Mars: Jurnal Teknik Mesin, Industri, Elektro dan Ilmu Komputer
Volume 3, Nomor 4, Agustus 2025
e-ISSN: 3031-8742; p-ISSN: 3031-8750, Hal. 169-176
DOI: https://doi.org/10.61132/mars.v3i4.978
Available online at: https://journal.arteii.or.id/index.php/mars

Implementasi Kriptografi dengan *Caesar Cipher* pada Fitur Pesan di WhatsApp untuk Keamanan

Ratih Adinda Destari
Fakultas Teknik dan Ilmu Komputer, Sistem Informasi, Universitas Potensi Utama, Indonesia

Alamat: K.L. Yos Sudarso KM 6,5 No. 3A Tj. Mulia – Medan, Sumatera Utara, Indonesia
Korepsondensi penulis : adindaalkarim0384@gmail.com

Abstract. *Rapid technological developments have penetrated various aspects of human life, including data and information security. Amidst the threat of data leaks and misuse, information protection has become crucial. One solution to maintain data confidentiality is to implement cryptography technology. Cryptography is the study of techniques to secure messages so they cannot be read by unauthorized parties. This process is carried out by encoding the original message (plain text) into an unreadable form (cipher text), which can only be understood by those who possess the key to decrypt it. This study used the Caesar Cipher algorithm, a form of classical cryptography. This algorithm uses a substitution method, where each letter in the message is shifted by a certain amount based on a predetermined key. Caesar Cipher is a symmetric algorithm, meaning the key used for encryption is also used for decryption. The security of this algorithm lies in the secrecy of the key, which is known only to the sender and recipient of the message. This method is relatively simple, but still relevant for securing data with low to medium sensitivity levels. This study used WhatsApp messages as the object to be encrypted using the Caesar Cipher algorithm. The results show that encrypted messages become unintelligible without prior decryption. This demonstrates that the Caesar Cipher can protect messages from unauthorized parties. Therefore, implementing this algorithm can be an initial solution for maintaining data confidentiality in digital communications, especially on platforms vulnerable to eavesdropping or unauthorized access. Its primary benefit is maintaining message integrity and confidentiality to prevent misuse.*

Keywords: *Cryptography, Caesar Cipher, Encryption, Security, WhatsApp.*

Abstrak. Perkembangan teknologi yang sangat pesat telah merambah ke berbagai aspek kehidupan manusia, termasuk dalam hal keamanan data dan informasi. Di tengah ancaman kebocoran dan penyalahgunaan data, perlindungan terhadap informasi menjadi hal yang sangat penting. Salah satu solusi yang digunakan untuk menjaga kerahasiaan data adalah dengan menerapkan teknologi kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik-teknik untuk mengamankan pesan agar tidak dapat dibaca oleh pihak yang tidak berwenang. Proses ini dilakukan dengan cara menyandikan pesan asli (plain text) menjadi bentuk yang tidak terbaca (*cipher text*), yang hanya bisa dipahami oleh pihak yang memiliki kunci untuk mendekripsinya. Dalam penelitian ini digunakan algoritma *Caesar Cipher*, yaitu salah satu bentuk kriptografi klasik. Algoritma ini menggunakan metode substitusi, di mana setiap huruf dalam pesan digeser dengan jumlah tertentu berdasarkan kunci yang telah ditentukan. Caesar Cipher merupakan algoritma simetris, artinya kunci yang digunakan untuk enkripsi juga digunakan untuk dekripsi. Keamanan algoritma ini terletak pada kerahasiaan kunci, yang hanya diketahui oleh pengirim dan penerima pesan. Metode ini tergolong sederhana, namun masih relevan untuk pengamanan data dengan tingkat sensitivitas rendah hingga sedang. Penelitian ini mengambil data berupa pesan WhatsApp sebagai objek untuk dienkripsi menggunakan algoritma *Caesar Cipher*. Hasil yang diperoleh menunjukkan bahwa pesan yang telah dienkripsi menjadi tidak bisa dipahami tanpa proses dekripsi terlebih dahulu. Hal ini membuktikan bahwa *Caesar Cipher* dapat memberikan perlindungan terhadap pesan dari pihak yang tidak berhak. Dengan demikian, penerapan algoritma ini dapat menjadi solusi awal untuk menjaga kerahasiaan data dalam komunikasi digital, terutama pada platform yang rentan terhadap penyadapan atau akses ilegal. Manfaat utamanya adalah menjaga integritas dan kerahasiaan pesan agar tidak disalahgunakan.

Kata Kunci: Kriptografi, *Caesar Chiper*, Enkripsi, Keamanan, WhatsApp

Received: Mei 30, 2025; Revised: Juni 14, 2025; Accepted: Juli 28, 2025; Online Available: Juli 30, 2025

1. LATAR BELAKANG

Keamanan menjadi aspek yang sangat penting saat ini di mana pertukaran data dan informasi menjadi tuntutan baik pekerjaan dan lainnya. Berbagai cara dilakukan untuk mengamankan data atau informasi di antaranya menggunakan Kriptologi (Sutoyo, dkk., 2020). Kriptografi merupakan bagian ilmu yang mempelajari tentang cara menjaga agar data atau pesan tetap aman. Beragam macam teknik digunakan untuk upaya mengamankan data atau informasi yang penting (Rifa'i, dkk., 2020).

Pada pengamanan dalam kriptografi ini banyak metode atau algoritma yang dapat digunakan, seperti Caesar, Abjad Majemuk, DES, IDEA, RSA dan lain sebagainya (Permana, dkk., 2022). Sedangkan pada penelitian ini menggunakan metode Caesar Cipher. Algoritma Caesar cipher termasuk pada kriptografi klasik yang memiliki kunci simetris (hanya ada satu kunci) yang mana biasa digunakan dalam mengekripsi ataupun mendekripsi data dan informasi (Nasari, dkk., 2023). Karena Caesar Cipher merupakan kriptografi klasik maka proses enkripsi dan dekripsinya dilakukan dengan cara substitusi atau perpindahan (Nasari, dkk., 2023).

Kriptografi merupakan dasar untuk memahami keamanan pada komputer (anwar., dkk, 2022). Caesar Chiper merupakan sistem persandian berbasis substitusi (Sutoyo., dkk, 2022). Adapun dalam proses Enskripsi dan deskripsi pada metode Caesar menggunakan operasi shift. Cara kerja operasi shift adalah dengan cara mensubstitusikan huruf-huruf pada alfabet yang berada di sebelah kiri atau sebelah kanan huruf tersebut. Sedangkan chiper alphabet majemuk adalah chiper substitusi ganda yang melibatkan penggunaankunci berbeda atau huruf kapital dan lainnya. (Manurung. ,dkk, 2023)

Begitu pentingnya kriptografi untuk keamanan informasi (Ningsih., dkk, 2024), sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka orang tidak bisa memisahkannya dengan kriptografi. Maka dari itu upaya yang dilakukan untuk melakukan pengamanan data tersebut yaitu dengan melakukan enkripsi.(Putra., dkk 2024)

2. KAJIAN TEORITIS

Jenis Penelitian

Jenis penelitian yang dilakukan adalah penelitian terapan, yaitu penelitian yang bertujuan untuk menyelesaikan masalah yang ada dengan menerapkan teori-teori yang mendasari penelitian yang dikaji dengan terlebih dahulu menyusun konsep-konsep yang berkaitan dengan kriptografi secara matematis, dengan DELPHI sebagai alat bantu komputasi. (Fauzi. ,dkk, 2024)

Pada bagian ini dijelaskan mengenai metode yang digunakan dalam penelitian ini. Metode penelitian ini meliputi penentuan model enkripsi, penyelesaian algoritma enkripsi, pembuatan simulasi enkripsi dan analisa hasil dari simulasi enkripsi.

Metode pengembangan sistem

Metode pengembangan sistem yang penulis gunakan dalam penelitian ini adalah metode Extreme Programming. Extreme Programming yaitu sebuah metode dalam pengembangan sistem yang dilakukan untuk :

a. Planning/Perencanaan Pada tahap perencanaan ini dimulai dari pengumpulan kebutuhan yang membantu tim teknikal untuk memahami konteks bisnis dari sebuah aplikasi. Selain itu pada tahap ini juga mendefinisikan output yang akan dihasilkan, fitur yang dimiliki oleh aplikasi dan fungsi dari aplikasi yang dikembangkan.
b. Design/Perancangan Metode ini menekankan desain aplikasi yang sederhana, bagaimana sebuah aplikasi bisa berjalan dengan baik.
c. Coding/Pengkodean

   Konsep utama dari tahapan pengkodean pada extreme programming adalah bagaimana menyusun kode yang sederhana sehingga mudah dipahami.
d. Testing/Pengujian Pada tahapan ini lebih fokus pada pengujian fitur dan fungsionalitas dari aplikasi.

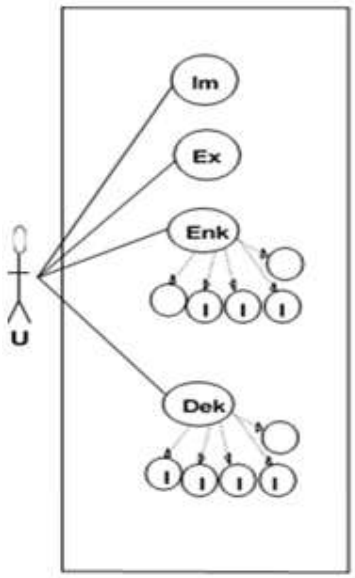
3. METODE PENELITIAN

Borland Delphi pada awalnya adalah proyek rahasia yang berevolusi menjadi produk yang disebut dengan *App Builder*. Namun sebelum rilis pertama dari *borland delphi*, novell yang menjadi app builder sudah dirilis sehingga borland harus memberikan nama baru untuk proyek tersebut. Adapun tujuan dari delphi pada waktu itu adalah menyediakan konektivitas database untuk programmer yang akan menjadi fitur kunci pada *database* karena pada waktu itu yang paling populer adalah *database oracle*. Adapun alat rancang yang digunakan adalah sebagai berikut:

a. Usecase

Diagram Use Case merupakan bagian tertinggi dari fungsionalitas yang dimiliki sistem yang akan menggambarkan bagaimana seseorang atau actor akan menggunakan dan memanfaatkan sistem. Diagram ini juga mendeskripsikan apa yang akan dilakukan oleh sistem.

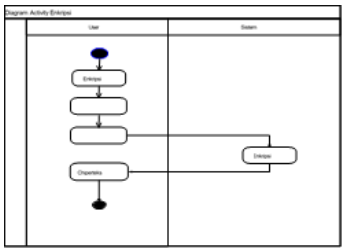
Diagram use case pusat peminjaman ruangan dan peralatan dapat dilihat pada gambar dibawah ini:



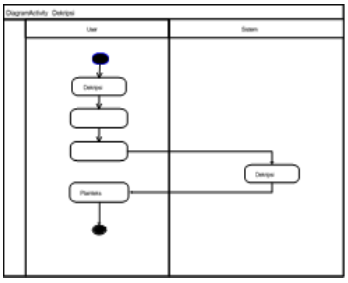
Gambar 1. Usecase sistem enkripsi dan dekripsi

b. Activity Diagram

Activity Diagram memberikan gambaran rancangan alur disetiap fungsi yang ada di dalam system. Activity diagram menggambarkan berbagai alir aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, decision yang mungkin terjadi, dan bagaimana mereka berakhir.



Gambar 2. Diagram activity enkripsi



Gambar 3. Diagram activity enkripsi

Pada gambar 3 di atas dapat dilihat panel kiri atas merupakan pilihan antara enkripsi atau dekripsi, kemudian di sampingnya ada pilihan untuk melakukan pergeseran antara 1 sampai 5 pergeseran, dan di bawah panel itu adalah input untuk plainteks yaitu teks yang akan di

enkripsi, kemudian di bawah panel itu ada chiper text yaitu hasil dari proses enkripsi. Pada panel sebelah kanan merupakan fitur untuk import dan export, yaitu fitur untuk mengambil file yang ada di dalam komputer kemudian export untuk menyimpan hasil enkripsi ke dalam komputer dalam bentuk file teks yang bisa dibuka dengan notepad.

4. HASIL DAN PEMBAHASAN

Hasil Perhitungan Matematis Data yang digunakan untuk pesan (plaintext) yaitu berupa karakter dalam bentuk karakter huruf a-z, angka 1-9, dan tanda baca seperti koma(,), titik (␣), tanda tanya (?), tanda seru (!) dan lainnya, tetapi pada penelitian ini hanya dilakukan enkripsi dan dekripsi pada karakter huruf saja, di mana pesan tersebut akan dilakukan proses enkripsi menggunakan Adapun jika ingin substitusi dengan metode kriptografi caesar chiper, kemudian setelah di enkripsi akan menghasilkan ciphertext. Ciphertext ini kemudian bisa di dekripsi agar bisa dibaca kembali atau plaintext. Tabel substitusi dari perubahan metode caesar adalah sebagai berikut:

Tabel 1. C*aesar Chiper*

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

Pada tabel 1 yang merupakan tabel sumber untuk dijadikan rujukan dalam proses enkripsi, dengan pergeseran 4 karakter. maka jika dilakukan proses enkripsi adalah sebagai berikut:

Plainteks : saya kuliah di pu

Proses enkripsi pada kalimat “saya kuliah di pu” adalah sebagai berikut:

Tabel 2. Substitusi *caesar chiper* bergeser 4 huruf.

y	c
a	e
k	o
u	y
l	p
i	m
a	e
h	l
d	h
i	m
p	t
u	y

Huruf	Substitusi 5
s	x
a	f
y	d
a	f
k	p
u	z
l	q
i	n
a	f
h	j
d	i
i	n
p	u
u	z

Adapun pergeseran sebanyak 5 huruf maka jika dilakukan proses enkripsi adalah sebagai berikut: Plainteks : saya kuliah di pu Proses enkripsi pada kalimat "saya kuliah di pu" adalah sebagai berikut:

Contoh Kasus :

Tabel 3. Substitusi caesar chiper bergeser 5 huruf.

U	P	U
20	15	20

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	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

DIK : Plaintext : U P U K : 3

DIT : chipertext/enkripsi

a. (P1+K) mod 26 (U+3) mod 26
   (20+3) mod 26
   23 mod 26 X
b. (P2+K) mod 26 (P+3) mod 26
   (15+3) mod 26
   18 mod 26 S
c. (P3+K) mod 26 (U+3) mod 26
   (20+3) mod 26
   23 mod 26 X

Jadi chipertextnya adalah : **XSX**

a. (C1-K) mod 26 (X-3) mod 26
b. (C2-K) mod 26 (S-3) mod 26
   (18-3) mod 26
   mod 26 P

- (C3-K) mod 26 (X-3) mod 26
  (23-3) mod 26
  20 mod 26 U

Jadi plaintextnya adalah : **UPU**

5. KESIMPULAN DAN SARAN

Dalam pesan rahasia ini dibantu dengan sistem keamanan pesan teks WhatsApp yang digunakan untuk mengirimkan pesan atau sesuatu yang sifatnya tidak dapat diketahui oleh orang lain, seperti mengirimkan pesan rahasia atau dokumen rahasia melalui fitur chat WhatsApp. Dimana plaintext dienkripsi menjadi cryptic text atau Ciphertext yang dapat membantu pertukaran dan mengamankan pesan dalam bentuk teks. Oleh karena itu dapat disimpulkan bahwa kriptografi masih merupakan sistem yang efektif dari segi keamanan dan perlindungan serta dapat digunakan secara luas di berbagai bidang bisnis dan teknologi.

Untuk pengembangan lebih lanjut pada metode ini , maka dapat diberikan beberapa saran diantaranya pertama, Sebaiknya sistem yang telah dibuat dapat dikembangkan dengan menggunakan metode yang lain. Kedua, Sebaiknya sistem yang telah dibuat dapat menggunakan persentase minat pembeli dalam memilih produk pada PT. XYZ. Dan ketiga, sebaiknya sistem yang telah dibuat dapat diterapkan dengan menggunakan system berbasis *online.*

UCAPAN TERIMA KASIH

Ucapkan terima kasih kepada semua orang yang terlibat dalam pembuatan jurnal ini

DAFTAR REFERENSI

Anwar, S., Nugroho, I., & Ahmadi, A. (2022). Implementasi kriptografi dengan enkripsi shift Vigenere Cipher serta checksum menggunakan CRC32 pada data teks. *Jurnal Sistem Informasi Indonesia*, *2*, 51–58. https://doi.org/10.30656/jsii.v2i0.6

Fauzi, M. K., & Setiawan, A. (2024). Implementasi algoritma Vigenere Cipher dan Caesar Cipher untuk pengamanan password dalam penerimaan siswa baru. *Jurnal Info Digit*, *2*(3), 1083–1094. E-ISSN: 2988-0289

Febriana, I., & G. A. S. (2017). Penerapan teknik kriptografi pada keamanan SMS Android. *JOEICT (Jurnal Educ. Inf. Commun. Technol.)*, *1*(1), 29–36.

Manurung, J., Sihombing, A. P. E., & Pandiangan, B. (2023). Sosialisasi dan edukasi tentang keamanan data dan privasi di era digital untuk meningkatkan kesadaran dan perlindungan masyarakat. *Jurnal Pengabdian Masyarakat Nauli*, *2*(1), 1–7. E-ISSN: 2985-3702

Nasari, F., & Darma, S. (2023). Penerapan k-means clustering pada data penerimaan mahasiswa baru (Studi kasus: Universitas Potensi Utama). *Semnas Teknomedia Online*, *3*(1), 2-1.

Nasari, R., and T. Prabowo. "Penerapan Kriptografi Caesar Cipher pada Aplikasi Keamanan Pesan Pengguna." *Jurnal Sistem Informasi dan Komputer*, vol. 5, no. 3, pp. 123-132, 2023.

Ningsih, U. J., Salsabila, S., Hutapea, I., Santika, D., & Gunawan, I. (2024). Pendekripsian Caesar Cipher dengan menggunakan teknik-teknik kriptanalisis. *Jurnal ILKOMEDIA, 1*(1). https://doi.org/10.46510/ilkomedia.v1i1.10

Permana, A. (2022). Penerapan kriptografi pada teks pesan dengan menggunakan metode Vigenere Cipher berbasis Android. *Jurnal Al-AZHAR Indonesia Seri Sains dan Teknologi, 4*(3), 110. https://doi.org/10.36722/sst.v4i3.280

Permana, I., and A. Wibawa. "Aplikasi Enkripsi Menggunakan Algoritma Caesar Cipher Pada Sistem Keamanan Data." *Jurnal Teknologi dan Sistem Informasi*, vol. 17, no. 2, pp. 45–59, 2022.

Putra, B. J. M., Bawani, R. S., & Hikmahwan, B. (2024). Aplikasi makanan sehat bagi penderita hipertensi berbasis Android. *Jurnal ILKOMEDIA, 1*(1). https://doi.org/10.46510/ilkomedia.v1i1.9

Rifa'i, & Sumartini, L. C. (2020). Implementasi kriptografi menggunakan metode Blowfish dan Base64 untuk mengamankan database informasi akademik pada Kampus Akademi Telekomunikasi Bogor berbasis web-based. *Jurnal E-Komtek, 3*(2), 87–96. https://doi.org/10.37339/ekomtek.v3i2.133

Rifa'i, and L. C. Sumartini. "Implementasi Kriptografi Menggunakan Metode Blowfish Dan Base64 Untuk Mengamankan Database Informasi Akademik Pada Kampus Akademi Telekomunikasi Bogor Berbasis Web-Based." *J. EKomtek*, vol. 3, no. 2, pp. 87–96, 2020.

Sutoyo, N., Nurhayati, & Gultom, I. (2020). Implementasi super enkripsi algoritma One Time Pad (OTP) dan Beaufort Cipher untuk mengamankan data. *Jurnal Sistem Informasi Kaputama, 3*(1), 1–5. https://jurnal.kaputama.ac.id/index.php/JSIK/article/view/144

Sutoyo, N., Nurhayati, & Gultom, I. (2022). Implementasi super enkripsi algoritma One Time Pad (OTP) dan Beaufort Cipher untuk mengamankan data dokumen pegawai. *Jurnal Sistem Informasi Kaputama, 3*(1), 1–5.

Sutoyo, Nurhayati, and I. Gultom. "Implementasi Super Enkripsi Algoritma One Time Pad (OTP) dan Beaufort Cipher untuk Mengamankan Data." *J. Sist. Inf. Kaputama*, vol. 3, no. 1, pp. 1–5, 2020.