Jurnal Sistem dan Teknologi Informasi (JSTI)

https://journalpedia.com/1/index.php/jsti Vol. 06, No. 3 Agustus 2024

IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PYTHON

Diah Triana Sanjaya[1]
Email: diahtriana12@gmail.com

Muhlis Tahir[2]
Email: muhlis.tahir@trunojoyo.ac.id

Ida Fitriana[3]
Email: idafffitriana@gmail.com

Zhafran Elian[4]
Email: zhafranelian2@gmail.com

Rizal Efendi[5]
Email: 210631100124@student.trunojoyo.ac.id

Mustofa Amien[6]
Email: mustofaamien177@gmail.com

Moh. Masudillah[7]
Email: muhammadmasudillah@gmail.com

[1,2,3,4,5,6,7]Universitas Trunojoyo Madura

ABSTRAK

Di era digital seperti sekarang, komunikasi berkembang sangat cepat. Ada banyak faktor yang mempengaruhi kecepatan komunikasi, seperti kemajuan teknologi informasi dan kemudahan mendapatkan alat komunikasi. Di balik perkembangan teknologi dan kemudahan tersebut ada sejumlah risiko. Di antaranya adalah peretasan oleh entitas yang tidak bertanggung jawab. Oleh karena itu, sistem keamanan yang kuat diperlukan untuk proses komunikasi melalui media yang sudah terhubung ke internet untuk mencegah pihak ketiga yang tidak berwenang membocorkan data rahasia dan memanfaatkannya. Salah satu teknik sistem keamanan data dengan menggunakan *kriptografi*. *Kriptografi* bekerja dengan mengacak rangkaian karakter yang dipahami dan dibaca oleh manusia menjadi rangkaian kata atau karakter yang tidak dipahami manusia. Penelitian ini menerapkan rumus algoritma *Vigenere* untuk proses *enkripsi* dan *deskripsi* pada pesan dan hasil pengujiannya dengan mempergunakan bahasa pemrograman *Python*. Hasil penelitian ini diharapkan dapat membantu dalam penerjemahan file yang telah dimodifikasi ke dalam *ciphertext* dan *plaintext*, sehingga pesan yang telah dimodifikasi dapat diterjemahkan dengan tepat.

Kata Kunci: Kriptografi, Vigenere Cipher, dan Python

ABSTRACT

In the digital era like now, communication is developing very quickly. There are many factors that influence the speed of communication, such as advances in information technology and the ease of obtaining communication tools. Behind the development of technology and convenience there are a number of risks. Among these is hacking by irresponsible entities. Therefore, a strong security system is needed for the communication process via media that is connected to the internet to prevent unauthorized third parties from leaking confidential data and making use of it. One of the data security system techniques using cryptography. Cryptography works by scrambling a series of characters that humans understand and read into a series of words or characters that humans cannot understand. This research applies the Vigenere algorithm formula for the encryption process and description of messages and test results using the Python programming language. It is hoped that the results of this research can help in translating modified files into ciphertext and plaintext, so that modified messages can be translated correctly.

Keywords: *Cryptography, Vigenere Cipher, and Python.*

1. PENDAHULUAN

Di era kemajuan teknologi pada masa sekarang, manusia dapat mengirimkan berbagai jenis data. Kebanyakan informasi yang tersebar di dunia digital memicu peningkatan kejahatan siber seperti peretasan dan pencurian data pribadi. Kemajuan teknologi memberikan pengaruh yang besar terhadap hidup manusia. Ini juga membawa suatu perubahan besar dalam masalah keamanan jaringan yang terus menerus berkembang, sehingga kita harus selalu awas atau waspada dalam hal tersebut.

Kriptografi merupakan bidang ilmu yang menggunakan metode matematika yang berkaitan dengan elemen keamanan data seperti kerahasiaan, keutuhan data, dan otentikasi entitas (Triono, Budi and Abdillah, 2023). Kriptografi disebut juga seni serta ilmu yang mempelajari bagaimana membuat pesan yang dikirim pengirim dapat diterima dengan aman. Kriptografi digunakan untuk menjaga kerahasian data sehingga pihak yang tidak berhak tidak dapat mengaksesnya. Kriptografi mempunyai 2 konsep utama yakni enkripsi serta dekripsi. Salah satu teknik kriptografi yang cukup terkenal adalah sandi vigenere.

Vigenere cipher adalah salah satu algoritma kriptografi klasik yang dikembangkan oleh Blaise de Vigenère sejak abad ke 16. Jenis cipher abjad majemuk yang paling sederhana adalah Vigenere cipher, dengan menggunakan metode substitusi polialfabetik. Ini termasuk di kategori kunci simetris, artinya kunci yang dipergunakan untuk enkripsi dan dekripsi sama (Ziaurrahman, Utami and Wibowo, 2019).

Python dibuat Guido Van Rossum di tahun 1991 dan terus dikembangkan oleh Python

Software Foundation hingga saat ini (Ridho and Niani, 2022). Python adalah bahasa pemrograman yang dirancang untuk membantu programmer membuat program dengan cepat, mudah dibuat, dan kompatibel dengan system (Triono, Budi and Abdillah, 2023). Pada penelitian ini, sandi Vigenère akan diimplementasikan dalam bahasa pemrograman Python, untuk melaksanakan enkripsi dan dekripsi data.

Penelitian ini bertujuan melakukan implementasi kriptografi menggunakan metode vigenere cipher dengan python untuk mempermudah mempelajari dan menerjemahkan sandi vigenere cipher

2. LANDASAN TEORI

Kriptografi

Kriptografi bersumber dari bahasa Yunani yang terdiri atas 2 kata yakni *kryptos* dan *graphein*. *Kryptos* yang bermakna tersembunyi dan graphein yang bermakna tulisan. Jadi kriptografi bermakna seni dalam menulis pesan rahasia. Kriptografi ialah teknik menulis pesan rahasia dengan tujuan untuk menyembunyikan makna sebenarnya (Ziaurrahman et al., 2019). Kriptografi terdiri atas 2 proses yakni enkripsi dan deskripsi. Deskripsi ialah fungsi yang digunakan untuk mengembalikan teks sandi atau teks cipher menjadi teks normal atau teks plain, sehingga menjadi data awal atau asli. Di sisi lain, enkripsi adalah fungsi yang dipergunakan untuk mengubah teks plain menjadi teks cipher (Sugeng Murdowo dalam Wibisono et al., 2023).

Vigenere Cipher

Vigenere Cipher mengacu pada metode kriptografi klasik untuk menyandikan pesan dengan mempergunakan tabel alfabet yang terdiri atas 26 huruf standar yang dimulai dari A hingga Z. Dengan mempergunakan deretan sandi caesar yang didasarkan pada huruf-huruf yang terlibat dalam kata kunci, Vigenere Cipher dapat digunakan untuk menyandikan teks alfabet (Bima Putra et al., 2023). Metode ini memungkinkan penggunaan berbagai baris atau kolom dalam tabel Vigenere untuk menyandikan setiap huruf dalam pesan, tergantung pada kata kunci yang diulang (Danuputri et al., 2022).

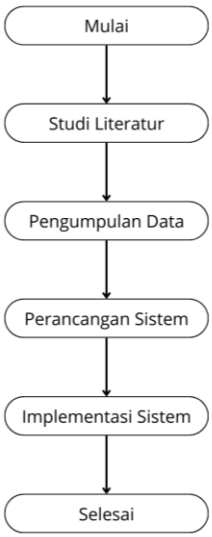
Python

Python mengacu pada bahasa pemrograman interpretatif umum yang menekankan keterbacaan kode guna membuat sintaks lebih mudah dipahami (Ridho & Niani, 2022). Python

berfokus pada kejelasan dan kemudahan pemahaman kode, Python biasanya digunakan untuk script, tetapi cakupannya lebih luas dalam hal kegunaannya.

3. METODE PENELITIAN

Pada tahapan ini, peneliti merancang kerangka kerja penelitian yang meliputi beberapa tahapan yang ada di gambar berikut



A. Uraian kerangka kerja

Kerangka kerja dalam penelitian ini dijelaskan di uraian di bawah ini:

1. Studi Literatur

   Penelitian ini mempergunakan studi pustaka (library research) yakni tinjauan kepustakaan untuk mendapatkan referensi mengenai kriptografi dan vigenere cipher.

2. Pengumpulan Data

   Di penelitian ini, peneliti mengumpulkan data melalui penelitian sebelumnya yang berkaitan dengan kriptografi dan sandi vigenere cipher. Peneliti juga menggunakan penelitian dengan judul terkait dengan penelitian ini.

3. Perancangan Sistem

   Di tahap ini, aplikasi kriptografi vigenere cipher dirancang dan diimplementasikan menggunakan bahasa pemrograman python pada Google Collab.

4. Implementasi Sistem

   Pada tahap ini, pengimplementasian dari program dilakukan dengan metode pelaksanaan program yang sudah dibuat dan melakukan proses enkripsi serta deskripsi pada sandi atau pesan.

4 HASIL DAN PEMBAHASAN

Disini peneliti membuat string berisi alfabet A-Z, yang akan digunakan sebagai indeks dari setiap huruf, di tahap main ini, pengguna akan di minta untuk memasukan inputan, terdapat 3 inputan yang akan diminta, pertama inputan pesan yang ingin di enkripsi atau dekripsi, inputan kedua adalah kata kuncinya, dan inputan terakhir untuk memilih modenya yang berfungsi untuk melakukan proses enkripsi atau dekripsi karena akan di proses dengan kondisi yang digunakan.

```
import pyperclip

HURUF = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

def main():
    pesanSaya = input("Masukkan pesan: ")
    kunciSaya = input("Masukkan kunci: ")
    modeSaya = input("Masukkan mode (enkripsi/dekripsi): ").lower()

    if modeSaya == 'enkripsi':
        ubah = enkripsiPesan(kunciSaya, pesanSaya)
    elif modeSaya == 'dekripsi':
        ubah = dekripsiPesan(kunciSaya, pesanSaya)

    print('%sed pesan : ' % (modeSaya.title()))
    print(ubah)
    print()
```

Bagian ini berfungsi untuk mengubah plaint text menjadi chiper text atau sebaliknya sesuai dengan inputan text, kunci dan modenya

```
def ubahPesan(kunci, pesan, mode):
    ubah = []
    kunciIndex = 0
    kunci = kunci.upper()

    for symbol in pesan:
        nomor = HURUF.find(symbol.upper())
        if nomor != -1:
            if mode == 'enkripsi':
                nomor += HURUF.find(kunci[kunciIndex])
            elif mode == 'dekripsi':
                nomor -= HURUF.find(kunci[kunciIndex])

            nomor %= len(HURUF)

            if symbol.isupper():
                ubah.append(HURUF[nomor])
            elif symbol.islower():
                ubah.append(HURUF[nomor].lower())

            kunciIndex += 1
            if kunciIndex == len(kunci):
                kunciIndex = 0

        else:
            ubah.append(symbol)

    return ''.join(ubah)
```

Full code :

```
import pyperclip

HURUF = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

def main():
    pesanSaya = input("Masukkan pesan: ")
    kunciSaya = input("Masukkan kunci: ")
    modeSaya = input("Masukkan mode (enkripsi/dekripsi):
").lower()

    if modeSaya == 'enkripsi':
        ubah = enkripsiPesan(kunciSaya, pesanSaya)
    elif modeSaya == 'dekripsi':
        ubah = dekripsiPesan(kunciSaya, pesanSaya)

    print('%sed pesan : ' % (modeSaya.title()))
    print(ubah)
    print()

def enkripsiPesan(kunci, pesan):
    return ubahPesan(kunci, pesan, 'enkripsi')

def dekripsiPesan(kunci, pesan):
    return ubahPesan(kunci, pesan, 'dekripsi')

def ubahPesan(kunci, pesan, mode):
    ubah = []
    kunciIndex = 0
    kunci = kunci.upper()

    for symbol in pesan:
        nomor = HURUF.find(symbol.upper())
        if nomor != -1:
            if mode == 'enkripsi':
                nomor += HURUF.find(kunci[kunciIndex])
            elif mode == 'dekripsi':
                nomor -= HURUF.find(kunci[kunciIndex])

            nomor %= len(HURUF)

            if symbol.isupper():
                ubah.append(HURUF[nomor])
            elif symbol.islower():
                ubah.append(HURUF[nomor].lower())

            kunciIndex += 1
            if kunciIndex == len(kunci):
                kunciIndex = 0
        else:
            ubah.append(symbol)

    return ''.join(ubah)

if __name__ == '__main__':
    main()
```

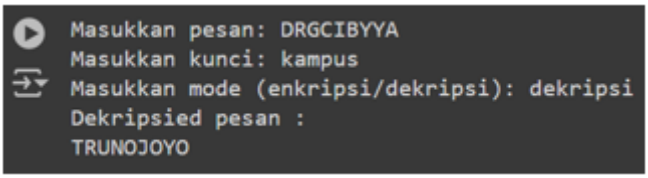
Implementasi Sistem

Dalam penelitian ini, kami memilih kata "TRUNOJOYO" sebagai objek untuk dienkripsi menggunakan bahasa pemrograman Python. Proses enkripsi ini diimplementasikan melalui Google Colab, Hasil dari proses enkripsi ini dapat diperhatikan pada gambar di bawah

```
Masukkan pesan: TRUNOJOYO
Masukkan kunci: kampus
Masukkan mode (enkripsi/dekripsi): enkripsi
Enkripsied pesan :
DRGCIBYYA
```

Hasil enkripsi yang didapatkan dari proses ini adalah "DRGCIBYYA". Untuk memastikan keabsahan dan validitas hasil enkripsi tersebut, kami melakukan langkah tambahan berupa enkripsi lanjutan. Dalam enkripsi lanjutan ini, kami menggunakan metode Reverse Cipher, yang juga diimplementasikan dengan bahasa pemrograman Python. Dengan

melakukan enkripsi tambahan ini, kami dapat lebih yakin bahwa hasil enkripsi awal telah diuji dan diverifikasi dengan benar, menunjukkan ketepatan dan kehandalan dari proses enkripsi yang diterapkan. Implementasi Reverse Cipher ini memberikan lapisan tambahan dalam pengujian, memastikan bahwa semua tahap enkripsi dan dekripsi berfungsi sebagaimana mestinya



Pengujian yang telah kami lakukan menunjukkan bahwa implementasi yang kami kembangkan berhasil dalam mengenkripsi dan mendekripsi pesan dengan benar. Hasil ini memberikan bukti bahwa metode yang kami gunakan berfungsi sesuai dengan yang diharapkan. Keberhasilan ini menegaskan bahwa Vigenère Cipher, meskipun menjadi salah satu metode enkripsi yang sederhana, tetap dapat dipergunakan secara efektif untuk melindungi informasi.

Proses enkripsi dan dekripsi yang berjalan dengan baik menunjukkan bahwa Vigenère Cipher dapat diandalkan dalam situasi yang membutuhkan enkripsi dasar namun tetap efektif. Kami yakin bahwa dengan pemahaman dan penerapan yang tepat, metode ini bisa menjadi solusi yang praktis bagi banyak kebutuhan enkripsi sehari-hari. Hasil ini tidak hanya memperkuat kepercayaan kami terhadap efektivitas Vigenère Cipher, tetapi juga menunjukkan potensi besar dari metode ini untuk diaplikasikan dalam berbagai skenario lain di bidang keamanan data

5 KESIMPULAN

Penelitian ini berhasil mengimplementasikan algoritma kriptografi Vigenère Cipher mempergunakan bahasa pemrograman Python untuk proses enkripsi dan dekripsi pesan. Algoritma Vigenère Cipher terbukti efektif dalam mengamankan informasi dengan mengubah pesan plaintext menjadi ciphertext yang sulit dipahami oleh pihak yang tidak berwenang, dan memungkinkan pengembalian ciphertext ke bentuk plaintext yang dapat dimengerti. Hasil pengujian menunjukkan bahwa pesan yang dienkripsi dan didekripsi menggunakan Vigenère Cipher menghasilkan output yang konsisten dan sesuai dengan yang diharapkan. Dengan pemahaman dan penerapan yang tepat, Vigenère Cipher dapat digunakan untuk berbagai kebutuhan enkripsi sehari-hari, menawarkan solusi praktis dan efektif untuk melindungi

informasi. Penelitian ini menegaskan relevansi Vigenère Cipher dalam konteks keamanan data modern dan membuka peluang untuk pengembangan lebih lanjut serta aplikasi dalam berbagai skenario.

DAFTAR PUSTAKA

Astuti, D. and Sundari, C. (2022) 'Implementasi Algoritma Vigenere Cipher Untuk Enkripsi Dan Dekripsi Pada Peresepan Data Obat Di Puskesmas Mertoyudan 1 Kabupaten Magelang', *Jurnal Teknik Informasi dan Komputer (Tekinkom)*, 5(2), p. 341. doi: 10.37600/tekinkom.v5i2.534.

Gomathi Jawahar, G. *et al.* (2023) 'A Study on Encryption and Decryption using the Caesar Cipher Method', *International Journal of Intelligent Systems and Applications in Engineering IJISAE*, 2023(3), pp. 357–360. Available at: www.iosrjournals.org.

Gulo, T. and Rustam, M. T. (2024) 'Implementasi Keamanan Data Dana Desa Denggan Metode Railfence Cipher Dan Beaufort Cipher (Studi Kasus Kantor Desa Ataualuo)', (1).

Hersan Pratama, H., Fergy Pamungkas, Rw. and Rahmadika, N. (2023) 'Evaluasi Performa Sandi Vigenère pada Data Digital Terenkripsi', 1(1), pp. 32–41. Available at: https://jurnal.ittc.web.id/index.php/jct/.

Irianti, E. *et al.* (2023) 'Implementasi Kriptografi Vigenere Cipher untuk Keamanan Data Informasi Desa', *Progressive Information, Security, Computer, and Embedded System*, 1(1), pp. 8–15. doi: 10.61255/pisces.v1i1.24.

Nepla Bima Putra *et al.* (2023) 'Implementasi Sandi Vigenere Cipher dalam Mengenkripsikan Pesan', *JOCITIS-Journal Science Infomatica and Robotics*, 1(1), pp. 42–50. Available at: https://jurnal.ittc.web.id/index.php/jct/article/view/25.

Noviyanti. P and Mira (2022) 'Analisa Algoritma Kriptografi Klasik Caesar Cipher Viginere Cipher dan Hill Cipher – Study Literature', *Journal of Information Technology*, 2(1), pp. 23–30. doi: 10.46229/jifotech.v2i1.387.

Padmanaban, K. and Apoorva, V. (2024) 'Message Encode-Decode Using Python', 7(2), pp. 126–131.

Pamungkas, C. A., Pratama, Z. and Setiarso, I. (2024) 'Naive Bayes Sentiment Analysis Study on Street Boba And Gildak Kediri Consumen Reviews', 9(1), pp. 109–121.

Putra, M. A. *et al.* (2023) 'Securing Text File Using Combination of Vigenere and One - Time Pad Cipher Algorithm', *Procedia Computer Science*, 227, pp. 1030–1038. doi:

10.1016/j.procs.2023.10.612.

Ridho, A. and Niani, C. R. (2022) 'Implementasi Enkripsi Dengan Vigenere Cipher Dan Reverse Cipher Menggunakan Bahasa Pemrograman Python', *Jurnal Teknologi Informasi*, 1(1), pp. 9–15. doi: 10.35308/.v1i1.5486.

Simangunsong, J. (2018) 'Modifikasi Algoritma Vigenere Cipher Untuk Pengamanan Pesan Rahasia', *... Informasi Neumann (Pitin)*, pp. 23–27. Available at: http://jurnalnya.stmikneumann.ac.id/index.php/pitin/article/download/31/32.

Triono, A., Budi, A. S. and Abdillah, R. (2023) 'Implementasi Peretasan Sandi Vigenere Chipper Menggunakan Bahasa Pemograman Python', *Jurnal JOCOTIS - Journal Science Informatika and Robotics*, 1(1), pp. 1–9. Available at: https://jurnal.ittc.web.id/index.php/jumri.

Wibisono, G. *et al.* (2023) 'Penerapan Dekripsi pada Sandi Vigenere Chiper Menggunakan Metode Kasiski', *Jurnal JOCOTIS-Journal Science Informatica and Robotics E-ISSN : xxxx-xxxx*, 1(1), pp. 52–63.

Ziaurrahman, M., Utami, E. and Wibowo, F. W. (2019) 'Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut', *Jurnal Informatika Interaktif*, 4(2), pp. 63–68.