ESCAF 3rd 2025
p-ISSN : xxx-xxx
e-ISSN:xxx-xxx

Teknik Enkripsi dan Dekripsi Teks dengan Algoritma Caesar Cipher Menggunakan Bahasa Pemrograman Python

Andysah Putera Utama Siahaan[1*], Muhammad Hasanuddin[2]
[1,2]Magister Teknologi Informasi, Universitas Pembangunan Panca Budi, Medan, Indonesia

e-mail: *[1]andiesiahaan@gmail.com, muhammadhasan20feb@gmail.com
*Corresponding Author

Abstrak

Penelitian ini berfokus pada pengembangan aplikasi enkripsi dan dekripsi teks menggunakan algoritma Caesar Cipher dengan antarmuka grafis berbasis Python dan Tkinter. Tujuan dari penelitian ini adalah untuk memberikan pemahaman dasar mengenai konsep enkripsi dan dekripsi, serta menyediakan alat yang memudahkan pengguna dalam melakukan proses tersebut. Dalam penelitian ini, algoritma Caesar Cipher diterapkan untuk mengenkripsi dan mendekripsi teks berdasarkan kunci pergeseran yang ditentukan pengguna. Aplikasi ini menyediakan dua fungsi utama, yaitu enkripsi dan dekripsi, yang dapat diakses dengan antarmuka grafis yang sederhana dan mudah digunakan. Hasil penelitian menunjukkan bahwa meskipun algoritma Caesar Cipher memiliki keterbatasan dalam hal keamanan, aplikasi ini berhasil memberikan pengalaman pembelajaran yang efektif tentang prinsip dasar kriptografi. Saran untuk pengembangan lebih lanjut mencakup peningkatan keamanan dengan menggunakan algoritma enkripsi yang lebih kuat, serta penambahan fitur-fitur tambahan yang dapat memperkaya fungsionalitas aplikasi. Penelitian ini memberikan kontribusi dalam memperkenalkan dan mempermudah pemahaman tentang enkripsi teks dasar bagi para pemula dalam bidang kriptografi.

Kata kunci-Caesar Cipher, enkripsi, dekripsi, data, python

Abstract

This research focuses on the development of an encryption and decryption application using the Caesar Cipher algorithm with a graphical user interface based on Python and Tkinter. The objective of this study is to provide a fundamental understanding of encryption and decryption concepts while offering a tool that simplifies these processes for users. In this study, the Caesar Cipher algorithm is applied to encrypt and decrypt text based on a shift key defined by the user. The application provides two main functions: encryption and decryption, accessible through a simple and user-friendly graphical interface. The results show that although the Caesar Cipher algorithm has limitations in terms of security, the application effectively provides an educational experience on the basic principles of cryptography. Suggestions for further development include enhancing security by using stronger encryption algorithms and adding additional features to enrich the functionality of the application. This research contributes to introducing and simplifying the understanding of basic text encryption for beginners in the field of cryptography.

Keywords- Caesar Cipher, encryption, decryption, data, python

ESCAF 3rd 2024
p-ISSN : xxx-xxx
e-ISSN:xxx-xxx

I. PENDAHULUAN

Keamanan informasi merupakan aspek yang sangat penting dalam era digital saat ini, di mana informasi sensitif sering kali disalurkan melalui jaringan yang rentan terhadap ancaman dan pencurian data. Salah satu cara untuk melindungi data adalah dengan menggunakan teknik enkripsi, yang mengubah data asli menjadi format yang tidak dapat dibaca tanpa proses dekripsi yang sesuai. Enkripsi memainkan peran penting dalam menjaga kerahasiaan data di dunia maya, mulai dari transaksi perbankan hingga pertukaran informasi pribadi (Amin, 2017; Prameshwari & Sastra, 2018). Dalam konteks ini, algoritma Caesar Cipher menjadi salah satu metode enkripsi yang paling sederhana dan terkenal. Meskipun tidak sekuat algoritma enkripsi modern, Caesar Cipher memberikan pemahaman dasar yang baik mengenai prinsip enkripsi dan dekripsi, serta menjadi titik awal yang baik untuk eksplorasi teknik enkripsi lainnya (Pamungkas & Muhammad, 2022; Angriani & Saharaeni, 2019; Noviyanti. & Mira, 2022).

Caesar Cipher bekerja dengan cara mengganti setiap huruf dalam teks dengan huruf lain yang bergeser sejumlah tertentu dalam alfabet. Metode ini, meskipun sederhana, memberikan wawasan yang berharga tentang bagaimana enkripsi dapat dilakukan dan bagaimana informasi dapat dilindungi dari pihak yang tidak berwenang (Noviyanti. & Mira, 2022; saputra & Muhammad, 2021). Dalam penerapannya, pengolahan enkripsi dan dekripsi melalui program komputer dapat menjadi rumit bagi pengguna yang tidak memiliki latar belakang teknis. Oleh karena itu, penggunaan antarmuka grafis pengguna (GUI) yang ramah pengguna menjadi solusi untuk menyederhanakan interaksi antara pengguna dengan sistem. Tkinter, pustaka GUI di Python, memungkinkan pembuatan aplikasi desktop yang mudah digunakan, di mana pengguna dapat dengan mudah memasukkan teks yang ingin dienkripsi atau didekripsi, memilih kunci pergeseran, dan melihat hasilnya secara langsung (Bancin, 2023; Sutoyo, 2024).

Tujuan dari penelitian ini adalah untuk mengembangkan aplikasi enkripsi dan dekripsi teks menggunakan algoritma Caesar Cipher dengan memanfaatkan bahasa pemrograman Python dan pustaka Tkinter untuk membangun antarmuka grafis yang memudahkan interaksi pengguna. Dengan adanya aplikasi ini, diharapkan pengguna dapat memahami dan menggunakan teknik enkripsi dasar ini secara efisien dan efektif (Frobenius & S, 2020; Pasaribu et al., 2022). Penelitian sebelumnya menunjukkan bahwa penggunaan algoritma kriptografi, termasuk Caesar Cipher, dapat meningkatkan keamanan data dan informasi yang ditransmisikan melalui jaringan komunikasi (Amin, 2017; Priambudi & Mufti, 2023). Dengan demikian, aplikasi yang dikembangkan diharapkan dapat memberikan kontribusi signifikan dalam meningkatkan kesadaran dan pemahaman pengguna tentang pentingnya keamanan informasi di era digital ini.

II. TEORI PENDUKUNG

A. Caesar Cipher

Caesar Cipher adalah salah satu teknik enkripsi paling sederhana dan paling awal yang dikenal dalam sejarah kriptografi, dinamai setelah Julius Caesar, yang menggunakannya untuk mengamankan pesan-pesannya kepada jenderal dan sekutunya "undefined" (2021)"Caesar Cipher Techniques", 2024). Teknik ini beroperasi dengan cara menggeser setiap huruf dalam teks asli (plaintext) sejumlah posisi tertentu dalam alfabet. Misalnya, dengan menggunakan kunci pergeseran 3, huruf 'A' akan menjadi 'D', 'B' menjadi 'E', dan seterusnya. Jika huruf yang digeser melewati huruf 'Z', maka pergeseran akan kembali ke huruf 'A' ("Caesar Cipher Techniques", 2024; Berret, 2024).

Meskipun kesederhanaannya, Caesar Cipher dapat memberikan tingkat kerahasiaan dasar yang cukup untuk tujuan pendidikan dan sebagai titik awal untuk

ESCAF 3rd 2024
p-ISSN : xxx-xxx
e-ISSN:xxx-xxx

memahami metode enkripsi yang lebih kompleks ("Caesar Cipher Techniques", 2024; Seyi, 2024). Teknik ini juga memiliki kelemahan yang signifikan; karena hanya melibatkan pergeseran huruf, ia rentan terhadap serangan analisis frekuensi, di mana penyerang dapat dengan mudah memecahkan kode dengan menganalisis frekuensi kemunculan huruf dalam ciphertext (Utomo, 2025; Yu, 2023).

Meskipun Caesar Cipher tidak lagi dianggap aman untuk aplikasi yang memerlukan tingkat keamanan tinggi, teknik ini tetap digunakan dalam pendidikan untuk memperkenalkan konsep dasar kriptografi dan enkripsi (Seyi, 2024; Taher et al., 2022). Selain itu, variasi dan modifikasi dari Caesar Cipher, seperti kombinasi dengan metode lain (misalnya, transposisi), telah dikembangkan untuk meningkatkan keamanan (Lubis et al., 2017; Sparrow et al., 2016). Dengan demikian, Caesar Cipher tetap relevan sebagai alat pembelajaran dan sebagai bagian dari sejarah perkembangan teknik kriptografi.

Tabel 1. Contoh Caesar Cipher

No.	Kata	Pergeseran	Ciphertext	Decrypttext
1	HELLO	3	KHOOR	HELLO
2	WORLD	5	BTAQI	WORLD
3	PYTHON	2	RAVJQP	PYTHON
4	ENCRYPT	4	ISIRXW	ENCRYPT
5	DECRYPT	6	JKUZBT	DECRYPT
6	ALGORITHM	1	BMHSUIJN	ALGORITHM
7	SECURE	3	VHFXUH	SECURE
8	MESSAGE	7	JTLLZJL	MESSAGE
9	SYSTEM	5	XJXJQY	SYSTEM
10	SECURITY	2	UGTGCV	SECURITY

Tabel 1 menunjukkan contoh penerapan algoritma Caesar Cipher pada 10 kata yang berbeda, dengan masing-masing kata menggunakan pergeseran yang berbeda pula. Setiap kata dalam kolom "Kata" dienkripsi dengan pergeseran tertentu pada alfabet, yang ditunjukkan pada kolom "Pergeseran". Hasil enkripsi dari setiap kata ditampilkan pada kolom "Ciphertext", yang merupakan teks yang telah digeser sesuai dengan nilai pergeseran yang diberikan. Misalnya, kata "HELLO" yang memiliki pergeseran 3 menghasilkan ciphertext "KHOOR".

Pada kolom "Decrypttext", proses dekripsi dilakukan untuk mengembalikan ciphertext ke bentuk asli kata yang tidak terpengaruh oleh pergeseran. Dengan menggunakan nilai pergeseran yang sama, kata "KHOOR" yang sebelumnya dienkripsi dengan pergeseran 3 dapat didekripsi kembali menjadi "HELLO". Proses ini menggambarkan cara kerja dasar dari algoritma Caesar Cipher, di mana pergeseran huruf dalam alfabet digunakan untuk mengamankan pesan dan dapat dengan mudah dikembalikan jika diketahui kunci pergeseran yang digunakan. Tabel ini memberikan gambaran bagaimana enkripsi dan dekripsi dengan Caesar Cipher dapat diterapkan pada berbagai kata dengan nilai pergeseran yang berbeda-beda.

B. Python

Python adalah bahasa pemrograman tingkat tinggi yang sangat populer dan banyak digunakan untuk berbagai tujuan pengembangan perangkat lunak. Dikenal karena sintaksisnya yang sederhana dan mudah dipahami, Python memungkinkan programmer untuk menulis kode yang jelas dan efisien, bahkan untuk pemula. Bahasa ini dikembangkan oleh Guido van Rossum pada akhir 1980-an dan pertama kali dirilis pada 1991. Python bersifat interpretatif, artinya kode program dieksekusi baris per baris oleh interpreter, tanpa perlu proses kompilasi yang terpisah.

Python mendukung berbagai paradigma pemrograman, termasuk pemrograman berorientasi objek,

ESCAF 3rd 2024
p-ISSN : xxx-xxx
e-ISSN:xxx-xxx

prosedural, dan fungsional, yang memberi fleksibilitas dalam merancang program. Bahasa ini dilengkapi dengan berbagai pustaka standar dan modul eksternal yang sangat berguna, seperti untuk pengolahan data (pandas, numpy), pengembangan web (Django, Flask), kecerdasan buatan (TensorFlow, scikit-learn), dan banyak lainnya. Keberagaman aplikasi yang dapat dibangun menggunakan Python, ditambah dengan komunitas yang aktif dan banyaknya dokumentasi serta sumber daya pembelajaran, menjadikan Python pilihan utama bagi pengembang perangkat lunak di seluruh dunia.

C. Tkinter

Tkinter adalah pustaka (library) standar di Python yang digunakan untuk membuat aplikasi berbasis antarmuka grafis pengguna (GUI). Sebagai bagian dari Python Standard Library, Tkinter memungkinkan pengembang untuk dengan mudah membuat jendela aplikasi, tombol, label, teks input, dan berbagai elemen grafis lainnya yang diperlukan untuk membangun aplikasi desktop yang interaktif. Tkinter merupakan pembungkus (wrapper) untuk toolkit Tk, yang merupakan pustaka GUI pertama yang dikembangkan untuk bahasa pemrograman Tcl dan kemudian diintegrasikan dengan Python.

Dengan Tkinter, pengguna dapat membangun aplikasi yang mudah digunakan tanpa harus menangani kode yang kompleks untuk antarmuka grafis. Pustaka ini mendukung berbagai komponen GUI seperti kotak dialog, menu, dan kontrol untuk menangani input pengguna, memungkinkan pembuatan aplikasi yang lebih ramah pengguna. Selain itu, Tkinter juga memungkinkan pengembangan aplikasi yang ringan dan portabel, karena aplikasi yang dibangun menggunakan Tkinter dapat dijalankan di berbagai platform, termasuk Windows, macOS, dan Linux, tanpa memerlukan perubahan besar pada kode. Hal ini menjadikan Tkinter pilihan yang sangat populer untuk pembuatan aplikasi desktop yang sederhana hingga menengah di Python.

III. METODOLOGI PENELITIAN

Metodologi dalam pembahasan Caesar Cipher dapat mencakup beberapa langkah utama, sebagai berikut:

1. Pengertian Caesar Cipher: Menjelaskan konsep dasar dari Caesar Cipher, yang merupakan salah satu algoritma enkripsi simetris paling sederhana. Tujuannya adalah untuk mengamankan pesan dengan menggantikan setiap huruf dalam teks dengan huruf lain yang berada pada posisi tertentu dalam alfabet, sesuai dengan jumlah pergeseran yang ditentukan. Proses ini juga membahas bagaimana Caesar Cipher bekerja dan mengapa ia digunakan dalam konteks sejarah enkripsi.
2. Proses Enkripsi: Menjelaskan langkah-langkah yang terlibat dalam proses enkripsi teks menggunakan algoritma Caesar Cipher, termasuk pemilihan pergeseran kunci, penerapan pergeseran pada setiap karakter dalam pesan asli, dan menghasilkan ciphertext. Langkah ini juga mencakup bagaimana teks asli diubah menjadi bentuk yang tidak dapat dibaca tanpa kunci pergeseran yang sesuai.
3. Proses Dekripsi: Menjelaskan langkah-langkah yang terlibat dalam proses dekripsi untuk mengembalikan ciphertext menjadi teks asli. Proses ini melibatkan penggunaan kunci pergeseran yang sama yang digunakan pada saat

ESCAF 3rd 2024
p-ISSN : xxx-xxx
e-ISSN:xxx-xxx

enkripsi, di mana pergeseran diterapkan kembali pada ciphertext untuk memperoleh pesan yang dapat dibaca.

4. Kelebihan dan Kekurangan: Menguraikan kelebihan dan kekurangan dari penggunaan Caesar Cipher, termasuk kesederhanaan dan kemudahan implementasinya, serta keterbatasannya dalam hal keamanan. Caesar Cipher sangat rentan terhadap serangan brute force karena hanya ada 25 kemungkinan pergeseran kunci, yang membuatnya mudah dipecahkan oleh pihak yang tidak berwenang.
5. Perhitungan: Memberikan contoh perhitungan dalam proses enkripsi dan dekripsi menggunakan Caesar Cipher. Contoh ini akan mencakup langkah-langkah pergeseran karakter dalam teks dan bagaimana hasil enkripsi dapat didekripsi kembali menjadi teks asli dengan pergeseran yang benar.
6. Kesimpulan: Meringkaskan dengan menyimpulkan pentingnya Caesar Cipher sebagai salah satu metode enkripsi yang sederhana dengan pemahaman yang baik tentang cara kerjanya, kita dapat menggunakan teknik ini untuk mempelajari prinsip dasar kriptografi sebelum beralih ke algoritma yang lebih kompleks.

IV. HASIL DAN PEMBAHASAN

A. Overview

Program yang ditampilkan dalam screenshot adalah sebuah Aplikasi Kriptografi Caesar Cipher yang digunakan untuk mengenkripsi dan mendekripsi teks. Kriptografi Caesar Cipher adalah salah satu metode kriptografi klasik, di mana setiap huruf dalam teks digeser berdasarkan jumlah kunci tertentu (key). Aplikasi ini dibuat dengan menggunakan antarmuka grafis yang intuitif, memungkinkan pengguna untuk dengan mudah mengenkripsi dan mendekripsi teks sesuai dengan metode Caesar Cipher.

B. Komponen Antarmuka

Program ini memiliki beberapa komponen antarmuka penting yang dirancang secara sederhana dan efektif. Berikut adalah rincian elemen-elemen yang terdapat pada antarmuka pengguna:

1. Judul Program: Terletak di bagian atas aplikasi dengan tulisan “Aplikasi Kriptografi Caesar Cipher” pada latar belakang berwarna hijau. Ini memberikan informasi jelas mengenai fungsi utama program ini.
2. Input Teks (Plaintext): Bagian ini merupakan area input bagi pengguna untuk memasukkan teks yang akan dienkripsi. Pada screenshot, teks yang dimasukkan adalah "Andysah Putera Utama Siahaan."
3. Kode ASCII (ASCII Code): Setelah memasukkan teks, program akan menampilkan representasi ASCII dari setiap karakter dalam teks input. ASCII (American Standard Code for Information Interchange) adalah skema pengkodean yang digunakan untuk merepresentasikan karakter teks dalam komputer. Pada screenshot, kode ASCII dari input teks "Andysah Putera Utama Siahaan" telah ditampilkan dengan angka-angka seperti 65, 110, 100, 121, 115, dan seterusnya.
4. Key (Kunci Enkripsi): Pengguna diminta untuk memasukkan kunci (key) enkripsi, yaitu jumlah pergeseran yang akan diterapkan pada setiap karakter. Dalam program ini, kunci yang digunakan

ESCAF 3rd 2024
p-ISSN : xxx-xxx
e-ISSN:xxx-xxx

adalah "105." Nilai ini menunjukkan berapa banyak posisi yang akan digeser dalam alfabet ASCII untuk mengenkripsi teks.

5. Hasil Enkripsi (Ciphertext): Setelah proses enkripsi, program akan menampilkan ciphertext di area yang disediakan. Ciphertext ini adalah teks terenkripsi yang tidak dapat dibaca tanpa mengetahui kuncinya. Pada contoh ini, ciphertext ditampilkan dengan karakter-karakter yang sudah berubah menjadi simbol-simbol yang sulit dimengerti, seperti "*~íáÛÊÑ→¥ÍÛ£±ÝÍÐ±¥ÊÜÈ£*."
6. Hasil Dekripsi (Decrypttext): Program juga memiliki kemampuan untuk mendekripsi teks yang sudah dienkripsi, mengembalikan ciphertext ke bentuk aslinya (plaintext). Di screenshot, hasil dekripsi menunjukkan teks asli "Andysah Putera Utama Siahaan," yang berarti proses enkripsi dan dekripsi berhasil dilakukan dengan benar menggunakan kunci yang sama.
7. Tombol Fungsi:
   a. Enkrip: Tombol ini digunakan untuk memulai proses enkripsi setelah pengguna memasukkan teks dan kunci.
   b. Dekrip: Tombol ini digunakan untuk mendekripsi ciphertext yang dihasilkan, mengembalikannya ke bentuk asli dengan menggunakan kunci yang sama.
   c. Reset: Tombol ini digunakan untuk menghapus semua input dan hasil yang ada di aplikasi, mengembalikannya ke kondisi semula.
   d. Keluar: Tombol ini digunakan untuk menutup aplikasi.

C. Fungsi Utama Program

Program ini memiliki dua fungsi utama:

1. Enkripsi: Proses enkripsi mengubah teks asli (plaintext) menjadi teks yang tidak dapat dibaca (ciphertext) dengan cara mengganti setiap karakter dalam teks dengan karakter lain yang terletak pada posisi tertentu dalam tabel ASCII. Posisi karakter baru ditentukan oleh kunci yang dimasukkan oleh pengguna. Misalnya, jika pengguna memasukkan kunci "3," maka huruf 'A' akan digeser tiga posisi menjadi huruf 'D'. Dalam contoh di atas, kunci yang digunakan adalah "105," sehingga hasil enkripsinya menghasilkan simbol-simbol yang lebih kompleks karena pergeserannya sangat jauh.
2. Dekripsi: Proses dekripsi mengembalikan ciphertext ke teks asli. Untuk mendekripsi teks, program menggunakan kunci yang sama dengan yang digunakan dalam proses enkripsi. Jika kunci yang digunakan tidak sama, hasil dekripsi tidak akan sesuai dengan teks aslinya. Pada screenshot, teks asli "Andysah Putera Utama Siahaan" berhasil dikembalikan setelah proses dekripsi menggunakan kunci yang tepat.

D. Logika Program

Algoritma Caesar Cipher bekerja berdasarkan pergeseran (shift) karakter dalam alfabet atau kode ASCII. Setiap karakter teks asli (plaintext) diubah dengan menambahkan nilai kunci tertentu ke nilai numeriknya dalam tabel ASCII. Sebagai contoh:

1. Jika plaintext berisi huruf 'A' yang memiliki nilai ASCII 65, dan kunci yang digunakan adalah 3, maka nilai huruf tersebut akan digeser

ESCAF 3rd 2024
p-ISSN : xxx-xxx
e-ISSN:xxx-xxx

menjadi 65 + 3 = 68, yang dalam ASCII adalah huruf 'D'.

2. Proses sebaliknya diterapkan pada dekripsi, yaitu mengurangi nilai kunci dari ciphertext untuk mendapatkan kembali plaintext.

Karakter ASCII dari teks yang dimasukkan dihitung dan digeser sesuai dengan kunci yang diberikan. Pengguna bisa memasukkan kunci apa pun, dan program akan melakukan operasi matematika sederhana pada nilai ASCII untuk menghasilkan ciphertext.

E. Manfaat Program

Program ini sangat bermanfaat untuk tujuan pendidikan atau untuk memahami dasar-dasar kriptografi, khususnya metode Caesar Cipher. Meskipun Caesar Cipher adalah salah satu algoritma enkripsi yang paling sederhana, konsep dasar yang digunakan dalam program ini mencerminkan prinsip umum enkripsi modern, seperti penggunaan kunci untuk mengamankan data. Program ini bisa digunakan untuk:

1. Pelajaran Kriptografi: Digunakan sebagai alat pembelajaran untuk memperkenalkan siswa atau pemula pada konsep dasar enkripsi dan dekripsi.
2. Demo Algoritma Enkripsi: Dapat digunakan oleh dosen atau pengajar untuk mendemonstrasikan bagaimana algoritma Caesar Cipher bekerja dalam praktik.
3. Eksperimen Keamanan: Digunakan untuk eksperimen kecil dalam kriptografi, meskipun algoritma ini tidak cocok untuk aplikasi keamanan yang sebenarnya karena terlalu sederhana.

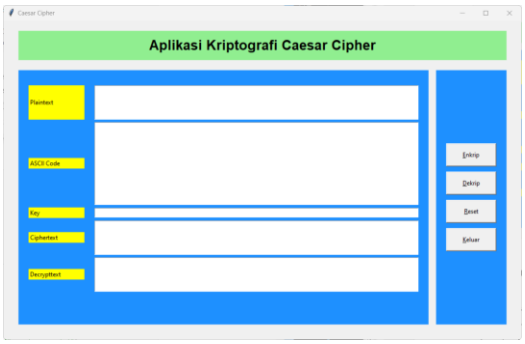
F. Pengujian Program

Program ini dibuka melalui python dengan cara melakukan perintah berikut ini:

1. Tekan tombol Start pada Windows, dan kemudian cari IDLE
2. Klik File, Open dan cari File program Caesar Cipher.py

Gambar 1. Kode program Caesar Cipher

Editor IDLE akan menampilkan kode program dari Caesar Cipher. Langkah berikutnya adalah melakukan Run Module atau menekan F5 sehingga akan tampil program Caesar Ciphernya. Pada tahap ini sudah dapat dilakukan pengujian terhadap program tersebut dalam melakukan enkripsi dan dekripsi dengan algoritma Caesar Cipher.



Gambar 2. Tampilkan program Caesar Cipher

Program yang ditampilkan pada gambar 2 adalah aplikasi untuk enkripsi dan dekripsi menggunakan algoritma Caesar Cipher. Pengguna dapat mengikuti langkah-langkah berikut untuk menggunakan program tersebut:

ESCAF 3rd 2024
p-ISSN : xxx-xxx
e-ISSN:xxx-xxx

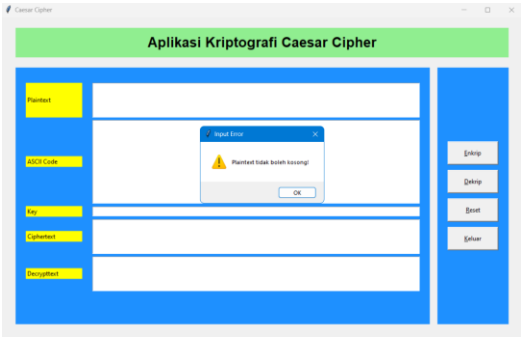
Untuk enkripsi, pertama, masukkan teks yang ingin dienkripsi ke dalam kotak teks yang berlabel "Plaintext" di sebelah kiri. Kemudian, masukkan kunci (key) untuk enkripsi ke dalam kotak teks yang berlabel "Key". Setelah itu, klik tombol "Encrypt" untuk mengenkripsi teks. Hasil enkripsi akan ditampilkan di kotak teks yang berlabel "Ciphertext".

Untuk dekripsi, masukkan teks yang telah terenkripsi (ciphertext) ke dalam kotak teks yang tersedia di sebelah kanan. Masukkan kunci (key) yang sama dengan yang digunakan untuk enkripsi ke dalam kotak teks yang berlabel "Key". Klik tombol "Decrypt" untuk mendekripsi teks. Hasil dekripsi akan ditampilkan di kotak teks yang berlabel "Plaintext".

Selain itu, terdapat tombol lain yang dapat digunakan, seperti tombol "Reset" untuk menghapus semua input dan output, sehingga pengguna dapat memulai proses baru. Tombol "Keluar" digunakan untuk keluar dari aplikasi.

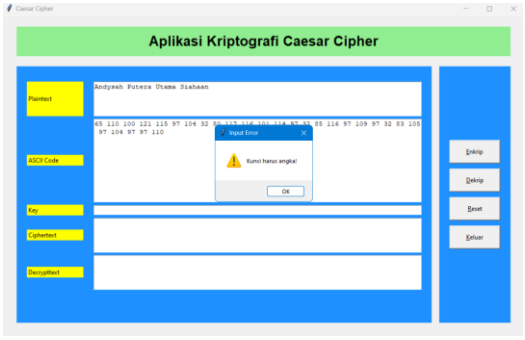
G. Penanganan Kesalahan

Program akan menampilkan error jika tombol Enkrip ditekan ketika tidak ada string yang diinputkan pada textbox Plaintext.



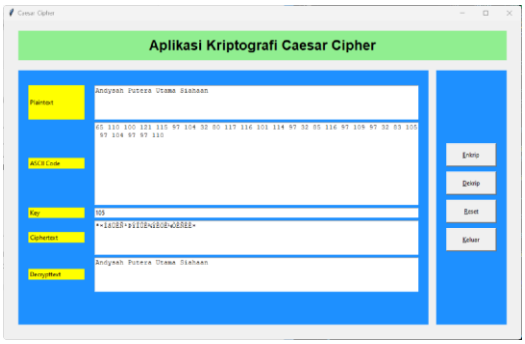
Gambar 3 Pesan kesalahan plaintext

Program akan menampilkan error ketika tombol Enkrip ditekan ketika textbox Key tidak diisi dengan kunci yang sesuai.



Gambar 4. Pesan kesalahan kunci

Program berhasil melakukan proses enkripsi dan dekripsi setelah semua komponen pada textbox dimasukkan dengan benar.



Gambar 5. Program sukses

V. KESIMPULAN

Kesimpulan dari penelitian ini adalah bahwa penggunaan algoritma Caesar Cipher untuk enkripsi dan dekripsi teks memberikan pemahaman yang mendalam mengenai prinsip dasar kriptografi, meskipun algoritma ini memiliki keterbatasan dalam hal keamanan. Dalam penelitian ini, aplikasi yang dibangun dengan menggunakan Python dan Tkinter berhasil mempermudah interaksi pengguna dengan menyediakan antarmuka grafis yang intuitif. Program ini memungkinkan pengguna untuk dengan mudah mengenkripsi dan mendekripsi teks dengan memasukkan teks dan kunci yang sesuai.

Meskipun Caesar Cipher sangat sederhana dan rentan terhadap serangan brute force, aplikasi ini berguna sebagai alat pembelajaran untuk mengenal konsep

ESCAF 3rd 2024
p-ISSN : xxx-xxx
e-ISSN:xxx-xxx

enkripsi dan dekripsi. Penelitian ini juga menunjukkan pentingnya antarmuka grafis dalam meningkatkan pengalaman pengguna, memungkinkan mereka untuk lebih mudah memahami dan mengimplementasikan teknik enkripsi dasar. Dengan pemahaman ini, pengguna dapat melanjutkan eksplorasi lebih lanjut ke algoritma enkripsi yang lebih kompleks dan aman.

VI. SARAN

Berikut beberapa saran yang dapat diberikan berdasarkan hasil penelitian ini:

1. Peningkatan Keamanan Algoritma: Mengingat bahwa Caesar Cipher memiliki keterbatasan dalam hal keamanan, disarankan untuk mengembangkan aplikasi dengan menggunakan algoritma enkripsi yang lebih kuat, seperti AES atau RSA, yang lebih aman dan tidak rentan terhadap serangan brute force. Hal ini akan meningkatkan nilai praktis aplikasi dalam pengamanan data yang lebih sensitif.
2. Fitur Pengaturan Pergeseran Dinamis: Sebagai pengembangan dari aplikasi ini, dapat ditambahkan fitur untuk secara dinamis menghasilkan kunci pergeseran yang lebih kompleks, sehingga pengguna tidak hanya bergantung pada nilai pergeseran statis. Misalnya, memungkinkan penggunaan kunci pergeseran yang lebih panjang atau kunci yang dihasilkan secara acak.
3. Peningkatan Antarmuka Pengguna: Meskipun aplikasi ini sudah menggunakan antarmuka grafis yang sederhana, disarankan untuk menambahkan elemen-elemen desain yang lebih menarik, seperti pemilihan tema atau tampilan yang lebih responsif agar lebih ramah pengguna. Hal ini dapat membantu meningkatkan kenyamanan dan keterlibatan pengguna.
4. Implementasi Penyimpanan dan Pengelolaan Data: Untuk aplikasi yang lebih praktis, dapat ditambahkan fitur untuk menyimpan hasil enkripsi dan dekripsi dalam format yang dapat diakses kembali, seperti file teks atau database. Ini akan memudahkan pengguna dalam mengelola data yang telah terenkripsi.
5. Peningkatan Dokumentasi dan Panduan Penggunaan: Menyediakan panduan atau tutorial yang lebih mendalam tentang cara kerja algoritma Caesar Cipher dalam aplikasi ini akan sangat membantu, terutama bagi pengguna yang baru mengenal konsep enkripsi. Menyediakan penjelasan lebih lanjut mengenai kelebihan dan kekurangan dari algoritma yang digunakan juga akan menambah wawasan pengguna.
6. Eksperimen dengan Berbagai Jenis Input: Untuk memperluas pengujian dan pemahaman pengguna, disarankan untuk melakukan eksperimen dengan berbagai jenis input, seperti teks dengan karakter khusus atau panjang yang bervariasi, untuk memastikan aplikasi dapat menangani semua jenis teks dengan baik.

VII. DAFTAR PUSTAKA

Amin, M. (2017). Implementasi kriptografi klasik pada komunikasi berbasis teks. Pseudocode, 3(2), 129-136. https://doi.org/10.33369/pseudocode.3.2.129-136

Angriani, H. and Saharaeni, Y. (2019).

ESCAF 3rd 2024
p-ISSN : xxx-xxx
e-ISSN:xxx-xxx

Implementasi algoritma caesar cipher pada keamanan data sistem e-voting pemilihan ketua organisasi kemahasiswaan. Inspiration Jurnal Teknologi Informasi Dan Komunikasi, 9(2), 123. https://doi.org/10.35585/inspir.v9i2.2499

Bancin, H. (2023). Implementation of cryptography with the caesar cipher method to secure data files in java netbeans. Jtecs Jurnal Sistem Telekomunikasi Elektronika Sistem Kontrol Power Sistem Dan Komputer, 3(1), 79. https://doi.org/10.32503/jtecs.v3i1.3210

Frobenius, A. and S, E. (2020). Steganografi lsb dengan modifikasi kriptografi: caesar, vigenere, hill cipher dan playfair pada image. Melek It Information Technology Journal, 6(1). https://doi.org/10.30742/melek-it.v6i1.301

Noviyanti., P. (2022). Analisa algoritma kriptografi klasik caesar cipher viginere cipher dan hill cipher – study literature. Journal of Information Technology, 2(1), 23-30. https://doi.org/10.46229/jifotech.v2i1.387

Pamungkas, P. and Muhammad, A. (2022). Modifikasi algoritma kriptografi caesar chiper pada deretan simbol dan huruf di smarphone dan laptop. Journal of Information Technology, 2(1), 1-5. https://doi.org/10.46229/jifotech.v2i1.234

Pasaribu, R., Dewi, R., & Parlina, I. (2022). Implementasi kombinasi algoritma rinjdael dengan caesar cipher pada pengamanan dokumen digital. Hello World Jurnal Ilmu Komputer, 1(1), 36-52. https://doi.org/10.56211/helloworld.v1i1.11

Prameshwari, A. and Sastra, N. (2018). Implementasi algoritma advanced encryption standard (aes) 128 untuk enkripsi dan dekripsi file dokumen. Eksplora Informatika, 8(1), 52. https://doi.org/10.30864/eksplora.v8i1.139

Priambudi, I. and Mufti, M. (2023). Implementasi kriptografi dengan metode aes-128 untuk pengamanan file berbasis web pada smp yapipa. Skanika Sistem Komputer Dan Teknik Informatika, 6(1), 22-31. https://doi.org/10.36080/skanika.v6i1.2997

Supiyandi, S., & Mailok, R. B. Web-Based Geographic Information System to Find Viral Culinary Tourist Spots. *International Journal of Advances in Data and Information Systems*, *5*(2), 588179.

Sutoyo, M. (2024). Pengamanan data berbasis hill cipher dengan operasi modulo pada karakter ascii. Techno Com, 23(4), 786-795. https://doi.org/10.62411/tc.v23i4.11523

saputra, m. and Muhammad, A. (2021). Penerapan kombinasi algoritma caesar cipher pada block acak dan cipher transposisi dalam mengamankan pesan. Journal of Information Technology, 1(1), 22-28. https://doi.org/10.46229/jifotech.v1i1.235