QISTINA: Jurnal Multidisiplin Indonesia
Vol. 3 No. 2 Desember 2024
P-ISSN: 2964-6278 E-ISSN: 2964-1268

Implementasi Metode Caesar Chiper Dalam Kriptografi Untuk Keamanan Data Pesan

Muhammad Ferdiansyah Hidayat[1] Muhammad Ridho[2] Zulfahmi Indra[3]
Program Studi Ilmu Komputer, Universitas Negeri Medan, Kota Medan, provinsi Sumatera Utara, Indonesia[1,2,3]
Email: ferdihidayat404@gmail.com[1] mhdridhojw2260@gmail.com[2]

Abstrak

Keamanan data dalam era digital merupakan salah satu aspek yang sangat penting, terutama dalam menjaga kerahasiaan dan integritas informasi yang ditransmisikan melalui jaringan. Salah satu metode kriptografi klasik yang sering digunakan untuk mengamankan pesan adalah Caesar Cipher. Metode ini menggunakan teknik substitusi sederhana, di mana setiap huruf dalam pesan digeser sejumlah langkah tertentu dalam alfabet. Penelitian ini membahas implementasi metode Caesar Cipher sebagai solusi dasar untuk keamanan data pesan. Meskipun algoritma ini relatif mudah diterapkan dan dipahami, Caesar Cipher memiliki kelemahan, terutama karena pola penggeseran yang tetap sehingga rentan terhadap serangan brute force atau analisis frekuensi. Melalui pengujian dan implementasi, penelitian ini menunjukkan bagaimana Caesar Cipher bekerja dalam proses enkripsi dan dekripsi, serta mengevaluasi efektivitasnya dalam melindungi pesan dari akses yang tidak sah. Hasilnya menunjukkan bahwa metode ini, meskipun kurang kuat dibandingkan algoritma modern, masih bisa digunakan untuk skenario tertentu yang tidak memerlukan tingkat keamanan yang tinggi. Di sisi lain, kelemahan-kelemahannya menggarisbawahi pentingnya mengembangkan dan menggunakan metode kriptografi yang lebih kompleks untuk melindungi informasi yang lebih sensitif di era digital saat ini.
Kata Kunci: Keamanan Data, Kriptografi, Caesar Cipher, Enkripsi, Dekripsi

Abstract

Data security in the digital era is a very important aspect, especially in maintaining the confidentiality and integrity of information transmitted over the network. One of the classic cryptographic methods that is often used to secure messages is the Caesar Cipher. This method uses a simple substitution technique, where each letter in the message is shifted a certain number of steps in the alphabet. This research discusses the implementation of the Caesar Cipher method as a basic solution for message data security. Although this algorithm is relatively easy to implement and understand, the Caesar Cipher has weaknesses, mainly due to its fixed shifting pattern making it vulnerable to brute force attacks or frequency analysis. Through testing and implementation, this research shows how Caesar Cipher works in the encryption and decryption process, and evaluates its effectiveness in protecting messages from unauthorized access. The results show that this method, although less powerful than modern algorithms, can still be used for certain scenarios that do not require a high level of security. On the other hand, the weaknesses underscore the importance of developing and using more complex cryptographic methods to protect more sensitive information in today's digital era.
Keywords: *Data Security, Cryptography, Caesar Cipher, Encryption, Decryption*

PENDAHULUAN

Dalam era digital yang semakin maju, keamanan data menjadi salah satu fokus utama bagi banyak sektor, termasuk komunikasi, perdagangan elektronik, dan sistem pemerintahan. Peningkatan penggunaan internet dan teknologi informasi menyebabkan pertukaran data secara global terjadi dengan cepat. Namun, hal ini juga memunculkan tantangan baru, yaitu perlindungan terhadap data yang dikirimkan melalui jaringan publik [7]. Keamanan data bertujuan untuk memastikan bahwa informasi yang dikirim hanya dapat diakses oleh pihak

yang berwenang, menjaga integritas data agar tidak dimanipulasi, serta menjaga kerahasiaan dari pihak ketiga yang tidak berwenang. Kriptografi adalah salah satu disiplin ilmu yang berkembang untuk menjawab kebutuhan tersebut. Secara umum, kriptografi melibatkan proses enkripsi dan dekripsi pesan, yang bertujuan untuk mengubah informasi menjadi bentuk yang tidak dapat dibaca oleh orang yang tidak memiliki otoritas [4]. Dalam proses ini, pesan asli disebut plaintext, dan hasil enkripsi disebut ciphertext. Penerima yang memiliki kunci dekripsi dapat mengembalikan ciphertext menjadi plaintext yang dapat dibaca [6]. Teknik ini penting dalam menjaga kerahasiaan dan keamanan data dalam berbagai situasi, termasuk pengiriman pesan, transaksi online, dan penyimpanan informasi sensitif.

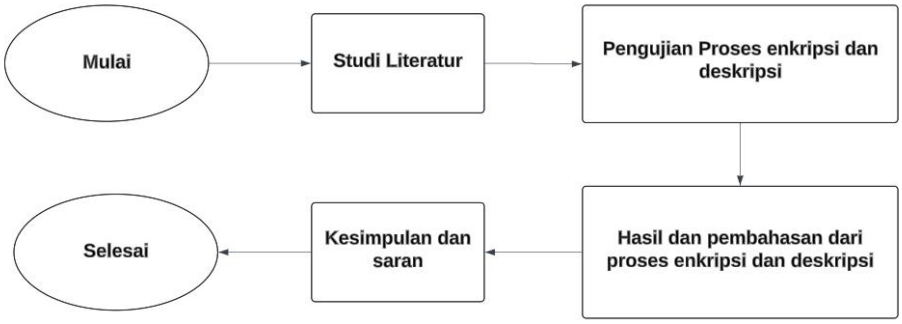
Caesar Cipher adalah salah satu metode enkripsi paling klasik yang dikenal dalam kriptografi. Metode ini diperkenalkan oleh Julius Caesar sebagai alat untuk mengamankan komunikasi militernya. Teknik ini bekerja dengan menggantikan setiap huruf dalam pesan dengan huruf lain yang terletak sejumlah posisi tertentu di dalam alfabet [2]. Misalnya, dengan kunci pergeseran sebesar 3, huruf 'A' akan digantikan dengan 'D', huruf 'B' digantikan dengan 'E', dan seterusnya. Proses ini menghasilkan ciphertext yang sulit dipahami oleh pihak yang tidak mengetahui kunci pergeseran yang digunakan. Meskipun Caesar Cipher dianggap sebagai teknik enkripsi yang sederhana dan mudah dipahami, penting untuk mengenali bahwa metode ini memiliki kelemahan. Dengan perkembangan teknologi dan teknik kriptoanalisis modern, Caesar Cipher dapat dengan mudah dipecahkan menggunakan metode brute force atau analisis frekuensi [5]. Hal ini disebabkan oleh terbatasnya jumlah kemungkinan kunci yang bisa digunakan dalam sistem ini, sehingga mempermudah penyerang untuk menebak kunci yang benar. Meskipun demikian, Caesar Cipher tetap memberikan dasar yang kuat untuk memahami konsep enkripsi dan dekripsi dalam kriptografi.

Penggunaan Caesar Cipher di era modern lebih banyak digunakan sebagai alat pembelajaran dalam pengenalan konsep dasar kriptografi daripada sebagai solusi keamanan yang handal [1]. Namun, metode ini tetap memiliki relevansi sebagai contoh sederhana dalam pengembangan algoritma enkripsi yang lebih kompleks. Dengan mempelajari prinsip-prinsip dasar yang diterapkan dalam Caesar Cipher, seseorang dapat lebih memahami bagaimana metode enkripsi yang lebih maju, seperti Advanced Encryption Standard (AES) atau RSA, bekerja untuk melindungi informasi dalam skala yang lebih luas [3]. Artikel ini akan membahas implementasi metode Caesar Cipher dalam konteks keamanan data pesan. Selain menguraikan mekanisme kerja algoritma ini, artikel ini juga akan mengevaluasi tingkat keamanan yang ditawarkan serta membahas tantangan yang muncul saat menerapkan metode ini di dunia nyata. Tujuannya adalah untuk memberikan pemahaman yang lebih mendalam tentang bagaimana teknik enkripsi sederhana seperti Caesar Cipher dapat berfungsi dan bagaimana batasan-batasannya memengaruhi penggunaannya dalam konteks keamanan informasi.

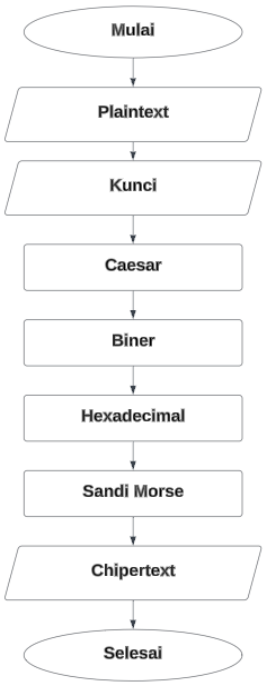
METODE PENELITIAN

Desain Penelitian

Penelitian ini menggunakan metode studi literatur untuk menganalisis implementasi metode Caesar Cipher dalam kriptografi untuk keamanan data pesan. Studi literatur adalah pendekatan yang melibatkan pengumpulan, analisis, dan sintesis berbagai sumber yang relevan dengan topik penelitian. Dalam konteks ini, literatur yang digunakan mencakup buku, jurnal, artikel ilmiah, dan sumber online yang membahas topik kriptografi secara umum serta metode Caesar Cipher secara khusus [8]. Melalui pendekatan ini, penelitian bertujuan untuk mengkaji berbagai aspek teoritis dan praktis terkait dengan penggunaan Caesar Cipher sebagai metode enkripsi pesan, termasuk mekanisme kerjanya, tingkat keamanannya, serta kelemahan yang dimiliki.



Gambar 1. Alur Penelitian



Gambar 2. Flowchart Enkripsi Pesan Teks

Pada penelitian ini, implementasi metode Caesar Cipher dilakukan sebagai salah satu teknik kriptografi untuk mengamankan data pesan [9]. Metode ini melibatkan penggeseran setiap karakter dalam pesan asli (plaintext) dengan sejumlah posisi tertentu dalam alfabet, sehingga menghasilkan pesan terenkripsi (ciphertext).

Persiapan Data dan Penentuan Kunci (Key)

Pesan yang akan diamankan disiapkan dalam bentuk teks biasa (plaintext). Teks ini terdiri dari karakter-karakter alfabet yang akan diproses oleh algoritma Caesar Cipher. Kunci berupa angka bulat digunakan untuk menentukan jumlah pergeseran yang akan diterapkan pada setiap karakter. Misalnya, jika kunci yang digunakan adalah 3, maka setiap karakter dalam pesan akan digeser 3 posisi ke depan dalam alfabet.

Implementasi dalam Program

Algoritma Caesar Cipher diimplementasikan menggunakan bahasa pemrograman Python. Pesan teks diubah menjadi bentuk ciphertext menggunakan fungsi enkripsi, dan pesan asli dapat dikembalikan menggunakan fungsi dekripsi. Implementasi ini juga menangani karakter besar dan kecil, serta mempertahankan karakter non-alfabet tanpa perubahan.

Uji Coba dan Evaluasi

Uji coba dilakukan dengan menginput beberapa pesan plaintext dan kunci yang berbeda untuk melihat hasil enkripsi dan dekripsinya. Selain itu, efektivitas algoritma juga dievaluasi dalam hal keamanan data dan kecepatan pemrosesan. Evaluasi ini dilakukan dengan membandingkan hasil dari berbagai kunci dan panjang pesan untuk melihat apakah pesan dapat dikembalikan dengan benar tanpa kehilangan informasi.

HASIL PENELITIAN DAN PEMBAHASAN

Proses Enkripsi

Sebuah proses mengubah data atau informasi asli (plaintext) menjadi bentuk yang tidak bisa dibaca (ciphertext) dengan menggunakan algoritma tertentu dan sebuah kunci enkripsi [10]. Setiap karakter dalam plaintext diubah menjadi karakter lain dengan aturan berikut:

1. Jika karakter adalah huruf alfabet, maka karakter tersebut digeser sebanyak posisi yang ditentukan oleh kunci. Jika posisi melebihi jumlah huruf alfabet (misalnya huruf "Z" dengan kunci 3), maka perhitungan dilakukan dengan melingkar kembali ke awal alfabet (misalnya, "Z" akan berubah menjadi "C").
2. Karakter non-alfabet seperti spasi, tanda baca, atau angka tidak diubah.

   Contoh kasus, Jika diberikan plaintext sebagai berikut :

   Plaintext : “JURUSAN ILMU KOMPUTER”

   Dengan mengubah setiap huruf menjadi bilangan bulat A = 0, B = 1, ..., Z = 25, Persamaan berikut dapat digunakan untuk memindahkan tiga huruf alfabet secara matematis dari plaintext P ke ciphertext C. Ini sama dengan melakukan operasi modulo [11].

   Kunci: 3

   Rumus yang digunakan untuk proses enkripsi adalah:

   $C=(P+K) \bmod 26$

   J (9) → (9 + 3) mod 26 = 12 → M
   U (20) → (20 + 3) mod 26 = 23 → X
   R (17) → (17 + 3) mod 26 = 20 → U
   U (20) → (20 + 3) mod 26 = 23 → X
   S (18) → (18 + 3) mod 26 = 21 → V
   A (0) → (0 + 3) mod 26 = 3 → D
   N (13) → (13 + 3) mod 26 = 16 → Q
   I (8) → (8 + 3) mod 26 = 11 → L
   L (11) → (11 + 3) mod 26 = 14 → O
   M (12) → (12 + 3) mod 26 = 15 → P
   U (20) → (20 + 3) mod 26 = 23 → X
   K (10) → (10 + 3) mod 26 = 13 → N
   O (14) → (14 + 3) mod 26 = 17 → R
   M (12) → (12 + 3) mod 26 = 15 → P
   P (15) → (15 + 3) mod 26 = 18 → S
   U (20) → (20 + 3) mod 26 = 23 → X
   T (19) → (19 + 3) mod 26 = 22 → W
   E (4) → (4 + 3) mod 26 = 7 → H
   R (17) → (17 + 3) mod 26 = 20 → U

   Kemudian didapat hasil ciphertext: “MXUXVDQ LOPX NRPSXWHU”

Proses Dekripsi

Untuk mengembalikan pesan terenkripsi ke bentuk aslinya, dilakukan proses dekripsi. Setiap karakter dalam ciphertext digeser ke belakang dengan jumlah posisi yang sama dengan

kunci yang digunakan saat enkripsi.

Ciphertext: “MXUXVDQ LOPX NRPSXWHU”
Kunci: 3
Rumus untuk proses dekripsi adalah:
P=(C-K) mod 26
M (12) → (12 - 3) mod 26 = 9 → J
X (23) → (23 - 3) mod 26 = 20 → U
U (20) → (20 - 3) mod 26 = 17 → R
X (23) → (23 - 3) mod 26 = 20 → U
V (21) → (21 - 3) mod 26 = 18 → S
D (3) → (3 - 3) mod 26 = 0 → A
Q (16) → (16 - 3) mod 26 = 13 → N
L (11) → (11 - 3) mod 26 = 8 → I
O (14) → (14 - 3) mod 26 = 11 → L
P (15) → (15 - 3) mod 26 = 12 → M
X (23) → (23 - 3) mod 26 = 20 → U
N (13) → (13 - 3) mod 26 = 10 → K
R (17) → (17 - 3) mod 26 = 14 → O
P (15) → (15 - 3) mod 26 = 12 → M
S (18) → (18 - 3) mod 26 = 15 → P
X (23) → (23 - 3) mod 26 = 20 → U
W (22) → (22 - 3) mod 26 = 19 → T
H (7) → (7 - 3) mod 26 = 4 → E
U (20) → (20 - 3) mod 26 = 17 → R
Maka plaintext yang di dapat adalah: “JURUSAN ILMU KOMPUTER”

Implementasi

Antarmuka Pengguna

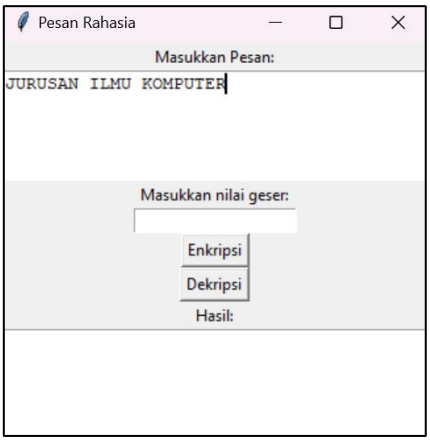
Aplikasi ini dilengkapi dengan antarmuka yang sederhana dan mudah digunakan. Pengguna cukup memasukkan pesan pada kolom input, memberikan nilai geser yang diinginkan, lalu memilih tombol **"Enkripsi"** atau **"Dekripsi"** sesuai dengan kebutuhan. Hasil dari proses enkripsi atau dekripsi akan ditampilkan pada kolom output di bagian bawah aplikasi.

Gambar 3. Tampilan Antarmuka

Fitur antarmuka yang digunakan memanfaatkan pustaka **Tkinter** pada Python, yang menyediakan elemen-elemen seperti kotak teks untuk input pesan dan output hasil, serta tombol interaktif untuk mengontrol proses enkripsi dan dekripsi.

Tulis Pesan

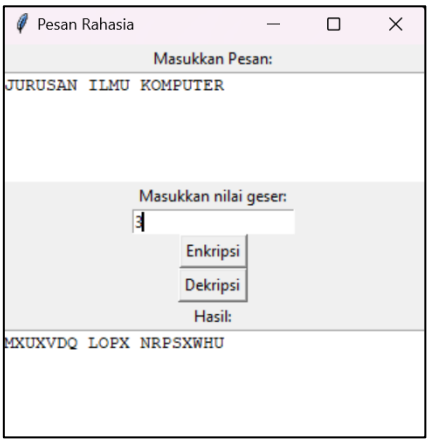
Pada bagian ini pengguna dapat menginputkan data atau pesan dan melakukan proses enkripsi dan dekripsi.



Gambar 4. Halaman Input Data

Pesan enkripsi

Pada bagian ini pengguna dapat memasukkan kunci yang diinginkan dan melakukan proses enkripsi. Halaman

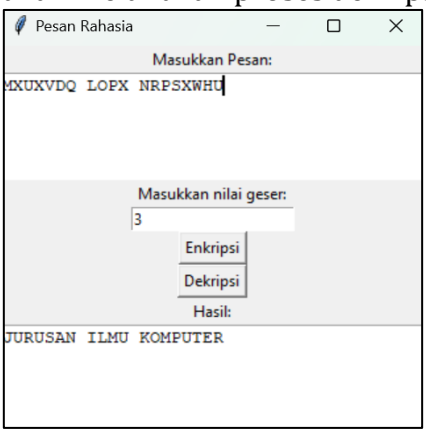


Gambar 5. Halaman Enkripsi

Maka hasil enkripsi akan terlihat pada bagian hasil (output).

Pesan dekripsi

Pada bagian ini pengguna akan melakukan proses dekripsi.



Gambar 6. Halaman Dekripsi

KESIMPULAN

Implementasi Caesar Cipher dalam kriptografi memberikan dasar pemahaman yang kuat terkait prinsip enkripsi dan dekripsi pesan. Meskipun metode ini tergolong sederhana dan memiliki kelemahan keamanan yang dapat dengan mudah ditembus menggunakan teknik modern seperti brute force atau analisis frekuensi, Caesar Cipher tetap relevan sebagai alat pembelajaran. Metode ini membantu memperkenalkan konsep dasar kriptografi dan memberikan fondasi untuk memahami teknik enkripsi yang lebih kompleks. Dalam dunia modern, penggunaannya lebih banyak pada tujuan pendidikan daripada sebagai solusi keamanan yang dapat diandalkan.

DAFTAR PUSTAKA

Amalya, Nanda, et al. "Kriptografi Dan Penerapannya Dalam Sistem Keamanan Data." Jurnal Media Informatika, vol. 4, no. 2, 9 June 2023, pp. 90–93, https://doi.org/10.55338/jumin.v4i2.428. Accessed 12 Oct. 2024.

Aranski, Alvendo Wahyu, et al. "Implementasi Algoritma Caesar Cipher Untuk Keamanan Data Anggota Perpustakaan Di Universitas Xyz." Jurnal Siteba, Vol. 2, No. 1, 2023, Https://Journal.Iteba.Ac.Id/Index.Php/Jurnalsiteba/Index.

Febrianingsih, Rindy, And Aliy Hafiz. "Implementasi Kriptografi Berbasis Caesar Chiper Untuk Keamanan Data." Jurnal Informasi Dan Komputer, Vol. 7, No. 2, 24 Oct. 2019, Pp. 81–86, Https://Doi.Org/10.35959/Jik.V7i2.163. Accessed 29 July 2021.

Nasution, Adnan Buyung. "Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher Dan Transposisi Cipher." Jurnal Teknologi Informasi, Vol. 3, No. 1, 20 July 2019, P. 1, Https://Doi.Org/10.36294/Jurti.V3i1.680. Accessed 15 Dec. 2019.

Ningsih, Uci Julya, Et Al. "Pendekripsian Caesar Chiper Dengan Menggunakan Teknikteknik Kriptanalisis." Jurnal Ilkomedia, vol. 1, no. 1, June 2024, https://doi.org/10.46510/ilkomedia.v1i1.10.

Pratiwi, Radila, et al. "Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher." Bulletin of Information Technology, vol. 3, no. 4, 27 Dec. 2022, pp. 367–373, https://doi.org/10.47065/bit.v3i4.420. Accessed 12 June 2024.

Zahwani, Syfa Tasya, and Muhammad Irwan Padli Nasution. "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi Di Era Digital." JoSES: Journal of Sharia Economics Scholar, vol. 2, no. 2, June 2023, pp. 105–109, https://doi.org/10.5281/zenodo.12608751.

Amalia, Rizky, et al. Analisis Performa Algoritma Kriptografi Caesar Cipher Untuk Keamanan Data Menggunakan Phyton Pada Puisi "Kenangan." 2023.

Purnamasari, Dewi. "Implementasi Algoritma Kriptografi Caesar Cipher Dan Rail Fence Cipher Untuk Keamanan Data Teks Menggunakan Python." Journal of Informatics Education, vol. 4, no. 1, 2021. Accessed 12 Oct. 2024.

Harun Alfirdaus, Mohammad, et al. "Perancangan Aplikasi Enkripsi Deskripsi Mengunakan Metode Caesar Chiper Berbasis Web." Jurnal Teknik Mesin, Industri, Elektro Dan Informatika (JTMEI), vol. 2, no. 2, 2023, pp. 64–76. Accessed 12 Oct. 2024.

Ziliwu, Krisma Budi. Implementasi Caesar Cipher Pada Algoritma Kriptografi Klasik Dalam Penyandian Pesan. Aug. 2022.

Pratiwi, Radila, et al. "Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher." Bulletin of Information Technology (BIT), vol. 3, no. 4, 27 Dec. 2022, pp. 367–373, https://doi.org/10.47065/bit.v3i4.420. Accessed 12 Oct. 2024.