ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.3 No.1 Tahun 2024
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-3 2024
Fakultas Teknik, Universitas Pelita Bangsa, Januari 2024

Implementasi Kriptografi Caesar Chiper dalam Mengubah Pesan Teks Terenkripsi

Implementation of Caesar Ciper cryptography in changing encrypted text messages

Fauzi Farhansyah[1], Muhammad Farhan Atila[2], Ahmad Ridho[3], Medistra Aldrin[4]
[1 2 3 4]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]fauzi.f6703@gmail.com, [2]frhnattila@gmail.com, [3]Ar27production@gmail.com, [4]medistra37@gmail.com

Abstract

This research aims to implement Caesar Cipher cryptography in converting text messages into encrypted messages. The research methods used are literature studies and experiments. The data used in this research are text messages which will be encrypted using the Caesar Cipher.

The research results show that the implementation of the Caesar Cipher cryptography successfully converts text messages into encrypted messages using the correct encryption key. The encryption process using Caesar Cipher can maintain the confidentiality of text messages and can only be read by recipients who have the appropriate encryption key.

Based on the research results, it can be concluded that Caesar Cipher is an effective encryption method and can be used to maintain the confidentiality of text messages. However, Caesar Cipher also has weaknesses, such as being vulnerable to brute force attacks if the encryption key length is too short.

Keywords: *Cryptography, Caesar Cipher, text message, encrypted message, encryption, description.*

Abstrak

Penelitian ini bertujuan untuk mengimplementasikan kriptografi Caesar Cipher dalam mengubah pesan teks menjadi pesan terenkripsi. Metode penelitian yang digunakan adalah studi pustaka dan eksperimen. Data yang digunakan dalam penelitian ini adalah pesan teks yang akan dienkripsi menggunakan Caesar Cipher.

Hasil penelitian menunjukkan bahwa implementasi kriptografi Caesar Cipher berhasil mengubah pesan teks menjadi pesan terenkripsi dengan menggunakan kunci enkripsi yang tepat. Proses enkripsi menggunakan Caesar Cipher dapat menjaga kerahasiaan pesan teks dan hanya dapat dibaca oleh penerima yang memiliki kunci enkripsi yang sesuai.

Berdasarkan hasil penelitian, dapat disimpulkan bahwa Caesar Cipher adalah metode enkripsi yang efektif dan dapat digunakan untuk menjaga kerahasiaan pesan teks. Namun, Caesar Cipher juga memiliki kelemahan, seperti rentan terhadap serangan brute force jika panjang kunci enkripsi terlalu pendek..

Kata kunci: Kriptografi, Caesar Cipher, pesan teks, pesan terenkripsi, enkripsi.

Pendahuluan

Kriptografi adalah ilmu yang mempelajari teknik-teknik untuk menjaga kerahasiaan informasi. Dalam era digital saat ini, keamanan informasi menjadi sangat penting[1]. Salah satu teknik kriptografi yang telah digunakan sejak lama adalah Caesar Cipher. Caesar Cipher adalah metode enkripsi sederhana yang menggunakan tabel Caesar untuk mengubah pesan teks menjadi pesan terenkripsi[2]. Namun, dengan kemajuan teknologi, metode ini dapat dipecahkan dengan mudah menggunakan komputasi yang kuat[3]. Oleh karena itu, implementasi kriptografi Caesar Cipher perlu diperbarui dan ditingkatkan untuk menjaga kerahasiaan pesan teks[4].

Dalam tinjauan literatur, beberapa penelitian terkait dengan implementasi kriptografi Caesar Cipher telah dilakukan. Penelitian-penelitian ini mencoba untuk meningkatkan keamanan dan efisiensi dari metode Caesar Cipher. Sebagai contoh, penelitian yang dilakukan oleh Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks, sementara penelitian yang dilakukan oleh] membahas tentang tinjauan pustaka terkait kriptografi dan Caesar Cipher. Selain itu, melakukan implementasi Caesar Cipher dengan menggunakan metode enkripsi pada teks. Terakhir, membuat implementasi kriptografi Caesar Cipher dengan menggunakan Python.

Penelitian ini dilakukan untuk mengatasi kelemahan-kelemahan yang ada dalam implementasi kriptografi Caesar Cipher yang telah ada[5]. Dengan memperbarui dan meningkatkan metode ini, diharapkan dapat meningkatkan keamanan dan efisiensi dalam mengubah pesan teks menjadi pesan terenkripsi[6]. Selain itu, penelitian ini juga bertujuan untuk menemukan solusi baru yang dapat mengatasi serangan-serangan yang mungkin terjadi pada metode Caesar Cipher[7].

Tujuan dari penelitian ini adalah untuk mengimplementasikan kriptografi Caesar Cipher dengan memperbarui dan meningkatkan metode yang telah ada[8]. Penelitian ini juga bertujuan untuk menguji keamanan dan efisiensi dari implementasi yang baru[9]. Dengan demikian, diharapkan dapat memberikan kontribusi dalam pengembangan teknik kriptografi dan meningkatkan keamanan informasi dalam era digital saat ini[10].

Metode Penelitian

Berikut adalah metode penelitian yang dapat digunakan dalam implementasi kriptografi Caesar Cipher: Dalam penelitian ini bertujuan untuk membuat aplikasi Caesar cipher yang dapat mengenkripsi teks secara rahasia dengan tujuan meningkatkan tingkat keamanan data pesan atau teks.

Penerapan Program

Dalam penelitian ini, kami merinci implementasi program Caesar Cipher menggunakan bahasa pemrograman Python. Tujuan dari penerapan ini adalah untuk mendemonstrasikan proses enkripsi dan dekripsi pesan teks menggunakan metode kriptografi Caesar Cipher. Penelitian ini menggunakan metode studi pustaka untuk mengumpulkan informasi dari berbagai jurnal dan sumber terkait implementasi kriptografi Caesar Cipher. Selain itu, metode eksperimen juga dapat digunakan untuk merancang dan mengimplementasikan sistem baru yang memperbarui dan meningkatkan metode Caesar Cipher yang telah ada.

Rancangan Kegiatan

Rancangan kegiatan penelitian ini meliputi langkah-langkah untuk merancang dan mengimplementasikan metode Caesar Cipher yang baru. Ini melibatkan pemahaman mendalam tentang teori dasar Caesar Cipher, analisis kelemahan yang ada, dan pengembangan solusi baru yang dapat meningkatkan keamanan dan efisiensi.

Ruang Lingkup atau Objek Penelitian

Fokus penelitian ini adalah metode penelitian yang diperlukan untuk mencapai tujuan utama, yaitu menciptakan aplikasi yang menggunakan kombinasi algoritma kriptografi Caesar Cipher untuk meningkatkan tingkat keamanan data teks di aplikasi.

Tempat Penelitian

Lokasi penelitian mencakup lingkungan akademik dan pusat penelitian yang memiliki fasilitas yang sesuai untuk melaksanakan penelitian ini, seperti laboratorium komputer dan akses internet.

Teknik Pengumpulan Data dan Analisis Penelitian

Teknik pengumpulan data dalam penelitian ini dapat melibatkan simulasi komputer, pengujian dengan contoh pesan teks, dan analisis kualitatif terhadap hasil implementasi. Data yang diperoleh akan dianalisis untuk mengevaluasi keamanan dan efisiensi dari implementasi baru Caesar Cipher.

Algoritma Caesar Cipher

Berikut Merupakan Algoritmadasar untuk implementasi Caesar Cipher dalam mengubah teks atau pesan terenkripsi:

Menerima input teks atau pesan yang ingin dienkripsi.

Menerima input jumlah pergeseran yang diinginkan.

Inisialisasi variabel encrypted_text dan decrypted_text sebagai string kosong.

Untuk setiap karakter char dalam teks:

Jika char adalah huruf, lakukan langkah-langkah berikut:

Tentukan ascii_offset berdasarkan huruf kecil atau huruf besar.

Enkripsi karakter dengan mengubah nilai ASCII menggunakan rumus:

(ord(char) - ascii_offset + shift) % 26 + ascii_offset .

Tambahkan karakter terenkripsi ke encrypted_text .

Jika char bukan huruf, tambahkan karakter tersebut ke encrypted_text tanpa mengenkripsinya.

Untuk setiap karakter char dalam teks terenkripsi:

Jika char adalah huruf, lakukan langkah-langkah berikut:

Tentukan ascii_offset berdasarkan huruf kecil atau huruf besar.

Dekripsi karakter dengan mengubah nilai ASCII menggunakan rumus:

(ord(char) - ascii_offset - shift) % 26 + ascii_offset .

Tambahkan karakter terdekripsi ke decrypted_text .

Jika char bukan huruf, tambahkan karakter tersebut ke decrypted_text tanpa mendekripsinya.

Tampilkan teks terenkripsi dengan pergeseran yang diberikan.

Tampilkan teks terdekripsi dengan pergeseran yang diberikan.

Rumus Encrypsi dan Deskrypsi Caesar cipher

Berikut adalah rumus Caesar Cipher untuk mengenkripsi dan mendekripsi teks:

Enkripsi

Pada langkah ini, setiap huruf dalam teks akan digeser ke kanan sebanyak n posisi.

Rumus Caesar Cipher untuk mengenkripsi adalah:

Jika karakter adalah huruf kecil: $E(x) = (x + n) \bmod 26$

Jika karakter adalah huruf besar: $E(x) = (x + n) \bmod 26$

Di sini, x adalah nilai ASCII dari karakter awal dan n adalah jumlah pergeseran yang diinginkan.

Dekripsi

Pada langkah ini, setiap huruf dalam teks terenkripsi akan digeser ke kiri sebanyak n posisi untuk mendapatkan teks asli.

Rumus Caesar Cipher untuk mendekripsi adalah:

Jika karakter adalah huruf kecil: $D(x) = (x - n) \bmod 26$

Jika karakter adalah huruf besar: $D(x) = (x - n) \bmod 26$

Di sini, x adalah nilai ASCII dari karakter terenkripsi dan n adalah jumlah pergeseran yang sama dengan saat mengenkripsi.

Dalam rumus ini, mod adalah operasi modulus yang menghasilkan sisa pembagian.

Ini adalah rumus dasar untuk Caesar Cipher yang dapat digunakan untuk mengenkripsi dan mendekripsi teks.

Apakah ada yang bisa saya bantu?

Hasil dan Pembahasan

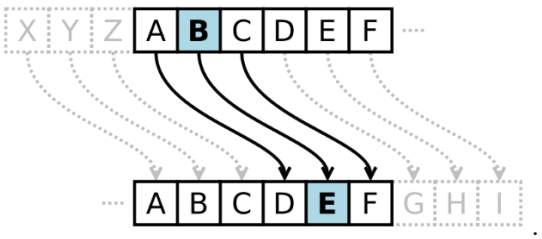
Langkah awal, kita akan mengulas implementasi kriptografi Caesar Cipher dalam mengubah pesan teks terenkripsi dengan menggunakan kunci tertentu. Caesar Cipher merupakan salah satu metode kriptografi klasik yang relatif sederhana, di mana setiap huruf dalam teks diubah sesuai dengan jumlah langkah tertentu.

Inisialisasi Algoritma Caesar Cipher :

Langkah awal melibatkan memulai algoritma Vigenere dengan menetapkan kunci kriptografi yang akan digunakan untuk melindungi teks data. Seperti yang sudah ditentukan pada table Caesar Cipher, yang terdapat pada Tabel 1 dan gambar 1 dibawah.

Tabel 1 Caesar mengganti Huruf dengan Pegeseran 3 huruf

Plainteks	A	B	C	D	E	F	G	H	I	J
Cipherteks	D	E	F	G	H	I	J	K	L	M



Gambar 1 Caesar Mengganti Setiap Huruf Dengan Menggeser 3 huruf

Enkripsi Data Text

Penerapan algoritma Caesar digunakan untuk mengenkripsi data teks yang akan disimpan atau ditukar.Proses ini melibatkan penggunaan kunci sebagai Pergeseran huruf yang akan di enkripsi.

Tabel 2 Hasil Proses Mengencrypsi

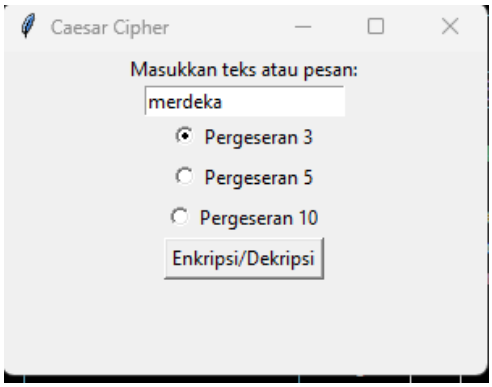
No	Pesan	Kunci	Hasil Enkripsi
1	Merdeka	3	Phughnd
2	Merdeka	5	Rjwijpf
3	Merdeka	10	Wobnouk

Informasi pada pesan awal berubah menjadi bentuk terenkripsi dengan menggunakan suatu kunci Pergeseran 3 huruf, 5 huruf, dan 10 huruf, dan selanjutnya dapat dikembalikan ke bentuk aslinya melalui proses dekripsi. Kunci yang sesuai memiliki peran krusial dalam memastikan keberhasilan proses dekripsi dan mengembalikan teks ke bentuk semula.

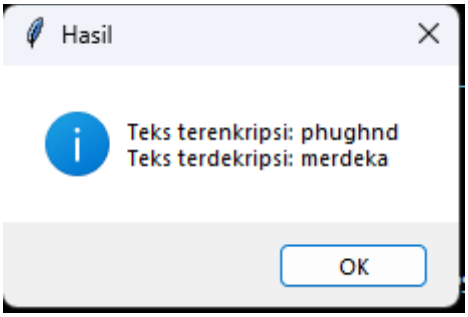
Desain Antarmuka

Desain Antarmuka merupakan suatu sarana komunikasi antara pengguna dan sistem dengan tujuan membuat penggunaan sistem menjadi lebih mudah. Berikut adalah perancangan antarmuka untuk Implementasi Kriptografi Caesar Chiper dalam Mengubah Pesan Teks Terenkripsi. Sebagaimana ilustrasi antarmuka pada program aplikasi terdapat pada gambar dibawah ini:

Program Output:

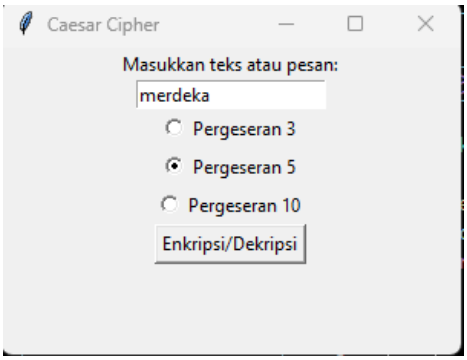


Gambar 2 Proses encrypsi1

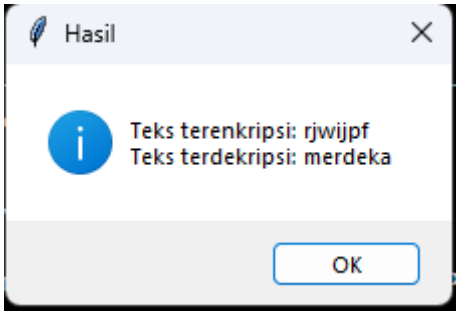


Gambar 3 Hasil encrypsi1

Pada Gambar 2 dan Gambar 3 merupakan contoh tentang proses mengencripsi huruf dengan cara pergeseran 3 huruf. Pada gambar 2 merupakan plainteks yang berisi "Merdeka" yang akan melakukan encrypsi pergeseran 3 ke depan yang menghasilkan encrypsi "phughnd" pada gambar 3.

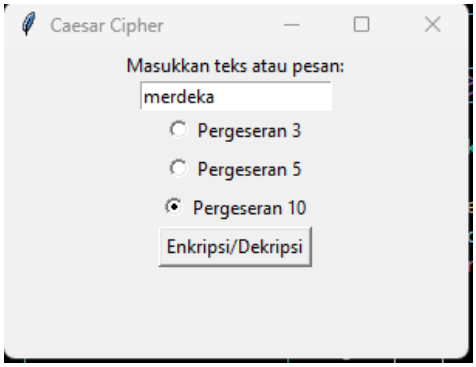


Gambar 4 Proses encrypsi2

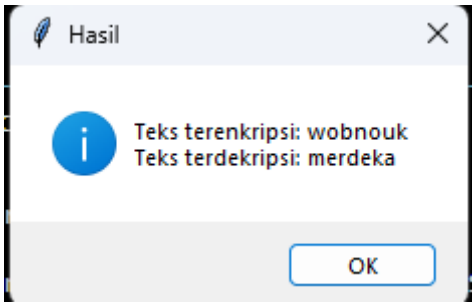


Gambar 5 Hasil encrypsi2

Pada Gambar 4 dan Gambar 5 merupakan contoh tentang proses mengencripsi huruf dengan cara pergeseran 5 huruf. Pada gambar 4 merupakan plainteks yang berisi "Merdeka" yang akan melakukan encrypsi pergeseran 5 ke depan yang menghasilkan encrypsi "rjwijpf" pada gambar 5.



Gambar 6 Proses encrypsi3



Gambar 7 Hasil Encripsi3

Pada Gambar 6 dan Gambar 7 merupakan contoh tentang proses mengencripsi huruf dengan cara pergeseran 10 huruf. Pada gambar 6 merupakan plainteks yang berisi "Merdeka" yang akan melakukan encrypsi pergeseran 10 ke depan yang menghasilkan encrypsi "wobnouk" pada gambar 7.

Kesimpulan

Berdasarkan implementasi kriptografi Caesar Cipher dalam mengubah pesan teks terenkripsi, dapat diambil beberapa kesimpulan sebagai berikut:

Caesar Cipher merupakan metode enkripsi yang sederhana namun dapat memberikan tingkat keamanan yang cukup baik tergantung pada panjang kunci enkripsi yang digunakan.

Implementasi Caesar Cipher berhasil dalam mengubah pesan teks menjadi pesan terenkripsi, namun perlu diperhatikan bahwa metode ini juga memiliki kelemahan, seperti rentan terhadap serangan brute force jika panjang kunci enkripsi terlalu pendek.

Panjang kunci enkripsi Caesar Cipher perlu diperhatikan untuk mencapai tingkat keamanan yang optimal. Panjang kunci minimal yang disarankan adalah 10 karakter.

Saran

Berdasarkan hasil penelitian ini, beberapa saran yang dapat diberikan adalah:

Dalam penggunaan Caesar Cipher, disarankan untuk menggunakan panjang kunci enkripsi yang lebih panjang untuk meningkatkan keamanan. Panjang kunci minimal yang disarankan adalah 10 karakter.

Selain itu, penelitian lebih lanjut dapat dilakukan untuk mengembangkan teknik atau algoritma baru yang dapat meningkatkan keamanan dan efisiensi Caessar Cipher.

Penting untuk memperhatikan kelemahan Caesar Cipher, seperti rentan terhadap serangan brute force. Oleh karena itu, perlu dipertimbangkan penggunaan metode enkripsi lain yang lebih kuat dan aman untuk mengamankan data sensitif.

Dalam implementasi Caesar Cipher, perlu dilakukan pengujian dan evaluasi yang lebih mendalam terhadap keamanan dan efisiensi metode ini, termasuk dalam skenario penggunaan yang berbeda.

Dengan mengikuti saran-saran tersebut, diharapkan dapat meningkatkan keamanan dan efisiensi dalam penggunaan kriptografi Caesar Cipher dalam mengamankan pesan teks.

Daftar Rujukan

[1] V. M. Hidayah, D. Iskandar Mulyana, and Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks," *Journal on Education*, vol. 05, no. 03, pp. 8563–8573, 2023.

[2] D. Veera, R. Mangrulkar, C. Bhadane, K. Bhowmick, and P. Chavan, "Modified Caesar Cipher and Card Deck Shuffle Rearrangement Algorithm for Image Encryption," *Journal of Information and Telecommunication*, 2023, doi: 10.1080/24751839.2023.2285549.

[3] L. Elvitaria and W. Ayu Barus, "Face recognition system with vigenere cipher cryptography for document security," 2023.

[4] "A Secure Substitution Technique for Text Encryption and Decryption Based on ASCII Value." [Online]. Available: www.ijisrt.com

[5] A. Hermawan, A. Halim, D. Susilawati, and I. A. Putri, "Implementasi Algoritma Advance Encryption Standard dan Caesar Cipher pada Pesan Terenkripsi," *Jurnal Informatika dan Rekayasa Perangkat Lunak*, vol. 5, no. 1, p. 13, Mar. 2023, doi: 10.36499/jinrpl.v5i1.6714.

[6] H. Bancin, M. A. Panjaitan, S. Putri, and A. B. Nasution, "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*, vol. 3, no. 1, p. 79, Feb. 2023, doi: 10.32503/jtecs.v3i1.3210.

[7] K. Andrea, A. Wardana, B. S. Wanandi, and A. Ikhwan, "Penerapan Kriptografi Caesar Cipher Pada Fitur Aplikasi Chatting Whatsapp," *Januari*, vol. 2, no. 1, p. 6, 2023, doi: 10.47233/jppie.v2i1.660.

[8] M. Hidayat, M. Tahir, A. Sukriyadi, A. Sulton, C. Ajeng, and S. Abduh, "PENERAPAN KRIPTOGRAFI CAESAR CHIPER DALAM PENGAMANAN DATA," vol. 2, no. 3, doi: 10.56127/jukim.v2i0.

[9] Srivastava, M., Srivastava, U., & Srivastava, S. (2023, Maret). Modifikasi Caesar Cipher dengan Steganografi Gambar. Pada tahun 2023 Konferensi Internasional ke-6 tentang Sistem Informasi dan Jaringan Komputer (ISCON) (hlm. 1-6). IEEE. doi: 10.1109/ISCON57294.2023.10111954

[10] G. Gomathi Jawahar, D. Silvester Anto, T. John Thomas, and M. Jousva, "International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING A Study on Encryption and Decryption using the Caesar Cipher Method." [Online]. Available: www.iosrjournals.org