

# Keamanan Komputer

## KONSEP DASAR KRIPTOGRAFI

Muhammad Adri, MT

## PENDAHULUAN

- Bidang **Cryptography** yang dalam bahasa Indonesia disebut dengan **Ilmu Sandi** merupakan salah satu bidang kajian dalam bidang Informatika yang sangat populer dewasa ini.
- Hal ini seiring dengan semakin berkembangnya teknologi jaringan komputer dan internet
- Semakin banyaknya aplikasi yang muncul memanfaatkan teknologi jaringan ini
- Beberapa aplikasi tersebut menuntut tingkat aplikasi pengiriman data yang aman

## Secure Application

- Aplikasi yang aman dituntut karena adanya proses transaksi data yang bernilai ekonomis dan bisnis
- Beberapa aplikasi tersebut seperti *electronic banking (e-banking)*, *electronic bussiness (e-bussiness)*, *electronic market (e-market)*, *electronic publishing (e-publishing)*, *electronic university (e-university)*
- Semua aplikasi berbasis teknologi internet tersebut di atas, menuntut adanya jaminan keamanan terhadap semua paket data yang dikirim dalam proses *bussiness transaction*

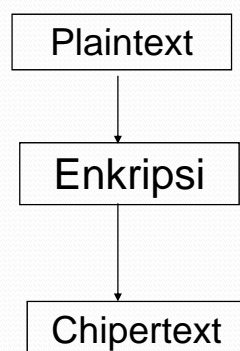
## PENDAHULUAN

- Private information
- Secret information dan data
- Data dan informasi yang akan dikirimkan harus dirahasiakan
- Data diubah menjadi kode-kode rahasia yang hanya bisa dimengerti oleh orang tertentu

## TUJUAN ENKRIPSI

- Mengubah data rahasia menjadi kode-kode tertentu
- The purpose is to protect transmitted information from being read and understood by anyone except the intended recipient
- Encryption is a method of transforming original data into a form that appears to be unreadable (ciphertext)

## PROSES ENKRIPSI



Plaintext yaitu isi pesan yang akan dikirim dalam format normal

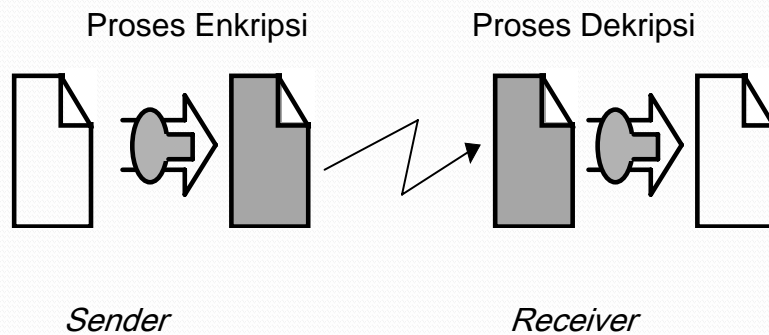
Pesan Plaintext dikonversikan ke dalam bentuk kode-kode tertentu

Chipertext yaitu isi pesan yang dikodekan (*coded message*)

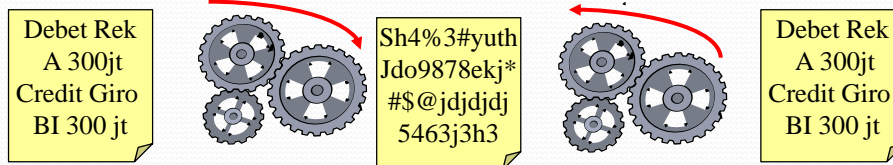
## KATEGORI ENKRIPSI

- Enkripsi Kunci rahasia (*private key encryption*), terdapat sebuah kunci yang digunakan untuk meng-enkripsi dan men-dekripsi informasi
- Enkripsi Kunci publik (*public key encryption*), terdapat dua kunci yang digunakan, satu untuk enkripsi, lainnya untuk dekripsi
- Fungsi *One-Way*, informasi dienkripsi untuk menciptakan *signature* dari informasi asli yang digunakan untuk keperluan autentikasi

## EKRIPSI DAN DEKRIPSI

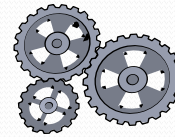


## PROSES ENKRIPSI DAN DEKRIPSI



## KOMPONEN ENKRIPSI

- Algoritma Enkripsi (DES, 3DES, AES dll)
- Key dan Key Management
- Integrity Checking



## Algoritma Enkripsi

- Metoda yang digunakan dalam usaha mengubah Plaintext menjadi Cipher Text
- Secara garis besar dibagi menjadi dua :
  - Conventional Algorithms
  - Modern Algorithms

## Algoritma Enkripsi - Conventional

- Suatu metoda yang dengan menggunakan teknik-teknik sederhana
- Metoda konvensional yang terkenal, dikategorikan menjadi dua bagian :
  - Metoda Substitusi
  - Metoda Transposisi

## Apa itu Kunci ?

An Encryption Key is:

- ❖ A series of numbers and letters...
- ❖ ...used in conjunction with an encryption algorithm
- ❖ ...to turn plain text into encrypted text and back into plain text
- ❖ *The longer the key, the stronger the encryption*



## Contoh Sederhana

Plaintext : halo apa kabar

```
1101000110000111011001101111010000
11000011110000110000101000001101011
1100001110001011000011110010
```

Algorithma : XOR

Key : dx 11001001111000

Chipertext : DD

```
000110000110010001000001011110001
000011001001010000110011000100001
00110000101001101000001010001010
```

## Integrity Checking

- Proses yang dilakukan untuk mendeteksi isi pesan/ data yang telah dienkripsi terhadap kesalahan dan kekeliruan serta kesesuaian key
- Digunakan untuk melihat keutuhan dari pesan/ data yang telah ditransmisikan
- Berkaitan dengan integritas dan keabsahan

## To be Continued.....

- Teknik Algoritma Konvensional
  - Teknik Substitusi
    - Caesar Chiper
    - Deret dengan kata kunci
    - dll
  - Teknik Transposisi
    - Kode Rahasia VIC
    - Desain Chiper