Jurnal Pendidikan dan
Pembelajaran (JPP)
https://journalversa.com/s/index.php/jpp Volume 6, Nomor 2 Juni 2024

ANALISIS PERBANDINGAN CRIPTOGRAFI KLASIK CAESAR CHIPER DAN PLAYFAIR CIPHER PADA SISTEM KEAMANAN DATA

Poppy Fantika Sari[1], Muhlis Tahir[2], Alfina Kusuma Nilasari[3], Ananda Amilus Sholikhah[4], Tria Wulandari[5]
Universitas Trunojoyo Madura[1,2,3,4,5]
poppyfantika@gmail.com[1], muhlis.tahir@trunojoyo.ac.id[2], alvinakusumaaa@gmail.com[3], ananda.emil88@gmail.com[4], triaw53@gmail.com[5]

The development of information technology has had a major impact on various aspects of our lives. One of the areas affected is data security, where classical cryptography plays an important role in maintaining the confidentiality of messages. In this study, we analyze two classic cryptographic techniques, namely Caesar Cipher and Playfair Cipher, for data security systems. Caesar Cipher is a simple substitution technique that shifts letters in the alphabet, while Playfair Cipher uses a 5x5 matrix of key letters to encrypt letter pairs. We carried out a comparison between these two techniques based on this research method in the form of a literature study using a qualitative approach with data collection techniques in the form of notes, books, papers or articles, and journals. The results of the analysis show that the Playfair Cipher tends to be more secure and complex than the Caesar Cipher, although it may require more resources to implement. However, the choice of cryptographic technique must be tailored to the specific needs of the system and the desired level of security.
Keywords**:** *Classical Cryptography, Caesar Cipher, Playfair Cipher, Data Security.*

Abstrak

Perkembangan teknologi informasi telah membawa dampak besar dalam berbagai aspek kehidupan kita. Salah satu bidang yang terpengaruh adalah keamanan data, di mana kriptografi klasik memainkan peran penting dalam menjaga kerahasiaan pesan. Dalam kajian ini, kami menganalisis dua teknik kriptografi klasik, yaitu Caesar Cipher dan Playfair Cipher, untuk sistem keamanan data. Caesar Cipher adalah teknik substitusi sederhana yang menggeser huruf-huruf dalam alfabet, sementara Playfair Cipher menggunakan matriks 5x5 dari huruf-huruf kunci untuk mengenkripsi pasangan huruf. Kami melakukan perbandingan antara kedua teknik ini berdasarkan Metode penelitian ini adalah studi kepustakaan yang menggunakan pendekatan kualitatif dengan menggunakan teknik pengumpulan data berupa catatan, buku, artikel dan serta jurnal. Hasil analisis menunjukkan bahwa Playfair Cipher cenderung lebih aman dan kompleks daripada Caesar Cipher, meskipun mungkin memerlukan lebih banyak sumber daya dalam implementasinya. Namun, pemilihan teknik kriptografi harus disesuaikan dengan kebutuhan spesifik sistem dan tingkat keamanan yang diinginkan.
Kata Kunci: Kriptografi Klasik, Caesar Cipher, Playfair Cipher, Keamanan Data.

A. PENDAHULUAN

Perkembangan teknologi informasi, yang berlangsung dengan kecepatan yang luar biasa, telah menjadi kekuatan dominan yang melibatkan setiap aspek kehidupan kita (Nazwa &

Muhammad, 2023). Perkembangan TIK telah memberikan kontribusi besar bagi peradaban dari waktu ke waktu. TIK dapat diartikan sebagai penerapan pengetahuan dan keterampilan yang digunakan masyarakat untuk menyampaikan informasi, dengan menggunakan perangkat komputasi sebagai alat untuk menyajikan dan mengolah data informasi. Pemanfaatan TIK dapat diterapkan di banyak bidang, termasuk keamanan lapangan. (Nuke , et al., 2019).

Kriptografi klasik adalah ilmu dan seni yang digunakan untuk menjaga keamanan pesan yang bersifat pribadi dan rahasia. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi sebuah kode yang tidak dapat dimengerti pihak lain Kriptografi klasik beroperasi dalam mode karakter, yakni menggunakan huruf abjad (A - Z). Algoritma kriptografi klasik digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Metode menyembunyikan pesannya adalah dengan teknik substitusi atau transposisi atau keduanya. Namun algoritma kripografi klasik saat ini tidak lagi digunakan karena sudah dianggap tidak aman. Kriptografi klasik memberikan konsep dasar pemahaman kriptografi dan dijadikan sebagai dasar algoritma kriptografi modern.

Kriptografi Caesar Cipher adalah teknik kriptografi klasik yang mengenkripsi teks dengan menggunakan teknik substitusi sederhana. Caesar Cipher merupakan teknik enkripsi yang paling sederhana dan banyak digunakan. Chiper ini berjenis chiper substitusi, dimana setiap huruf pada plaintextnya digantikan dengan huruf lain yang tetap pada posisi alfabet (Yuningrat , Rosihan, & Salkin , 2019). Terlepas dari metode yang sederhana ini, Julius Caesar menggunakan Cipher sebagai cara untuk berkomunikasi secara rahasia dengan para panglimanya.

Metode Playfair Cipher adalah salah satu teknik dalam kriptografi klasik yang melibatkan pengolahan data dalam blok-blok besar. Proses enkripsi menggunakan Playfair Cipher melibatkan pembuatan tabel kunci berdasarkan kata kunci yang telah diketahui. Tabel cipher yang digunakan untuk enkripsi dan dekripsi adalah tabel matriks berukuran 5x5 yang berisi huruf kapital dari A hingga Z, dengan huruf J dihilangkan. Tabel ini tidak mampu mengenkripsi teks biasa yang mengandung angka (0-9) atau simbol-simbol khusus. (Nurkifli , 2014).

B. KAJIAN TEORI

Konsep Algoritma

Algoritma merupakan inti dari ilmu komputer (Nuke, et al. , 2019) dan sering disebut sebagai salah satu cabang ilmu komputer. Namun, kita tidak boleh berasumsi bahwa algoritma selalu identik dengan ilmu komputer. Instruksi algoritma mencakup banyak proses . Setiap resep memiliki serangkaian langkah, sama seperti proses memasaknya.

Jika langkahnya tidak logis, maka tidak akan bisa memasak makanan yang Anda inginkan. Umumnya unit yang melakukan pemrosesan disebut prosesor. Prosesor dapat berupa manusia, komputer, robot, atau perangkat elektronik lainnya. Prosesor menjalankan proses dan dieksekusi sesuai dengan algoritma yang ada. Mereka melakukan langkah-langkah secara algoritmik, seperti seorang koki yang mengikuti buku resep atau seorang pianis yang memainkan lagu mengikuti notasi pada lembaran musik. Oleh karena itu, algoritma harus dinyatakan dalam format yang mudah dipahami oleh prosesor seperti manusia, komputer, dan perangkat lainnya.

Konsep Kriptografi

- Pesan, plainteks, dan cipherteks.

  Pesan berupa plainteks adalah teks awal sebelum melalu proses enkripsi. Sementara itu, cipherteks adalah pesan yang sulit untuk dapat diketahui isi pesannya.
- Enkripsi dan dekripsi.

  Enkripsi adalah proses ketika informasi atau data dirubah menjadi keadaan yang sulit untuk diketahui akan informasi dasarnya menggunakan algoritma tertentu, Deskripsi adalah proses ketika keadaan yang sulit tersebut dikembalikan ke dalam bentuk semula. Sumber yang lain mengutarakan hal yang sama yaitu konversi data antara bentuk terenkripsi atau cipherteks dan bentuk ditunjukkan.
- Pesan, plainteks, dan cipherteks.

  Pesan yang dianggap plainteks tersebut adalah teks awal sebelum melalu proses enkripsi. Sementara itu, cipherteks adalah pesan yang butuh dilalui oleh dekripsi terlebih dahulu untuk dapat dilihat isinya. (Herlambang, Nilma, & Pravitasari, 2024).

Tujuan Kriptografi

Kriptografi mempunyai empat tujuan (Surnawani, Sodikin , & Umul , 2022), dan aspek-aspek tersebut merupakan aspek fundamental dari tujuan dan aspek keamanan kriptografi.

1. Confidentiality (Kerahasiaan) Menciptakan pesan yang sangat sulit dipahami orang lain, sehingga menjadikannya pesan rahasia.
2. Data Integrity (Integritas) Pesan yang dibuat seolah-olah belum pernah dirusak sebelumnya.
3. Autentication (Otentikasi) Cari solusi yang disesuaikan dengan orang yang berkomunikasi dengan Anda.
4. Non-repudiation (Penyangkalan) Mencegah pesan dibatalkan dan sebaliknya.

Caesar Chiper

Caesar Cipher adalah salah satu algoritma substitusi klasik tertua yang tersebar luas di dunia (Nasution, 2024). Algoritma ini enkripsi pesan dengan cara menggantikan setiap karakter teks sederhana dengan karakter lain sesuai dengan urutan alfabet yang digeser beberapa kali. Teknik imitasi ini tidak memerlukan kunci khusus untuk melakukan dekripsi, tetapi hanya keberadaan algoritma dan banyaknya langkah karakter yang diubah posisinya. Secara tradisional, Caesar Cipher telah mulai ditinggalkan dalam pengaturan terkini karena itu diketahui bahwa pesan yang dienkripsi dengan cara ini mudah ditembus oleh hacker biasa. Maka dari itu, lebih aman untuk menggabungkan beberapa cara dari teknik substitusi dengan cara lain dari metode klasik Caesar, yaitu, misalnya, dengan transposisi. Olahraga yang dikedalikan ini bisa memberikan jumlah masalah lebih baik, serta dengan itu, artikel substansial sebagai berbahan dekripsi karena apa yang tidak ada solusi untuk dianggap menjadi teknik brute force.

Playfair Cipher

Komponen penting dari metode Playfair adalah tabel sandi dan penerapannya dalam proses pengkodean dan penguraian kode. Tabel dasar Playfair diformat sebagai matriks berdimensi 5 kali 5, berisi semua huruf kapital dari A sampai Z tetapi bukan J. Namun, tabel bawaan sandi Playfair tidak berguna untuk menghitung semua karakter teks (0–9) dan simbol. (Irmayani, Putriani, Resky, & Asrun, 2023).

C. METODE PENELITIAN

Penelitian ini menerapkan metode penelitian pustaka atau library research, di mana peneliti mengandalkan berbagai literatur sebagai sumber referensi untuk data penelitian, dan menggunakan pendekatan kualitatif dengan data yang diperoleh berbentuk kata-kata atau

deskripsi. Tujuan penelitian ini adalah untuk membandingkan algoritma Caesar Cipher dan Playfair Cipher yang telah ada sebelumnya atau sedang dibahas. Informasi yang diperoleh berasal dari berbagai sumber seperti buku, internet, jurnal, dan artikel yang relevan dengan penelitian.

Teknik pengumpulan data yang digunakan adalah melalui dokumen, di mana peneliti mencari informasi mengenai suatu permasalahan atau variabel yang berbentuk karya, buku, esai, artikel, atau majalah. Alat penelitian yang digunakan meliputi format memo, daftar gaya penulisan, dan kategori bahan penelitian. Teknologi pengumpulan data yang dipilih adalah data sekunder, yaitu data yang telah tersedia dan diperoleh melalui pencarian dan pengumpulan. Dalam memperoleh data yang akurat sesuai mengenai tujuan penelitian, ada beberapa aspek yang perlu diperhatikan. Tahap analisis data meliputi proses pencarian dari berbagai sumber dengan cara menyusun data dan mengkategorikannya hingga sampai pada kesimpulan yang dapat dipahami oleh penulis dan pembaca.

Teknik analisis data yang diterapkan adalah analisis isi, yang berguna untuk memahami dan menganalisis teks dengan cara investigasi sistematis dan kuantitatif. Fokus analisis ini adalah pada perbedaan antara Caesar Cipher dan Playfair Cipher, dengan tujuan memperoleh kesimpulan yang dapat diverifikasi kembali sesuai konteksnya. Proses analisis melibatkan perbandingan, pemilihan, penggabungan, dan penyaringan makna yang berbeda untuk menemukan makna yang relevan.

D. HASIL UJI COBA DAN PEMBAHASAN

Deskripsi Data Uji Coba

1. Caesar Cipher

Caesar Cipher adalah salah satu algoritma substitusi klasik tertua yang tersebar luas di dunia (Nasution, 2024). Algoritma ini enkripsi pesan dengan cara menggantikan setiap karakter teks sederhana dengan karakter lain sesuai dengan urutan alfabet yang digeser beberapa kali. Teknik imitasi ini tidak memerlukan kunci khusus untuk melakukan dekripsi, tetapi hanya keberadaan algoritma dan banyaknya langkah karakter yang diubah posisinya.

Enkripsi :

$$C = E(k, p) = (p + k) \bmod 26 \quad \text{..... (1)}$$

Dekripsi :

$$p = D(k, C) = (C - k) \bmod 26 \quad \text{..... (2)}$$

Contoh bentuk enkripsi chipertext dari plaintext bertuliskan “IKHLAS” dengan menggunakan metode Caesar Cipher dengan k=3, dilakukan perhitungan dengan cara sebagai berikut:

p_1 = ‘I’ = 8 → $c_1 = E(8) = (8+3)$ **mod** 26 = 11 = ‘L’

p_2 = ‘K’ = 10 → $c_2 = E(10) = (10+3)$ **mod** 26 = 13 = ‘N’

p_3 = ‘H’ = 7 → $c_3 = E(7) = (7+3)$ **mod** 26 = 10 = ‘K’

p_4 = ‘L’ = 11 → $c_4 = E(11) = (11+3)$ **mod** 26 = 14 = ‘O’

p_5 = ‘A’ = → $c_5 = E(0) = (0+3)$ **mod** 26 = 3 = ‘D’

p_6 = ‘S’ = 18 → $c_6 = E(18) = (18+3)$ **mod** 26 = 21 = ‘V’

Dan diperolehlah hasil enskripsi bertuliskan “LNKODV” dari plaintext yang bertuliskan kata “IKHLAS” tersebut.

Contoh bentuk deskripsi plaintext dari ciphertext text bertuliskan “LNKODV” dengan menggunakan metode Caesar Chiper dengan k=3 dilakukan perhitungan dengan cara sebagai berikut:

c_1 = ‘L’ = 11 → $p_1 = D(11) = (11 - 3)$ **mod** 26 = 8 = ‘i’

c_2 = ‘N’ = 13 → $p_2 = D(13) = (13 - 3)$ **mod** 26 = 10 = ‘k’

c_3 = ‘K’ = 10 → $p_3 = D(10) = (10 - 3)$ **mod** 26 = 7 = ‘h’

c_4 = ‘O’ = 14 → $p_4 = D(14) = (14 - 3)$ **mod** 26 = 11 = ‘l’

c_5 = ‘D’ = 3 → $p_5 = D(3) = (3 - 3)$ **mod** 26 = 0 = ‘a’

$$c_6 = \text{‘V’} = 21 \rightarrow p_6 = D(21) = (21 - 3) \textbf{ mod } 26 = 18 = \text{‘s’}$$

Dan diperolehlah hasil deskripsi bertuliskan “IKHLAS” dari ciphertext yang bertuliskan kata “LNKODV” tersebut.

2. Playfair Cipher

Komponen penting dari metode Playfair adalah tabel sandi dan penerapannya dalam proses pengkodean dan penguraian kode(Irmayani, Putriani, Resky, & Asrun, 2023). Tabel dasar Playfair diformat sebagai matriks berdimensi 5 kali 5, berisi semua huruf kapital dari A sampai Z tetapi bukan J. Namun, tabel bawaan sandi Playfair tidak berguna untuk menghitung semua karakter teks (0–9) dan simbol.

Contoh bentuk enkripsi ciphertext dari plaintext bertuliskan “PASTI BISA” dengan menggunakan metode Playfair Cipher dengan kunci dengan kata “BANGKIT”, dilakukan perhitungan dengan cara sebagai berikut:

P = PASTI BISA

K = BANGKITCDEFHLMOPQRSUVWXYZ

Kemudian susunlah kunci tersebut dalam tabel 5 kali 5.

B	A	N	G	K
I	T	C	D	E
F	H	L	M	O
P	Q	R	S	U
V	W	X	Y	Z

Kemudian susun plaintext menjadi dua huruf-dua huruf agar mudah.

PA ST IB IS A

Jika huruf yang dicari tidak berada pada satu baris dan satu kolom maka hasil ciphertextnya adalah sudut diagonal dari kedua huruf yang dicari.

- PA = QB

B	A	N	G	K
I	T	C	D	E
F	H	L	M	O
P	Q	R	S	U
V	W	X	Y	Z

- ST = DQ

B	A	N	G	K
I	T	C	D	E
F	H	L	M	O
P	Q	R	S	U
V	W	X	Y	Z

Dan jika huruf plaintext dalam satu kolom yang sama maka huruf ciphertextnya turun satu kolom dibawahnya. Dan jika dalam satu baris yang sama maka huruf plaintextnya digeser satu huruf ke kanan. Pada contoh berikut huruf I dan B berada pada satu kolom yang sama maka I menjadi F dan B menjadi I.

- IB = FI

B	A	N	G	K
I	T	C	D	E
F	H	L	M	O
P	Q	R	S	U
V	W	X	Y	Z

- IS = DP

B	A	N	G	K

I	T	C	D	E
F	H	L	M	O
P	Q	R	S	U
V	W	X	Y	Z

- A = T

B	A	N	G	K
I	T	C	D	E
F	H	L	M	O
P	Q	R	S	U
V	W	X	Y	Z

Dari hasil plaintext bertuliskan “PASTI BISA” dengan kunci “BANGKIT”, maka diperoleh hasil ciphertext berupa “QB QD FI BP T”. Dan sebaliknya untuk ciphertext ke plaintext. untuk ciphertext ke plaintext.

Pembahasan

Hasil yang diperoleh dari perbandingan antara kriptografi Caesar Cipher dan Playfair Cipher dapat dilihat pada tabel berikut :

Perbedaan	***Caesar Cipher***	***Playfair Cipher***
Fungsi	Substitusi sederhana dengan pergeseran	Substitusi menggunakan matriks bigram
Kunci Average	Jumlah kunci rata-rata	Matriks kunci 5×5
Jumlah Rumus	Menggeser huruf sesuai dengan kunci	Mencari posisi huruf pada matriks kunci
Cara Penyelesaian	Pergeseran huruf sesuai dengan kunci	Mencocokkan pasangan huruf pada matriks

Caesar Cipher dan Playfair Cipher adalah dua teknik klasik dalam kriptografi yang digunakan untuk menyandikan teks. Namun, keduanya berbeda secara signifikan dalam cara

mereka beroperasi. Caesar Cipher adalah jenis substitusi sederhana di mana setiap huruf digeser beberapa posisi dalam abjad, sedangkan Playfair Cipher menggunakan matriks 5x5 dari huruf-huruf kunci untuk menyandikan pasangan huruf. Dalam Caesar Cipher, kunci adalah jumlah pergeseran dalam alfabet, sementara dalam Playfair Cipher, kunci adalah matriks 5x5 yang dibentuk oleh huruf-huruf unik. Kelemahan Caesar Cipher terletak pada jumlah kunci yang terbatas, sementara Playfair Cipher lebih kompleks karena menggunakan matriks kunci yang rumit, membuatnya sulit untuk ditembus dengan metode analisis frekuensi. Sebagai contoh, dalam Caesar Cipher, huruf diubah dengan cara yang konsisten berdasarkan jumlah pergeseran, sedangkan dalam Playfair Cipher, pasangan huruf diganti dengan aturan tertentu berdasarkan posisi mereka dalam matriks kunci. Dengan demikian, perbedaan utama antara keduanya terletak pada metode enkripsi, penggunaan kunci, dan tingkat keamanan relatif.

E. KESIMPULAN

Berdasarkan penjelasan pembahasan sebelumnya dapat disimpulkan dari pembahasan Algoritma Caesar Cipher dengan Playfair Cipher sebagai berikut:

1. Metode Enkripsi: Caesar Cipher menggunakan metode substitusi sederhana dengan pergeseran karakter dalam alfabet, sementara Playfair Cipher menggunakan matriks 5x5 dari huruf-huruf kunci untuk menyandikan pasangan huruf. Perbedaan dalam metode enkripsi memengaruhi kompleksitas dan keamanan masing-masing teknik.
2. Kunci: Caesar Cipher memiliki kunci tunggal berupa jumlah pergeseran karakter, sedangkan Playfair Cipher menggunakan matriks kunci yang terdiri dari huruf-huruf unik. Keterbatasan jumlah kunci dalam Caesar Cipher dapat menjadi kelemahan, sementara matriks kunci dalam Playfair Cipher memberikan lebih banyak variasi.
3. Keamanan: Playfair Cipher cenderung lebih aman daripada Caesar Cipher karena menggunakan matriks kunci yang lebih kompleks, membuatnya lebih sulit untuk ditembus dengan metode analisis frekuensi atau serangan brute force. Namun, keamanan relatif dari masing-masing teknik juga tergantung pada implementasi dan panjangnya kunci yang digunakan.
4. Kinerja dan Efisiensi: Dalam konteks kinerja dan efisiensi, Caesar Cipher dapat diimplementasikan dengan lebih sederhana dan memerlukan waktu pemrosesan yang lebih sedikit daripada Playfair Cipher. Namun, penting untuk mempertimbangkan keamanan yang diperlukan terhadap kebutuhan kinerja sistem.

DAFTAR PUSTAKA

Lubis, N. S., & Nasution, M. I. P. (2023). Perkembangan Teknologi Informasi Dan Dampaknya Pada Masyarakat. *Kohesi: Jurnal Sains dan Teknologi*, *1*(12), 41-50.

Sephiana, N., Tahir, M., Wulandari, S. D., Rahmansyah, F. R., Nuvitasari, R. N., & Prakasa, R. A. (2023). Analisis Perbandingan Algoritma Monoalphabetic Cipher dan Polyalphabetic Substitution Cipher pada Sistem keamanan Data. *Explore IT: Jurnal Keilmuan dan Aplikasi Teknik Informatika*, *15*(1), 16-21.

Amin, M. M. (2016). Implementasi kriptografi klasik pada komunikasi berbasis teks. *Pseudocode*, *3*(2), 129-136.

Putri, Y. D., Rosihan, R., & Lutfi, S. (2019). Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance. *JIKO (Jurnal Informatika dan Komputer)*, *2*(2), 87-94.

Susanti, D. (2020). Analisis Modifikasi Metode Playfair Cipher Dalam Pengamanan Data Teks. *Indonesian Journal of Data and Science*, *1*(1), 11-18.

Hanifah, A. (2021). Perbandingan Kriptografi Cipher Substitusi Homofonik dan Poligram dengan Caesar Cipher. *Univ. Langlang Buana*, 1-10.

Herlambang, D. N. R., Nilma, N., & Pravitasari, N. (2024). Penerapan Kriptografi AES untuk Keamanan Data Aplikasi Pemesanan Bibit Ternak pada BPSI UAT. *REMIK: Riset dan E-Jurnal Manajemen Informatika Komputer*, *8*(1), 29-44.

Nasution, S. D. (2024, Januari). Modifikasi Algoritma Caesar Cipher Menggunakan Linear Congruent Method Untuk Mengamankan Data. KETIK : Jurnal Informatika, 95-101.

Irmayani, A. P., A. R., & B. A. (2023). DOUBLE PENGAMANAN DATA DENGAN PLAYFAIR CHIPER DAN HILL CHIPER. EDUTECH : JURNAL PENDIDIKAN DAN TEKNOLOGI, 50-57.

Jarkasih, S., & Fatimah, U. (2023). PENGGUNAAN PUBLIC KEY INFRASTRUCTURE KUNCI PERSETUJUAN (KEY AGREEMENT). *Authentication Authorization Accounting Pendidikan Teknologi Informasi dan Teknologi Informasi*, *1*(2), 97-102.