JOINED JOURNAL
JOURNAL OF INFORMATICS EDUCATION

Analisis Performansi Kriptografi Berbasis Algoritma *Caesar Cipher* dan *Rail Fence Cipher* pada Tembang Macapat

Dewi Purnamasari[1], Henny Prasetyani[2]

Prodi Pendidikan Informatika, Fakultas Sains dan Teknologi, Universitas IVET, Indonesia

Info Articles

Keywords:
Caesar Cipher, Rail Fence Cipher, Key, ziq zaq, Plaintext, Chipertext

Abstrak

Penerapan kriptografi pada asset budaya sangat perlu dilakukan, karena banyaknya klaim budaya Indonesia oleh negara asing. Oleh karena itu penelitian ini menggunakan tembang macapat Sinom, Pangkur, Pocung, Kinanti. Pada penelitian ini membandingkan algoritma *Caesar Cipher* dan *Rail Fence Cipher* untuk mengetahui proses penyandian dan efektifitas waktu enkripsi dan deskripsi. Waktu proses menunjukkan waktu deskripsi lebih lama dibandingkan enkripsi. Waktu rata-rata enkripsi algoritma *Rail Fence Cipher* lebih cepat yaitu adalah 0.000254 detik dibandingkan dengan *Caesar*. Waktu rata-rata enkripsi *Rail Fence Cipher* adalah 0.000254 detik dan waktu deskripsi adalah 0.000475 detik. Waktu enkripsi terpendek Pocung dan Kinanti. *Rail Fence* lebih aman dibanding *Caesar Cipher*.

Abstract

The application of cryptography on cultural assets is very necessary, because of the many claims of Indonesian culture by foreign countries. Therefore, this study uses the songs macapat Sinom, Pangkur, Pocung, Kinanti. This study aims to compare the Caesar Cipher and Rail Fence Cipher algorithms to determine the encoding process and the effectiveness of encryption and decryption time. The processing time of the two methods shows a longer description time than encryption. The average execution time of the Rail fence Cipher algorithm is faster than Caesar Cipher. The average Rail Fence Cipher encryption time is 0.000254 seconds and the description time is 0.000475 seconds. The shortest encryption times are Pocung and Kinanti. Rail Fence is safer more than Caesar Cipher

✉ Alamat Korespondensi:
E-mail: dewi.poernamasari.09@gmail.com

p-ISSN 2621-9484
e-ISSN 2620-8415

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 kebudayaaan 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 pihak ke 3 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* dan *Rail Fence Cipher.*

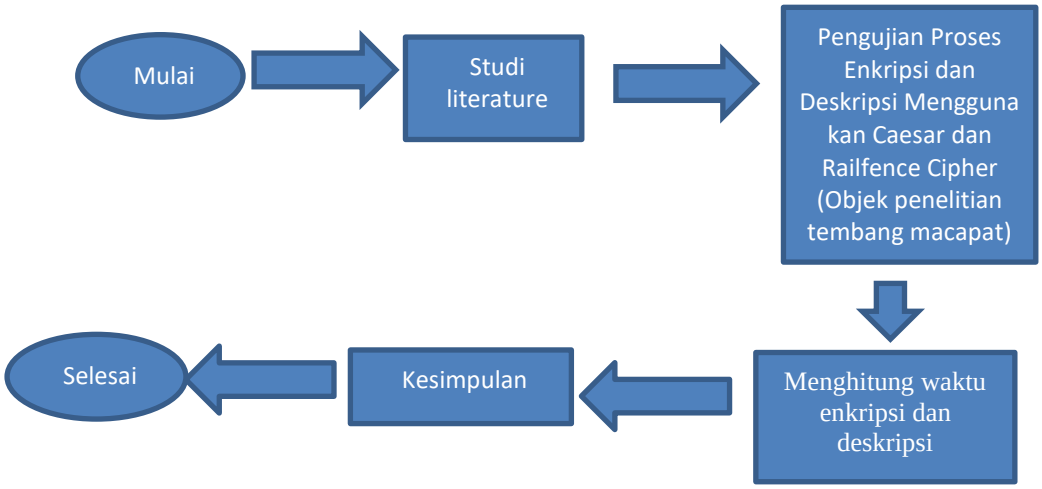
Beberapa penelitian terdahulu yang relevan dengan yang dilakukan oleh penulis antara lain seperti algoritma *Caesar Cipher* menggunakan Matlab yang diterapkan bertujuan untuk mengetahui proses enkripsi dan deskripsi [2]. Enas Ismael Imran dan Farah Abdulameerabdul kareem pada penelitiannya tentang peningkataan *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. Menurut penelitian Kusumaningtyas membahas tentang Analisa Algoritma *Ciphers Transposition*: Studi Litearure, hasil penelitiannya menunjukkan bahwa Algoritma *Rail Fence Cipher* mempunyai kelebihan dalam kerumitan cipherteks yang dihasilkan [4]. Dela Febriani dalam penelitiannya menggunakan *Rail Fence Cipher* dan subjek penelitian menggunakan android dan merupakan data teks bukan tembang macapat [5]. Dewi Purnamasari dalam penelitian sebelumnya menggunakan metode *Caesar Cipher* dan *Rail Fence Cipher* dengan pengujian tidak menggunakan objek peneliti tembang macapat dan berupa data teks pendek k=3 dan k=4 [6]. Dewi Purnamasari dalam penelitiam berikutnya menggunakan objek tembang macapat dengan menerapkan algoritma Caesar Cipher dengan kunci yang sama k=3 dan k=4 [7].

Berdasarkan latar belakang masalah yang ada, yang membedakan penelitian ini dengan penelitian sebelumnya adalah penelitian ini menggunakan macam-macam tembang macapat berupa lirik teks: Sinom, Pocung, Pangkur, dan Kinanti sebagai objek penelitian dan menggunakan pemrograman Python dengan menggunakan kunci sama yaitu k=3 dan k=4 dan algoritma kriptografi yang digunakan adalah membandingkan performansi algoritma *Caesar Cipher* dan *Rail Fence Cipher* sedangkan pada penelitian sebelumnya hanya menggunakan Caesar Cipher dan subjek pada tembang macapat.

Penelitian ini bertujuan untuk membandingkan implementasi dan efektivitas waktu enkripsi dan diskripsi untuk metode *Caesar Cipher* dan *Rail Fence Cipher* yang digunakan untuk keamanan data teks pada tembang macapat dengan kunci yang sama yaitu k=3 dan k=4

METODE

Penelitian yang dilakukan merupakan penelitian yang bersifat studi literatur dan metode eksperimen pengujian menggunakan Algoritma Kriptografi berbasis *Caesar Cipher* dan *Railfence Cipher*. Bahasa Pemrograman yang digunakan menggunakan Python. Penelitian dilakukan adalah untuk melindungi asset keamanan budaya tembang macapat. Adapun alur penelitian yang digunakan dapat dilihat pada Gambar 1.



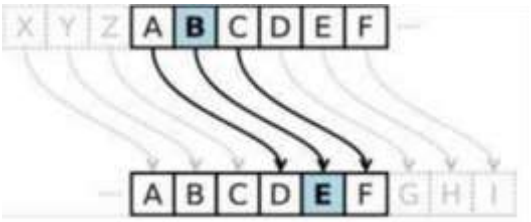
Gambar 1. Alur Penelitian

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*, dan *Rail fence Cipher* serta pemrograman Python yang digunakan untuk pemrograman menguji enkripsi dan deskripsi.
2. Proses Enkripsi dan Deskripsi menggunakan dua algoritma *Caesar Cipher*, dan *Railfence Cipher* dengan menggunakan K=3 dan K=4.

Caesar Cipher

Metode penyandian dalam kriptografi klasik yang paling terkenal adalah *Caesar Cipher*. Teknik kriptografi ini merupakan kriptografi yang paling sedrhana dan banyak digunakan diaman setiap huruf pada plainteksnya digantikan dengan huruf lain dengan pergeseran sebanyak nilai kunci [8-9]. 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 Cipher*

Contoh:
Plaintext : Universitas Ivet
Kunci : 3
Ciphertext : qlyhuvlwdvcLyhw

Rail Fence Cipher

Merupakan salah satu algoritma *cipher transposisi* yang mengacak urutan huruf-huruf pesan. Algoritma ini melibatkan penulisan *plainteks* ke bawah secara berturut turut yang memiliki baris atas dan baris bawah. Sedangkan *ciphertext* nya diperoleh dengan membaca hutruf berdasarkan baris. Algoritma *Rail Fence Cipher* menyusun plainteks secara *ziq-zag* dengan turun kebawah dan naik keatas sesuai ukuran kolom dan baris yang ditentukan oleh *key* [10].

Contoh:

*Plaintex*t : Universitas Ivet
Kunci : 3
Ciphertext: UetInvria vtisse

U				e				t					v		
	n		v		r		i		a		I			e	
		i				s				s					t

Gambar 3. *Zig Za*g Kriptografi *Rail Fence* [6]

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

HASIL DAN PEMBAHASAN

Pada proses ini akan dilakukan pengujian dengan 4 sampel plainteks tembang macapat: Sinom, Pocung, Pangkur dan Kinanti dengan kunci yang berbeda K1=3 dan K2=4. Tujuan dari penelitian sebelumnya adalah untuk membandingkan efektivitas waktu yang digunakan masing masing teknik kriptografi *Caesar Cipher* pada masing masing tembang macapat dimana mempunyai data teks panjang, sedangkan pada penelitian *Caesar Cipher* dan *Rail Fence Cipher* sebelumnya menggunakan data relative pendek karena bukan pada tembang macapat yang berebntuk lirik.

Hasil pengujian pada Tabel 1 menunjukan waktu eksekusi enkripsi dan deskripsi pada tembang macapat Sinom, Pocung, Pangkur dan Kinanti dengan menggunakan kunci 3 dan 4 dengan Kriptografi *Caesar Cipher* [7]. Masing masing tembang macapat mempunyai Panjang karakter yang berbeda beda. Tembang Sinom mmepunyai Panjang karakter 30 word, tembang Pocung mempunyai 19 word, tembangPangkur mempunyai panjang kaarkter 28 word dan tembang Kinanti 20 word.

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	0.00104
Kinanti (20 word)	3	0.000235	0.000269
Kinanti (20 word)	4	0.000251	0.000277

Pada 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 enskripsi.

Hasil pengujian pada Tabel 2 menunjukan waktu eksekusi enkripsi dan deskripsi pada tembang macapat Sinom, Pocung, Pangkur dan Kinanti dengan menggunakan kunci 3 dan 4 dengan Kriptografi *Rail Fence Cipher*.

Tabel 2. Enkripsi dan Deskripsi *Rail Fence Cipher*

PLAIN TEXT	**KEY**	***TIME*** **(detik)**	***TIME*** **(detik)**
Sinom (30 word)	3	0.000242	0.000317
Sinom (30 word)	4	0.000412	0.000590
Pocung, (19 word)	3	0.000192	0.000258
Pocung (19 word)	4	0.000280	0.000281
Pangkur (28 word)	3	0.000240	0.000506
Pangkur (28 word)	4	0.000347	0.00136
Kinanti (20 word)	3	0.000158	0.000293
Kinanti (20 word)	4	0.000206	0.000259

Pada Tabel 2 pada *Plaintext* Tembang macapat Pocung dengan Key 3 dan Key 4 menggunakan algoritma *Rail Fence 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 0,000412 detik sedangkan deskripsi waktu eksekusi menjadi 0,000590 detik. Waktu terpendek adalah tembang Pocung dan Kinanti. Rata rata waktu enkripsi adalah 0,000254 detik. Sedangkan waktu deskripsi adalah 0,000475 detik. Hal ini menunjukkan bahwa waktu deskripsi lebih lama dibandingkan waktu enskripsi.

Gambar 4. Pengujian enkripsi pada tembang pocung k=4

Gambar 5. Pengujian deskripsi pada tembang pocung k=4

Pada Gambar 4 dan 5 menunjukkan contoh pengujian *Rail fence Cipher* dengan Bahasa pemrogramana Python digunakan untuk mengetahui waktu ekeskusi proses dan hasil enkripsi dan deskripsi. Waktu eksekusi didapatkan dari *time stop* dikurangkan dengan *time start*. Perintah ini mempunyai arti adalah waktu berhenti proses dikurangi waktu ketika proses dimulai dimana waktu mulai memasukkan *plaintext* dan kunci. Pada masing masing metode kriptografi mempunyai algoritma sendiri sendiri contoh *Caesar Cipher* dengan menggeser huruf berdasarkan kunci yang dipakai, sedangkan prinsip kerja *Rail fence Cipher* menggunakan kunci angka dengan susunan teks tidak digeser melainkan berbentuk *ziq zag*. Oleh karena itu dari segi keamanan *Rail fence Cipher* lebih aman dibandingkan *Caesar Cipher*.

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 dan Rail Fence* masih sangat berguna terhadap eksperimen yang lebih praktis terhadap informasi yang memadai. Waktu eksekusi *Rail Fence* pada tembang macapat lebih cepat dibanding *Caesar Cipher*. Sedangkan waktu rata rata deskripsi *Rail Fence Cipher* lebih lama dibanding *Caesar Cipher*. Meskipun demikian tingkat keamanan *Rail Fence Cipher* lebih aman dari *Caesar Cipher*. Hal ini berbeda jika menggunakan data teks pendek bukan data teks yang berbentuk lirik. Saran untuk penelitian selanjutnya adalah perlu adanya kombinasi teknik kriptografi klasik dengan modern dan pemakaian kunci yang berlapis supaya data tidak dapat dicuri oleh kriptanalis.

DAFTAR PUSTAKA

Dyah Permata. Perlindungan Hukum Terhadap Kebudayaan Melalui World Herritage Centre UNESCO. Journal Hukum Lus Quia Lustum. 25 (2), 256-275

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.

P. E. Ismael Imran and P. F. abdulameerabdulkareem. 2014. Enhancement Caesar Cipher for Better Security IOSR J.Comput.Eng.16 (3), 01-05.

J. A. Kusumaningtyas.2018. Analisa Algoritma Ciphers Transposition: Study Literature. Multimatrix.1 (1), 1-12.

D.Febriani. 2020. Penerapan Algoritma Rail Fence Untuk Penghasil Pesan Rahasia Berbasis Android. *JurTI (Teknologi Informasi)*.1 (1). 745-755.

D.Purnamasari. 2021. Implementasi Algoritma Kriptografi Caesar Cipher dan Rail Fence Cipher Untuk Keamanan Data Teks Menggunakan Python. Joined.Vol.4 (1), 1-7

D.Purnamasari. 2021. Analisis Performansi Kriptografi Berbasis Caesar Cipher Untuk Keamanan Data Menggunakan Python Pada Tembang Macapat. J-SITE (Journal of System, Information Technology, and Electronic Engineering.Vol.1(2), 50-54

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.

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.

Nardiati. D.G. 2019. Kombinasi Algoritma Kriptografi Transposisi rail Fence Cipher dan Route Cipher. *Prosiding Seminar Nasional Teknologi Informatika*. Politeknik Negeri Medan: Teknik Informatika.

Retnani latifah, Sitti nurbaya ambo, Syafitri indah kurnia. 2017. Modifikasi Algoritma Caesar Chiper Dan Rail Fence Untuk Peningkatan Keamanan Teks Alfanumerik Dan Karakter Khusus. ISSN: 2407-1946, Jurnal Semnastek. Jakarta

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.

Purba, D. F., & Puspasari, R. 2020. Penerapan Algoritma Rail Fence Untuk Penghasil Pesan Rahasia Berbasis Android. Jurnal Mahasiswa Fakultas Teknik dan Ilmu Komputer, 1(1), 745-756

Ratna, D. 2018. Implementasi Algoritma Rail Fence Chiper dalam Keamanan Data Gambar 2 Dimensi. Pelita Informatika: Informasi dan Informatika, 7(1).

Sembiring, N. S. B. 2018. Perancangan Aplikasi Kriptografi Dengan Metode Modifikasi Caesar Cipher Yang Diperkuat Dengan Vernam Cipher Untuk Keamanan Teks. E-JURNAL JUSITI: Jurnal Sistem Informasi dan Teknologi Informasi, 5(1), 10-17.