KRIPTOGRAFI

Pendahuluan :

- 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
- Hal ini seiring dengan semakin berkembangnya teknologi jaringan komputer dan internet
- Semakin banyaknya aplikasi yang muncul memanfaatkan teknologi jaringan
- Beberapa aplikasi tersebut menuntut tingkat aplikasi pengiriman data yang aman

Proses Utama pada Kriptografi :

- **Enkripsi**
  adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu
- **Dekripsi**
  adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal

Istilah dalam Kriptografi :

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi :

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

Prinsip yang mendasari kriptografi yakni:

- Confidentiality
- Integrity
- Availability
- Authentication
- Non-Repudiation

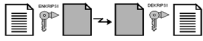
Algoritma Kriptografi :

- Berdasarkan jenis kunci yang digunakan :
  - o Algoritma Simetris
  - o Algoritma Asimetris
- Berdasarkan besar data yang diolah :
  - o Algoritma Block Cipher
  - o Algoritma Stream Cipher

Berdasarkan jenis kunci yang digunakan :

- 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*.



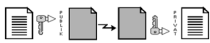
Berdasarkan jenis kunci yang digunakan :

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

Berdasarkan jenis kunci yang digunakan :

- 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.



Berdasarkan jenis kunci yang digunakan :

- Kelebihan algoritma asimetris :
  - Masalah keamanan pada distribusi kunci dapat lebih baik
  - Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit
- Kelemahan algoritma asimetris :
  - Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris
  - Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris.

Berdasarkan besar data yang diolah :

- 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.

- 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.