Jurnal Jumatiko
LPPM Universitas Graha Nusantara Volume 2 Nomor 1 Juli 2026
E-ISSN : XXXX-XXXX

IMPLEMENTASI ALGORITMA CAESAR CIPHER UNTUK PENGAMANAN PESAN TEKS

Nenni Parida[*1], Jainal Abidin [2], Aris Munandar Harahap [3]

[*1]Mahasiswa Ilmu Komputer, Fakultas Teknik, Universitas Graha Nusantara Padangsidimpuan
[2,3]Dosen Ilmu Komputer, Fakultas Teknik, Universitas Graha Nusantara Padangsidimpuan

Email : [*1] bidinjai27@gmail.com

ABSTRACT

This study aims to implement the Caesar Cipher algorithm for securing text messages. The background of this research is the increasing need for information security in digital communication, particularly to protect data from unauthorized access. The method used is the design and development of a system based on the Java programming language that performs encryption and decryption processes using character shifting techniques. The results show that the developed system is capable of converting plaintext into ciphertext and restoring it to its original form based on the given key. System testing indicates that the Caesar Cipher algorithm can be used as a simple method for securing text messages, although it has limitations in terms of security strength. This study is expected to serve as a learning medium for understanding the basic concepts of cryptography.

Keywords: *Caesar Cipher, cryptography, encryption, decryption, message security*

ABSTRAK

Penelitian ini bertujuan untuk mengimplementasikan algoritma Caesar Cipher dalam pengamanan pesan teks. Latar belakang penelitian ini adalah meningkatnya kebutuhan akan keamanan informasi dalam komunikasi digital, khususnya untuk melindungi data dari akses yang tidak sah. Metode yang digunakan adalah perancangan dan pembangunan sistem berbasis bahasa pemrograman Java yang mampu melakukan proses enkripsi dan dekripsi pesan teks dengan menggunakan teknik pergeseran karakter. Hasil penelitian menunjukkan bahwa sistem yang dibangun mampu mengubah pesan plaintext menjadi ciphertext dan mengembalikannya ke bentuk semula sesuai dengan kunci yang digunakan. Pengujian sistem menunjukkan bahwa algoritma Caesar Cipher dapat digunakan sebagai metode sederhana dalam pengamanan pesan teks, meskipun memiliki keterbatasan dalam tingkat keamanan. Penelitian ini diharapkan dapat menjadi media pembelajaran dalam memahami konsep dasar kriptografi.

Kata kunci: Caesar Cipher, kriptografi, enkripsi, dekripsi, keamanan pesan

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah meningkatkan kemudahan dalam proses pertukaran informasi melalui media digital. Namun, kemudahan tersebut juga diiringi dengan meningkatnya risiko terhadap keamanan data, seperti penyadapan, pencurian, dan manipulasi informasi oleh pihak yang tidak berwenang. Oleh karena itu, diperlukan suatu mekanisme untuk menjaga kerahasiaan dan integritas pesan, khususnya pada pengiriman pesan teks. Salah satu pendekatan yang dapat digunakan untuk mengamankan informasi adalah kriptografi, yaitu teknik untuk mengubah pesan asli (plaintext) menjadi bentuk yang tidak dapat dipahami (ciphertext) tanpa kunci tertentu (Sasono et al., 2023). Kriptografi memiliki peran penting dalam menjaga keamanan data, baik dari segi kerahasiaan, integritas, maupun otentikasi. Dalam perkembangannya, kriptografi terbagi menjadi kriptografi klasik dan modern. Meskipun kriptografi modern memiliki tingkat keamanan yang lebih tinggi, kriptografi klasik tetap relevan untuk tujuan pembelajaran dan implementasi dasar (Sasono et al., 2023).

Algoritma Caesar Cipher merupakan salah satu metode kriptografi klasik yang menggunakan teknik substitusi dengan cara menggeser karakter berdasarkan nilai kunci tertentu. Metode ini memiliki keunggulan dalam hal kemudahan implementasi, tetapi memiliki keterbatasan dalam tingkat keamanan karena jumlah kemungkinan kuncinya relatif terbatas (Ariansyah et al., 2023). Beberapa penelitian sebelumnya menunjukkan bahwa Caesar Cipher cukup efektif untuk pengamanan data sederhana serta sebagai media edukasi dalam pengembangan sistem keamanan.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengimplementasikan algoritma Caesar Cipher dalam pengamanan pesan teks berbasis aplikasi. Sistem yang dibangun diharapkan mampu melakukan proses enkripsi dan dekripsi secara efektif serta memberikan gambaran mengenai penerapan algoritma kriptografi sederhana dalam menjaga keamanan informasi.

.

TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi merupakan ilmu yang digunakan untuk mengamankan informasi dengan cara mengubah data asli (plaintext) menjadi bentuk yang tidak dapat dipahami (ciphertext) menggunakan algoritma dan kunci tertentu. Proses utama dalam kriptografi terdiri dari enkripsi dan dekripsi. Enkripsi adalah proses mengubah plaintext menjadi ciphertext, sedangkan dekripsi adalah proses mengembalikannya ke bentuk semula. Kriptografi klasik menggunakan teknik substitusi dan transposisi, sedangkan kriptografi modern menggunakan pendekatan matematis dan algoritma yang lebih kompleks (Sasono et al., 2023).

Tujuan utama kriptografi meliputi tiga aspek penting, yaitu kerahasiaan (confidentiality), integritas (integrity), dan otentikasi (authentication). Dalam perkembangannya, kriptografi dibagi menjadi dua jenis, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik menggunakan teknik sederhana seperti substitusi dan transposisi, sedangkan

kriptografi modern menggunakan pendekatan matematis yang lebih kompleks dan berbasis komputer.

2.2 Caesar Cipher

Caesar Cipher merupakan salah satu algoritma kriptografi klasik yang menggunakan metode substitusi dengan cara menggeser setiap karakter dalam plaintext berdasarkan nilai kunci tertentu (Ariansyah et al., 2023). Metode ini dikenal sebagai cipher abjad tunggal karena setiap huruf digantikan dengan huruf lain yang tetap.

Proses enkripsi dan dekripsi pada Caesar Cipher dapat dinyatakan sebagai berikut:

- Enkripsi:
  $Ci = (Pi + K) \bmod 26$
- Dekripsi:
  $Pi = (Ci – K) \bmod 26$

di mana Pi adalah plaintext, Ci adalah ciphertext, dan K adalah kunci pergeseran. Keunggulan algoritma ini adalah kemudahannya dalam implementasi, namun memiliki kelemahan pada tingkat keamanan yang rendah karena mudah dipecahkan dengan metode brute force.

2.3 Pesan Teks

Pesan teks merupakan informasi yang disampaikan dalam bentuk rangkaian karakter yang memiliki makna dan dapat dipahami oleh penerima. Dalam sistem digital, pesan teks direpresentasikan dalam bentuk kode numerik atau biner sehingga dapat diproses oleh komputer.

2.3.1 Karakteristik Pesan Teks

Pesan teks memiliki beberapa karakteristik, antara lain:

- Mengandung makna yang dapat dipahami
- Tersusun berdasarkan aturan bahasa (sintaksis)
- Direpresentasikan dalam bentuk kode seperti ASCII atau Unicode
- Dapat diproses secara algoritmik dalam sistem komputer

Karakteristik ini memungkinkan pesan teks untuk diolah menggunakan teknik kriptografi dalam proses pengamanan data.

2.3.2 Karakter dalam Pesan Teks

Karakter dalam pesan teks terdiri dari beberapa jenis, yaitu:

- Huruf (A–Z, a–z)
- Angka (0–9)
- Tanda baca (., ?, !, dll.)
- Karakter khusus (@, #, $, dll.)
- Karakter non-ASCII (Unicode)

Keberagaman karakter ini mempengaruhi proses enkripsi dan dekripsi dalam sistem yang dibangun.

2.4 Unified Modeling Language (UML)

Unified Modeling Language (UML) merupakan bahasa pemodelan visual yang digunakan untuk merancang dan mendokumentasikan sistem perangkat lunak. UML membantu pengembang dalam memahami kebutuhan sistem serta menggambarkan struktur dan perilaku sistem secara jelas. Dalam penelitian ini, UML digunakan untuk memodelkan sistem melalui beberapa diagram, antara lain use case diagram, class diagram, sequence diagram, dan activity diagram. UML membantu pengembang dalam menggambarkan struktur dan perilaku sistem secara sistematis (Suendri, 2018). Use case diagram digunakan untuk menggambarkan interaksi antara aktor dengan sistem serta fungsi-fungsi yang disediakan oleh sistem (Kurniawan, 2018).

2.4.1 Use Case Diagram

Use case diagram digunakan untuk menggambarkan interaksi antara aktor dengan sistem. Diagram ini menunjukkan fungsi-fungsi utama yang disediakan sistem serta hubungan antara pengguna dan sistem.

2.4.2 Class Diagram

Class diagram digunakan untuk menggambarkan struktur sistem dalam bentuk kelas-kelas beserta atribut dan metode yang dimiliki. Diagram ini juga menunjukkan hubungan antar kelas dalam sistem.

2.4.3 Sequence Diagram

Sequence diagram menggambarkan alur interaksi antar objek dalam sistem berdasarkan urutan waktu. Diagram ini menunjukkan bagaimana pesan dikirim dan diterima antar objek dalam suatu proses.

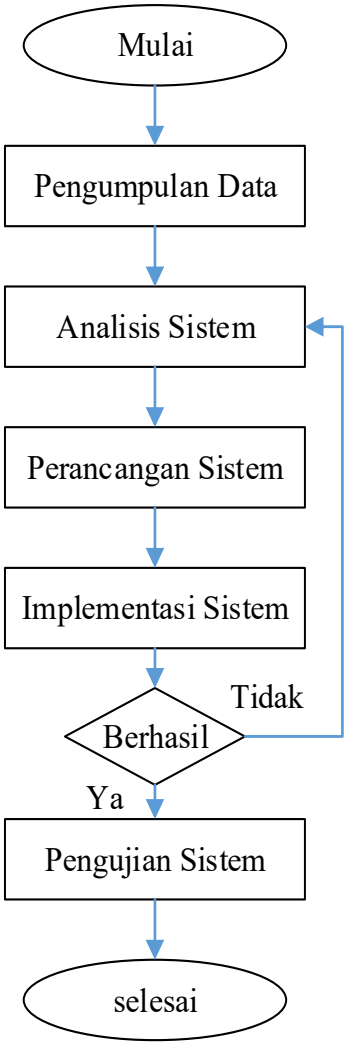
2.4.4 Activity Diagram

Activity diagram digunakan untuk menggambarkan alur aktivitas atau proses kerja sistem. Diagram ini menunjukkan langkah-langkah yang dilakukan dalam menjalankan suatu fungsi dalam sistem.

METOLOGI PENELITIAN

Penelitian ini menggunakan metode research and development (R&D) dengan tujuan merancang dan mengimplementasikan algoritma Caesar Cipher untuk pengamanan pesan teks. Pengumpulan data dilakukan melalui studi literatur dan eksperimen. Pengembangan sistem dilakukan menggunakan pendekatan Waterfall yang meliputi tahap analisis kebutuhan, perancangan, implementasi, dan pengujian (Pitrawati & Sanjaya, 2021).

Sistem yang dibangun mampu melakukan proses enkripsi dan dekripsi pesan berdasarkan nilai kunci tertentu. Pengujian dilakukan dengan membandingkan hasil plaintext dan ciphertext untuk memastikan bahwa proses enkripsi dan dekripsi berjalan dengan baik serta sesuai dengan algoritma yang digunakan.



Gambar 3.1 Kerangka Kerja Penelitian

HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan sebuah sistem yang mampu melakukan proses enkripsi dan dekripsi pesan teks menggunakan algoritma Caesar Cipher. Sistem dirancang berdasarkan metode Waterfall, dimulai dari analisis kebutuhan, perancangan menggunakan UML, hingga tahap implementasi dan pengujian. Hasil pengujian menunjukkan bahwa sistem dapat mengubah plaintext menjadi ciphertext dan mengembalikannya kembali ke bentuk semula dengan benar sesuai dengan nilai kunci yang diberikan. Proses enkripsi dan dekripsi berjalan dengan cepat, sederhana, dan mudah diimplementasikan.

Namun, dari sisi keamanan, algoritma Caesar Cipher memiliki keterbatasan karena relatif mudah dipecahkan dibandingkan algoritma kriptografi modern seperti AES (Ariansyah et al., 2023; Sasono et al., 2023).Meskipun demikian, algoritma ini tetap efektif digunakan sebagai dasar pembelajaran kriptografi dan pengamanan data sederhana. Secara keseluruhan, sistem

yang dibangun telah berjalan sesuai dengan tujuan penelitian dan dapat digunakan sebagai media untuk memahami konsep dasar enkripsi dan dekripsi serta sebagai dasar pengembangan sistem keamanan yang lebih kompleks.

Pesan asli : **UGN Mantap 09**

Kunci : 3

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

0	1	2	3	4	5	6	7	8	9

Jadi untuk enkripsi setiap karakter digeser kearah kanan sebanyak kunci, jika pergeseran telah sampai pada ujung, dan masih harus melakukan pergeseran maka akan di ulang dari karakter yang paling kiri.

U -> X
G -> J
N -> Q

M -> P
a -> d
n -> q
t -> w
a -> d
p -> s

0 -> 3
9 -> 2

Jadi hasil *ciphertext* untuk pesan diatas adalah **: XJQ Pdqwds 32.**

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa algoritma Caesar Cipher dapat diimplementasikan dengan baik dalam sistem pengamanan pesan teks. Sistem yang dibangun mampu melakukan proses enkripsi dan dekripsi secara benar sesuai dengan kunci yang diberikan. Proses pengembangan sistem menggunakan metode Waterfall berjalan dengan baik, mulai dari tahap analisis, perancangan, hingga implementasi dan pengujian. Hasil pengujian menunjukkan bahwa sistem bekerja secara efektif dalam mengubah plaintext menjadi ciphertext dan mengembalikannya kembali ke bentuk semula.

Meskipun demikian, dari segi keamanan, algoritma Caesar Cipher masih memiliki kelemahan karena mudah untuk dipecahkan. Oleh karena itu, algoritma ini lebih cocok digunakan sebagai media pembelajaran dasar kriptografi dan

pengamanan data sederhana, serta dapat dikembangkan lebih lanjut dengan metode yang lebih kompleks.

SARAN

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat diberikan untuk pengembangan selanjutnya:

1. Penggunaan algoritma Caesar Cipher sebaiknya dikombinasikan dengan algoritma kriptografi lain yang lebih kompleks untuk meningkatkan tingkat keamanan data.
2. Sistem yang dibangun dapat dikembangkan lebih lanjut dengan menambahkan fitur pengamanan tambahan, seperti penggunaan kunci yang lebih dinamis atau berbasis metode modern.
3. Penelitian selanjutnya diharapkan dapat mengimplementasikan algoritma kriptografi yang lebih kuat, seperti Vigenere Cipher atau algoritma berbasis kunci publik.
4. Sistem dapat dikembangkan ke dalam platform yang lebih luas, seperti aplikasi berbasis web atau mobile agar lebih mudah digunakan oleh pengguna.

DAFTAR PUSTAKA

Ariansyah, F.,D., Damayanti., A., Putri.,C.,A.,M (2023). Implementasi Kriptografi Caesar Chiper Pada Aplikasi Enkripsi Dan Dekripsi. *Jurnal Ilmiah Sistem Informasi Dan Ilmu Komputer* 3(1), 105-112.

Gumelar, D.,G., & Pramushinto., W (2018). Implementasi Algoritma Kriptografi Dengan Algoritma Caesar Cipher, Advanced Encryption Standard 256, Dan Rc6 Untuk Aplikasi Chatting Berbasis Android. *SKANIKA* 1(2), 71-717

Irfan, M., Siregar, H., & Handoko, J. T. (2023). Pengembangan Dan Integrasi Aplikasi Prediksi Jumlah Gagal Produksi PC Meggunakan Metode Triple Exponential Smoothing Pada Sistem Aplikasi Produksi Di PT Tera Data Indonusa,Tbk. *Prosiding Seminar Nasional Darmajaya*, *1*(November 2015), 80–96.

Khairunnisa, G., Voutama, A., Informasi, S., Karawang, U. S., Informasi, S., & Method, D. (2024). *PEMINJAMAN INVENTARIS BERBASIS WEB DI BEM FASILKOM UNSIKA*. *8*(3), 2748–2755.

Kurniawan, T. A. (2018). Pemodelan Use Case (UML): Evaluasi Terhadap beberapa Kesalahan dalam Praktik. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *5*(1), 77–86. https://doi.org/10.25126/jtiik.201851610

Pitrawati, & Sanjaya, A. (2021). Rekayasa Perangkat Lunak Perhitungan Harga Pokok Produksi Metode Full Costing Pada Umkm Mitra Cake Di Bandar Lampung. *Jurnal Informasi Dan Komputer*, *9*(2), 154–162.

https://doi.org/10.35959/jik.v9i2.243

Pramono, B. S., Luthfi, A., & Havatilla, D. R. (2024). Penerapan Kriptografi Caesar Cipher dan Transposisi Cipher PadaBot Aplikasi Pesan Telegram. *Prosiding SAINTEK: Sains Dan Teknologi*, *3*(1), 35–40.

Sasono, D.,M.,A, Tahir,M, Angel F.,M., V., Azizah,M., Utami.,L.,F, & Septiana.,N. (2023). Perbandingan Kriptography Klasik Caesar Cipher Dengan Kriptography Modern Aes Dalam Tingkat Keamanan Jaringan Komputer. *Jurnal Informasi, Sains Dan Teknologi*, *6*(1), 72–77. https://doi.org/10.55606/isaintek.v6i1.93,

Suendri. (2018). *Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem Informasi Remunerasi Dosen Dengan Database Oracle (Studi Kasus: UIN Sumatera Utara Medan) Suendri*. *6341*(November), 1–9.

Supriyatno.,A.,M & Ardhianto.,E (2024). Peningkatan keamanan Pesan teks menggunakan Supr Enkripsi *Algoritma Caesar Cipher Standard* dan *Vigenere Autokey. Jurnal Ilmiah KOMPUTASI,* 23 (2).

Syahputri, A. Z., Fallenia, F. Della, & Syafitri, R. (2023). *Kerangka Berfikir Penelitian Kuantitatif*.