Kriptografi

-> Mengubah data yang bermakna menjadi tidak bermakna

-> Kriptografi : ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi

-> ilmu untuk menjaga kerahasiaan pesan

-> Layanan Kriptografi

- Kerahasiaan pesan
- Keaslian pesan
- Keaslian pengirim dan penerima pesan
- Anti penyangkalan

-> Istilah dalam kriptografi

1. Pesan = informasi yang dapat dibaca dan dimengerti maknanya (baik dipersepsi secara visual maupun audial)

Rupa pesan = teks, gambar, musik, video | nama lain : plaintext

2. Pengirim = pihak yang menerima pesan
3. Penerima = pihak yang mengirim pesan
4. Cipherteks = pesan yang telah disandikan sehingga tidak bermakna lagi.

   Tujuan : agar tidak dapat dibaca
5. Enkripsi = proses menyandikan plainteks menjadi cipherteks
6. Dekripsi = proses mengembalikan cipherteks menjadi plainteks semula
7. Cipher
   - Algoritma enkripsi dan dekripsi
   - Aturan untuk enchipering dan dechipering

No.

Date:

8. Kunci = parameter yang digunakan dalan enkripsi dan dekripsi
   - Prinsip Kherkoff : semua algoritma kriptografi harus publik, sedangkan kunci harus rahasia
9. Penyadap = orang / mesin yang mencoba menangkap pesan selama ditransmisikan
10. Kriptanalisis : ilmu dan seni untuk memecahkan chiperteks menjadi plainteks tanpa mengetahui kunci yg digunakan
    - Pelaku disebut kriptanalis
    - Kriptanalisis : "lawan" kriptografi
    - Sudah ada sejak abad ke-9
11. Kriptologi : studi mengenai kriptografi dan kriptanalisis