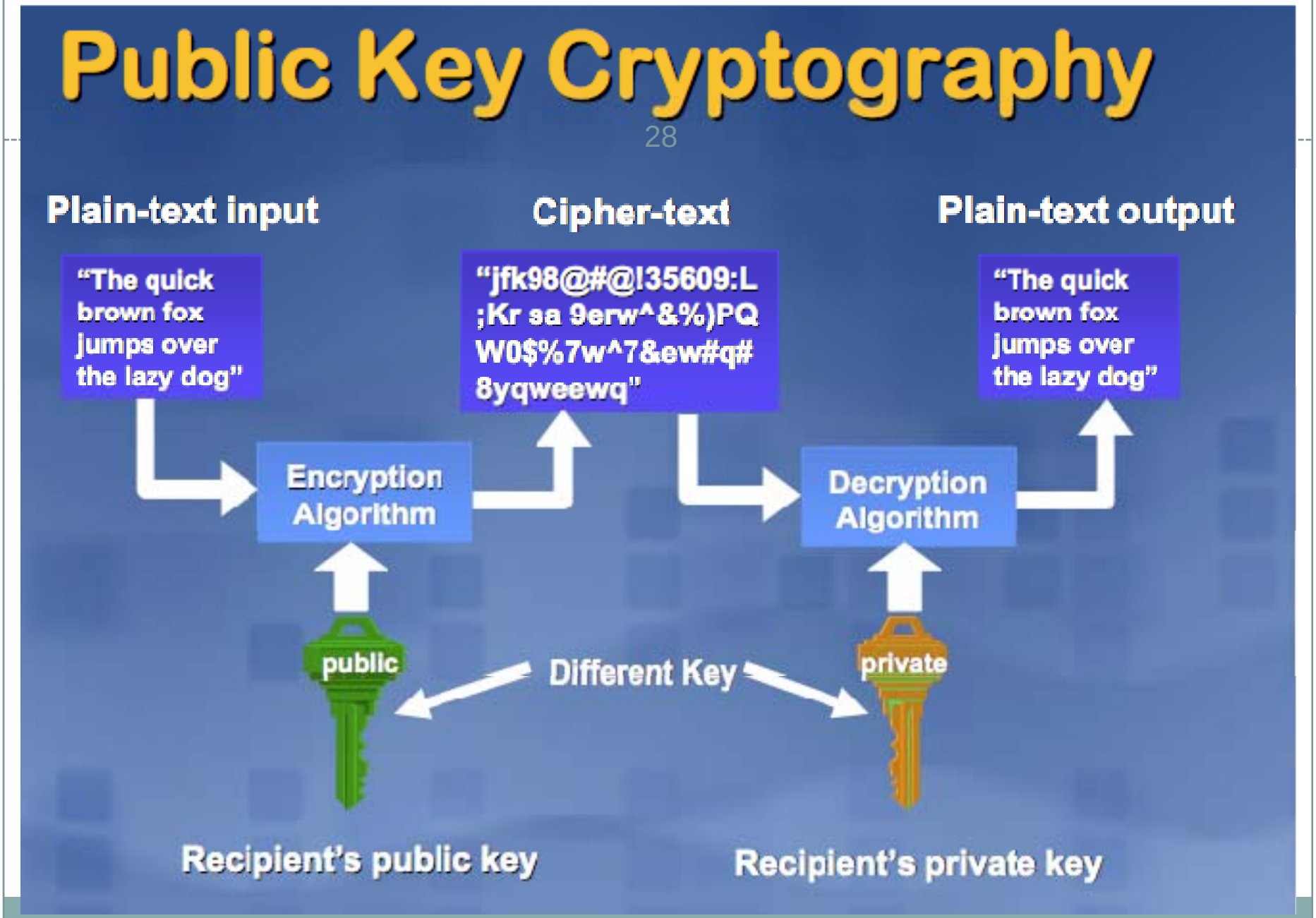
Mekanisme Kerja Asymetric Cryptography



Mekanisme Kerja Asymetric Cryptography

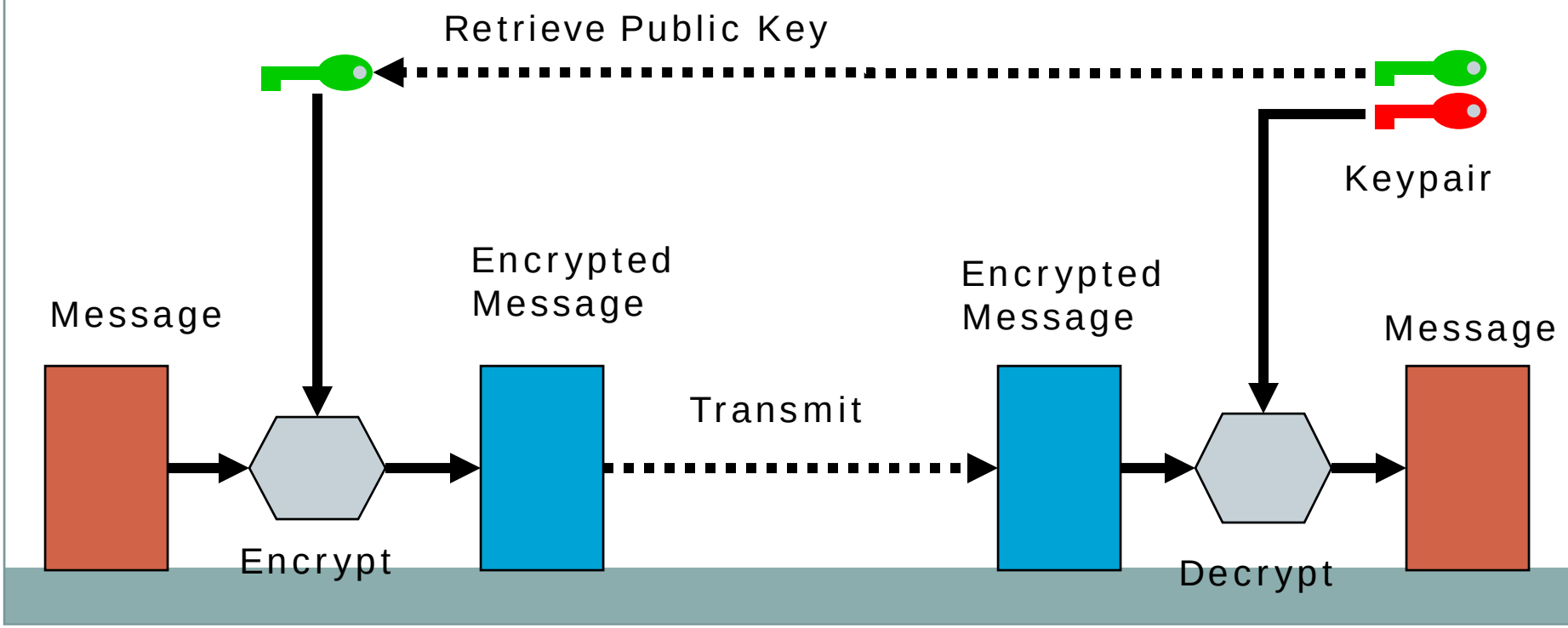
- Alice mengambil kunci publik milik Bob yang didistribusikan kepada umum.
- Alice melakukan enkripsi terhadap plaintext dengan kunci publik Bob tersebut sehingga menghasilkan ciphertext.
- Alice mengirimkan ciphertext kepada Bob.
- Bob yang menerima ciphertext tersebut melakukan proses dekripsi dengan menggunakan kunci pribadi miliknya sehingga mendapatkan plaintext semula.

Public Key Cryptography



Public Key Cryptography

- *Secure commnunication*



Kriptography Gabungan

- kombinasi antara kriptografi simetrik dengan asimetrik. Keunggulan dari kedua sistem kriptografi ini dapat dimanfaatkan sementara kekurangannya dapat diminimalisasi.
- Keuntungannya kecepatan proses kriptografi simetrik dimanfaatkan secara maksimal, sementara itu masalah ketiadaan jalur aman untuk transfer kunci simetrik diatasi dengan menggunakan kriptografi asimetrik.
- Dalam implementasi kriptosistem modern, skenario kriptografi gabungan ini sangat populer
- Digunakan untuk menghindari MITM (Man in the middle attack)

Mekanisme Kriptography Gabungan

- Alice mengambil kunci publik milik Bob yang didistribusikan kepada umum.
- Alice membangkitkan bilangan acak yang akan digunakan sebagai kunci simetriknya. Kunci simetrik ini kemudian dienkripsi dengan menggunakan kunci publik milik Bob.
- Kunci simetrik yang telah dienkripsi ini dikirimkan kepada Bob.
- Bob yang menerimanya melakukan proses dekripsi dengan menggunakan kunci pribadi miliknya sehingga mendapatkan kunci simetrik tersebut.
- Setelah kunci simetrik berhasil ditransfer dengan aman, selanjutnya keduanya berkomunikasi dengan menggunakan kunci simetrik tersebut.