

KRIPTOGRAFI

KELOMPOK 5

DONY SUBAGIO - 1310651006

ADHE PANDU DWI P - 1310651046

M AFFTHON ILMAN H - 1310651194

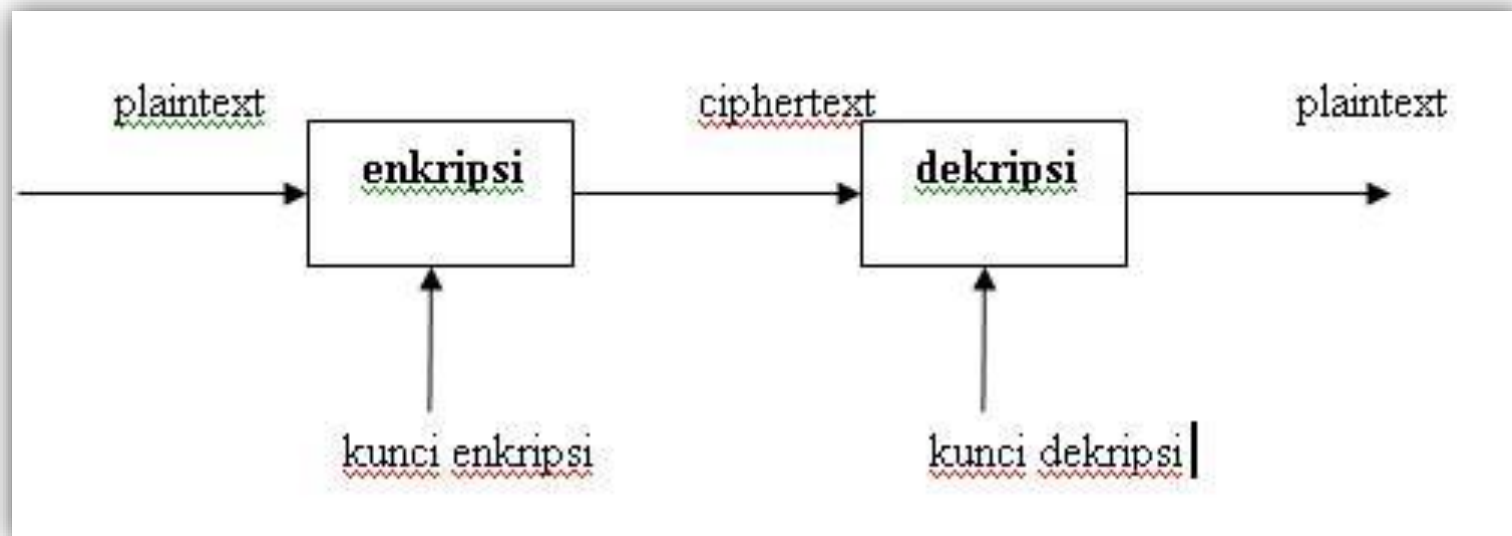
AHMAD AKBAR TANJUNG –

1310651209

Konsep kriptografi

Kata Kriptografi berasal dari bahasa Yunani
Kryptos (tersembunyi) dan Graphien (menulis).

Adapun algoritma matematis yang digunakan pada proses enkripsi yakin disebut cipher dan sistem yang memanfaatkan kriptografi untuk mengamankan sistem informasi disebut kriptosistem.





tujuan dari kriptografi adalah antara lain :

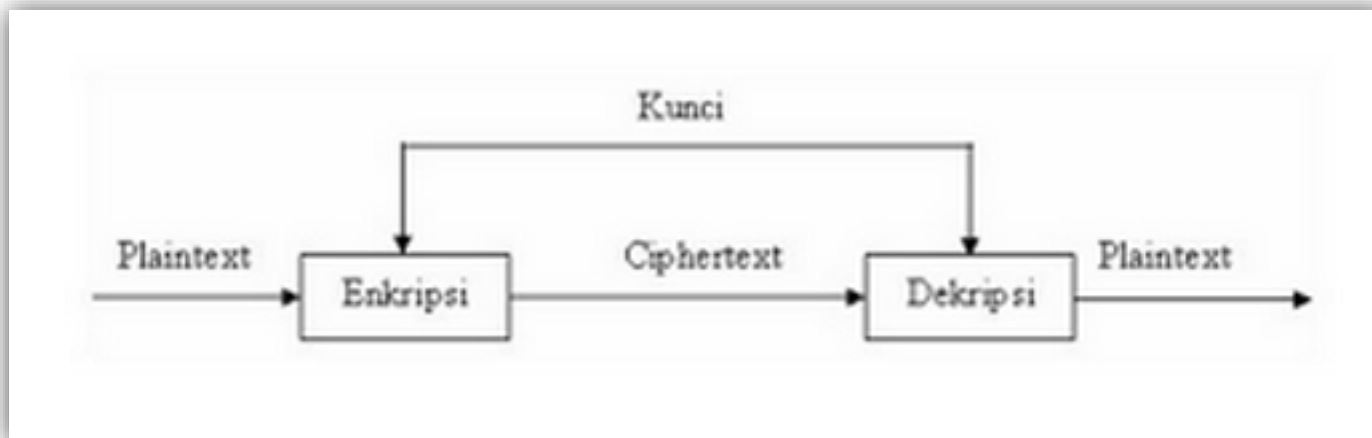
- Kerahasiaan
- Integritas data
- Authentifikasi
- Non-repudiasi

Teknik Kriptografi

untuk enkripsi data ada dua macam,
antara lain :

□ 1. Kriptografi Simetris

Algoritma simetris atau sering disebut algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses deskripsi



2. Kriptografi Asimetris

Kriptografi asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi.



Contoh criptografi

□ SUBSTITUSI

- Dalam kriptografi, sandi substitusi adalah jenis metode enkripsi dimana setiap satuan pada teks terang digantikan oleh teks tersandi dengan sistem yang teratur. Metode penyandian substitusi telah dipakai dari zaman dulu (kriptografi klasik) hingga kini (kriptografi modern).

• Caesar Cipher

Caesar Cipher

```
-----  
PLAINTEXT      : BELAJAR BERSAMA  
Alphabet        : 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  
Deret Inversi   : T E D A B C Z Y X W V U F S R Q P O N M L K J I H G  
Kunci           : A = T  
-----
```

```
Encrypt         : EBUTWTO EBONTFT  
Decrypt         : BELAJAR BERSAMA
```



Terima kasih