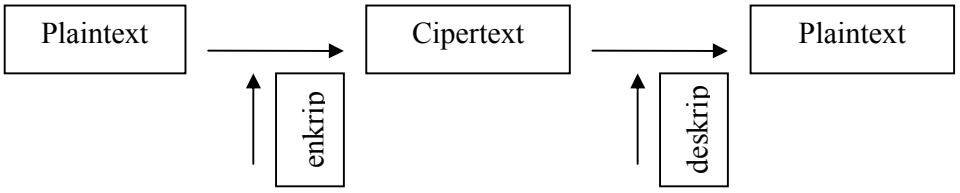
Penyelesaian kriptograpi dengan menggunakan metode cipher hill ditinjau secara analitik dan komputasi

Oleh Akik Hidayat *

Kriptograpi merupakan seni dan ilmu untuk menjaga keamanan pesan. Pesan atau informasi yang dapat dibaca disebut Plaintext, sedangkan pesan yang tidak dapat dibaca disebut Chipertex. Teknik untuk membuat pesan menjadi tidak dapat dibaca disebut Enkripsi sedangkan proses yang merupakan kebalikan dari enkripsi disebut Deskripsi. Jadi deskripsi akan membuat cipertext menjadi plaintext. Secara bagan dapat dinyatakan sbb:



Pada makalah ini akan dibahas metode Shift Cipher, Substitusi cipher, affine cipher, vigenere cipher dan Hill cipher baik secara analitik matematis maupun secara komputasi.

1. Shift Cipher.
$\mathcal{P} = C = \mathcal{K} = \mathcal{Z}_{26}$ untuk $0 <= \mathcal{K} = < 25$ didefinisikan

$E_k(x) = x + K \text{ Mod } 26$

Dan

$D_k(y) = y - K \text{ Mod } 26$

$x,y \in \mathcal{Z}_{26}$, $\mathcal{P}$ = Plaintext, C = Cipertext , $\mathcal{K}$ = Kunci, Z = 0,1,2…,25

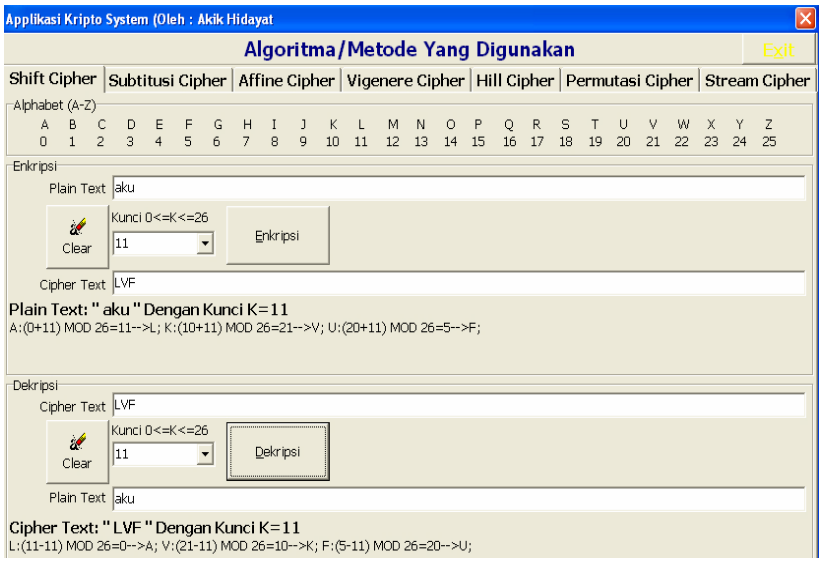
Contoh penyelesaian secara matematis:

Plaintext : aku(0,10,20)
Kunci : 11
Cipertext : $E_k(0) = 0 + 11 \text{ mod } 26 = 11 = L$
: $E_k(10) = 10 + 11 \text{ mod } 26 = 21 = V$
: $E_k(20) = 20 + 11 \text{ mod } 26 = 31 \text{ mod } 26 = 5 = F$

didapat cipertext LVF (11,21,5)

jika hasil cipertext di deskrip maka didapat :
$D_k(11) = 11 - 11 \text{ Mod } 26 = 0 = A$
$D_k(21) = 21 - 11 \text{ Mod } 26 = 10 = K$
$D_k(5) = 5 - 11 \text{ Mod } 26 = -6 \text{ mod } 26 = 20 = U$
Didapat plaintext AKU (0,10,20) yang merupakan plaintext

Contoh penyelesaian secara komputasi :



2. Affine cipher

Mempunyai bentuk umum Sbb :
$\mathcal{P} = C = \mathcal{Z}_{26}$
$\mathcal{K} = \{ (a , b) \in \mathcal{Z}_{26} \times \mathcal{Z}_{26} ; \gcd(a,26) = 1\}$
Untuk K = (a,b) $\in \mathcal{K}$, definisikan

$E_K(x) = ax + b \bmod 26$,
dan
$D_K(y) = a^{-1}(y – b) \bmod 26$
$x,y \in \mathcal{Z}_{26}$, a^{-1} = invers dari a

contoh penyelesaian secara matematis

ambil K = (7,3), plaintext = dago (3,0,6,14)
a = 7, b = 3, gcd(7,26) = 1, $a^{-1} = 15$

$E_K(3) = 7.3+ 3 \bmod 26 = 24 = Y$
$E_K(0) = 7.0+ 3 \bmod 26 = 3 = D$
$E_K(6) = 7.6+ 3 \bmod 26 = 19 = T$
$E_K(14) = 7.14+ 3 \bmod 26 = 23 = X$

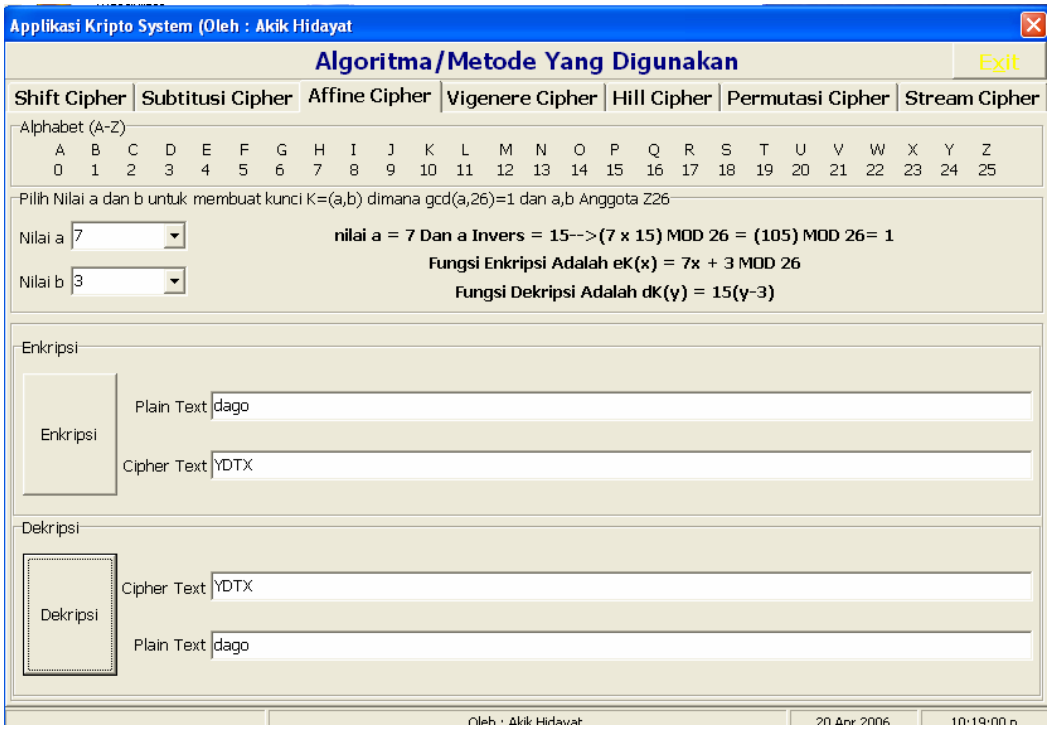
Hasilnya cipertext = YDTX (24,3,19,23)

Jika dideskrip

$D_K(24) = 15(24 – 3) \bmod 26 = 215 \bmod 26 = 3 = D$
$D_K(3) = 15(3 – 3) \bmod 26 = 0 \bmod 26 = 0 = A$
$D_K(19) = 15(19 – 3) \bmod 26 = 240 \bmod 26 = 6 = G$
$D_K(23) = 15(23 – 3) \bmod 26 = 300 \bmod 26 = 14 = O$

Didapat plaintext = DAGO(3,0,6,14)

Contoh penyelesaian Secara komputasi



3. metode cipher hill

Ambil m bilangan bulat positif, dan definisikan $\mathcal{P} = C = (Z_{26})^m$. Diambil m kombinasi linier dari m character alphabetic dalam satu elemen plaintext, maka akan menghasilkan character alphabetic dalam satu elemen cipertext. Dimana P = plaintext, C = cipertext, Z_{26} = Bilangan bulat positif Mod 26.
Misalkan diambil character sebanyak m , maka dapat dibuat elemen plaintext sebagai X = (x_1 , x_2 ,…x_m) dan sebuah elemen cipertext sebagai Y = (y_1 , y_2,....y_m). y_1 merupakan kombinasi linier x_1 dan y_2 merupakan kombinasi linier x_2 . y_m merupakan kombinasi linier x_m , Sehingga dapat dinyatakan sbb :

$y_1 = k_{1,1}x_1 + k_{1,2}x_2 + ...+ k_{1,m}x_m$
$y_2 = k_{2,1}x_1 + k_{2,2}x_2 + ...+ k_{2,m}x_m$
……..
$y_m = k_{m,1}x_1 + k_{m,2}x_2 + ...+ k_{m,m}x_m$

Secara umum persamaan diatas dapat dinyatakan sbb :
$(y_1,y_2,…..,y_m) = (x_1,x_2,…,x_m)$ K (enkrip), dengan kata lain dapat dinyatakan Y = XK.
dimana K matrik ordo mXm, K^{-1} invers matrik K, K = $(k_{i,j})$, i = baris, j = kolom,
$X \in \mathcal{P}$, $\mathcal{Y} \in C$, $K \in \mathcal{K}$, K sebagai kunci.
jika persamaan diatas x_i diganti menjadi y_i, K diganti K^{-1}, maka persamaan tsb menjadi $(x_1,x_2,…..,x_m) = (y_1,y_2,…,y_m)\ K^{-1}$ (deskrip)
dengan kata lain dapat dinyatakan $X = YK^{-1}$.
Jika plaintext di enkript menjadi plaintext dinyatakan sbb :
$(y_1y_2,…,y_m) = (x_1,x_2,…,x_m)$ K
dan sebaliknya cipertext di descript menjadi plaintext dinyatakan sbb :

$(x_1,x_2,\ldots,x_m) = (y_1,y_2,\ldots,y_m)\ K^{-1}$.
CONTOH :

Plantext Dago, Tentukan Chipertext.

$$K = \begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} 1 & 25 \\ 17 & 18 \end{pmatrix}$$

$$DA = (3,0)$$

$$(Y_1, Y_2) = (3 \quad 0)\begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}$$

$$(Y_1, Y_2) = (6 \quad 9)$$

$$= Gj$$

$$GO = (6,14)$$

$$(Y_3, Y_4) = (6 \quad 14)\begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}$$

$$= 12 + 14 \longrightarrow 8 + 42$$

$$= 26 \longrightarrow 60$$

$$= 0 \longrightarrow 8$$

$$= AI$$

Plantext Dalto, Tentukan Chiperter.

$$K = \begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} 1 & 25 \\ 17 & 18 \end{pmatrix}$$

$$DA = (3,0)$$

$$(Y_1, Y_2) = (3 \quad 0)\begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}$$

$$(Y_1, Y_2) = (6 \quad 9)$$

$$= Gj$$

$$GO = (6,14)$$

$$(Y_3, Y_4) = (6 \quad 14)\begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}$$

$$= 12 + 14 \longrightarrow 8 + 42$$

$$= 26 \longrightarrow 60$$

$$= 0 \longrightarrow 8$$

$$= AI$$

Cephertext GJAI

- Deskriptip GJAI = (6,9,0,8)
-

$$(X_1, X_2) = (Y_1, Y_2)K^{-1}$$
$$= (6 \quad 9)\begin{pmatrix} 1 & 25 \\ 17 & 18 \end{pmatrix}$$
$$= (6+153 \longrightarrow 150+162)$$
$$= (159 \longrightarrow 312)$$
$$= (3.0)$$
$$= (DA)$$
$$(X_3, X_4) = (Y_3, Y_2)K^{-1}$$
$$= (0 \quad 8)\begin{pmatrix} 1 & 25 \\ 17 & 18 \end{pmatrix}$$
$$= (136 \quad 144)$$
$$= (6,14)$$
$$= GO$$

Contoh penyelesaian secara komputasi