Kriptografi

ILMU DAN SENI UNTUK MENJAGA KEAMANAN PESAN

Subianto | AMIK JTC SEMARANG

Pengertian

Berasal dari bahasa Yunani *"Cryptos"* artinya *"Secret"* (Rahasia), sedangkan *"Graphein"* artinya *"Writing"* (Tulisan).

Dahulu :

Ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikan kedalam bentuk yang tidak dapat dimengerti lagi maknanya.

Sekarang :

Ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan, integeritas data, serta otentikasi.

Terminologi

Beberapa istilah yang penting untuk diketahui

- Pesan (plainteks)
- Cipherteks
- Pengirim (sender)
- Penerima (receiver)
- Enkripsi
- Dekripsi
- Cipher
- Kunci (Key)
- Sistem Kriptografi
- Penyadap
- Kriptonalisis dan kriptologi

Tujuan Kriptografi

- Kerahasiaan (confidentiality)
- Integritas data (data integrity)
- Otentikasi (authentication)
- Nirpenyangkalan (nonrepudiation)

Komponen Kriptografi

- Plainteks
- Cipherteks
- Algoritma & kunci (key)

Sejarah Kriptografi

- **KRIPTOGRAFI MEMPUNYAI SEJARAH YANG PANJANG**
- **INFORMASI LENGKAP TENTANG SEJARAH KRIPTOGRAFI DAPAT DITEMUKAN D I DALAM BUKU DAVINCI KHAN BERJUDUL *"THE CODEBREAKERS"***

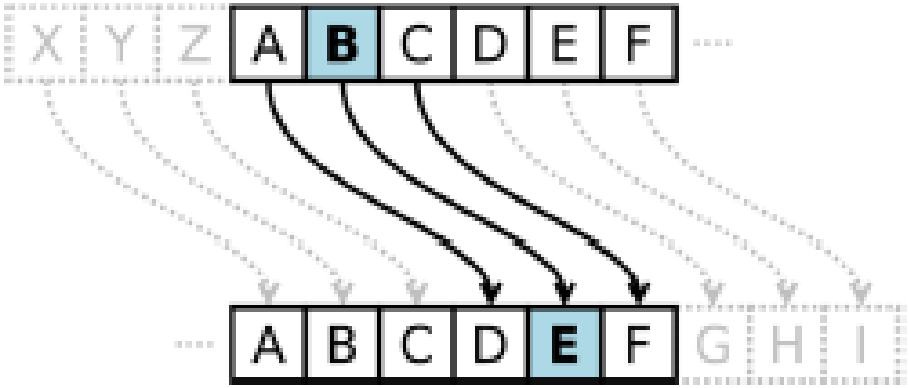
MESIR KUNO 4000 TAHUN LALU

HIEGROGLYPH **=** TULISAN YANG DITULIS PADA PIRAMID YANG BUKANLAH BENTUK STANDAR DALAM PENULISAN PESAN



ROMAWI KUNO

JULIUS CAESAR = MENGIRIM PESAN KEPADA JENDERAL DI MEDAN PERANG, PESAN YANG DIKIRIM DIACAK DENGAN MENGGANTI SEMUA SUSUANAN ALFABET, YAITU DENGAN MENGGANTI **A** DENGAN **D**, **B** DENGAN **E**, **C** DENGAN **F**, DAN SETERUSNYA YANG DIKENAL DENGAN **CAESAR CIPHER**



Tentara Sparta di Yunani

MENGGUNAKAN **CIPHER TRANSPOSISI** DENGAN MENGGUNAKAN ALAT **SCYTALE**

Kalangan Gereja

PADA MASA AWAL AGAMA KRISTEN MENGGUNAKAN KRIPTOGRAFI UNTUK MENGAMANKAN TULISAN **RELIJIUS** DARI GANGUAN OTORITAS POLITIK ATAU BUDAYA YANG DOMINAN DIMASA ITU.

India

KRIPTOGRAFI DIGUNAKAN OLEH PENCINTA *(LOVERS)* UNTUK BERKOMUNIKASI TANPA DIKETAHUI ORANG LAIN. DITEMUKAN DALAM BUKU *"KAMA SUTRA"*

Ratu Skotlandia *(Queen Mary)*

QUEEN MARY DI PANCUNG SETELAH SURAT RAHASIANYA DARI BALIK PENJARA BERHASIL DIPECAHKAN OLEH SEORANG PEMECAH KODE

ISI SURAT ***"RENCANA PEMBUNUHAN RATU ELIZABETH I"***

Perang Dunia II

PEMERINTAH **NAZI JERMAN** MEMBUAT MESIN ENKRIPSI YANG DINAMAKAN ENIGMA

Kriptografi Klasik vs Modern

- **Klasik** Dilakukan dengan menggunakan kertas dan pensil, berbasis karakter yaitu enkripsi dan deskripsi dilakukan setiap karakter pesan.

- Teknik substitusi (penggantian)
  - Caesar cipher
  - Affine cipher
  - Viginere cipher
  - Playfair cipher
  - Enigma cipher
  - One-time pad
- Teknik transposisi (permutasi)

- **Modern** Beroperasi dalam mode bit, algoritma enkripsi dan deskripsi memproses semua data dan informasi dalam bentuk rangkaian bit.
- Didorong oleh penggunaan komputer digital.
- Jenis :
  - DES
  - RC2, RC4, RC5, RC6
  - IDEA
  - AES
  - OTP
  - A5
  - DSA
  - RSA
  - DH
  - ECC
  - Quantum

3 Macam algoritma kriptografi

ALGORITMA SIMETRI

- Menggunakan kunci yang sama untuk proses enkripsi dan deskripsi
- Semua kriptografi klasik termasuk ke dalam sistem kriptografi simetri
- DES | RC2, RC4, RC5, RC6 | IDEA | AES | OTP | A5
- 2 kategori operasi mode bit
  - Cipher aliran (steam cipher)
  - 2. Cipher Blok (block cipher)

ALGORITMA ASIMETRI

- Kunci yang digunakan untuk proses enkripsi dan deskripsi berbeda.
- Kunci umum (public) dan Kunci rahasia (private)
- DSA | RSA | DH | ECC | Quantum

HASH FUNCTION

- Suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya kedalam urutan biner dengan panjang yang tetap.
- MD2, MD4, MD5 | SHA | RIPEMD | WHILRLPOOL