

LAPORAN TUGAS

MATAKULIAH KRIPTOGRAFI

“Implementasi Vegenere Chiper pada Bahasa Pemrograman python”

KELOMPOK 3

Dosen Pengampu : Saiful Nur Budiman, S.Kom,M.Kom



Disusun Oleh:

| | |
|-----------------------------------|--------------------|
| Zoulvia Hanest Khinanti | 22104410011 |
| Rizky Yuniz Teresya | 22104410013 |
| Umi Hanik | 22104410021 |
| Asshyffatul Aina Ni'mah | 22104410044 |
| Bintang Lailatul Mukaromah | 22104410062 |
| M. Lazuardi Al Ghiffary | 22104410045 |

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS ISLAM BALITAR

2025

DAFTAR ISI

| | |
|---|----|
| DAFTAR ISI..... | i |
| BAB I..... | 1 |
| PENDAHULUAN | 1 |
| 1.1 Latar belakang | 1 |
| 1.2 Rumus Masalah..... | 2 |
| 1.3 Tujuan..... | 2 |
| BAB II..... | 3 |
| DASAR TEORI | 3 |
| 2.1 Kriptografi..... | 3 |
| 2.2 Kriptografi Klasik | 3 |
| 2.3 Dua macam cipher algoritma kriptografi klasik..... | 4 |
| 2.4 Vigenere Cipher | 4 |
| 2.5 Visual studio Code | 5 |
| 2.6 Proses Dasar Kriptografi | 5 |
| 2.7 Tujuan Keamanan Kriptografi | 5 |
| 2.8 Python..... | 6 |
| BAB III | 7 |
| PEMBAHASAN..... | 7 |
| 3.1 Rumus Perhitungan Vigenere Chipper..... | 7 |
| 3.2 Implementasi Program Vigenere Chipper Menggunakan Python..... | 9 |
| BAB IV | 12 |
| PENUTUP..... | 12 |
| 4.1 Kesimpulan..... | 12 |
| DAFTAR PUSTAKA | 13 |
| LAMPIRAN..... | 14 |

BAB I

PENDAHULUAN

1.1 Latar belakang

Dalam era digital saat ini, keamanan data menjadi salah satu aspek yang sangat penting dalam proses pertukaran informasi. Setiap hari, data pribadi, pesan, dan informasi sensitif dikirimkan melalui jaringan internet yang sangat rentan terhadap ancaman penyadapan, manipulasi, maupun peretasan. Oleh karena itu, diperlukan suatu metode untuk melindungi data agar tidak mudah dibaca atau diubah oleh pihak yang tidak berwenang. Salah satu cara yang paling umum digunakan untuk menjaga kerahasiaan data adalah dengan menerapkan algoritma kriptografi.

Menurut Renaldi Munir (2019), kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti oleh pihak lain yang tidak berhak. Proses ini melibatkan dua tahap utama, yaitu enkripsi (penyandian pesan asli menjadi bentuk rahasia) dan dekripsi (pengembalian pesan rahasia ke bentuk aslinya). Dengan demikian, hanya pihak yang memiliki kunci tertentu yang dapat membaca isi pesan yang telah dienkripsi.

Algoritma kriptografi klasik merupakan dasar dari perkembangan sistem keamanan modern. Algoritma ini bersifat berbasis karakter, yang artinya proses enkripsi dan dekripsi dilakukan terhadap setiap karakter di dalam pesan. Semua algoritma kriptografi klasik termasuk ke dalam sistem kriptografi simetris, karena kunci yang digunakan untuk proses enkripsi juga digunakan kembali pada proses dekripsi. Contoh algoritma kriptografi klasik antara lain Caesar Cipher, Affine Cipher, dan Vigenere Cipher.

Salah satu algoritma yang terkenal dan sering digunakan dalam pembelajaran kriptografi klasik adalah Vigenere Cipher. Algoritma ini merupakan pengembangan dari Caesar Cipher yang menggunakan kunci polialfabetik, di mana setiap huruf pada pesan akan digeser sesuai dengan huruf kunci yang bersesuaian. Dengan demikian, tingkat keamanannya lebih tinggi dibandingkan Caesar Cipher yang hanya menggunakan satu nilai pergeseran tetap.

Untuk memahami dan mengimplementasikan konsep tersebut secara praktis, dibuatlah sebuah program penerapan algoritma Vigenere Cipher menggunakan bahasa

pemrograman Python. Python dipilih karena memiliki sintaks yang sederhana, mudah dipahami, serta banyak digunakan dalam bidang keamanan data dan penelitian akademik. Program ini dirancang agar pengguna dapat memilih menu interaktif untuk melakukan proses enkripsi dan dekripsi dengan mudah.

Melalui penerapan program ini, diharapkan pengguna dapat memahami bagaimana proses penyandian pesan bekerja, mengenal konsep dasar kriptografi klasik, serta mengetahui penerapan algoritma simetris dalam pengamanan data secara sederhana namun efektif.

1.2 Rumus Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka rumusan masalah dalam pembuatan program ini adalah:

1. Bagaimana cara menerapkan algoritma Vigenere Cipher untuk proses enkripsi dan dekripsi pesan menggunakan bahasa pemrograman Python?
2. Bagaimana program dapat membantu memahami konsep dasar kriptografi klasik berbasis karakter dan sistem kriptografi simetris?

1.3 Tujuan

Adapun tujuan dari pembuatan program ini adalah:

1. Untuk mengimplementasikan algoritma Vigenere Cipher dalam bentuk program Python yang dapat melakukan proses enkripsi dan dekripsi pesan.
2. Untuk memberikan pemahaman praktis tentang penerapan kriptografi klasik dan mekanisme kerja sistem kriptografi simetris.

BAB II

DASAR TEORI

2.1 Kriptografi

Kriptografi berasal dari Bahasa Yunani dan memiliki makna seni dalam menulis pesan rahasia (The art of secret writing), dimana kriptografi terdiri dari 2 kata yaitu κρυπτοψανγ yang berarti rahasia atau tersembunyi dan γραφη yang berarti tulisan. Kriptografi juga disebut ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. (Putra dkk., 2023)

Kriptografi adalah ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data, autentiifikasi entitas dan autentifikasi keaslian data. (Mukhtar, 2018)

2.2 Kriptografi Klasik

Algoritma kriptografi klasik (classical cipher) merupakan jenis algoritma yang berbasis karakter, artinya proses enkripsi dan dekripsi dilakukan terhadap setiap karakter di dalam pesan. Semua algoritma klasik termasuk ke dalam sistem kriptografi simetris, yaitu sistem yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma ini telah digunakan jauh sebelum ditemukannya sistem kriptografi kunci publik, sehingga pembahasan mengenai algoritma klasik juga erat kaitannya dengan sejarah perkembangan kriptografi. (Munir, 2019)

Pentingnya algoritma kriptografi klasik tidak hanya terletak pada nilai historisnya, tetapi juga pada pengaruhnya terhadap pengembangan algoritma kriptografi modern. Hal ini disebabkan karena hampir semua algoritma kriptografi modern, meskipun lebih kompleks, tetap menggunakan dua teknik dasar yang berasal dari algoritma klasik, yaitu substitusi dan transposisi.

2.3 Dua macam cipher algoritma kriptografi klasik

Berdasarkan kedua teknik dasar tersebut, algoritma kriptografi klasik dapat dikelompokkan menjadi dua macam cipher, yaitu:

- a. Cipher Substitusi (Substitution Cipher), yaitu teknik yang mengganti setiap karakter dalam pesan dengan karakter lain sesuai pola atau kunci tertentu.
- b. Cipher Transposisi (Transposition Cipher), yaitu teknik yang menyusun ulang posisi karakter dalam pesan tanpa mengubah karakter itu sendiri. (Nusa, 2019)

Salah satu contoh cipher substitusi yang terkenal adalah Vigenere Cipher, yang bekerja dengan cara menggantikan huruf dalam pesan menggunakan kombinasi kunci huruf yang berulang. Dengan prinsip tersebut, algoritma ini menjadi salah satu pondasi penting dalam memahami dasar-dasar keamanan data melalui kriptografi klasik.

2.4 Vigenere Cipher

Vigenere Cipher merupakan salah satu contoh terbaik dari cipher abjad-banyak (polyalphabetic cipher). Algoritma ini dipublikasikan oleh seorang diplomat dan kriptolog asal Perancis bernama Blaise de Vigenere pada tahun 1586, meskipun konsep awalnya telah diperkenalkan lebih dahulu oleh Giovan Batista Belaso pada tahun 1553 dalam bukunya *La Cifra del Sig. Giovan Batista Belaso*. Algoritma ini baru dikenal luas sekitar dua abad kemudian dan kemudian dinamakan Vigenere Cipher. (Munir, 2019)

Pada pertengahan abad ke-19, algoritma Vigenere berhasil dipecahkan oleh Charles Babbage dan Friedrich Kasiski (Piper, 2002). Cipher ini pernah digunakan oleh Tentara Konfederasi (Confederate Army) pada masa Perang Sipil Amerika, namun pesan-pesan yang dienkripsi dengan metode ini akhirnya berhasil diuraikan oleh pihak lawan.

Vigenere Cipher dikenal luas karena sederhana, mudah dipahami, dan mudah diimplementasikan. Proses enkripsi dilakukan menggunakan bujursangkar Vigenere, yaitu tabel alfabet di mana kolom paling kiri menyatakan huruf-huruf kunci dan baris paling atas menyatakan huruf-huruf plainteks. Setiap baris dalam tabel berisi hasil cipherteks yang diperoleh melalui prinsip Caesar Cipher. Jumlah pergeseran huruf plainteks ditentukan oleh nilai huruf pada kunci — misalnya, huruf kunci C (= 2) berarti setiap huruf plainteks digeser dua huruf ke kanan dari urutan alfabet untuk menghasilkan cipherteks. (V. M. Hidayah dkk., 2023)

2.5 Visual studio Code

Visual Studio Code merupakan editor kode sumber gratis dan open source yang dikembangkan oleh Microsoft. Ini tersedia untuk Windows, macOS, Linux, dan bahkan dapat dijalankan di web browser. VS Code dikenal dengan antarmuka yang ringan dan dapat disesuaikan serta berbagai fitur yang membantu programmer menulis kode dengan lebih efisien.

Dalam beberapa tahun terakhir, Visual Studio Code telah menjadi salah satu editor kode sumber yang paling banyak digunakan di kalangan pengembang. Meskipun demikian, masih ada beberapa aspek usability yang perlu dievaluasi untuk meningkatkan pengalaman pengguna. (N. A. Hidayah & Rofiqoh, 2024)

2.6 Proses Dasar Kriptografi

Kriptografi merupakan ilmu dan seni yang digunakan untuk mengamankan pesan ketika pesan dikirim dari suatu sumber ke tempat tujuan. Proses ini terdiri dari tiga fungsi dasar antara lain:

1. Enkripsi, proses mengubah pesan asli menjadi berbentuk kode-kode yang susah atau bahkan tidak bisa dimengerti.
2. Dekripsi, proses kebalikan dari enkripsi yaitu mengubah pesan yang sudah terenkripsi menjadi pesan asli.
3. Kunci, sekumpulan parameter yang digunakan dalam proses enkripsi maupun dekripsi. (Nusa, 2019)

2.7 Tujuan Keamanan Kriptografi

Kriptografi memiliki beberapa tujuan pada beberapa aspek keamanan sebagai berikut:

1. Kerahasiaan (confidentiality), bertujuan agar pesan tidak bisa dibaca oleh pihak-pihak yang tidak berhak.
2. Integritas data (data integrity), bertujuan agar mendapat jaminan bahwa pesan masih asli/utuh dan tidak dimanipulasi saat pengiriman.
3. Otentikasi (authentication), bertujuan untuk mengidentifikasi kebenaran pihak-pihak yang saling berkomunikasi maupun mengidentifikasi kebenaran pesan.

4. Nirpenyangkalan (non-repudiation), bertujuan agar tidak ada penyangkalan oleh pihak-pihak yang berkomunikasi.(Harahap, 2016)

2.8 Python

Python merupakan bahasa pemrograman simpel untuk pembuatan aplikasi berbasis kecerdasan buatan atau artificial intelligence. Python juga dianggap memiliki fleksibilitas untuk menangani pembuatan aplikasi-aplikasi kekinian yang mengandung kata kunci big data, data mining, deep learning, data science, hingga machine learning (Agung, 2021)

BAB III

PEMBAHASAN

3.1 Rumus Perhitungan Vigenere Chiper

Vigenere cipher merupakan hasil pengembangan lebih lanjut dari Caesar cipher dan termasuk dalam kategori polyalphabetic substitution cipher. Vigenere cipher dapat dilakukan dengan dua cara yaitu dengan cara manual memakai bujur sangkar Vigenere (tabula recta) maupun dengan substitusi angka (matematis). Secara matematis, enkripsi dan dekripsi menggunakan Vigenere cipher dalam kondisi standar dapat dituliskan seperti

$$C_i = (P_i + K_i) \bmod 26 \text{ (ENKRIPSI)}$$

$$P_i = (C_i - K_i) \bmod 26 \text{ (DEKRIPSI)}$$

Berikut ini contoh penggunaan Vigenere cipher dengan susunan alfabet dibawah ini

- **Enkripsi**

Plaintext :

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M | A | H | A | S | I | S | W | A | A | K | H | I | R |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Key :

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | K | R | I | P | S | I | S | K | R | I | P | S | I |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Rumus Enkripsi

$$C_i = (P_i + K_i) \bmod 26$$

Konversi huruf ke angka (A=0, B=1, ..., Z=25).

Proses Enkripsi

Keterangan:

- (P_i) : huruf plaintext ke-i
- (K_i) : huruf key ke-i
- (C_i) : huruf ciphertext ke-i

| Huruf | P (angka) | K | K (angka) | $(P+K) \bmod 26$ | C |
|-------|-----------|---|-----------|------------------|---|
| M | 12 | S | 18 | 4 | E |
| A | 0 | K | 10 | 10 | K |
| H | 7 | R | 17 | 24 | Y |
| A | 0 | I | 8 | 8 | I |
| S | 18 | P | 15 | 7 | H |

| | | | | | |
|---|----|---|----|----|---|
| I | 8 | S | 18 | 0 | A |
| S | 18 | I | 8 | 0 | A |
| W | 22 | S | 18 | 14 | O |
| A | 0 | K | 10 | 10 | K |
| A | 0 | R | 17 | 17 | R |
| K | 10 | I | 8 | 18 | S |
| H | 7 | P | 15 | 22 | W |
| I | 8 | S | 18 | 0 | A |
| R | 17 | I | 8 | 25 | Z |

Ciphertext Hasil Enkripsi: EKYIHAAOKRSWAZ

- **Dekripsi**

Ciphertext

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E | K | Y | I | H | A | A | O | K | R | S | W | A | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Key

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | K | R | I | P | S | I | S | K | R | I | P | S | I |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Rumus Dekripsi

$$P_i = (C_i - K_i + 26) \bmod 26$$

(di mana A=0, B=1, ..., Z=25)

Keterangan:

- (P_i) : huruf plaintext ke-i
- (K_i) : huruf key ke-i
- (C_i) : huruf ciphertext ke-i

Proses Dekripsi

| No | Cipher (C) | Nilai C | Key (K) | Nilai K | $(C - K + 26) \bmod 26$ | Plaintext (P) |
|----|------------|---------|---------|---------|-------------------------------|---------------|
| 1 | E | 4 | S | 18 | $(4 - 18 + 26) \bmod 26 = 12$ | M |
| 2 | K | 10 | K | 10 | $(10 - 10 + 26) \bmod 26 = 0$ | A |
| 3 | Y | 24 | R | 17 | $(24 - 17 + 26) \bmod 26 = 7$ | H |
| 4 | I | 8 | I | 8 | $(8 - 8 + 26) \bmod 26 = 0$ | A |

| | | | | | | |
|----|---|----|---|----|--------------------------------|---|
| 5 | H | 7 | P | 15 | $(7 - 15 + 26) \bmod 26 = 18$ | S |
| 6 | A | 0 | S | 18 | $(0 - 18 + 26) \bmod 26 = 8$ | I |
| 7 | A | 0 | I | 8 | $(0 - 8 + 26) \bmod 26 = 18$ | S |
| 8 | O | 14 | S | 18 | $(14 - 18 + 26) \bmod 26 = 22$ | W |
| 9 | K | 10 | K | 10 | $(10 - 10 + 26) \bmod 26 = 0$ | A |
| 10 | R | 17 | R | 17 | $(17 - 17 + 26) \bmod 26 = 0$ | A |
| 11 | S | 18 | I | 8 | $(18 - 8 + 26) \bmod 26 = 10$ | K |
| 12 | W | 22 | P | 15 | $(22 - 15 + 26) \bmod 26 = 7$ | H |
| 13 | A | 0 | S | 18 | $(0 - 18 + 26) \bmod 26 = 8$ | I |
| 14 | Z | 25 | I | 8 | $(25 - 8 + 26) \bmod 26 = 17$ | R |

Hasil Akhir Dekripsi : MAHASISWAAKHIR

Menggabungkan semua huruf plaintext hasil dekripsi:

3.2 Implementasi Program Vigenere Chiper Menggunakan Python

1. Tampilan Awal Program

```

PS D:\kuliah\Semester 7\Kripto Grafi\UTS> py .\VegenereChiper.py

=====
      KELOMPOK 3 KRIPTOGRFI
      PROGRAM VIGENÈRE CHIPER
=====
1. Enkripsi Teks
2. Dekripsi Teks
3. Keluar
=====
Pilih menu (1/2/3): █

```

Program ini memiliki tampilan awal berupa menu pilihan untuk pengguna. Pada saat program dijalankan, pengguna akan ditampilkan tiga opsi utama, yaitu:

1. Enkripsi Teks, digunakan untuk melakukan proses perubahan teks asli (plaintext) menjadi teks sandi (ciphertext) menggunakan algoritma Vigenere Cipher dengan kunci tertentu.
2. Deskripsi Teks , digunakan untuk mengubah teks sandi (ciphertext) kembali menjadi teks asli (plaintext) menggunakan kunci yang sama.

3. Exit , digunakan untuk keluar dari program.

2. Pilihan Enkripsi Teks

```
=====
      KELOMPOK 3 KRIPTOGRFI
      PROGRAM VIGENÈRE CHIPER
=====
1. Enkripsi Teks
2. Dekripsi Teks
3. Keluar
=====
Pilih menu (1/2/3): 1

Masukkan teks yang ingin dienkrpsi: Mahasiswa Akhir
Masukkan kunci (key): Skripsi

Hasil Enkripsi : EKYIHAAOK RSWAZ
```

Pilihan Enkripsi Teks digunakan untuk mengenkripsi teks asli (*plaintext*) menjadi teks sandi (*ciphertext*) atau kode. Pada menu ini, memasukkan teks asli dan kunci (*key*). Setelah kunci diinputkan, program akan memproses teks menggunakan algoritma Vigenere Cipher, dan hasil enkripsi berupa teks sandi akan ditampilkan di layar seperti gambar diatas.

3. Pilihan Dekripsi teks

```
=====
      KELOMPOK 3 KRIPTOGRFI
      PROGRAM VIGENÈRE CHIPER
=====
1. Enkripsi Teks
2. Dekripsi Teks
3. Keluar
=====
Pilih menu (1/2/3): 2

Masukkan teks yang ingin didekripsi: EKYIHAAOK RSWAZ
Masukkan kunci (key): Skripsi

Hasil Dekripsi : MAHASISWA AKHIR
```

Pilihan Desripsi Teks digunakan untuk mendekripsi atau menguraikan kode *ciphertext* yang telah dienkrpsi sebelumnya menjadi teks asli (*plaintext*) kembali. Pada menu ini, pengguna diminta untuk memasukkan teks sandi (*ciphertext*) dan kunci (*key*). Setelah data dimasukkan, program akan memproses dekripsi menggunakan algoritma Vigenere Cipher, dan hasilnya berupa teks asli yang dapat dibaca akan ditampilkan di layar seperti gambar diatas.

4. Pilihan Exit

```
=====
          KELOMPOK 3 KRIPTOGRAFI
          PROGRAM VIGENÈRE CHIPER
=====
1. Enkripsi Teks
2. Dekripsi Teks
3. Keluar
=====
Pilih menu (1/2/3): 3

Terima kasih telah menggunakan program ini! 🙌
█
```

Menu Exit berfungsi untuk keluar dari program. Saat menu ini dipilih, program akan berhenti berjalan dan menampilkan pesan “Terima kasih telah menggunakan program ini.”

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan pembuatan dan penerapan program Vigenere Cipher menggunakan bahasa pemrograman Python, dapat disimpulkan bahwa algoritma Vigenere Cipher mampu melakukan proses enkripsi dan dekripsi teks dengan baik menggunakan metode substitusi huruf berdasarkan kunci tertentu. Program ini mempermudah pengguna dalam memahami cara kerja dasar kriptografi klasik yang bersifat simetris, di mana proses enkripsi dan dekripsi menggunakan kunci yang sama.

Melalui menu Enkripsi Teks, Deskripsi Teks, dan Exit, pengguna dapat secara interaktif mengubah teks asli menjadi teks sandi dan sebaliknya dengan hasil yang akurat. Pembuatan program ini juga menunjukkan bagaimana konsep dasar kriptografi klasik, khususnya algoritma Vigenere Cipher, dapat diimplementasikan dalam bahasa pemrograman modern seperti Python secara sederhana namun efektif. Dengan demikian, program ini dapat menjadi sarana pembelajaran yang baik untuk memahami prinsip dasar keamanan data melalui proses penyandian dan penguraian pesan.

DAFTAR PUSTAKA

- Agung, G. (2021). *Belajar Sendiri Mengolah Data Dengan Python Dan Pandas Jubilee Enterprise*. PT Elex Media Komputindo.
- Harahap, M. K. (2016). *Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad*. InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan), 1(1), 61–64. <https://doi.org/10.30743/infotekjar.v1i1.43>
- Hidayah, N. A., & Rofiqoh, N. (2024). *Evaluasi Software Visual Studio Code Menggunakan Metode Quetionnaires Nelsen's Attributes Of Usability (Nau)*. Jurnal Perangkat Lunak, 6(3), 382–391. <https://doi.org/10.32520/jupel.v6i3.3383>
- Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). *Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks*. Journal on Education, 5(3), 8563–8573. <https://doi.org/10.31004/joe.v5i3.1647>
- Mukhtar, H. (2018). *Kriptografi Untuk Keamamanan Data*. Cv Budi Utama.
- Munir, R. (2019). *KRIPTOGRAFI*. Informatika Bandung.
- Nusa, A. C. L. (2019). *Kriptoanalisis Algoritma Vigenere Cipher Perbandingan Multi Bahasa*.
- Putra, N. B., Andika, B. C., Bagas, A. D. P., & Ridwan, M. (2023). *Implementasi Sandi Vigenere Cipher Dalam Mengenkripsikan Pesan*. Jurnal JOCOTIS - Journal Science Informatica and Robotics.

LAMPIRAN

```
1
2 def vigenere_encrypt(plaintext, key):
3     plaintext = plaintext.upper()
4     key = key.upper()
5     ciphertext = ""
6     key_index = 0
7     for ch in plaintext:
8         if ch.isalpha():
9             p = ord(ch) - ord('A')
10            k = ord(key[key_index % len(key)]) - ord('A')
11            c = (p + k) % 26
12            ciphertext += chr(c + ord('A'))
13            key_index += 1
14        else:
15            ciphertext += ch
16    return ciphertext
17
18 def vigenere_decrypt(ciphertext, key):
19     ciphertext = ciphertext.upper()
20     key = key.upper()
21     plaintext = ""
22     key_index = 0
23     for ch in ciphertext:
24         if ch.isalpha():
25             c = ord(ch) - ord('A')
26             k = ord(key[key_index % len(key)]) - ord('A')
27             p = (c - k + 26) % 26
28             plaintext += chr(p + ord('A'))
29             key_index += 1
30        else:
31            plaintext += ch
32    return plaintext
33
34
35 def main():
36     while True:
37         print("\n=====")
38         print("      KELOMPOK 3 KRIPTOGRAFI ")
39         print("      PROGRAM VIGENÈRE CHIPHER")
40         print("=====")
41         print("1. Enkripsi Teks")
42         print("2. Dekripsi Teks")
43         print("3. Keluar")
44         print("=====")
45
46         pilihan = input("Pilih menu (1/2/3): ")
47
48         if pilihan == "1":
49             teks = input("\nMasukkan teks yang ingin dienkripsi: ")
50             key = input("Masukkan kunci (key): ")
51             hasil = vigenere_encrypt(teks, key)
52             print(f"\nHasil Enkripsi : {hasil}")
53
54         elif pilihan == "2":
55             teks = input("\nMasukkan teks yang ingin didekripsi: ")
56             key = input("Masukkan kunci (key): ")
57             hasil = vigenere_decrypt(teks, key)
58             print(f"\nHasil Dekripsi : {hasil}")
59
60         elif pilihan == "3":
61             print("\nTerima kasih telah menggunakan program ini! 🍀")
62             break
63
64         else:
65             print("\nPilihan tidak valid! Silakan coba lagi.")
66
67
68 if __name__ == "__main__":
69     main()
```


