JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 2 Edisi Januari-April 2025, Page 1058-1065
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Analisis Performa Beaufort Cipher Dan ROT13 Dalam Proses Enkripsi Dan Dekripsi Pada Data Teks

Stephen Pratama Kurnia[1*], Serius Ndruru[2], Nicky Pascal Tambunan[3], Muhammad Hasbiallah[4], Ahmad Turmudi Zy[5]

[1,2,3,4,5]Universitas Pelita Bangsa
Email: [1]kurnia16j@gmail.com, [2]nickypascal521@gmail.com, [3]seriusndruru@mhs.pelitabangsa.ac.id, [4]hasbimuhammad273@gmail.com

Abstrak− Penelitian ini bertujuan untuk menganalisis performa algoritma Beaufort Cipher dan ROT13 dalam proses enkripsi dan dekripsi data teks digital. Kedua algoritma ini memiliki karakteristik yang berbeda, di mana Beaufort Cipher menggunakan kunci dengan panjang yang sama dengan teks, sedangkan ROT13 menggunakan pergeseran tetap sebesar 13 karakter. Metode penelitian melibatkan pengumpulan data berupa teks digital dengan ukuran yang bervariasi, yaitu 100, 1.000, 10.000, dan 100.000 karakter. Pengujian dilakukan menggunakan skrip Python untuk mengukur waktu eksekusi enkripsi dan dekripsi, dengan setiap algoritma diuji sebanyak 10 kali pada masing-masing ukuran teks. Hasil pengujian menunjukkan bahwa ROT13 memiliki waktu eksekusi yang lebih cepat dibandingkan Beaufort Cipher untuk semua ukuran teks yang diuji. Waktu eksekusi kedua algoritma menunjukkan peningkatan linear seiring dengan bertambahnya panjang teks. Penelitian ini menyimpulkan bahwa algoritma ROT13 sangat cocok untuk aplikasi sederhana yang membutuhkan efisiensi waktu, seperti penyamaran teks. Sebaliknya, Beaufort Cipher, meskipun lebih lambat, menawarkan manfaat edukasi dalam memahami prinsip enkripsi berbasis kunci. Dengan demikian, hasil penelitian ini memberikan wawasan tentang efisiensi kedua algoritma dalam konteks modern dan penggunaannya yang sesuai berdasarkan kebutuhan spesifik.

Kata Kunci: Beaufort Cipher, ROT13, Kriptografi, Enkripsi, Dekripsi

Abstract− This study aims to analyze the performance of the Beaufort Cipher and ROT13 algorithms in the encryption and decryption of digital text data. These two algorithms have distinct characteristics, with the Beaufort Cipher employing a key length equal to the text, while ROT13 uses a fixed 13-character shift. The research method involved collecting digital text data of varying sizes, namely 100, 1,000, 10,000, and 100,000 characters. The testing was conducted using Python scripts to measure encryption and decryption execution times, with each algorithm tested 10 times for each text size. The results showed that ROT13 consistently demonstrated faster execution times compared to the Beaufort Cipher across all tested text sizes. The execution times for both algorithms exhibited a linear increase with text length. This study concludes that the ROT13 algorithm is highly suitable for simple applications requiring time efficiency, such as text obfuscation. Conversely, although slower, the Beaufort Cipher provides educational value in understanding key-based encryption principles. Thus, the findings offer insights into the efficiency of both algorithms in modern contexts and their appropriate use based on specific needs.

Keywords: Beaufort Cipher, ROT13, cryptography, encryption, decryption

1. PENDAHULUAN

Dalam dunia keamanan informasi, kriptografi memainkan peran penting dalam melindungi data dari akses yang tidak sah. Algoritma substitusi klasik seperti Beaufort Cipher dan ROT13 sering menjadi fokus penelitian karena kesederhanaannya, namun efektivitas dan efisiensinya masih memerlukan evaluasi mendalam, terutama dalam konteks modern. Beaufort Cipher menggunakan tabel Vigenère untuk melakukan substitusi teks dengan pola inversi yang unik, sedangkan ROT13 menggunakan pergeseran tetap sejauh 13 langkah pada tabel ASCII.

Beaufort Cipher merupakan salah satu algoritma substitusi klasik yang menggunakan tabel Vigenère untuk melakukan enkripsi dan dekripsi. Cipher Beaufort ditemukan oleh Sir Francis Beaufort, Angkatan Laut Kerajaan Inggris, yang juga merupakan pencipta skala Beaufort, yang merupakan alat yang digunakan oleh ahli meteorologi untuk menunjukkan kecepatan angin (Pertiwi, Fauzi dan Syahputra, 2023)[1]. Perbedaan dalam metode ini adalah peran kunci, dalam cipher Vigenere digunakan sebagai penambahan pada teks asli dan pengurangan pada teks sandi. Teknik ini dikenal dengan pola inversinya, di mana operasi substitusi dilakukan dengan cara membalikkan penggunaan kunci dibandingkan dengan metode Vigenère standar (Pertiwi, Fauzi dan Syahputra, 2023)[1]. Di sisi lain, Rot 13 adalah algoritma sederhana yang umum digunakan dalam sistem operasi UNIX yang menggunakan kode Caesar dengan pergeseran k = 13 (Risman, 2021)[2]. Proses enkripsi menggunakan Algoritma Rot13 menggeser karakter sejauh 13 langkah ke depan alphabet 13 (Risman, 2021)[2]. ROT13 dirancang untuk keamanan pada sistem operasi UNIX yang sering digunakan di forum daring, yang berfungsi untuk menyamarkan konten artikel sehingga hanya orang yang berwenang yang dapat membacanya 13 (Risman, 2021)[2].

Penelitian sebelumnya seperti yang dilakukan oleh Pertiwi et al. (2023) telah memanfaatkan Beaufort Cipher dan ROT13 dalam pengamanan citra digital, sedangkan Risman (2021) membandingkan kinerja ROT13 dengan algoritma Caesar Cipher pada basis data. Namun, sedikit penelitian yang secara eksplisit menganalisis

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/12/2024**; Accepted **15/01/2024;** Published: **18/01/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 2 Edisi Januari-April 2025, Page 1058-1065
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

perbandingan efisiensi kedua algoritma ini dalam konteks enkripsi dan dekripsi teks dengan ukuran yang bervariasi. Penelitian yang ada lebih fokus pada keamanan daripada efisiensi waktu eksekusi. Hal ini menunjukkan adanya kesenjangan penelitian dalam memahami efisiensi kedua algoritma untuk data teks sederhana dengan ukuran besar.

Tujuan dari penelitian ini adalah untuk menganalisis dan membandingkan kinerja Beaufort Cipher dan ROT13 berdasarkan waktu eksekusi enkripsi dan dekripsi. Penelitian ini berkontribusi pada literatur dengan memberikan wawasan baru tentang efisiensi kedua algoritma dan rekomendasi penggunaannya dalam aplikasi modern, terutama yang memerlukan keseimbangan antara kecepatan dan kebutuhan keamanan sederhana. Evaluasi performa terhadap kedua algoritma ini menjadi menarik untuk dipelajari, mengingat perbedaan kompleksitas operasionalnya. Dengan memahami efisiensi masing-masing metode, kita dapat mengidentifikasi potensi penggunaan serta keterbatasan dari algoritma-algoritma ini dalam konteks modern.

Pada tulisan ini, evaluasi sederhana dilakukan dengan membandingkan waktu pemrosesan algoritma. Hasil evaluasi diharapkan memberikan wawasan yang bermanfaat bagi para pembelajar dan penggiat kriptografi klasik

2. METODOLOGI PENELITIAN

Penelitian ini bertujuan untuk membandingkan performa algoritma Beaufort Cipher dan ROT13 dalam proses enkripsi dan dekripsi berdasarkan kecepatan eksekusi. Adapun langkah-langkah penelitian yang dilakukan adalah sebagai berikut:

2.1 Pengumpulan Data

Data yang digunakan adalah teks digital dengan berbagai ukuran sebagai input. Teks akan diproses dalam bentuk string.

2.2 Analisa dan Perbandingan dengan Penelitian Sebelumnya

Hasil penelitian ini dibandingkan dengan penelitian sebelumnya, seperti yang dilakukan oleh Pertiwi et al. (2023), yang memanfaatkan Beaufort Cipher dan ROT13 untuk pengamanan citra digital. Dalam penelitian tersebut, efisiensi kedua algoritma tidak menjadi fokus utama, melainkan aspek keamanan data. Sementara itu, Risman (2021) membandingkan ROT13 dengan Caesar Cipher pada basis data, namun hanya untuk aplikasi spesifik tanpa mengevaluasi performa algoritma pada teks dengan ukuran besar.

2.3 Implementasi Algoritma

Implementasi algoritma Beaufort Cipher dan ROT13 menggunakan bahasa pemrograman Python.

a. Beaufort Cipher: Algoritma ini akan diterapkan dengan kunci yang panjangnya sama dengan panjang teks. Proses enkripsi dilakukan dengan formula $C_i = (K_i - P_i) \bmod 256$, sedangkan dekripsi menggunakan formula $P_i = (K_i - C_i) \bmod 256$, di mana P adalah plaintext, C adalah ciphertext, dan K adalah kunci.
b. ROT13: Algoritma ini akan menggantikan setiap karakter teks atau nilai RGB dengan karakter atau nilai yang berjarak 13 langkah sesuai dengan tabel ASCII untuk enkripsi. Dekripsi dilakukan dengan cara yang sama karena ROT13 bersifat reversibel.

Formula enkripsi dan dekripsi untuk masing – masing algoritma:

a. Beaufort Cipher: Enkripsi $C_i = (K_i – P_i) \bmod 256$, Dekripsi $P_i = (K_i – C_i) \bmod 256$
b. ROT13. Enkripsi: Menggeser karakter sejauh 13 langkah kedepan, Dekripsi: Menggeser karakter sejauh 13 langkah ke belakang.

2.4 Pengujian Performa

Dilakukan pengujian terhadap waktu eksekusi enkripsi dan dekripsi menggunakan perangkat keras dan perangkat lunak yang sama untuk kedua algoritma. Ukuran data yang diuji adalah teks dengan panjang 100, 1.000, 10.000, dan 100.000 karakter.

2.5 Pengukuran Waktu Eksekusi

Waktu eksekusi dihitung menggunakan fungsi pengukur waktu sistem (misalnya yang akan digunakan dalam penelitian ini adalah time pada Python). Setiap algoritma dieksekusi sebanyak 10 kali untuk setiap ukuran data, dan rata-rata waktu eksekusi dicatat sebagai hasil.

2.6 Analisis Data

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/12/2024**; Accepted **15/01/2024;** Published: **18/01/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 2 Edisi Januari-April 2025, Page 1058-1065
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Data hasil pengukuran waktu diekspresikan dalam satuan milidetik (ms). Perbandingan dilakukan berdasarkan kecepatan rata – rata enkripsi dan dekripsi dari masing – masing algoritma untuk setiap ukuran data.

2.7 Alat dan Lingkungan Pengujian

a. Bahasa Pemrograman: Python versi 3.8 atau lebih baru.
b. Perangkat keras: Prosesor Intel Core i3 12100f atau setara, RAM 16GB.
c. Perangkat Lunak: Sistem operasi Windows, pustaka tambahan seperti NumPy untuk pengolahan matriks.

3. HASIL DAN PEMBAHASAN

Pengujian dilakukan untuk mengukur waktu eksekusi algoritma Beaufort Cipher dan ROT13 pada teks dengan panjang 100, 1.000, 10.000, dan 100.000 karakter. Hasil menunjukkan bahwa ROT13 secara konsisten memiliki waktu eksekusi yang lebih cepat dibandingkan Beaufort Cipher pada semua ukuran teks. Rata-rata waktu eksekusi ROT13 meningkat secara linear terhadap panjang teks, sedangkan Beaufort Cipher, meskipun lebih lambat, juga menunjukkan peningkatan linear.

Untuk mendukung analisis performa algoritma Beaufort Cipher dan ROT13, pengujian dilakukan dengan menggunakan skrip Python yang dirancang untuk mengukur waktu eksekusi enkripsi dan dekripsi. Skrip ini memanfaatkan pustaka standar Python seperti time untuk mencatat durasi proses dengan akurasi tinggi. Data teks dengan berbagai panjang digunakan sebagai input, sedangkan hasil rata-rata waktu eksekusi diolah untuk setiap algoritma.

3.1 Implementasi kode algoritma dengan Python.

Gambar berikut menunjukan implementasi kode Python yang digunakan dalam pengujian. Skrip ini mengatur proses pengukuran waktu untuk masing – masing algoritma secara sistematis, meliputi fungsi enkripsi, dekripsi dan penghitugan rata – rata waktu eksekusi.

Gambar 1. Kode Implementasi Algoritma Beaufot Cipher

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/12/2024**; Accepted **15/01/2024;** Published: **18/01/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 2 Edisi Januari-April 2025, Page 1058-1065
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Gambar 2. Kode Implementasi Algoritma ROT13

Penelitian ini dilakukan untuk membandingkan kecepatan eksekusi enkripsi dan dekripsi antara algoritma Beaufort Cipher dan ROT13. Data uji yang digunakan berupa teks sepanjang 100, 1.000, 10.000, dan 100.000 karakter. Setiap pengujian dilakukan sebanyak 10 kali, dan rata – rata waktu eksekusi dicatat sebagai hasil.

3.2 Hasil Implementasi

Tabel 1. Tabel Rata – Rata Waktu Eksekusi Enkripsi dan Dekripsi

Panjang Teks (Karakter	**Beaufort Cipher (Enkripsi)**	**Beaufort Cipher (Dekripsi)**	**ROT13 (Enkripsi)**	**ROT13 (Dekripsi)**
100	0 ms	0 ms	0.1 ms	0 ms
1.000	0.1 ms	0.4 ms	0.3 ms	0.3 ms
10.000	1.2 ms	1.1 ms	0.7 ms	1 ms
100.000	12.5 ms	11.1 ms	8.1 ms	8 ms

Dari hasil pengujian yang ditunjukan pada Tabel 1, dapat dilihat bahwa algoritma ROT13 memiliki waktu eksekusi yang lebih cepat dibandingkan dengan Beaufort Cipher, baik pada proses enkripsi dan dekripsi.

Performa ROT13

a. ROT13 Memiliki keunggulan dalam hal waktu eksekusi karena algoritmanya sederhana dan hanya melibatkan operasi pergeseran karakter sebesar 13 langkah.
b. Waktu eksekusi ROT13 menunjkan peningkatkan yang linear terhadapt panjang teks, yang mengindikasikan efisensi tinggi pada data berukuran besar.

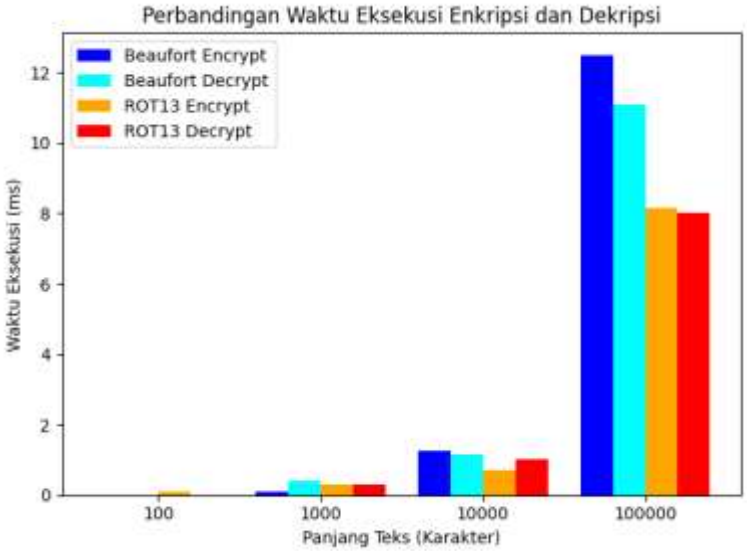
Performa Beaufort Cipher

a. Beaufort Cipher memiliki waktu eksekusi yang lebih lambat dibandingkan ROT13 karena algoritmanya melibatkan operasi aritmatika modular dengan kunci yang perlu diulang sepanjang teks.
b. Meskipun lebih lambat, waktu eksekusi Beaufort Cipher juga menunjukan peningkatan linear terhadap panjang teks.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/12/2024**; Accepted **15/01/2024;** Published: **18/01/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 2 Edisi Januari-April 2025, Page 1058-1065
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin



Gambar 3. Grafik Perbandingan Waktu Eksekusi Enkripsi dan Dekripsi

Perbandingan dengan Penelitian Sebelumnya

Hasil penelitian ini dibandingkan dengan beberapa studi sebelumnya:

a. **Pertiwi et al. (2023):** Penelitian mereka menggunakan Beaufort Cipher dan ROT13 untuk pengamanan citra digital. Fokus utamanya adalah pada aspek keamanan algoritma, bukan efisiensi waktu eksekusi. Penelitian ini memperluas cakupan dengan mengevaluasi performa algoritma pada teks digital, memberikan wawasan baru mengenai kecepatan eksekusi kedua algoritma pada berbagai ukuran data.
b. **Risman (2021):** Penelitian ini membandingkan ROT13 dengan Caesar Cipher untuk basis data, menunjukkan efisiensi ROT13 dalam tugas penyamaran data. Namun, penelitian Risman hanya mencakup data dalam konteks spesifik dan tidak mengevaluasi panjang teks secara mendalam. Penelitian ini melengkapi studi Risman dengan menyajikan analisis performa ROT13 dan Beaufort Cipher dalam berbagai skenario ukuran teks.
c. **Rachmawati & Lubis (2023):** Penelitian mereka menggabungkan Beaufort Cipher dengan algoritma RSA-CRT untuk keamanan data citra digital. Penelitian ini berfokus pada performa tunggal Beaufort Cipher tanpa membandingkannya dengan algoritma lain. Sebaliknya, penelitian ini mengeksplorasi perbedaan performa dua algoritma klasik secara langsung.

Keterbatasan Algoritma dan Penelitian

Meskipun algoritma Beaufort Cipher dan ROT13 menunjukkan performa yang cukup baik dalam proses enkripsi dan dekripsi data teks sederhana, ada beberapa keterbatasan yang perlu dicatat:

a. Keterbatasan Algoritma

1) **Beaufort Cipher**: Algoritma ini memerlukan kunci yang panjangnya sama dengan teks yang akan dienkripsi. Hal ini menjadi kurang praktis untuk implementasi dalam skala besar atau pada data dengan ukuran yang sangat besar, mengingat kompleksitas pengelolaan dan penyimpanan kunci. Selain itu, sifat algoritma ini sebagai cipher substitusi klasik menjadikannya rentan terhadap analisis kriptografi modern, seperti analisis frekuensi.
2) **ROT13**: Kesederhanaan ROT13 merupakan kelemahan signifikan dalam konteks keamanan. Algoritma ini dirancang bukan untuk keamanan tingkat tinggi melainkan untuk menyamarkan teks sederhana. Dengan hanya menggunakan pergeseran karakter sejauh 13 langkah, ROT13 dapat dengan mudah dipecahkan tanpa memerlukan kunci atau pengetahuan kriptografi yang mendalam.

b. Keterbatasan Penelitian

1) **Skala Data**: Penelitian ini hanya menguji data berupa teks dengan panjang karakter terbatas hingga 100.000 karakter. Pada data dengan ukuran lebih besar atau tipe data yang berbeda, seperti file biner atau citra digital, hasil performa kedua algoritma mungkin berbeda.
2) **Lingkungan Pengujian**: Pengujian dilakukan menggunakan perangkat keras dan perangkat lunak yang spesifik. Oleh karena itu, hasil yang diperoleh dapat bervariasi jika diterapkan pada konfigurasi perangkat keras atau sistem operasi lain.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/12/2024**; Accepted **15/01/2024;** Published: **18/01/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 2 Edisi Januari-April 2025, Page 1058-1065
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

3) **Aspek Keamanan**: Penelitian ini tidak mengevaluasi tingkat keamanan algoritma secara mendalam, seperti seberapa kuat algoritma ini terhadap serangan tertentu (misalnya brute force atau known plaintext attack). Studi lebih lanjut diperlukan untuk menguji keandalan algoritma dalam konteks keamanan.

Keterbatasan ini menunjukkan bahwa, meskipun algoritma Beaufort Cipher dan ROT13 memiliki keunggulan dalam kecepatan eksekusi (khususnya ROT13), penggunaannya sebaiknya dibatasi pada skenario yang sesuai dengan karakteristik dan kekuatan masing-masing algoritma. Penelitian di masa depan dapat difokuskan pada mengatasi kelemahan-kelemahan ini, seperti memodifikasi algoritma agar lebih efisien dan aman dalam konteks data modern.

Relevansi Algoritma Beaufort Cipher dan ROT13 Dalam Konteks Modern

Algoritma Beaufort Cipher dan ROT13, meskipun dikategorikan sebagai algoritma kriptografi klasik, masih memiliki relevansi tertentu dalam konteks modern, khususnya dalam pendidikan dan simulasi keamanan informasi. Kedua algoritma ini dapat digunakan untuk memberikan pemahaman mendasar kepada mahasiswa atau pemula dalam bidang kriptografi tentang prinsip dasar enkripsi dan dekripsi.

Relevansi Algoritma Beaufort Cipher dan ROT13 Dalam Konteks Modern

Algoritma Beaufort Cipher dan ROT13, meskipun dikategorikan sebagai algoritma kriptografi klasik, masih memiliki relevansi tertentu dalam konteks modern, khususnya dalam pendidikan dan simulasi keamanan informasi. Kedua algoritma ini dapat digunakan untuk memberikan pemahaman mendasar kepada mahasiswa atau pemula dalam bidang kriptografi tentang prinsip dasar enkripsi dan dekripsi.

1. **Pendidikan dan Pembelajaran Kriptografi**.
   Beaufort Cipher dapat digunakan untuk mengajarkan konsep operasi modular dan penggunaan kunci dalam proses enkripsi. Sifatnya yang melibatkan tabel substitusi memungkinkan siswa memahami dasar-dasar cipher substitusi serta peran penting kunci dalam menjaga keamanan. Di sisi lain, ROT13 dengan kesederhanaannya dapat menjadi titik awal untuk memperkenalkan algoritma kriptografi tanpa memerlukan pemahaman matematika yang kompleks. Hal ini menjadikannya alat yang ideal untuk pembelajaran pada tingkat dasar.
2. **Pengolahan Data Sederhana.**
   ROT13 sering digunakan dalam skenario di mana keamanan tinggi tidak menjadi prioritas, melainkan hanya untuk menyamarkan teks. Contohnya adalah dalam forum daring untuk menyembunyikan spoiler, komentar sensitif, atau konten tertentu sehingga tidak langsung terlihat oleh pembaca. Penggunaan ini menunjukkan bahwa ROT13 tetap relevan di era modern untuk aplikasi praktis dalam komunikasi digital.
3. **Simulasi Keamanan Informasi.**
   Beaufort Cipher dapat digunakan dalam simulasi keamanan informasi untuk menunjukkan bagaimana algoritma klasik berfungsi dan mengapa pendekatan modern diperlukan. Sebagai contoh, simulasi dapat dilakukan untuk menunjukkan bagaimana cipher ini rentan terhadap analisis frekuensi dan mengapa algoritma yang lebih kompleks seperti Advanced Encryption Standard (AES) lebih andal dalam melindungi data.

Perbandingan Penggunaan dalam Konteks Modern

1. **Kecepatan vs. Kompleksitas**: ROT13 unggul dalam kecepatan karena sifatnya yang sederhana, menjadikannya lebih cocok untuk aplikasi ringan seperti penyamaran teks. Sebaliknya, Beaufort Cipher, meskipun lebih lambat, menawarkan pemahaman mendalam tentang penggunaan kunci yang dapat diaplikasikan dalam kriptografi yang lebih kompleks.
2. **Keamanan**: Dalam hal keamanan, kedua algoritma ini tidak dirancang untuk menangkal ancaman modern. Namun, Beaufort Cipher memberikan pandangan mendalam tentang pentingnya kunci yang kuat dan pengaruhnya terhadap proses enkripsi, yang relevan untuk pengembangan algoritma yang lebih aman.

Relevansi ini menegaskan bahwa algoritma Beaufort Cipher dan ROT13, meskipun sederhana, memiliki peran penting dalam pembelajaran, pengolahan data sederhana, dan simulasi, menjadikannya alat yang masih berguna di era modern.

4. KESIMPULAN

Penelitian ini mengevaluasi performa algoritma Beaufort Cipher dan ROT13 dalam proses enkripsi dan dekripsi berdasarkan waktu eksekusi. Hasil penelitian menunjukkan bahwa:

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/12/2024**; Accepted **15/01/2024;** Published: **18/01/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 2 Edisi Januari-April 2025, Page 1058-1065
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

1. **ROT13** memiliki waktu eksekusi yang lebih cepat dibandingkan Beaufort Cipher pada semua ukuran teks yang diuji (100, 1.000, 10.000, dan 100.000 karakter). Waktu eksekusi algoritma ini menunjukkan peningkatan linear terhadap panjang teks, dengan rata-rata waktu eksekusi sebesar 0,1 ms untuk teks 100 karakter hingga 8,1 ms untuk teks 100.000 karakter dalam proses enkripsi.
2. **Beaufort Cipher**, meskipun lebih lambat dibandingkan ROT13, juga menunjukkan peningkatan waktu eksekusi yang linear terhadap panjang teks. Waktu eksekusi rata-rata pada teks dengan panjang 100 karakter adalah 0,0 ms untuk enkripsi dan mencapai 12,5 ms pada teks 100.000 karakter. Data ini menunjukkan bahwa Beaufort Cipher, meskipun kurang efisien dalam hal kecepatan, tetap dapat diandalkan untuk aplikasi dengan ukuran data besar.

Simpulan ini didukung oleh analisis data rata-rata waktu eksekusi dari pengujian 10 kali untuk setiap ukuran teks. Berdasarkan hasil ini, penelitian ini memberikan kontribusi sebagai berikut:

1. ROT13 lebih cocok untuk aplikasi sederhana seperti penyamaran teks dalam forum daring atau komunikasi ringan, di mana efisiensi waktu menjadi prioritas.
2. Beaufort Cipher, dengan karakteristiknya yang lebih kompleks, memiliki relevansi dalam pendidikan dan simulasi konsep enkripsi berbasis substitusi, memberikan pemahaman mendalam tentang penggunaan kunci dalam kriptografi.

Kesimpulan ini melengkapi penelitian sebelumnya seperti Pertiwi et al. (2023) dan Risman (2021), yang lebih menekankan aspek keamanan daripada efisiensi algoritma. Dengan demikian, penelitian ini memberikan wawasan baru yang menjembatani kesenjangan antara efisiensi dan keamanan algoritma kriptografi klasik.

Untuk penelitian selanjutnya, disarankan untuk mengevaluasi performa algoritma ini pada jenis data yang lebih kompleks, seperti citra digital atau file biner, serta mengembangkan algoritma baru yang menggabungkan kecepatan ROT13 dengan kompleksitas Beaufort Cipher.

UCAPAN TERIMAKASIH

Terima kasih kepada kawan-kawan yang telah berkontribusi dalam penelitian ini, yaitu Stephen Pratama Kurnia, Serius Ndruru, Nicky Pascal Tambunan, dan Muhammad Hasbiallah, atas kerjasama dan dedikasi mereka selama proses penelitian. Kami juga menyampaikan rasa hormat dan terima kasih kepada Bapak Ahmad Turmudi Zy, selaku dosen pengampu mata kuliah Kriptografi, atas bimbingan dan arahannya yang berharga selama penelitian ini berlangsung

REFERENCES

[1] A. D. Pertiwi, A. Fauzi, and S. Syahputra, "Application Of Super Encryption Using Rot 13 Algorithm Method and Algorithm Beaufort Cipher For Image Security Digital," Journal of Artificial Intelligence and Engineering Applications, vol. 2, no. 3, pp. 84-92, Oct. 2023. doi : https://doi.org/10.59934/jaiea.v3i1.263.

[2] R. Risman, "Comparison of Performance Rot13 and Caesar Cipher Method for Registration Database of Vessels Berthed at P.T. Samudera Indonesia ", ijobas, vol. 10, no. 3, pp. 91–98, Dec. 2021. doi : https://doi.org/10.35335/ijobas.v10i3.61.

[3] D. Rachmawati and A. N. Lubis, "Combining Beaufort cipher and RSA-CRT algorithm in a hybrid scheme to secure images," Journal of Physics: Conference Series, vol. 2421, no. 1, p. 012028, 2023, doi: 10.1088/1742-6596/2421/1/012028.

[4] D. Sanjaya and K. Puspita, "Perancangan Aplikasi Validasi Keaslian Sertifikat OSMB Pada Universitas Potensi Utama Menggunakan Algoritma Beaufort", SmartAI Journal, vol. 2 No.1, pp. 31-40, Jan. 2023. Available : https://ejournal.abivasi.id/index.php/SmartAI/article/view/52.

[5] Z. A. Harahap and Nurhayati, "Kombinasi Metode Beaufort Cipher dan Diffie Hellman Untuk Kerahasiaan Isi Tabel MySQL", JID (Jurnal Info Digit), vol. 2 No. 3, pp. 1000-1013, Sept. 2024. Available : https://kti.potensi-utama.org/index.php/JID/article/view/1419.

[6] A. Abiyuda and L. Nababan, "Rancang Bangun Aplikasi Chatting dengan Wireless LAN Menggunakan Metode Beaufort Cipher", Jurnal InSeDS (Information System and Data Science), vol 1. No. 2, Dec. 2022, Available : http://repository.potensi-utama.ac.id/jspui/handle/123456789/5926.

[7] E. Ndruru and Taronisokhi Zebua, "Pembangkitan Kunci Beaufort Cipher Dengan Teknik Blum-blum Shub pada Pengamanan Citra Digital", Bulletin of Information Technology (BIT), vol. 3 No. 1. pp 149-154. June. 2022. doi : https://doi.org/10.47065/ekuitas.v3i2.1167.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/12/2024**; Accepted **15/01/2024;** Published: **18/01/2025**

[8] L. B. Handoko and C. Umam, "Data Security Using Color Image Based on Beaufort Cipher, Column Transposition and Least Significant Bit (LSB), Journal of Applied Intelligent System, vol. 8 No. 2. pp. 140-151. July. 2023. doi : https://doi.org/10.33633/jais.v8i2.7863.

[9] M. Fadlan, Suprianto, Muhammad, Y. Amaliah, "Double Layered Text Encryption using Beaufort and Hill Cipher Techniques", IEEE. Dec. 2020. doi : https://doi.org/10.1109/ICIC50835.2020.9288538.

[10] A. H. Hasugian, Y. R. Nasution and N. A. Simanjuntak, "Kombinasi Algoritma Beaufort Cipher dan LS2BIT Untuk Keamanan File Text", JIRE (Jurnal Informatika & Rekayasa Elektronika), vol. 6 No. 1. April 2023. doi : https://doi.org/10.36595/jire.v6i1.730.

[11] Mahyudi, "Implementasi Kombinasi Algoritma Beaufort Cipher dan Algoritma RSA Dalam Skema Super Enkripsi Untuk Pengamanan File Teks", Skripsi, Departemen Teknik Informatika, Universitas Islam Negri Sumatra Utara, Medan, Indoensia, 2023.

[12] C. Irawan, E. H. Rachmawanto, C. A. Sari, and C. A. Sugianto, "Super Enkripsi File Dokumen Menggunakan Beaufort Cipher dan Transposisi Kolom", LPPM – Universitas Muhammadiyah Purwokerto. 2020. Available : http://download.garuda.kemdikbud.go.id/article.php?article=3195351&val=28102&title=SUPER%20ENKRIPSI%20FILE%20DOKUMEN%20MENGGUNAKAN%20BEAUFORT%20CIPHER%20DAN%20TRANSPOSISI%20KOLOM.

[13] Y. R. Nasution, A. H. Hasugian, and Mahyudi, "Penerapan Teknik Super Enkripsi Untuk Keamanan File Teks Menggunakan Gabungan Algoritma Beaufort Cipher dan Algoritma RSA", Jurnal Penerapan Sistem Informasi (Komputer dan Manajemen), vol. 4 No. 4, Okt. 2023. Pp. 868–889. Available : https://pkm.tunasbangsa.ac.id/index.php/kesatria/article/view/238.

[14] E. Sugiarto, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, Md. K. Sarker, and B. Widjajanto, "Securing Text Messages using the Beaufort-Vigenere Hybrid Method", Journal of Physics: Conference Series, vol 1577. 2020. Doi : https://doi.org/10.1088/1742-6596/1577/1/012032.

[15] P. A. D. Kusumah, K. Kusrini, K Kusnawi, "Optimizing Data Security: A Literature Review on The Implementation of Beaufort Cipher for Vigenere Affine Cipher", International Journal of Innovative Science and Research Technology, vol. 9, issue. 2, Feb. 2024, doi : https://doi.org/10.5281/zenodo.10685974.

[16] A. Rachmadsyah, A. Perdana, and A. Budiman, "Kombinasi Algoritma Beaufort Cipher Dan Vigenere Cipher Untuk Pengamanan Pesan Teks Berbasis Mobile Application", Jurnal Minfo Polgan (Jurnal Manajemen Informatika Politeknik Ganesha), vol. 9 no. 2. Sept. 2020. Available : https://jurnal.polgan.ac.id/index.php/jmp/article/view/10943.

[17] Muhammad Ridho Utomo, "Rancangan Keamanan Informasi Pesan Teks Menggunakan Algoritma Beaufort Cipher", Skripsi, Sains dan Teknologi/Sistem Komputer, Universitas Pembangunan Panca Budi, Medan, Indonesia, 2020.

[18] T. Zebua, "Implementasi Algoritma Freivalds pada Pembangkitan Kunci Algoritma Beaufot Cipher", KETIK Jurnal Informatika, vol. 1 no. 3. Pp. 88-94. Jan. 2024. Available : https://jurnal.faatuatua.com/index.php/KETIK/article/view/51.

[19] Md. Z. Rangga, "Modifikasi Algoritma Beaufort Cipher Dengan Transposisi Grup Simetri Untuk Mengamankan Pesan", Skripsi, Program Studi Matematika, Universitas Negri Islam Maulana Malik Ibrahim, Malang, Indonesia, 2022.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/12/2024**; Accepted **15/01/2024;** Published: **18/01/2025**