Syahrul Imardi, MT

STMIK Amik Riau

#7

MATAKULIAH

KEAMANAN PERANGKAT LUNAK

KONSEP KRIPTOGRAFI KLASIK

P7

STMIK
Amik Riau

MATAKULIAH
KEAMANAN PERANGKAT LUNAK

Syahrul Imardi, MT

Pertemuan 7 : **Kriptografi Klasik**

Pembahasan

- Cryptography
- Algorithm
  - Symmetric key algorithm
  - Asymmetric key algorithm
  - Hashing algorithm

Apa itu Kriftografi ?

- Kriptografi (*cryptography*):
  - Bahasa Yunani
  - *Crypto & Graphia* → penulisan rahasia
  - Ilmu yang mempelajari penulisan secara rahasia
  - Cabang ilmu matematika → *cryptology*

- Ilmu dan seni untuk menjaga kerahasiaan berita *(**bruce Schneier - Applied Cryptography**)*

- Umum :
  - Ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data serta autentikasi data *(**A. Menezes, P. van Oorschot and S. Vanstone - Handbook of Applied Cryptography**)*

- Proses enkripsi informasi sehingga arti atau maksudnya tersembunyi dari orang yang tidak bisa membukanya.

- Kriptografi → Enkripsi (*Encryption*).

KRIPTOGRAFI

Pendahuluan :

1. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga
2. Hal ini seiring dengan semakin berkembangnya teknologi jaringan komputer dan internet
3. Semakin banyaknya aplikasi yang muncul memanfaatkan teknologi jaringan
4. Beberapa aplikasi tersebut menuntut tingkat aplikasi pengiriman data yang aman

J. Wang. Computer Network Security Theory and Practice. Springer, 2008

Tujuan Kriptografi

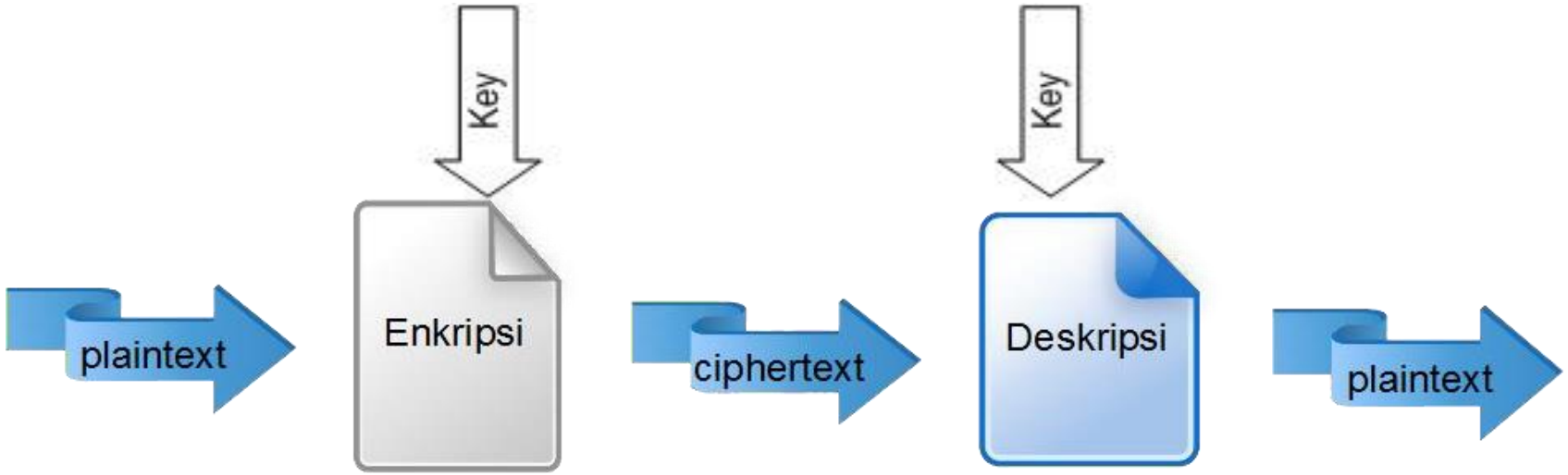
- Menjaga kerahasiaan yang terkandung di dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak berhak (tidak sah)
- Memberikan solusi terhadap masalah keamanan data
  - **Privacy** → data yang dikirimkan hanya dapat dimengerti oleh penerima yang sah
  - **Authentication** → mencegah pihak ketiga untuk mengubah data yang dikirim

- Tujuan sistem kriptografi :
  - **Convidentiality** → memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan informasi melalui teknik enkripsi
  - **Message Integrity** → memberikan jaminan bahwa setiap bagian yidak akan mengalami perubahan dari saat data dibuat/dikirim sampai pada saat data dibuka
  - **Non Repudiation** → memberikan cara untuk membuktikan bahwa suatu dokumen dari seseorang apabila ia menyangkal memiliki dokumen tersebut
  - **Authentication** → memberikan layanan :
    - Mengidentifikasi keaslian suatu pesan dan memberikan jaminan keotentikan
    - Menguji identitas seseorang apabila ia akan memasuki sebuah sistem

Salah satu hal yang dapat dilakukan untuk mengamankan sistem informasi adalah menggunakan kriptografi

Proses Utama pada Kriptografi

1. **Enkripsi :** Proses transformasi informasi (dikenal dengan *plaintext*) menggunakan algoritma (yang dikenal dengan *cipher*) untuk membuatnya menjadi tidak terbaca/tidak dikenali bagi semua orang (hasilnya dikenal dengan *ciphertext*) kecuali yang mempunyai informasi khusus atau algoritma tertentu yang dikenal dengan kunci (*key*).
2. **Dekripsi :** adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal/ Proses untuk membuat informasi yang ter-enkripsi (*ciphertext*) menjadi terbaca kembali



J. Wang. Computer Network Security Theory and Practice. Springer, 2008

ISTILAH DALAM KRIPTOGRAFI

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi :

1. **Plaintext** (M) adalah pesan yang hendak dikirimkan (berisi data asli).
2. **Ciphertext** (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
3. **Enkripsi** (fungsi E) adalah proses pengubahan *plaintext* menjadi *ciphertext*.
4. **Dekripsi** (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.
5. **Kunci** adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

J. Wang. Computer Network Security Theory and Practice. Springer, 2008

Istilah Dasar lainnya

- **Cipher** = Algoritma untuk melakukan proses enkripsi.
- **Cryptanalysis** = ilmu yg mempelajari metode mendapatkan arti dari informasi yang ter-enkripsi tanpa menggunakan key (kunci) = ilmu yang mempelajari bagaimana melakukan crack algoritma enkripsi atau implementasinya.
- **Cryptanalyst** = orang yang menjalankan *Cryptanalysis*.
- **Frequency analysis** = Analisa statistik dari banyaknya huruf atau karakter yang tampil, dapat digunakan untuk memecahkan enkripsi sederhana (semisal *subtitusion cipher*). Ditemukan oleh Al-Kindi pada abad ke-9.

Classical Cryptography

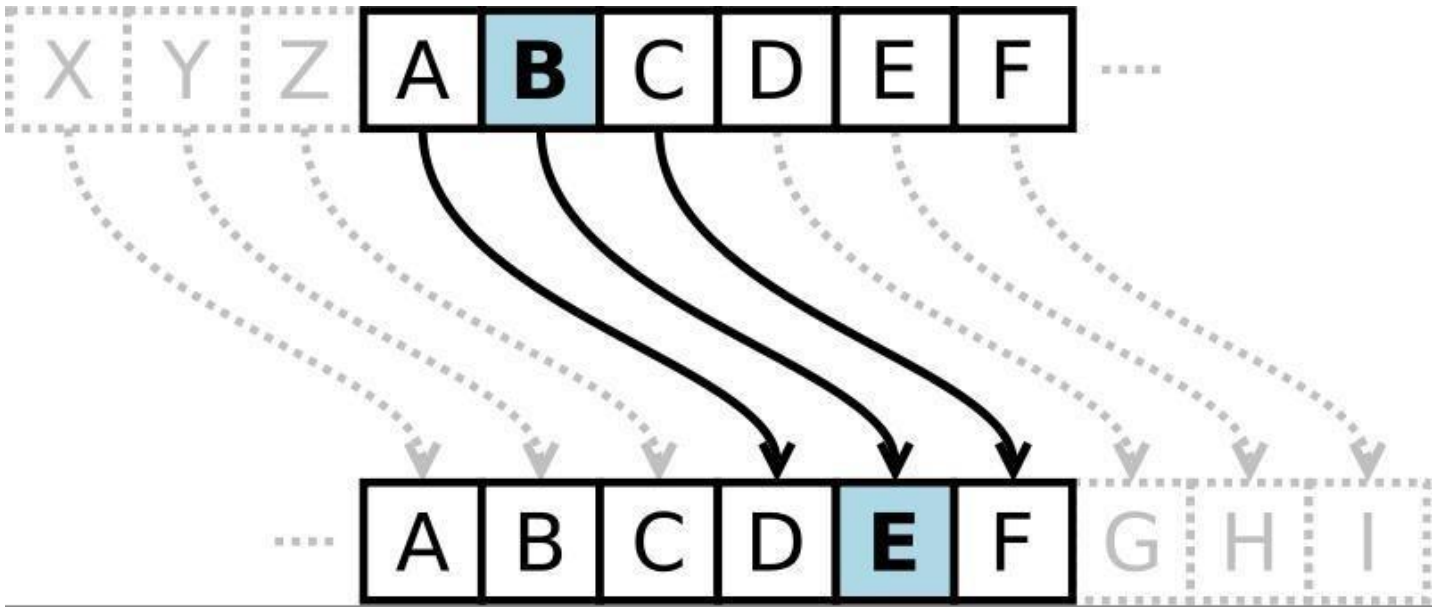
- **Transposition ciphers**, mengubah susunan huruf atau pesan. Misalnya pesan 'hello world' menjadi 'ehlol owrdl'
- **Substitution ciphers**, mengganti huruf atau kelompok huruf dengan huruf atau kelompok huruf lainnya.
  - Contoh yang populer adalah **Caesar Cipher**, **ROT 13**

Plain : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Ciphertext : WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ
Plaintext : the quick brown fox jumps over the lazy dog

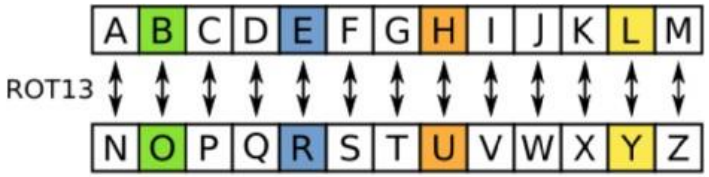
Caesar Cipher

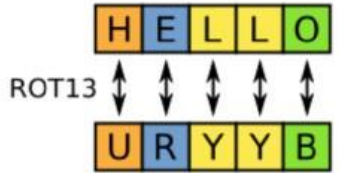
- Dipopulerkan oleh Julius Caesar pada Jaman Romawi.
- Untuk melindungi pesan militer penting dengan menggeser 3 huruf/alfabet



ROT 13

- ROT 13 ("rotate by 13 places“ / ROT-13), merupakan algoritma enkripsi yang sederhana dengan mengganti huruf dengan huruf ke 13 setelahnya di alfabet.
- Masih banyak digunakan di beberapa sistem di UNIX.





- Untuk mengembalikan ke bentuk semula dilakukan proses ROT13 dua kali.

M = ROT13(ROT13(M)

Enigma Rotor Machine

- Caesar Cipher, ROT13 merupakan *monoalphabetic cipher* (setiap huruf diganti dengan huruf yang lain) mudah dipecahkan
- **Enigma Rotor Machine** (1920-an), alat enkripsi dan dekripsi mekanik dibuat oleh Jerman yang digunakan pada perang dunia ke-2 untuk berkirim pesan rahasia.
- ERM menggunakan metode *polyalphabetic cipher*, menggunakan lebih dari 2 tabel konversi huruf.

PRINSIP YANG MENDASARI KRIPTOGRAFI YAKNI

1. **Confidentiality**
2. **Integrity**
3. **Availability**
4. **Authentication**
5. **Non-Repudiation**

ALGORITMA KRIPTOGRAFI

1. ***Berdasarkan jenis kunci yang digunakan :***
   - Algoritma Simetris
   - Algoritma Asimetris
2. ***Berdasarkan besar data yang diolah :***
   - Algoritma Block Cipher
   - Algoritma Stream Cipher

J. Wang. Computer Network Security Theory and Practice. Springer, 2008

Algoritma Kriptografi

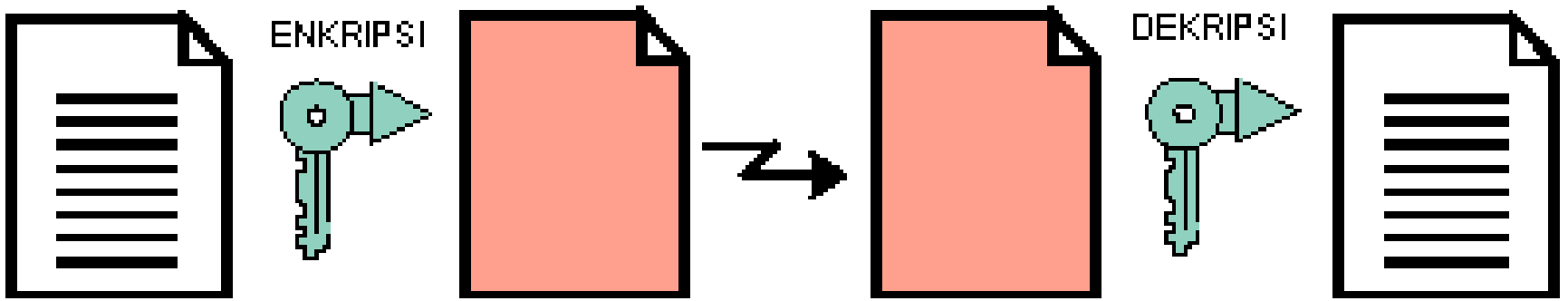
- Algoritma kriptografi harus memiliki kekuatan untuk melakukan proses enkripsi ***(Shannon)*** :
  - **Konfusi/pembingungan** (*confusion*), dari teks terang sehingga sulit untuk direkonstruksikan secara langsung tanpa menggunakan algoritma dekripsinya.
  - **Difusi/peleburan** (*difusion*), dari teks terang sehingga karakteristik dari teks terang tersebut hilang.

- Ada 3 macam atau jenis algoritma
  - Algoritma Hash (*Hashing algorithm*)
  - Algoritma Kunci Simetris (*Symmetric key algorithm*)
  - Algoritma Kunci Asimetris (*Asymmetric key algorithm*)

BERDASARKAN JENIS KUNCI YANG DIGUNAKAN

1. **Algoritma Simetris**

   Algoritma simetris *(symmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm.*



J. Wang. Computer Network Security Theory and Practice. Springer, 2008

BERDASARKAN JENIS KUNCI YANG DIGUNAKAN

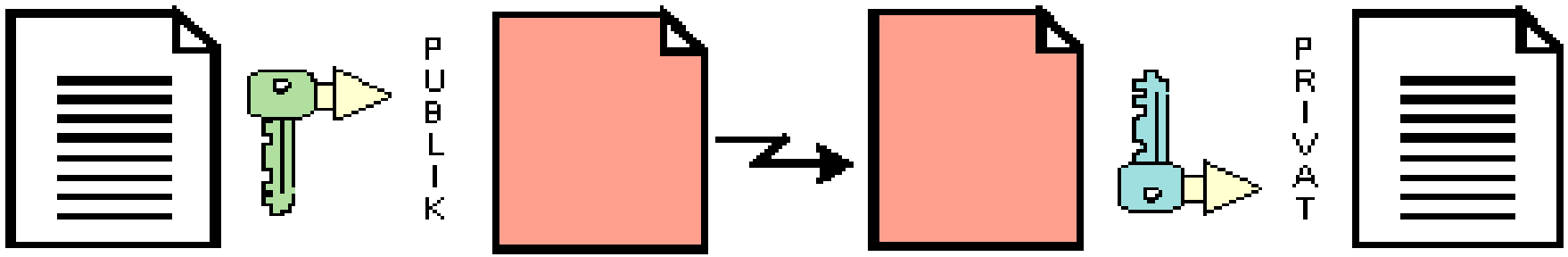
1. ***Kelebihan algoritma simetris :***
   a) Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.
   b) Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem *real-time*
2. ***Kelemahan algoritma simetris :***
   a) Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.
   b) Permasalahan dalam pengiriman kunci itu sendiri yang disebut *"key distribution problem"*

J. Wang. Computer Network Security Theory and Practice. Springer, 2008

BERDASARKAN JENIS KUNCI YANG DIGUNAKAN

2. Algoritma Asimetris

Algoritma asimetris *(asymmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik *(public key)* dan kunci privat *(private key).* Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan.



J. Wang. Computer Network Security Theory and Practice. Springer, 2008

BERDASARKAN JENIS KUNCI YANG DIGUNAKAN

1. ***Kelebihan algoritma asimetris :***
   a) Masalah keamanan pada distribusi kunci dapat lebih baik
   b) Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit

2· Kelemahan algoritma asimetris :

   a) Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris
   b) Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris.

J. Wang. Computer Network Security Theory and Practice. Springer, 2008

BERDASARKAN BESAR DATA YANG DIOLAH

1. Block Cipher

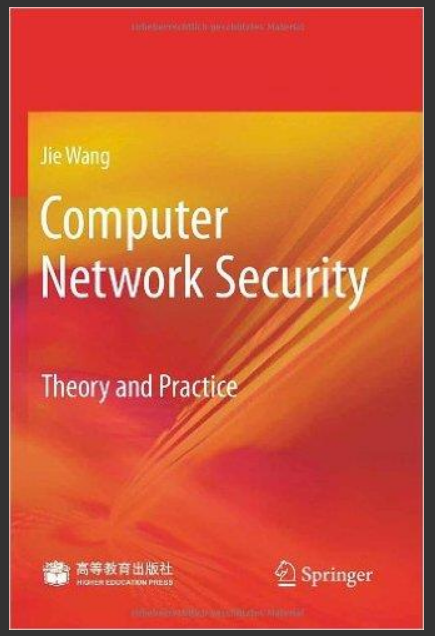
Algoritma kriptografi ini bekerja pada suatu data yang berbentuk blok/kelompok data dengan panjang data tertentu (dalam beberapa byte), jadi dalam sekali proses enkripsi atau dekripsi data yang masuk mempunyai ukuran yang sama.

2. Stream Cipher

Algoritma yang dalam operasinya bekerja dalam suatu pesan berupa bit tunggal atau terkadang dalam suatu byte, jadi format data berupa aliran dari bit untuk kemudian mengalami proses enkripsi dan dekripsi.

J. Wang. Computer Network Security Theory and Practice. Springer, 2008

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)

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

THANKS!