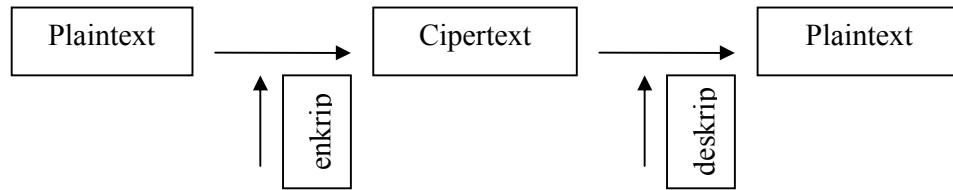


Penyelesaian kriptografi dengan menggunakan metode cipher hill ditinjau secara analitik dan komputasi

Oleh Akik Hidayat *

Kriptografi 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 ciphertext 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.

$P = C = K = \mathbb{Z}_{26}$ untuk $0 \leq K \leq 25$ didefinisikan

$$E_k(x) = x + K \bmod 26$$

Dan

$$D_k(y) = y - K \bmod 26$$

$x, y \in \mathbb{Z}_{26}$, P = Plaintext, C = Ciphertext, K = Kunci, $Z = 0, 1, 2, \dots, 25$

Contoh penyelesaian secara matematis:

| | |
|------------|--|
| Plaintext | : aku(0,10,20) |
| Kunci | : 11 |
| Ciphertext | : $E_k(0) = 0 + 11 \bmod 26 = 11 = L$ |
| | : $E_k(10) = 10 + 11 \bmod 26 = 21 = V$ |
| | : $E_k(20) = 20 + 11 \bmod 26 = 31 \bmod 26 = 5 = F$ |

didapat ciphertext LVF (11,21,5)

jika hasil ciphertext di deskrip maka didapat :

$$D_k(11) = 11 - 11 \bmod 26 = 0 = A$$

$$D_k(21) = 21 - 11 \bmod 26 = 10 = K$$

$$D_k(5) = 5 - 11 \bmod 26 = -6 \bmod 26 = 20 = U$$

Didapat plaintext AKU (0,10,20) yang merupakan plaintext

Contoh penyelesaian secara komputasi :

Algoritma/Metode Yang Digunakan

[Shift Cipher](#) | [Subtitusi Cipher](#) | [Affine Cipher](#) | [Vigenere Cipher](#) | [Hill Cipher](#) | [Permutasi Cipher](#) | [Stream Cipher](#)

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Alphabet (A-Z) | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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 |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Enkripsi:

Plain Text:

Kunci 0 <= K <= 26
11

Cipher Text:

Plain Text: "aku" Dengan Kunci K=11
A:(0+11) MOD 26=11-->L; K:(10+11) MOD 26=21-->V; U:(20+11) MOD 26=5-->F;

Dekripsi:

Cipher Text:

Kunci 0 <= K <= 26
11

Plain Text:

Cipher Text: "LVF" Dengan Kunci K=11
L:(11-11) MOD 26=0-->A; V:(21-11) MOD 26=10-->K; F:(5-11) MOD 26=20-->U;

2. Affine cipher

Mempunyai bentuk umum Sbb :

$$\mathcal{P} = C = \mathbb{Z}_{26}$$

$$\mathcal{K} = \{ (a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} ; \gcd(a, 26) = 1 \}$$

Untuk $K = (a, b) \in \mathcal{K}$ definisikan

$$E_K(x) = ax + b \text{ Mod } 26,$$

dan

$$D_K(y) = a^{-1}(y - b) \text{ Mod } 26$$

$x, y \in \mathbb{Z}_{26}$, a^{-1} = invers dari a

contoh penyelesaian secara matematis

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

$$E_K(3) = 7 \cdot 3 + 3 \text{ Mod } 26 = 24 = Y$$

$$E_K(0) = 7 \cdot 0 + 3 \text{ Mod } 26 = 3 = D$$

$$E_K(6) = 7 \cdot 6 + 3 \text{ Mod } 26 = 19 = T$$

$$E_K(14) = 7 \cdot 14 + 3 \text{ Mod } 26 = 23 = X$$

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

Jika dideskripsikan

$$D_K(24) = 15(24 - 3) \text{ Mod } 26 = 215 \text{ mod } 26 = 3 = D$$

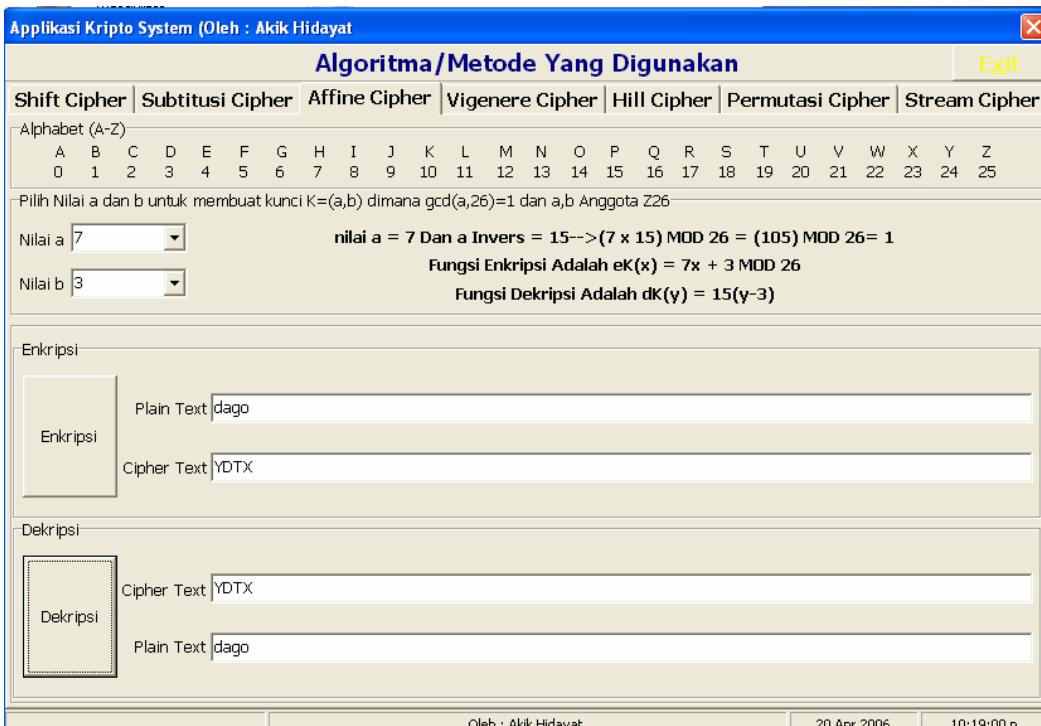
$$D_K(3) = 15(3 - 3) \text{ Mod } 26 = 0 \text{ mod } 26 = 0 = A$$

$$D_K(19) = 15(19 - 3) \text{ Mod } 26 = 240 \text{ mod } 26 = 6 = G$$

$$D_K(23) = 15(23 - 3) \text{ Mod } 26 = 300 \text{ mod } 26 = 14 = O$$

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

Contoh penyelesaian Secara komputasi



3. metode cipher hill

Ambil m bilangan bulat positif, dan definisikan $\mathcal{P} = C = (\mathbb{Z}_{26})^m$. Diambil m kombinasi linier dari m character alphabetic dalam satu elemen plaintext, maka akan menghasilkan character alphabetic dalam satu elemen ciphertext. Dimana P = plaintext, C = ciphertext, Z_{26} = Bilangan bulat positif Mod 26.

Misalkan diambil character sebanyak m , maka dapat dibuat elemen plaintext sebagai $X = (x_1, x_2, \dots, x_m)$ dan sebuah elemen ciphertext sebagai $Y = (y_1, y_2, \dots, y_m)$. 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 :

$$\begin{aligned} y_1 &= k_{1,1}x_1 + k_{1,2}x_2 + \dots + k_{1,m}x_m \\ y_2 &= k_{2,1}x_1 + k_{2,2}x_2 + \dots + k_{2,m}x_m \\ &\dots \\ y_m &= k_{m,1}x_1 + k_{m,2}x_2 + \dots + k_{m,m}x_m \end{aligned}$$

Secara umum persamaan diatas dapat dinyatakan sbb :

$(y_1, y_2, \dots, y_m) = (x_1, x_2, \dots, x_m) K$ (enkrip), dengan kata lain dapat dinyatakan $Y = XK$. dimana K matrik ordo $m \times m$, K^{-1} invers matrik K, $K = (k_{i,j})$, i = baris, j = kolom, $X \in \mathcal{P}$, $Y \in \mathcal{C}$, $K \in \mathcal{K}$, K sebagai kunci.

jika persamaan diatas x_i diganti menjadi y_i , K diganti K^{-1} , maka persamaan tsb menjadi $(x_1, x_2, \dots, x_m) = (y_1, y_2, \dots, y_m) K^{-1}$ (deskrip) dengan kata lain dapat dinyatakan $X = YK^{-1}$.

Jika plaintext di enkripsi menjadi ciphertext dinyatakan sbb :

$$(y_1, y_2, \dots, y_m) = (x_1, x_2, \dots, x_m) K$$

dan sebaliknya ciphertext di descript menjadi plaintext dinyatakan sbb :

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

CONTOH :

Plaintext Dago, Tentukan Chipertext.

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

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

$$DA = (3, 0)$$

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

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

$$= Gj$$

$$GO = (6, 14)$$

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

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

$$= 26 \longrightarrow 60$$

$$= 0 \longrightarrow 8$$

$$= AI$$

Plaintext Dalto, Tentukan Chipertext.

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

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

$$DA = (3, 0)$$

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

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

$$= Gj$$

$$GO = (6, 14)$$

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

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

$$= 26 \longrightarrow 60$$

$$= 0 \longrightarrow 8$$

$$= AI$$

Ciphertext 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

The screenshot shows the application window titled "Applikasi Kripto System (Oleh : Akik Hidayat)". The main title bar says "Algoritma/Metode Yang Digunakan". Below it is a menu bar with tabs: Shift Cipher, Subtitusi Cipher, Affine Cipher, Vigenere Cipher, Hill Cipher, Permutasi Cipher, and Stream Cipher. The "Hill Cipher" tab is selected.

The interface includes several input fields and buttons:

- Alphabet (a-z):** A grid from 0 to 25 corresponding to letters A-Z.
- Input Ordo Matriks Kunci:** An input field containing "2" and a button "Add Elemen".
- Ordo Matriks Kunci : 2 x 2**
- Input Elemen Matriks Kunci:** A grid with elements (2,3), (1,3), and a button "View K & K⁻¹".
- Det=3-->(3)²=9**
- Enkripsi:** A section where "Plain Teks" is "dago" and "Cipher Text" is "GJAI". It also shows the transformation "da(3,0)--go(6,14)--".
- Dekripsi:** A section where "Cipher Text" is "GJAI" and "Plain Teks" is "dago".