

# Kriptografi dengan Teknik Substitusi & Transposisi

Minggu, 28 Juni 2015 | 10:10:11 WIB | Endang Kurniawan

**Kriptografi (cryptography)** berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kriptos dan graphia. Kriptos artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi.

Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Pada prinsipnya, Kriptografi memiliki 4 komponen utama yaitu:

1. Plaintext, yaitu pesan yang dapat dibaca
2. Ciphertext, yaitu pesan acak yang tidak dapat dibaca
3. Key, yaitu kunci untuk melakukan teknik kriptografi
4. Algorithm, yaitu metode untuk melakukan enkripsi dan dekripsi

Kemudian, proses yang akan dibahas dalam artikel ini meliputi 2 proses dasar pada Kriptografi yaitu:

1. Enkripsi (Encryption)
2. Dekripsi (Decryption)

## 1. Teknik Substitusi

Teknik kriptografi dimana merubah huruf-huruf di plaintext (Pesan asli) dengan huruf-huruf lain, angka-angka atau dengan simbol-simbol.

Contoh dengan cara Caesar Cipher

Plain : 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

Cipher : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

### Contoh Kasus :

**Plain : NEWGEN**

**Cipher : q h z j h q**

Cara perhitungan dan algoritmanya adalah setiap huruf plaintext (p), akan disubstitusikan menjadi huruf ciphertext (c) dengan rumus :

### **Rumus Enkripsi**

$C = E(k, p) = (p + k) \bmod 26$  dimana k diambil dari rentang huruf 0 (huruf A) sampai 25 (huruf Z).

### **Rumus Deskripsi**

$P = D(k, c) = (c - k) \bmod 26$

Seperti contoh soal di atas maka untuk menghitung Enkripsi dan Deskripsinya sebagai berikut dengan  $k = 3$

### **Enkripsi**

$N = (13 + 3) \bmod 26 = 16 = q$

$G = (6 + 3) \bmod 26 = 9 = j$

$E = (4 + 3) \bmod 26 = 7 = h$

$E = (4 + 3) \bmod 26 = 7 = h$

$$W = (22 + 3) \bmod 26 = 25 = z$$

$$N = (13 + 3) \bmod 26 = 16 = q$$

Chipertext :  $q h z j h q$

### Deskripsi

$$q = (16 - 3) \bmod 26 = 13 = N$$

$$j = (9 - 3) \bmod 26 = 6 = G$$

$$h = (7 - 3) \bmod 26 = 4 = E$$

$$h = (7 - 3) \bmod 26 = 4 = E$$

$$z = (25 - 3) \bmod 26 = 22 = W$$

$$q = (16 - 3) \bmod 26 = 13 = N$$

Plaintext : **NEWGEN**

## 2. Teknik Transposisi

Teknik kriptografi dimana plaintext (Pesan asli) ditulis perhuruf dalam dua baris dan kemudian dibaca perbaris untuk dijadikan chipertext biasanya ditulis kedalam bentuk matriks.

Contoh dengan cara *The Rail Fence*

Plain : NEW GENERATION

Chiper : NWGNRTOE+EEAIN (disini saya mengganti Spasi dengan +)

Tabel Kriptographi

Image not readable or empty  
/files/tabel.jpg

Semoga bermanfaat.

---

All is about imagination - Endang Kurniawan

Sumber : <https://endangkurniawan.com/article-kriptografi-dengan-teknik-substitusi-amp-transposisi.html>