

Nama: Aliya Sania

NPM: 1408102110035

Tugas 3

Praktikum Kriptografi

Buatlah program untuk enkripsi, dekripsi, dan mencari kunci Hill Cipher (bahasa pemrograman bebas)

```
# Nama      : Aliya Sania
# NPM       : 1408102110035
# Kelas     : A
# Deskripsi : Tugas 3 Program Hill Cipher

import numpy as np

def hill_cipher(method, text, key, n):
    # Menghitung determinan matriks kunci
    key_det = int(np.linalg.det(key))

    # Cek jika determinan adalah genap atau 13
    if key_det % 2 == 0 or key_det == 13:
        print("Det atau bernilai 13. Tidak ada invers.")
        return

    if len(text) % n != 0:
        last_char = text[-1]
        text = last_char * (n - len(text) % n)

    text_in_number = list(map(char_to_number, list(text)))
    text_vector = np.array(text_in_number).reshape(int(len(text) / n), n)
    result = np.array([], dtype=int)

    if method == 'dekripsi':
        det_inverse = mod_inverse(key_det % 26, 26)
        key = (det_inverse * np.round(key_det *
np.linalg.inv(key)).astype(int) % 26)

    for i in range(len(text_vector)):
        temp = np.matmul(key, text_vector[i].reshape(n, 1)) % 26
        result = np.append(result, temp)

    result = list(map(number_to_char, result))
    output = ''.join(result)
    return output
```

```

def minor(m, i, j):
    m = np.array(m)
    minor = np.zeros(shape=(len(m) - 1, len(m) - 1))
    p = 0
    for s in range(len(minor)):
        if p == i:
            p += 1
        q = 0
        for t in range(len(minor)):
            if q == j:
                q += 1
            minor[s][t] = m[p][q]
            q += 1
        p += 1
    return minor

def find_key(x, y):
    if len(x) != len(y):
        print("Jumlah huruf plaintext dan ciphertext tidak sama!")
        return 0

    m = np.sqrt(len(x)).astype(int)
    x = list(x[: (m * m)].upper())
    mx = list()

    for i in x:
        mx.append(int(ord(i)) - 65)

    mx = np.array(mx).reshape(int(len(x) / m), m)
    adj = np.zeros(shape=(m, m))

    for i in range(m):
        for j in range(m):
            adj[i][j] = (-1) ** (i + j) * int(round(np.linalg.det(minor(mx, j,
i)))) % 26

    y = list(y[: (m * m)].upper())
    my = list()

    for i in y:
        my.append(int(ord(i)) - 65)

    my = np.array(my).reshape(int(len(y) / m), m)
    k = np.dot((int(mod_inverse(round(np.linalg.det(mx)), 26)) *
adj.astype(int) % 26), my) % 26
    return k

def char_to_number(x):

```

```

    x = ord(x) - 65
    return x

def number_to_char(x):
    x = chr(x + 65)
    return x

def mod_inverse(A, M):
    for X in range(1, M):
        if ((A % M) * (X % M)) % M == 1:
            return X
    return -1

def input_key(n):
    key = list(map(int, input("Input nilai matriks kunci (space-separated): ").split()))
    key = np.array(key).reshape(n, n) % 26
    print("Matriks kunci:")
    print(key)
    return key

def input_text(string):
    text = input("Masukkan " + string + ": ")
    text = text.replace(' ', '').upper()
    return text

while True:
    print("\n=== Program Hill Cipher ===")
    print("Menu:")
    print("1. Enkripsi\n2. Dekripsi\n3. Cari Key\n4. Exit")
    pilihan = input("Input opsi: ")

    if pilihan == '1' or pilihan == '2':
        n = int(input("\nSilahkan input ordo matriks kunci (n x n): "))
        key = input_key(n)
        print("\n")
        text = ''

        while len(text) < n:
            text = input_text("teks")
            if len(text) < n:
                print("n harus bil prima terkecil sebagai faktor dari jumlah karakter")

        if pilihan == '1':
            print("\nPlaintext: " + text)
            output = hill_cipher("enkripsi", text, key, n)
            print("Ciphertext: " + output)

```

```

elif pilihan == '2':
    print("\nCiphertext: " + text)
    output = hill_cipher("dekripsi", text, key, n)
    print("Plaintext: " + output)

elif pilihan == '3':
    print("\n")
    pt = input_text("plaintext")
    ct = input_text("ciphertext")
    print("\nPlaintext: " + pt + "\nCiphertext: " + ct)
    key = find_key(pt, ct)
    print("key:")
    print(key)

elif pilihan == '4':
    print("\n Terima kasih sudah memakai program ini. ")
    exit()

else:
    print("\nInput tidak sesuai.\n")

```

Penjelasan code:

Program ini merupakan program dengan Bahasa python untuk melakukan deskripsi, enkripsi, dan mencari key dengan memakai Hill Cipher, berikut penjelasan lebih rincinya:

1. Fungsi Hill Cipher: Ini adalah fungsi utama untuk enkripsi dan dekripsi menggunakan metode Hill Cipher. Fungsi ini mengambil empat argumen: method (untuk menentukan apakah enkripsi atau dekripsi), text (teks yang akan dienkripsi atau didekripsi), key (matriks kunci), dan n (ordo matriks kunci).
2. Validasi Determinan Kunci: Fungsi ini memvalidasi determinan dari matriks kunci. Jika determinan adalah genap atau 13, maka enkripsi atau dekripsi tidak dapat dilakukan.
3. Penyesuaian Teks: Jika panjang teks tidak habis dibagi oleh n, maka teks akan diisi dengan karakter terakhir sehingga panjangnya menjadi kelipatan n. Kemudian, teks diubah menjadi vektor angka dan disusun ulang menjadi matriks.
4. Enkripsi dan Dekripsi: Fungsi ini mengimplementasikan langkah-langkah enkripsi dan dekripsi Hill Cipher sesuai dengan metodenya. Jika metode adalah "dekripsi," maka matriks kunci akan diubah terlebih dahulu sesuai dengan aturan dekripsi.
5. Fungsi Minor: Fungsi ini digunakan untuk menghitung matriks minor dari sebuah matriks dengan menghapus baris dan kolom tertentu.
6. Fungsi Find Key: Fungsi ini digunakan untuk mencari matriks kunci berdasarkan pasangan plaintext dan ciphertext yang diberikan.
7. Fungsi char_to_number dan number_to_char: Fungsi-fungsi ini digunakan untuk mengonversi karakter ke angka dan sebaliknya.
8. Fungsi mod_inverse: Fungsi ini digunakan untuk menghitung invers modular dari suatu angka.
9. Fungsi input_key dan input_text: Fungsi-fungsi ini digunakan untuk meminta input matriks kunci dan teks dari pengguna.

Screenshot program:

1. Enkripsi

```
=== Program Hill Cipher ===
Menu:
1. Enkripsi
2. Dekripsi
3. Cari Key
4. Exit
Input opsi: 1

Silahkan input ordo matriks kunci (n x n): 3
Input nilai matriks kunci (space-separated): 1 4 3 22 15 3 11 3 9
Matriks kunci:
[[ 1  4  3]
 [22 15  3]
 [11  3  9]]

Masukkan teks: KARINA

Plaintext: KARINA
Ciphertext: JLDIHX
```

2. Dekripsi

```
=== Program Hill Cipher ===
Menu:
1. Enkripsi
2. Dekripsi
3. Cari Key
4. Exit
Input opsi: 2

Silahkan input ordo matriks kunci (n x n): 3
Input nilai matriks kunci (space-separated): 1 4 3 22 15 3 11 3 9
Matriks kunci:
[[ 1  4  3]
 [22 15  3]
 [11  3  9]]

Masukkan teks: JLDIHX

Ciphertext: JLDIHX
Plaintext: KARINA
```

3. Find key

=== Program Hill Cipher ===

Menu:

1. Enkripsi
2. Dekripsi
3. Cari Key
4. Exit

Input opsi: 3

Masukkan plaintext: KARINA

Masukkan ciphertext: JLDIHX

Plaintext: KARINA

Ciphertext: JLDIHX

key:

$\begin{bmatrix} 6 & 16 \\ 19 & 3 \end{bmatrix}$

=== Program Hill Cipher ===

Menu:

1. Enkripsi
2. Dekripsi
3. Cari Key
4. Exit

Input opsi: 4

Terima kasih sudah memakai program ini.

PS E:\Kuliah\Sem 5\Kripto\Prak Kripto\35-Kripto23\Hill-Cipher> █