



Analisis Performansi Kriptografi Berbasis Caesar Cipher Untuk Keamanan Data Menggunakan Python Pada Tembang Macapat

Dewi Purnamasari¹, Astric Kusuma Dewi², Adi Nova Trisetiyanto¹

¹Fakultas Sains dan Teknologi, Universitas IVET, Indonesia

²Politeknik Energi dan Mineral Akamigas, Indonesia

DOI:

Info Articles

Sejarah Artikel:

Disubmit 20 Februari 2022

Direvisi

Disetujui

Keywords:

Kriptografi; Caesar Cipher;

Key; Plaintext; Chiphertext.

Abstrak

Kriptografi tidak hanya menyediakan alat untuk keamanan informasi tetapi juga merupakan teknik yang berguna untuk kemananan dan kerahasiaan informasi. Implementasi kriptografi pada tembang macapat belum pernah dilakukan. Pada penelitian ini bertujuan mengimplementasikan algoritma *Caesar Cipher* untuk mengetahui proses penyandian dan juga untuk mengetahui efektifitas waktu enkripsi dan deskripsi dari teknik kriptografi tersebut. Waktu proses kedua metode tersebut menunjukkan bahwa waktu deskripsi lebih lama dibandingkan proses enkripsi. Waktu rata-rata enkripsi *Caesar Cipher* adalah 0.0003077 detik dan waktu deskripsi adalah 0.0003927 detik. Pada *Caesar Cipher* jika plain text data teks di tambah maka waktu enkripsi juga membutuhkan waktu yang lama. Tembang macapat Sinom merupakan tembang macapat yang membutuhkan waktu enkripsi dan deskripsi terlama, sedangkan tembang macapat Pocung dan Kinanti mempunyai waktu enkripsi dan deskripsi tercepat karena mempunyai karakter terpendek.

Abstract

Cryptography not only provides a tool for information security but is also a useful technique for the security and confidentiality of information. The implementation of cryptography on the macapat song has never been done. This study aims to implement the Caesar Cipher algorithm to determine the encoding process and also to determine the effectiveness of the encryption time and description of the two cryptographic techniques. The processing time of the two methods shows that the description time is longer than the encryption process. Caesar Cipher's average encryption time is 0.0003077 seconds and decryption time is 0.0003927 seconds. In Caesar Cipher if plain text data is added, the encryption time also takes a long time. The macapat song of Sinom is the macapat song that requires the longest encryption and description time, while the Pocung and Kinanti macapat songs have the fastest encryption and description time, because have tesks karakter shottest.

✉ Alamat Korespondensi:

E-mail: dewi.poernamasari.09@gmail.com

p-ISSN 2721-8341

e-ISSN XXX-XXXX

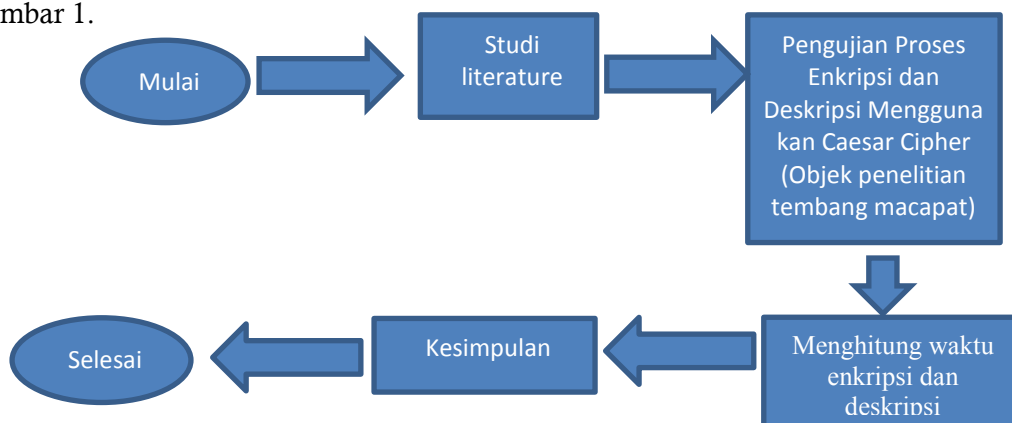
PENDAHULUAN

Indonesia merupakan negara yang tengah memasuki Era 5.0 yang merupakan era dimana teknologi berkembang sangat pesat sehingga mempengaruhi berbagai aspek kehidupan meliputi aspek sosial, budaya, ekonomi dan bisnis. Aspek budaya ini berkaitan dengan kebudayaan dan adat istiadat. Pembahasan tentang perlunya perlindungan bagi kebudayaan telah menjadi isu penting dewasa ini, hal ini disebabkan karena maraknya klaim terhadap kebudayaan-kebudayaan Indonesia yang diklaim kepemilikannya oleh negara asing akhir-akhir ini. Isu mengenai perlindungan terhadap kebudayaan Indonesia mulai menjadi “panas” kurang lebih dalam beberapa tahun terakhir, ketika persoalan tuduhan klaim atas tari Reog Ponorogo dan Pendet oleh Malaysia, dipublikasikan secara luas di media massa [1]. Kebudayaan itu sendiri dapat didefinisikan sebagai hasil karya, rasa, dan cipta masyarakat. Namun saat ini dengan masuknya budaya asing ke Indonesia sebagai akibat derasnya arus globalisasi sedikit banyak mengancam eksistensi kebudayaan daerah di Indonesia. Pengaruh tersebut berjalan sangat cepat dan berdampak sangat luas pada sistem budaya masyarakat. Adapun dampak yang ditimbulkan dengan adanya globalisasi budaya ini, dapat berupa dampak positif maupun dampak negatif. Untuk mencegah terjadinya pencurian keamanan informasi terhadap budaya bisa diujikan dengan kriptografi. Tujuan kriptografi adalah melindungi data atau informasi dari ancaman baik yang disengaja maupun tidak disengaja dari oknum yang tidak bertanggung jawab. Ada banyak sekali jenis kriptografi yang dikenal saat ini salah satunya adalah kriptografi klasik. Kriptografi klasik memiliki metode diantaranya *Caesar Cipher*.

Beberapa penelitian terdahulu yang relevan dengan yang dilakukan oleh penulis antara lain seperti algoritma *Caesar Cipher* menggunakan Matlab yang diterapkan bertujuan untuk mengetahui proses enkripsi dan deskripsi [2]. Enas Ismael Imran dan Farah Abdulameerabdul kareem pada penelitiannya tentang peningkatan *Caesar Cipher* untuk keamanan lebih baik menunjukkan bahwa *Caesar Cipher* menjadi salah satu algoritma untuk mengenkripsi yang paling sederhana dan banyak teknik yang dapat digunakan untuk memperkuat bahkan melebihi apa yang dicapai algoritma *Caesar Cipher* [3]. Penelitian Rindi dkk meneliti Caesar Cipher untuk keamanan data teks, data berupa kata pendek dengan Bahasa pemrograman Delphi. Dewi Purnamasari penelitian sebelumnya pengujian tidak menggunakan subjek tembang macapat dan berupa data teks pendek $k=3$ dan $k=4$ [4]. Pada penelitian ini menggunakan macam macam tembang macapat berupa lirik teks : Sinom, Pocung, Pangkur, Kinanti sebagai objek penelitian dan menggunakan pemrograman Python dengan menggunakan kunci sama yaitu $k=3$ dan $k=4$.

METODE

Penelitian yang dilakukan merupakan penelitian yang bersifat studi literatur dan metode eksperimen *Caesar Cipher*. Adapun alur penelitian yang digunakan dapat dilihat pada Gambar 1.



Gambar 1. Alur Penelitian

Tahapan penelitian yang dilakukan adalah:

1. Studi Literature

Pada tahap ini dilakukan peninjauan terhadap buku, artikel jurnal maupun hasil penelitian terdahulu sebagai referensi yang diperlukan dalam melakukan penelitian. Ini dilakukan untuk memperoleh informasi terkait dengan operasi *Caesar Cipher* serta pemrograman Python yang digunakan untuk pemrograman menguji enkripsi dan deskripsi.

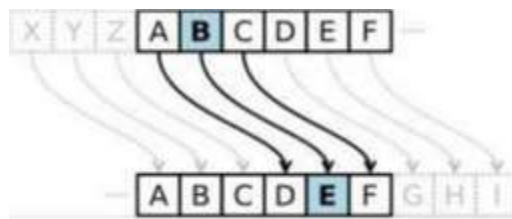
2. Proses Enkripsi dan Deskripsi

menggunakan dua algoritma dengan menggunakan $K=3$ dan $K=4$.

Enkripsi adalah proses menyembunyi sebuah data pesan, dengan cara mengubah plaintext menjadi ciphertext. Dekripsi merupakan kebalikan dari enkripsi, yang berarti bertujuan untuk memahami pesan yang ada agar dapat dibaca oleh user dengan baik.

Caesar Cipher

Metode penyandian dalam kriptografi klasik yang paling terkenal adalah *Caesar Cipher*. Teknik kriptografi ini merupakan kriptografi yang paling sederhana dan banyak digunakan diaman setiap huruf pada plainteksnya digantikan dengan huruf lain dengan pergeseran sebanyak nilai kunci [5-6]. Dalam penelitian ini nilai kunci dari *Caesar Cipher* adalah 3 dan 4. Untuk proses pergeseran karakter di *Caesar Cipher* dapat dilihat pada Gambar 2.



Gambar 2. Proses Pergeseran dalam *Caesar*

3. Menghitung waktu enkripsi dan deskripsi dengan Python adalah dengan mengurangi waktu berhenti proses dikurangi dengan waktu mulai proses
4. Evaluasi hasil pengujian dengan mengimplementasikan dan membandingkan hasil kebenaran metode *Caesar Cipher* dan juga membanding waktu proses enkripsi dan deskripsi.

HASIL DAN PEMBAHASAN

Pada proses ini akan dilakukan pengujian dengan 2 sampel plainteks tembang macapat dengan kunci yang berbeda $K1=3$ dan $K2=4$, tujuannya adalah untuk membandingkan efektivitas waktu yang digunakan masing masing teknik kriptografi tersebut. Hasil pengujian pada Tabel 1 menunjukkan waktu eksekusi enkripsi dan deskripsi pada tembang macapat Sinom, Pocung, Pangkur dan Kinanti dengan menggunakan kunci 3 dan 4. Pada Tabel 2 menunjukkan hasil enkripsi dan deskripsi pada tembang macapat Pocung dan Pangkur.

Hasil pengujian enkripsi dan deskripsi ini dapat dilihat pada Tabel 1 dan Tabel 2 berikut ini:

Tabel 1. Enkripsi dan Deskripsi *Caesar Cipher*

PLAIN TEXT	KEY	TIME (detik)	TIME (detik)
Sinom (30 word)	3	0.000252	0.000297
Sinom (30 word)	4	0.000439	0.000448
Pocung, (19 word)	3	0.000237	0.000257
Pocung (19 word)	4	0.000271	0.000230
Pangkur (28 word)	3	0.000307	0.000324
Pangkur (28 word)	4	0.000470	0.001104
Kinanti (20 word)	3	0.000235	0.000269
Kinanti (20 word)	4	0.000251	0.000277

Tabel 1 pada *Plaintext* Tembang macapat Pocung dengan Key 3 dan Key 4 menggunakan algoritma *Caesar Cipher* menunjukkan bahwa waktu enkripsi lebih cepat dibanding deskripsi. Proses enkripsi menunjukkan bahwa semakin kunci ditambah dari $K=3$ ke $K=4$ maka waktu eksekusi enkripsi menjadi semakin lama. Begitu juga sama halnya di waktu eksekusi deskripsi. Waktu terlama enkripsi dan deskripsi dapat dilihat pada tembang Sinom karena karakternya semakin panjang pada *plaintext* terdiri dari 30 data teks pada kunci 4 dari waktu enkripsi 0,000439 detik sedangkan deskripsi waktu eksekusi menjadi 0,000448 detik. Waktu terpendek adalah tembang Pocung dan Kinanti. Rata rata waktu enkripsi adalah 0,0003077 detik. Sedangkan waktu deskripsi adalah 0,0003927 detik. Hal ini menunjukkan bahwa waktu deskripsi lebih lama dibandingkan waktu enkripsi.

Tabel 2. Enkripsi dan Deskripsi *Caesar Cipher*

TEMBANG	PLAIN TEXT	K	ENKRIPSI	DESKRIPSI
POCUNG	BAPAK PUCUNG DUDU WATU DUDU GUNUNG SANGKAMU IN SABRANG NGON INGONE SANG BUPATI YEN LUMAMPAH SI PUCUNG LAMBEHAN GRANA	3	EDSDNcSXFQJcGXGXcZDWXcGX GXcJXQXQJcVDQJNDPXcLQcVDE UDQJcQJRQcLQJRQcVDQJcEXSD WLcaHQcOXPDPSDKcVLcSXFQJc ODPEHKDQcJUDQD	BAPAK PUCUNG DUDU WATU DUDU GUNUNG SANGKAMU IN SABRANG NGON INGONE SANG BUPATI YEN LUMAMPAH SI PUCUNG LAMBEHAN GRANA
POCUNG	BAPAK PUCUNG DUDU WATU DUDU GUNUNG SANGKAMU IN SABRANG NGON INGONE SANG BUPATI YEN LUMAMPAH SI PUCUNG LAMBEHAN GRANA	4	FETEodTYGYRkdHYHYdBEXYdHY HBdKYRYRkdWERKOEQYdMRdW EFVERKdRKSrdMRKSrdWERKdF YTEXMdbIRdPYQEQTeldWMDTYG YRkdPEQFILERdKVERE	BAPAK PUCUNG DUDU WATU DUDU GUNUNG SANGKAMU IN SABRANG NGON INGONE SANG BUPATI YEN LUMAMPAH SI PUCUNG LAMBEHAN GRANA
PANGKUR	SEKAR PANGKUR KANG WINARNA LELABUHAN KANG KANGGO WONG AURIP ALA LAN BECIK PUNIKU PRAYOGA KAWRUHANA ADAT WATON PUNIKU DIPUN	3	VHNDUcSDQJNXUcNDQJcZLQDUQ DcOHODEXKQDcNDQJcNDQJcZR QJcDXULScDODcODQcEHFLNcSXQ LNxcSUDaRJDcNDZUXKQDcDGD WcZWRQcSXQLNxcGLSXQcNDG XOXcPLZDcLQJNDQJcWDWDcNUD PdGcHQcNHHVWLcVLaDQJcUDW UL	SEKAR PANGKUR KANG WINARNA LELABUHAN KANG KANGGO WONG AURIP ALA LAN BECIK PUNIKU PRAYOGA KAWRUHANA ADAT WATON PUNIKU DIPUN KADULU MIWA

	KADULU MIWA INGKANG TATA KRAMA DEN KEESTI SIYANG RATRI			INGKANG TATA KRAMA DEN KEESTI SIYANG RATRI
PANGKUR	SEKAR PANGKUR KANG WINARNA LELABUHAN KANG KANGGO WONG AURIP ALA LAN BECIK PUNIKU PRAYOGA KAWRUHANA ADAT WATON PUNIKU DIPUN KADULU MIWA INGKANG TATA KRAMA DEN KEESTI SIYANG RATRI	4	WIOEVdTERKOYVdOERKd MREVREdPIPEFYLERdOERKdOERK KSdSRKdEYVMTdEPEDPERdFIGMO dTYRMOYdTVebSKEdOEBVYLERE dEHEXdEXSRdTYRMOYdHMTYRd OEHYPYdQMEdMRKOERKdXEXEd OVEQEHIRdOIIWXMdWMbERKdV EXVM	SEKAR PANGKUR KANG WINARNA LELABUHAN KANG KANGGO WONG AURIP ALA LAN BECIK PUNIKU PRAYOGA KAWRUHANA ADAT WATON PUNIKU DIPUN KADULU MIWA INGKANG TATA KRAMA DEN KEESTI SIYANG RATRI

Tabel 2 menunjukkan hasil dari empat tembang macapat melalui proses *Caesar Cipher*, didapatkan hasil enkripsi dan deskripsi. Hasil enkripsi merupakan berupa pesan yang tidak bisa dibaca. Sedangkan proses deskripsi dengan metode *Caesar Cipher* terbukti bahwa pesan yang tidak bisa dibaca tadi di enkripsi menjadi pesan yang dapat dibaca dan pesan dikirim Kembali seperti pesan awal dikirim.

SIMPULAN

Kesimpulan dari penelitian ini masih sebatas proses penerapan enkripsi dan deskripsi terhadap *plaintext* yang digunakan, dengan adanya keterbatasan dalam pengujian yang lebih efektif. Penggunaan algoritma *Caesar Cipher* masih sangat berguna terhadap eksperimen yang lebih praktis terhadap informasi yang memadai. Waktu eksekusi *Caesar Cipher* dengan kunci $k=3$ dan $k=4$ bervariasi. Waktu deskripsi lebih lama dibandingkan dengan waktu enkripsi. Saran untuk penelitian selanjutnya adalah perlu adanya kombinasi teknik kriptografi klasik dengan modern dan pemakaian kunci berlapis supaya informasi yang dikirim lebih aman dan terjamin kerahasiannya.

DAFTAR PUSTAKA

- [1] Dyah Permata. Perlindungan Hukum Terhadap Kebudayaan Melalui World Heritage Centre UNESCO. *Journal Hukum Lus Quia Lustum*. 25 (2), 256-275.
- [2] J. Singhand S.S. Yadav. 2014. Implementation of Caesar Cipher and Chaotic Neural Network by using MATLAB Simulator. *International Journal of Recent development in Engineering and Technology*. 2 (6), 2347-6435.
- [3] P. E. Ismael Imran and P. F. Abdulameerabdulkareem. 2014. Enhancement Caesar Cipher for Better Security *IOSR J. Comput. Eng.* 16 (3), 01-05.
- [4] D. Purnamasari. 2021. Implementasi Algoritma Kriptografi Caesar Cipher dan Rail Fence Cipher Untuk Keamanan Data Teks Menggunakan Python. *Joined*. Vol. 4 (1), 1-7
- [5] Y. Dwi Putri, R. Rosihan, and S. Lutfi, 2019. Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance. *JIKO (Jurnal Inform. dan Komputer)*. 2 (2). 97-94.
- [6] S. Y. Wulandari. 2020. Cryptography: A Combination of Caesar and Affine Cipher to Conceal the Message. *PROC. INTERNAT. CONF. SCI. ENGIN.* 3 (1), 741-744.
- [7] Priyono. 2016. Penerapan Algoritma Caesar Cipher Dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks. *Jurnal Riset Komputer (JURIKOM)*, 3(5), 351-356.
- [8] Latifah, R., Ambo, S. N., & Kurnia, S. I. 2017. MODIFIKASI ALGORITMA CAESAR CHIPER DAN RAIL FENCE UNTUK PENINGKATAN KEAMANAN TEKS ALFANUMERIK DAN KARAKTER KHUSUS. *Seminar Nasional Sains dan Teknologi*. Jakarta: Universitas Muhammadiyah Jakarta.