TECHNOLOGIC
Technology and Engineering for Intelligent and Computational Systems
Vol.1, No.1, June (2026) 21-27

ANALISIS KEAMANAN ALGORITMA CAESAR CIPHER TERHADAP SERANGAN KRIPTANALISIS BERDASARKAN PRINSIP KERCKHOFFS DENGAN IMPLEMENTASI MENGGUNAKAN BAHASA PEMROGRAMAN PYTHON

[1] Muhammad Habib Maulana
Teknik Informatika, Fakultas Ilmu Komputer, Universitas Nahdlatul Ulama Sumatera Utara
E-mail: [1] muhammdhabibmaulana@gmail.com

[2] Demonius Sarumaha
Teknik Informatika, Fakultas Ilmu Komputer, Universitas Nahdlatul Ulama Sumatera Utara
E-mail: [2] demonius213@gmail.com

[3] Hery Yusuf Simbolon
Teknik Informatika, Fakultas Ilmu Komputer, Universitas Nahdlatul Ulama Sumatera Utara
E-mail: [3] simbolonyusufheri@gmail.com

ABSTRACT

This study analyzes the security of the Caesar Cipher algorithm against cryptanalysis attacks based on the Kerckhoffs Principle through an implementation in the Python programming language. The Kerckhoffs Principle states that the security of a cryptographic system should rely solely on the secrecy of the key rather than the secrecy of the algorithm. Caesar Cipher is a classical monoalphabetic substitution cipher that encrypts data by shifting each letter by a fixed number of positions in the alphabet. The objectives of this research are to implement the Caesar Cipher algorithm, evaluate its security level, and simulate a brute-force cryptanalysis attack using Python. Experimental results demonstrate that the algorithm performs encryption and decryption with 100% accuracy. However, it exhibits a critical security weakness due to its extremely limited key space of only 25 possible keys. The brute-force simulation successfully recovered the ciphertext in less than one second, demonstrating that the algorithm fails to satisfy modern cryptographic security requirements. Furthermore, the evaluation based on the Kerckhoffs Principle confirms that the Caesar Cipher does not provide practical security because its protection depends on a very limited key space. This research provides educational insights into the importance of selecting robust cryptographic algorithms and highlights the relevance of the Kerckhoffs Principle as a framework for evaluating cryptographic security.

Keywords: *Caesar Cipher, Cryptanalysis, Kerckhoffs Principle, Brute Force, Python*

INTRODUCTION

Perkembangan teknologi informasi dan komunikasi yang sangat pesat pada era digital saat ini telah membawa dampak signifikan terhadap berbagai aspek kehidupan manusia(Nugroho & Tambunan, 2025). Salah satu aspek yang sangat penting adalah keamanan data dan informasi. Keamanan informasi menjadi perhatian utama terutama dalam proses transmisi data melalui jaringan komputer yang rentan terhadap berbagai ancaman keamanan seperti

penyadapan, pencurian data, dan manipulasi informasi(Ujung et al., 2023).

Kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan informasi dengan cara mengubah informasi asli (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext) melalui proses enkripsi(Amalya et al., 2023). Salah satu algoritma kriptografi klasik yang paling terkenal adalah Caesar Cipher, yang dikembangkan oleh Julius Caesar pada masa Romawi kuno untuk mengamankan komunikasi militer. Meskipun tergolong algoritma klasik dan sederhana, Caesar Cipher memiliki nilai historis dan edukatif yang tinggi dalam memahami konsep dasar kriptografi(Noviyanti, 2022).Caesar Cipher bekerja dengan cara menggeser setiap huruf dalam plaintext dengan sejumlah posisi tertentu dalam alfabet. Kunci enkripsi dalam Caesar Cipher adalah bilangan bulat yang menunjukkan besarnya pergeseran. Kesederhanaan algoritma ini membuatnya mudah dipahami dan diimplementasikan, namun di sisi lain juga menimbulkan kerentanan keamanan yang signifikan(Fachrul Dhika Ardiansyah, n.d.).Dalam konteks keamanan kriptografi modern, terdapat enam prinsip desain kriptografi yang dikemukakan oleh Auguste Kerckhoffs pada tahun 1883, yang dikenal sebagai Prinsip Kerckhoffs. Prinsip yang paling fundamental menyatakan bahwa keamanan sistem kriptografi tidak boleh bergantung pada kerahasiaan algoritma, melainkan hanya pada kerahasiaan kunci. Prinsip ini menjadi standar dalam evaluasi keamanan sistem kriptografi modern(Serikastawan et al., n.d.-a). Penelitian ini bertujuan untuk menganalisis keamanan algoritma Caesar Cipher terhadap berbagai serangan kriptanalisis dengan menggunakan Prinsip Kerckhoffs sebagai kerangka evaluasi. Implementasi algoritma dan serangan kriptanalisis akan dilakukan menggunakan bahasa pemrograman Python karena kemudahan sintaks, ketersediaan library yang lengkap, dan popularitasnya dalam bidang keamanan informasi dan analisis data. Melalui penelitian ini diharapkan dapat memberikan pemahaman yang komprehensif tentang kelemahan keamanan algoritma Caesar Cipher, pentingnya Prinsip Kerckhoffs dalam desain sistem kriptografi, serta memberikan kontribusi edukatif bagi mahasiswa dan praktisi keamanan informasi dalam memahami konsep dasar kriptanalisis. Penelitian ini mengeksplorasi secara empiris mengapa ketergantungan pada ruang kunci yang terbatas—hanya 25 kemungkinan—membuat sistem ini rentan terhadap teknik brute force yang dapat diselesaikan dalam hitungan detik oleh mesin komputasi kontemporer. Pemahaman mendalam mengenai kerentanan ini menjadi titik tolak penting bagi peneliti untuk mengapresiasi kompleksitas algoritma kriptografi modern yang dirancang untuk menahan serangan yang jauh lebih canggih. Selain itu, pemilihan Python sebagai bahasa implementasi dalam penelitian ini didorong oleh fleksibilitasnya dalam memanipulasi data teks dan kemampuannya dalam menjalankan simulasi kriptanalisis secara efisien. Dengan ketersediaan library yang mendukung komputasi matematis dan operasi string, peneliti dapat memvisualisasikan proses enkripsi dan dekripsi secara transparan, yang pada gilirannya memperjelas pergeseran karakter yang terjadi dalam Caesar Cipher. Kontribusi utama penelitian ini adalah menyajikan analisis kuantitatif mengenai durasi waktu pemecahan kode yang menunjukkan signifikansi celah keamanan, sekaligus memberikan edukasi praktis mengenai urgensi penerapan standar kriptografi yang lebih robust dalam ekosistem digital saat ini

METHOD

Metodologi penelitian yang digunakan adalah metode eksperimental dengan pendekatan kuantitatif. Eksperimen difokuskan pada pengujian ketahanan algoritma Caesar Cipher melalui simulasi serangan kriptanalisis berdasarkan Prinsip Kerckhoffs. Dalam pelaksanaannya, penelitian ini mengasumsikan bahwa seluruh mekanisme enkripsi telah diketahui oleh penyerang, sehingga fokus utama analisis terletak pada kekuatan kunci dalam menyembunyikan informasi.

A. Algoritma Caesar Cipher

Caesar Cipher adalah cipher substitusi monoalfabetik di mana setiap huruf dalam *plaintext* digeser sejumlah posisi tertentu dalam alfabet. Rumus matematis enkripsi dan dekripsi adalah sebagai berikut:

$$\mathbf{C = (P + K) \bmod 26}$$

$$\mathbf{P = (C - K) \bmod 26}$$

Mekanisme kerja Caesar Cipher didasarkan pada operasi aritmatika modular, yang merupakan fondasi dari banyak teknik kriptografi simetris. Dalam rumus C = (P + K) mod26, variabel P merepresentasikan posisi numerik dari karakter plaintext (A=0, B=1, ..., Z=25), K adalah kunci pergeseran (shift key), dan C

adalah posisi numerik dari karakter ciphertext hasil enkripsi. Penggunaan operator modulo 26 memastikan bahwa hasil pergeseran akan selalu berada dalam rentang alfabet standar, sehingga proses transformasi data tetap konsisten dan dapat dipetakan kembali ke karakter alfabet yang bersesuaian.Sebaliknya, proses dekripsi dilakukan dengan membalikkan operasi pergeseran tersebut menggunakan rumus P = (C – K) mod26. Pada tahap ini, nilai C dikurangi dengan kunci K, dan operasi modulo 26 kembali diterapkan untuk menangani nilai negatif yang mungkin muncul akibat proses pengurangan tersebut, sehingga mengembalikan nilai numerik ke posisi plaintext aslinya. Transformasi dua arah yang simetris ini menjamin bahwa informasi yang telah disandikan dapat dipulihkan sepenuhnya oleh penerima pesan yang mengetahui kunci K yang sama, meskipun secara praktis, kesederhanaan rumus ini menjadikannya sangat mudah untuk dipecahkan melalui teknik kriptanalisis dasar karena keterbatasan ruang kunci yang hanya berjumlah 25 kemungkinan.

B. Prinsip Kerckhoffs

Prinsip Kerckhoffs menyatakan bahwa keamanan sistem kriptografi harus terletak pada kerahasiaan kunci, bukan pada kerahasiaan algoritma. Dalam konteks penelitian ini, diasumsikan bahwa penyerang telah mengetahui: (1) algoritma kriptografi yang digunakan, (2) panjang tabel encoding, dan (3) *ciphertext*. Penyerang tidak mengetahui kunci (K) dan *plaintext* asli.

C. Implementasi Python

Implementasi dilakukan menggunakan Python versi 3.x dengan membangun fungsi *encrypt()* dan *decrypt()* berbasis operasi modulo 26 terhadap nilai ASCII. Program mencakup penanganan huruf besar dan kecil, serta pengabaian karakter non-alfabet. Serangan brute force diimplementasikan dengan menguji seluruh 25 kemungkinan kunci secara berurutan.

D. Proses Enkripsi

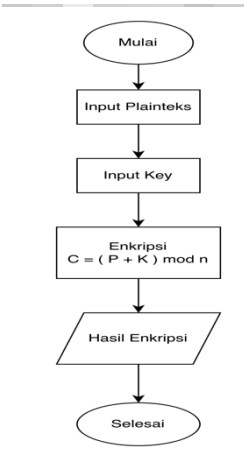

Figure 1. Proses enkripsi

Proses enkripsi dilakukan dengan tabel encoding alfabet Latin A–Z (nilai 0–25) dan kunci pergeseran K=4. Sebagai contoh, *plaintext* "UNUSU" dienkripsi sebagai berikut:

Table 1. Tabel Encoding Alfabet

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

C = (P + K) mod 26

Dengan K=4, setiap huruf pada UNUSU diproses: U(20)+4=24=Y, N(13)+4=17=R, U(20)+4=24=Y, S(18)+4=22=W, U(20)+4=24=Y. Hasil enkripsi adalah *ciphertext* "YRYWY".

E. Proses Dekripsi

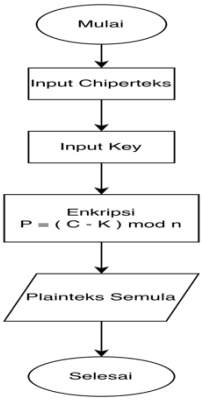

Figure 2. Proses Dekripsi

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

Proses dekripsi mengembalikan *ciphertext* "YRYWY" ke *plaintext* "UNUSU" menggunakan kunci yang sama K=4: Y(24)−4=20=U, R(17)−4=13=N, Y(24)−4=20=U, W(22)−4=18=S, Y(24)−4=20=U.

RESULT AND DISCUSSION

Hasil Pengujian Enkripsi dan Dekripsi

Pengujian dilakukan untuk memastikan bahwa fungsi kriptografi berjalan secara dua arah (simetris) dengan akurasi 100%. Pengujian menggunakan tiga pasang data uji dengan kunci yang berbeda-beda. Hasil seluruh pengujian tersaji pada Tabel 2.

Table 2. Hasil Pengujian Enkripsi dan Dekripsi Caesar Cipher

No	Plaintext (P)	Kunci (K)	Ciphertext (C)	Hasil Dekripsi	Status
1	UNUSU	5	ZSZXZ	UNUSU	Berhasil
2	UNUSU JAYA	12	GZGEG VMKM	UNUSU JAYA	Berhasil
3	Python Bisa	15	Eoiydc Oxbp	Python Bisa	Berhasil

Hasil pada Tabel 2 membuktikan bahwa implementasi Caesar Cipher menggunakan Python berfungsi dengan benar. Seluruh *plaintext* berhasil dienkripsi dan didekripsi kembali dengan tepat, memvalidasi kebenaran rumus $C = (P + K) \bmod 26$ dan $P = (C - K) \bmod 26$.

Analisis Keamanan Berdasarkan Prinsip Kerckhoffs

Pengujian simulasi serangan kriptanalisis dilakukan dengan kunci K=9 dan *plaintext* "keamanan kriptografi". Berdasarkan Prinsip Kerckhoffs, penyerang mengetahui algoritma dan *ciphertext*, tetapi tidak mengetahui kunci. Program brute force Python menguji seluruh kemungkinan kunci (K=1 hingga K=25) secara berurutan. Hasil menunjukkan:

- K=1 menghasilkan teks yang tidak bermakna
- K=9 berhasil mengembalikan pesan asli "keamanan kriptografi"
- Seluruh proses selesai dalam waktu kurang dari satu detik

Hal ini membuktikan bahwa Caesar Cipher memiliki ruang kunci yang sangat kecil — hanya 25 kemungkinan — sehingga serangan *brute force* dapat dilakukan tanpa sumber daya komputasi yang besar.

Evaluasi Keamanan

Evaluasi berdasarkan Prinsip Kerckhoffs menghasilkan tiga temuan utama. Pertama, Caesar Cipher sangat rentan terhadap serangan *brute force*. Seluruh kemungkinan kunci dapat diuji dalam waktu sangat singkat karena ruang kunci yang terbatas. Kedua, algoritma ini tidak memiliki kekuatan *confusion* yang memadai karena pola pergeseran yang linear dan statistik huruf yang tetap, sehingga analisis frekuensi pun dapat digunakan. Ketiga, Caesar Cipher tidak memenuhi standar keamanan modern karena bergantung pada keterbatasan kunci, bukan pada kompleksitas algoritma. Secara fungsional, Caesar Cipher berhasil berfungsi sebagai sistem kriptografi simetris sederhana, namun gagal memenuhi standar keamanan operasional modern.

CONCLUSION

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat ditarik kesimpulan sebagai berikut: (1) Algoritma Caesar Cipher berhasil diimplementasikan menggunakan Python dengan akurasi enkripsi dan dekripsi 100%, membuktikan bahwa secara fungsional algoritma ini bekerja dengan baik sebagai sistem kriptografi simetris sederhana.

(2) Melalui simulasi Prinsip Kerckhoffs, seluruh kemungkinan kunci (25 kunci) dapat diuji dalam waktu kurang dari satu detik, sehingga pesan asli "keamanan kriptografi" pada kunci K=9 dapat ditemukan dengan sangat mudah. (3) Caesar Cipher terbukti tidak memadai untuk melindungi data sensitif karena struktur matematisnya yang terlalu sederhana dan sangat rentan terhadap teknik kriptanalisis dasar. Penelitian ini memberikan kontribusi edukatif tentang pentingnya Prinsip Kerckhoffs dalam evaluasi keamanan sistem kriptografi dan pentingnya menggunakan algoritma modern seperti AES untuk kebutuhan keamanan data yang sesungguhnya.

REFERENCES

[1] Agung Prabowo. (n.d.). *16.bersains-2-2-sandi-dari-pacitan*.

[2] Amalya, N., Sopiana Silalahi, S. M., Nasution, D. F., Sari, M., & Gunawaan, I. (2023). *JURNAL MEDIA INFORMATIKA [JUMIN] Kriptografi dan Penerapannya Dalam Sistem Keamanan Data*.

[3] Basri. (2016). *KRIPTOGRAFI SIMETRIS DAN ASIMETRIS DALAM PERSPEKTIF KEAMANAN DATA DAN KOMPLEKSITAS KOMPUTASI*. http://ejournal.fikom-unasman.ac.id

[4] Bima Setiawan, A. (2025a). Penggunaan Cryptography dalam Keamanan Pesan Digital. *Journal of Computer Science and Information Technology*, *1*(2), 60–66. https://doi.org/10.70716/jocsit.v1i2.261

[5] Bima Setiawan, A. (2025b). Penggunaan Cryptography dalam Keamanan Pesan Digital. *Journal of Computer Science and Information Technology*, *1*(2), 60–66. https://doi.org/10.70716/jocsit.v1i2.261

[6] Cahya Hardita, V., Wahyu Sholeha, E., Raya Jl Obos No, P. G., Raya, P., Tengah, K., Informasi, T., Negeri Tanah Laut Jl Yani NoKm, P. A., Pelaihari, K., Tanah Laut, K., & Selatan, K. (n.d.). *PENERAPAN KOMBINASI METODE VIGENERE CIPHER, CAESAR CIPHER DAN SIMBOL BACA DALAM MENGAMANKAN PESAN*.

[7] Fachrul Dhika Ardiansyah. (n.d.). *5. 105-112*.

[8] Gading Nur Salmi. (2022). Implementation of the data encryption using caesar cipher and vernam cipher methods based on CrypTool2. *Journal of Soft Computing Exploration*, *3*(2). https://doi.org/10.52465/joscex.v3i2.86

[9] Hidayat, M., Tahir, M., Sukriyadi, A., Sulton, A., Ajeng, C., & Abduh, S. (n.d.). *PENERAPAN KRIPTOGRAFI CAESAR CHIPER DALAM PENGAMANAN DATA*. *2*(3). https://doi.org/10.56127/jukim.v2i0

[10] Hulu, S. (2024). Implementasi Algoritma Kriptografi Simetris Dalam Pengamanan Data Absensi Guru Dan Pegawai Pada Website Sekolah SMK Dharma Caraka Teluk Dalam Menggunakan RC4 Chiper. *KETIK : Jurnal Informatika*, *1*(04), 01–07. https://doi.org/10.70404/ketik.v1i04.58

[11] Latifah, U. W., & Prasetyo, P. W. (2021). IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK ELGAMAL DI LAPANGAN GALOIS PRIMA PADA PROSES ENKRIPSI DAN DEKRIPSI BERBANTUAN SOFTWARE PYTHON. *Journal of Fundamental Mathematics and Applications (JFMA)*, *4*(1), 45–60. https://doi.org/10.14710/jfma.v4i1.9278

[12] Noviyanti. (2022). Analisa Algoritma Kriptografi Klasik Caesar Cipher Viginere Cipher dan Hill Cipher-Study Literature. *JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY*, *2*(1).

[13] Nugroho, W., & Tambunan, L. A. (2025). Transformasi Digital dan Dampaknya terhadap Kompetensi Sumber Daya Manusia di Era Industri 5.0. *Jurnal Ilmiah Global Education*, *6*(3), 1959–1974. https://doi.org/10.55681/jige.v6i3.4172

[14] Prabowo, W., & Anwar, N. (n.d.). *Pengujian Model Simulasi Efek Avalanche Kriptografi Simetris Algoritma AES 128-bit, Mode ECB dan CBC*. https://doi.org/10.37817/ikraith-informatika.v9i1

[15] Rahman, F. (n.d.). *Penggunaan Beberapa Algoritma Kriptografi Kunci-Simetri untuk Mensimulasikan Kriptografi Kunci-Publik*.

[16] Ramadhan, G. I., Alfarisi, S., Raya, J., No, T., Gedong, K., Rebo, P., & Timur, J. (2021). PENERAPAN CAESAR CIPHER PADA ABSENSI DAN CUTI KARYAWAN PT DATACOMINDO MITRAUSAHA BERBASIS JAVA. In *Jurnal Rekayasa Komputasi Terapan)* (Vol. 01).

[17] Romzi, M., & Kurniawan, B. (2020). Implementasi Pemrograman Python Menggunakan Visual Studio Code. In *JIK: Vol. XI* (Issue 2). www.python.org

[18] Saputra, M., & Muhammad, A. H. (2021). Penerapan Kombinasi Algoritma Caesar Cipher pada Block Acak dan Cipher Transposisi Dalam Mengamankan Pesan. *JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY*, *1*(1).

[19] Sarumaha, D., Mohammad Andri Budiman, & Muhammad Zarlis. (2023). Performance

Analysis of Hybrid Cryptographic Algorithms Rabbit Stream and Enhanced Dual RSA. *Data Science: Journal of Computing and Applied Informatics*, *7*(1), 35–43. https://doi.org/10.32734/jocai.v7.i1-10483

[20] Serikastawan, G., Setiawan, T., & Ranova, D. (n.d.-a). *Teknik Kriptanalisis Linier*.

[21] Serikastawan, G., Setiawan, T., & Ranova, D. (n.d.-b). *Teknik Kriptanalisis Linier*.

[22] Uci Julya Ningsih, Sophia Salsabila, Isniar Hutapea, Dewi Santika, & Indra Gunawan. (2024). Pendekripsian Caesar Chiper Dengan Menggunakan Teknik-Teknik Kriptanalisis. *Jurnal Ilmu Komputer Dan Multimedia*, *1*(1), 11–15. https://doi.org/10.46510/ilkomedia.v1i1.10

[23] Ujung, A. M., Irwan, M., & Nasution, P. (2023). Pentingnya Sistem Keamanan Database untuk melindungi data pribadi. *JISKA: Jurnal Sistem Informasi Dan Informatika*, *1*(2), 44. http://jurnal.unidha.ac.id/index.php/jteksis