(2023), 2 (1): 31-37 Sabda 2962-5351
Jurnal Sastra dan Bahasa

ANALISIS PERFORMA ALGORITMA KRIPTOGRAFI CAESAR CIPHER UNTUK KEAMANAN DATA MENGGUNAKAN PHYTON PADA PUISI "KENANGAN"

Rizky Amalia[1)], Muhlis Tahir[2)], Era Kusuma Ningrum[3)], Muhammad Ali Efendi[4)], Lisda Nursanti[5)], Fahmi Arhami Hamdi[6)]
[1-6)] Program Studi Pendidikan Informatika, Universitas Trunojoyo Madura
email: [1)]190631100085@student.trunojoyo.ac.id,

Correspondence		
Email: 190631100085@student.trunojoyo.ac.id	No. Telp: +6285331612734	
Submitted 3 Mei 2023	Accepted 10 Mei 2023	Published 15 Mei 2023

ABSTRACT

This study aims to analyze the performance of the Caesar Cipher cryptographic algorithm in maintaining data security in a poem entitled "Memories" using an experimental method. This research was conducted by implementing the Caesar Cipher algorithm in Python and measuring the execution time between the original text and the encrypted and decrypted text. The method used in this study was an experiment with two groups of data, namely the original text data group and the encrypted and decrypted text data group. The results showed that the Caesar Cipher algorithm can properly maintain data security in poetry texts, with a relatively fast and efficient execution time. However, this algorithm is less effective in securing data on long texts or experiencing brute force attacks. Even so, this algorithm is still effective enough to be used on relatively small texts such as a poem.

Kata kunci: Caesar Cipher, Kriptografi, Python, Puisi, Eksperimen

Pendahuluan

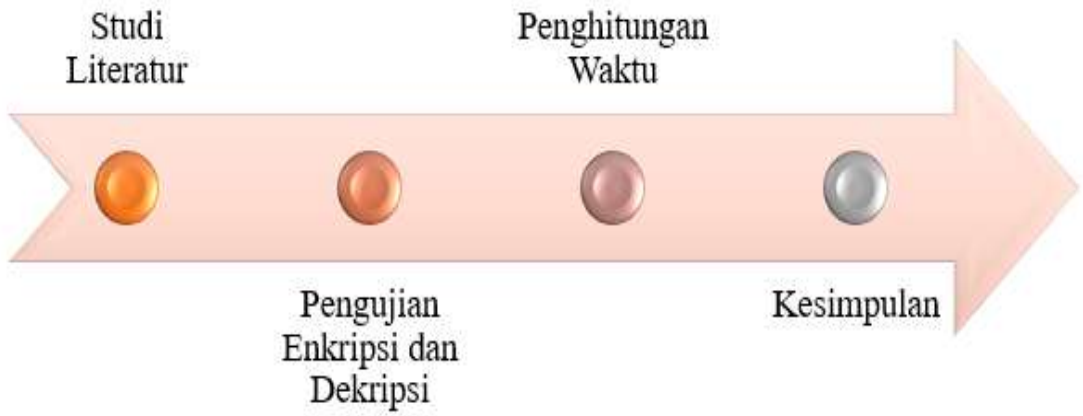
Keamanan data merupakan sesuatu persoalan yang harus dijaga dan diperhatikan. Menjaga keutuhan dan rahasia dari sebuah data sebagai bentuk informasi dalam pekerjaan bahkan kehidupan sosial sangatlah dibutuhkan, maka dari itu dibutuhkan salah satu teknik yang dibutuhkan untuk mengubah pesan teks bersandi ataupun mengubah bentuk aslinya dengan menggunakan kriptografi (Saputra, Efendi, & Kusuma, 2023). Tingkat keamanan data sebagai bentuk penjagaan keamanan data yang bersifat pribadi sangat dianjurkan agar tidak terjadi pencurian data pribadi yang termasuk dalam melanggar hukum teknologi informasi. Adanya kriptografi dapat membantu meningkatkan keamanan data pribadi karena kriptografi dapat menyamarkan sebuah pesan dengan menjadikan pesan tersebut sulit dibaca dan dimengerti. Kriptografi adalah sebuah seni dan ilmu menyembunyikan pesan (enkripsi) dengan menggunakan naskah asli (plaintext) diacak melalui kunci enkripsi sehingga menjadi naskah acak yang sulit untuk dibaca (ciphertext) oleh seseorang yang tidak memiliki dan mengetahui kunci deskripsi (Nasution, 2019; Pamungkas & Muhammad, 2022; Rinaldi, 2022).

Beberapa penelitian terdahulu yang relevan dengan yang dilakukan oleh penulis antara lain seperti Analisis Performansi Kriptografi Berbasis Caesar Cipher Untuk Keamanan Data Menggunakan Python Pada Tembang Macapat (Purnamasari, Dewi, & Trisetiyanto, 2019). Pada penelitian yang dilakukan oleh Dewi Purnamasari dkk bertujuan untuk menggunakan algoritma Caesar Cipher dalam proses penyandian dan untuk mengetahui efektifitas waktu enkripsi serta deskripsi dari teknik kriptografi tersebut pada tembang Macapat menggunakan bahasa pemrograman Python. Waktu proses kedua metode tersebut menunjukkan bahwa waktu deskripsi lebih lama dibandingkan proses enkripsi. Selanjutnya, penelitian yang dilakukan oleh Rizky Rinaldi tentang Analisis Keamanan Modifikasi Metode Caesar Chiper Dalam Teknik Enkripsi Dan Deskripsi bahwa menggunakan algoritma caesar ciphertext dapat meningkatkan keamanan data menjadi lebih baik dengan memodifikasi 62 karakter set pada metode caesar chipper. Kemudian dapat disimpulkan bahwa modifikasi tersebut berhasil dilakukan karena

modifikasi ini mampu meningkatkan keamanan metode enkripsi caesar chiper. Selain itu, dilakukannya modifikasi ini mampu menjadikan hasil enkripsi atau chipertext menjadi lebih bervariasi (Rinaldi, 2022).

Metode Penelitian

Metode penelitian yang digunakan yakni penelitian studi literatur dengan metode eksperimen algoritma Caesar Cipher. Berikut alur penelitian yang dilakukan dapat dilihat pada gambar 1.



Gambar 1 Alur Penelitian

Alur penelitian yang dilakukan adalah sebagai berikut:

a. Studi Literatur
   Tahap ini dilakukan dengan mencari khasanah atau sumber referensi berupa buku, jurnal ilmiah, atau hasil penelitian yang terdahulu yang terkait dengan algoritma Caesar cipher dan pemrograman dengan Bahasa pemrograman python yag digunakan untuk menguji enkripsi dan dekripsi.
b. Proses Enkripsi dan Deskripsi
   Proses enkripsi dan dekripsi dilakukan menggunakan Caesar cipher dengan kunci K=7 dan K=18. Proses enkripsi adalah proses penyembunyian data dengan cara mengubah dari plaintext ke ciphertext. Sedangkan proses deskripsi adalah kebalikannya, proses pengembalian dari ciphertext menjadi plaintext kembali. Yang memiliki tujuan untuk memahami pesan yang ada supaya dapat dibaca oleh user dengan baik. Berkaitan dengan Caesar Cipher. Caesar Cipher merupakan metode penyandian dalam kriptografi klasik yang paling terkenal. Dalam pengerjaannya algoritma kriptografi ini hanya melakukan pergeseran urutan karakter sebanyak nilai yang ada. Kriptogram dengan metode Caesar Chiper bekerja dengan cara huruf-huruf dalam plainteks digantikan oleh huruf lainnya dalam posisi tertentu dalam susunan alphabet yang menggeser sebanyak n huruf, jadi huruf chiper pada algoritma Caesar adalah hasil pergeseran sekian huruf dari huruf asli. Dalam penelitian ini nilai kunci dari Caesar Cipher adalah 7 dan 18.
c. Menghitung Waktu Enkripsi dan Deskripsi
   Proses penghitungan yang dilakukan dalam proses enripsi dan dekripsi ini dilakukan dengan python yakni dengan cara menghitung dengan menggunakan kode program pada python.
d. Kesimpulan
   Kesimpulan hasil pengujian dengan mengimplementasi serta membandingkan Caesar cipher dan membandingkan waktu proses enkripsi dan dekripsi.

Hasil dan Pembahasan

Pada proses pengujian dilakukan dengan 1 sampel plainteks berupa puisi yang terdiri dari 3 bait dengan kunci yang digunakan yakni K1= 7 dan K2 = 18. Bertujuan untuk membandingkan efektifitas waktu yang ditempuh dalam proses enkripsi dan dekripsi yang dilakukan pada saat pengujian berlangsung. Pada Tabel 1 menunjukkan waktu yang ditempuh dalam melakukan enkripsi dan dekripsi pada puisi "Kenangan". Pada Tabel 2 menunjukkan hasil dari proses enkripsi dan dekripsi pada puisi "Kenangan".

Tabel 1 Hasil Waktu Perhitungan Enkripsi dan Dekripsi

Plainteks	**Kunci**	**Enkripsi (Dtk)**	**Dekripsi (Dtk)**
Bait 1	7	1.4	1.6
Bait 1	18	1.3	1.29
Bait 2	7	1.4	1.79
Bait 2	18	1.69	1.89
Bait 3	7	1.4	1.5
Bait 3	18	1.4	1.7

Berdasarkan tabel diatas yaitu hasil perhitungan waktu dapat disimpulkan bahwa proses deskripsi membutuhkan waktu yang lama dibanding dengan proses enkripsi. Dapat dilihat dalam tabel bahwa rata-rata waktu yang dibutuhkan dalam proses enkri[si membutuhkan waktu 1.4 detik. Sedangkan waktu yang diperlukan dalam proses dekripsi yaitu 1.6 detik. Tetapi pada bait pertama dengan kunci 18 dapat dilihat bahwa proses dekripsi berdurasi lebih pendek dari yang lain.

Tabel 2 Hasil Enkripsi dan Dekripsi

Bait	**Plainteks**	**K**	**Enkripsi**	**Dekripsi**
1	IA MELETAKKAN KENANGANNYA DENGAN SANGAT HATI-HATI DI LACI MEJA DAN MENGUNCINYA MEMASUKKAN ANAK KUNCI KE SAKU CELANA SEBELUM BERANGKAT KE SEBUAH KOTA YANG SUDAH SANGAT LAMA HAPUS DARI PETA YANG PERNAH DIGAMBARNYA PADA SUATU MUSIM	7	PHTLSLAHRRHU RLUHUNHUUFHKLUNHU ZHUNHAOHAPOHAPKPSHJP TLQHKHUTLUNBUJPUFH TLTHZBRRHUHUHRRBUJPRL ZHRBJLSHUHZLILSBT ILYHUNRHARLZLIBHORVAH FHUNZBKHOZHUNHASHTH OHWBZKHYPWLAHFHUN WLYUHO KPNHTIHYUFH WHKH ZBHABTBZPTSHFHUNSHFHUN	IA MELETAKKAN KENANGANNYA DENGAN SANGAT HATI-HATI DI LACI MEJA DAN MENGUNCINYA MEMASUKKAN ANAK KUNCI KE SAKU CELANA SEBELUM BERANGKAT KE SEBUAH KOTA YANG SUDAH SANGAT LAMA HAPUS DARI PETA YANG PERNAH DIGAMBARNYA PADA SUATU MUSIM LAYANG-LAYANG

	LAYANG-LAYANG			
1	IA MELETAKKAN KENANGANNYA DENGAN SANGAT HATI-HATI DI LACI MEJA DAN MENGUNCINYA MEMASUKKAN ANAK KUNCI KE SAKU CELANA SEBELUM BERANGKAT KE SEBUAH KOTA YANG SUDAH SANGAT LAMA HAPUS DARI PETA YANG PERNAH DIGAMBARNYA PADA SUATU MUSIM LAYANG-LAYANG	18	ASEWDWLSCCSFCWFSFYS FFQSVWFYSFKSFYSLZSLAZSL AVADSUAEWBSVSFEWFYM FUAFQSEWESKMCCSFSFSC CMFUACWKSCMUWDSFSK WTWDMETWJSFYCSLCWKW TMSZCGLSQSFYKMVSZKSF YSLDSESZSHMKVSJAHWLSQ SFYHWJFSZVAYSETSJFQSHSV SKMSLMEMKAEDSQSFYDS QSFY	IA MELETAKKAN KENANGANNYA DENGAN SANGAT HATI-HATI DI LACI MEJA DAN MENGUNCINYA MEMASUKKAN ANAK KUNCI KE SAKU CELANA SEBELUM BERANGKAT KE SEBUAH KOTA YANG SUDAH SANGAT LAMA HAPUS DARI PETA YANG PERNAH DIGAMBARNYA PADA SUATU MUSIM LAYANG-LAYANG
2	TAK DIDENGARNYA LAGI SUARA AIR MULAI MENDIDIH DI LACI YANG RAPAT TERKUNCI	7	AHRKPKLUNHYUFHSHNP ZBHYHHPYTBSHPTLUKPKPO KPSHJPFHUNYHWHA ALYRBUJP	TAK DIDENGARNYA LAGI SUARA AIR MULAI MENDIDIH DI LACI YANG RAPAT TERKUNCI
2	TAK DIDENGARNYA LAGI SUARA AIR MULAI MENDIDIH DI LACI YANG RAPAT TERKUNCI	18	LSCVAVWFYSJFQSDSYA KMSJSSAJEMDSAEWFVAVAZ VADSUAQSFYJSHSLLWJCMFUA	TAK DIDENGARNYA LAGI SUARA AIR MULAI MENDIDIH DI LACI YANG RAPAT TERKUNCI

3	IA TELAH MELETAKKAN HIDUPNYA DI ANTARA TANDA PETIK	7	PHALSHOTLSLAHRRHU OPKBWUFHKPHUAHYH AHUKH WLAPR	IA TELAH MELETAKKAN HIDUPNYA DI ANTARA TANDA PETIK
3	IA TELAH MELETAKKAN HIDUPNYA DI ANTARA TANDA PETIK	18	ASLWDSZEWDWLSCCSF ZAVMHFQSV SFLSJSLSFVS HWLAC	IA TELAH MELETAKKAN HIDUPNYA DI ANTARA TANDA PETIK

Sama seperti tabel 1 diberikan keterangan berupa hasil yang sudah ada. Pad tabel 2 ini berisi hasil enkripsi yang sudah dilakukan dengan kunci yang berbeda yakni K=7 dan K=18. Hasil enkripsi yang didapat antara K=7 dan 18 memiliki hasil yang berbeda tergantung dengan pergeseran K yang sudah ditentukan. Yang mana berarti hasil enkripsi yang dilakukan sesuai dengan K yang ditentukan.

Kesimpulan

Penelitian ini menganalisis performa algoritma kriptografi Caesar Cipher untuk menjaga keamanan data pada sebuah puisi berjudul "Kenangan". Penelitian ini dilakukan dengan mengimplementasikan algoritma Caesar Cipher pada bahasa pemrograman Python dan menggunakan metode penelitian studi literatur dengan metode eksperimen. Penggunaan algoritma Caesar Cipher masih sangat berguna terhadap eksperimen yang lebih praktis terhadap informasi yang memadai. Waktu deskripsi lebih lama dibandingkan dengan waktu enskripsi.

Hasil penelitian menunjukkan bahwa algoritma Caesar Cipher dapat digunakan untuk menjaga keamanan data pada teks puisi dengan baik, dengan waktu eksekusi yang relatif cepat dan efisien. Namun, algoritma ini kurang efektif dalam mengamankan data pada teks yang panjang atau mengalami serangan brute force. Algoritma ini masih cukup efektif untuk digunakan pada teks dengan ukuran yang relatif kecil seperti sebuah puisi. Namun juga perlu diketahui bahwa penelitian ini terdapat beberapa batasan yang perlu diperhatikan. Pertama, penelitian ini hanya menggunakan satu teknik kriptografi, yaitu Caesar Cipher. Ada banyak teknik kriptografi lain yang dapat digunakan untuk menjaga keamanan data. Kedua, penelitian ini hanya dilakukan pada teks puisi yang memiliki ukuran yang relatif kecil. Penelitian selanjutnya dapat dilakukan pada teks dengan ukuran yang lebih besar untuk menguji performa algoritma Caesar Cipher dengan lebih baik.

Sehingga dapat diambil kesimpulan dari penelitian ini bahwa, algoritma Caesar Cipher dapat digunakan untuk menjaga keamanan data pada teks puisi dengan baik dan efisien, meskipun memiliki beberapa batasan. Algoritma ini dapat diimplementasikan dengan mudah menggunakan bahasa pemrograman Python. Saran untuk penelitian selanjutnya adalah dapat melibatkan teknik kriptografi lain dan menggunakan teks dengan ukuran yang lebih besar untuk menguji performa algoritma dengan lebih baik. Kemudian perlu adanya kombinasi teknik kriptografi klasik dengan modern dan pemakaian kunci berlapis supaya informasi yang dikirim lebih aman dan terjamin kerahasiannya.

Ucapan Terima Kasih

Segala puji dan syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa. Karena berkat, rahmat dan karunia serta mukjizat-Nya, sehingga penulis dapat menyelesaikan jurnal ini. Penulis menyadari betul bahwa ada orang-orang yang berjasa dibalik selesainya jurnal ini. Penulis mengucapkan terimakasih kepada Bapak Muhlis Tahir, S.pd, M.Tr.Kom selaku dosen yang telah sabar dan meluangkan waktu dalam memberikan pendampingan selama proses penulisan jurnal ini. Akhir kata, penulis berharap semoga jurnal ini dapat bermanfaat bagi semua pihak dan semoga amal baik yang telah diberikan mendapatkan balasan dari Tuhan.

Referensi

Nasution, A. B. (2019). *Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher Dan Transposisi Cipher*.

Pamungkas, P. G., & Muhammad, A. H. (2022). Modifikasi Algoritma Kriptografi Caesar Chiper pada Deretan Simbol dan Huruf di Smarphone dan Laptop. *Journal of Information Technology*, *2*(1), 1–5. https://doi.org/10.46229/jifotech.v2i1.234

Purnamasari, D., Dewi, A. K., & Trisetiyanto, A. N. (2019). Analisis Performansi Kriptografi Berbasis Caesar Cipher Untuk Keamanan Data Menggunakan Python Pada Tembang Macapat. *Information Technology*.

Rinaldi, R. (2022). *Analisis Keamanan Modifikasi Metode Caesar Chiper Dalam Teknik Enkripsi Dan Deskripsi*.

Saputra, W., Efendi, N. P., & Kusuma, J. F. (2023). *Pengamanan Aplikasi Pesan Dengan Algoritma Caesar Chiper Dan Affine*.