Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI) **e-ISSN 2830-3954**
Volume: 4, Nomor: 1, Januari 2025: 92-99 **p-ISSN 2830-6031**
https://jurnal.unity-academy.sch.id/index.php/jirsi/index

Pengembangan Algoritma Vigenere Cipher Berbasis Kunci Dinamis Dalam Pengamanan Pesan Teks

Development of Dynamic Key Based Vigenere Cipher Algorithm in Text Message Security
Text Message Security

Munjiat Setiani Asih[1], Rismayanti[2], M Imam Fadhlurahman*[3], Ade Zulkarnain Hasibuan[4]
[1,2,3]Fakultas Teknik dan Komputer, Program Studi Informatika, Universitas Harapan Medan
[4]Fakultas Sains dan Teknologi, Program Studi Informatika, Universitas Samudra
E-mail: [1]munjiat.stth@email.ac.id, [2]risma.stth@gmail.com, [3]10imamrahman@gmail.com, [4]adezulhsb@unsam.ac.id

Abstrak

Penelitian ini bertujuan untuk mengembangkan algoritma Vigenère Cipher berbasis kunci dinamis sebagai solusi untuk meningkatkan keamanan pengiriman pesan teks. Vigenère Cipher merupakan salah satu metode kriptografi klasik yang memiliki kelemahan terhadap analisis frekuensi, terutama ketika kunci yang digunakan bersifat statis. Dalam penelitian ini, kami mengusulkan pendekatan baru dengan menerapkan kunci dinamis yang berubah setiap kali pesan dikirim. Kunci dinamis ini dihasilkan melalui algoritma pseudorandom yang mempertimbangkan waktu pengiriman dan karakteristik pesan. Metodologi penelitian meliputi analisis teori kriptografi, implementasi algoritma, serta pengujian efektivitas dan efisiensi dalam menyandi dan mendekripsi pesan. Hasil pengujian menunjukkan bahwa algoritma yang dikembangkan tidak hanya meningkatkan keamanan pesan melalui kompleksitas kunci yang lebih tinggi, tetapi juga mempertahankan kecepatan proses enkripsi dan dekripsi. Selain itu, analisis terhadap berbagai skenario pengiriman pesan menunjukkan bahwa algoritma ini mampu mengatasi serangan analisis frekuensi yang sering kali menjadi ancaman dalam metode kriptografi tradisional. Dengan hasil ini, penelitian ini memberikan kontribusi signifikan terhadap pengembangan sistem pengamanan pesan teks yang lebih aman dan praktis, serta membuka peluang untuk aplikasi lebih lanjut dalam bidang kriptografi modern.

***Kata kunci**: Vigenère Cipher, Kunci Dinamis, Pengamanan Pesan, Kriptografi.*

Abstract

This research aims to develop a dynamic key-based Vigenère Cipher algorithm as a solution to improve the security of text messaging. Vigenère Cipher is one of the classical cryptographic methods that has a weakness against frequency analysis, especially when the key used is static. In this study, we propose a new approach by implementing a dynamic key that changes every time a message is sent. This dynamic key is generated through a pseudorandom algorithm that considers the time of transmission and the characteristics of the message. The research methodology includes analyzing cryptography theory, algorithm implementation, and testing the effectiveness and efficiency in encrypting and decrypting messages. The test results show

that the developed algorithm not only improves message security through higher key complexity, but also maintains the speed of encryption and decryption processes. In addition, analysis of various message delivery scenarios shows that the algorithm is able to overcome frequency analysis attacks that are often a threat in traditional cryptographic methods. With these results, this research makes a significant contribution to the development of more secure and practical text message security systems, and opens up opportunities for further applications in the field of modern cryptography.

***Keywords**: Vigenère Cipher, Dynamic Key, Message Security, Cryptography.*

1. PENDAHULUAN

Dalam era informasi digital yang berkembang pesat, keamanan data dan informasi telah menjadi salah satu prioritas utama. Seiring dengan meningkatnya ketergantungan kita pada teknologi, risiko terhadap integritas dan kerahasiaan informasi semakin besar. Dalam konteks ini, enkripsi data merupakan salah satu metode utama untuk melindungi informasi dari akses yang tidak sah. Vigenere cipher adalah salah satu metode enkripsi klasik yang telah digunakan sejak abad ke-16 [1][2]. Vigenere cipher merupakan salah satu teknik kriptografi, kriptografi adalah ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data, autentikasi entitas dan autentikasi keaslian data [3][4]. Kriptografi dibagi menjadi dua jenis yaitu kriptografi simetris dan kriptografi asimetris. Kriptografi simetris adalah algoritma kriptografi yang menggunakan kunci yang sama untuk proses enkrips dan proses dekripsinya[5]. Sedangkan kriptografi asimetris adalah kriptografi yang menggunakan dua buah kunci berbeda yang digunakan saat enkripsi dan dekripsi. Satu kunci disebrkan ke publik dan satu kunci bersifat privat [6]. Algoritma ini termasuk dalam kategori cipher polialfabetik, yang menggunakan kunci untuk mengenkripsi teks dengan menggantikan setiap huruf dari teks asli dengan huruf yang berbeda sesuai dengan kunci yang digunakan. Meskipun telah terbukti efektif pada masanya, Vigenère Cipher menghadapi berbagai tantangan dalam hal keamanan, terutama ketika kunci yang digunakan tetap dan tidak berubah selama proses enkripsi. Kriptografi memiliki beberapa tujuan antara lain untuk kerahasiaan data, integritas data, autentikasi, dan non-repudiasi [7]. Kriptografi memiliki dua konsep utama, yaitu enkripsi (*encryption*) dan dekripsi (*decryption*). Enkripsi adalah proses penyandian plainteks menjadi cipherteks, sedangkan dekripsi adalah proses mengembalikan cipherteks menjadi plainteks semula. Enkripsi dan dekripsi membutuhkan kunci sebagai parameter yang digunakan untuk transformasi [8][9].

Salah satu kelemahan utama dari algoritma Vigenère Cipher konvensional adalah ketergantungan pada kunci yang tetap dan cenderung mudah ditebak. Serangan frekuensi dan teknik kriptanalisis lainnya dapat mengeksploitasi kelemahan ini untuk mengungkapkan kunci dan, pada akhirnya, teks asli. Dalam konteks keamanan modern, di mana ancaman semakin canggih dan kompleks, metode enkripsi yang mengandalkan kunci tetap tidak lagi memadai. Untuk mengatasi

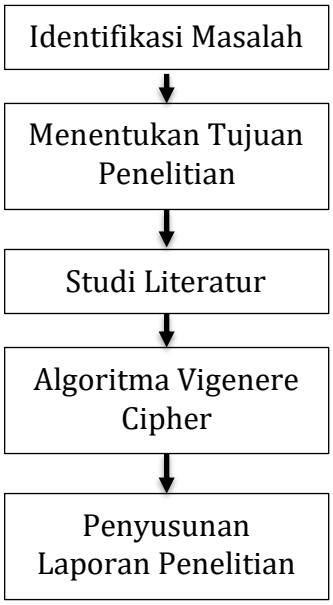
kelemahan ini, konsep kunci dinamis muncul sebagai solusi potensial. Kunci dinamis adalah metode di mana kunci enkripsi diperbarui secara berkala selama proses enkripsi atau berdasarkan aturan tertentu. Dengan menggunakan kunci dinamis, tingkat keamanan dapat ditingkatkan karena kunci yang digunakan untuk setiap bagian dari teks dapat berubah, membuatnya jauh lebih sulit untuk dipecahkan oleh pihak yang tidak berwenang.

Implementasi kunci dinamis pada algoritma Vigenère Cipher berpotensi membawa perbaikan signifikan dalam hal keamanan. Metode ini dapat memanfaatkan algoritma tambahan untuk menghasilkan kunci secara dinamis berdasarkan parameter tertentu, sehingga mengurangi risiko pengungkapan kunci dan informasi. Selain itu, pengembangan ini dapat memberikan wawasan baru tentang bagaimana algoritma klasik dapat diadaptasi untuk memenuhi standar keamanan modern.

Penelitian ini bertujuan untuk mengeksplorasi penerapan kunci dinamis pada Vigenère Cipher dan mengevaluasi efektivitasnya dalam meningkatkan keamanan enkripsi teks. Dengan menganalisis dampak penggunaan kunci dinamis terhadap keamanan dan performa algoritma, penelitian ini diharapkan dapat memberikan kontribusi penting dalam pengembangan teknik enkripsi yang lebih aman dan efektif.

2. METODOLOGI PENELITIAN

Dalam membuat penelitian ini diperlukan tahapan penelitian agar penelitian terarah. Adapun tahapan penelitian dapat dilihat pada gambar 1 berikut.



Gambar 1. Tahapan Penelitian

1. Identifikasi masalah
   Pada tahap ini, penelitia melakukan identifikasi kelemahan dari kriptografi Vigenere Cipher tradisional, terutama dalam hal keamanan dan kerentanan terhadap serangan kriptanalisis. Selanjutnya dilakukan identifikasi kebutuhan akan kunci dinamis untuk meningkatkan keamanan pesan teks.
2. Menentukan tujuan penelitian
   Penelitian ini memiliki tujuan yaitu untuk meningkatkan kemanan data dengan mengembangkan kunci dinamis dalam kriptografi Vigenere Cipher.

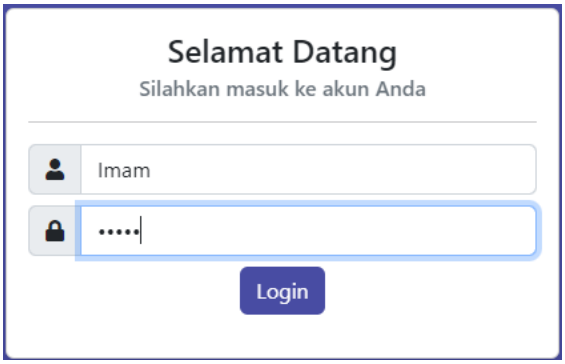
3. Studi literatur
   Tahap ini melibatkan kajian literatur yang relevan untuk memahami konsep dan teori yang berkaitan dengan metode Weighted Product dan aplikasinya dalam pengambilan keputusan. Peneliti akan meneliti penelitian sebelumnya yang membahas penyiangan buku, pengelolaan koleksi perpustakaan, serta teknik pengambilan keputusan multi-kriteria. Studi pustaka ini bertujuan untuk memberikan dasar teoritis yang kuat bagi penelitian yang akan dilakukan.
4. Algoritma vigenere cipher
   Adapun rumus metode vigenere cipher adalah sebagai berikut [10]:
   Rumus enkripsi vigenere cipher:
   $Ci = (Pi + Ki) \bmod 26$ (1)
   Ci = (Pi + Ki) – 26 kalau hasil penjumlahan Pi dan Ki lebih dari 26
   Rumus dekripsi vigenere cipher:
   $Pi = (Ci - Ki) \bmod 26$ (2)
   atau
   Pi = (Ci – Ki) + 26 kalau hasil pengurangan Ci dengan Ki minus
   Dengan:
   Ci = nilai desimal karakter ciphertext ke-i
   Pi = nilai desimal karakter plaintext ke-i
   Ki = nilai desimal karakter kunci ke-i

5. Penyusunan laporan penelitian

Pada tahap ini, peneliti menyusun laporan penelitian yang mencakup seluruh aspek penelitian, dimulai dari latar belakang, metodologi, hasil, analisis, hingga rekomendasi. Laporan ini disusun dalam format yang jelas dan sistematis, sehingga mudah dipahami oleh pembaca. Penyusunan laporan yang baik sangat penting untuk menyampaikan temuan penelitian secara efektif.

3. HASIL DAN PEMBAHASAN

Implementasi program dimulai dengan halaman login. Pada halaman login pengguna diminta untuk memasukkan username dan password yang benar. Jika username dan password pengguna benar, sistem akan melanjutkan ke halaman berikutnya. Adapun tampilan halaman login dapat dilihat pada gambar 2.

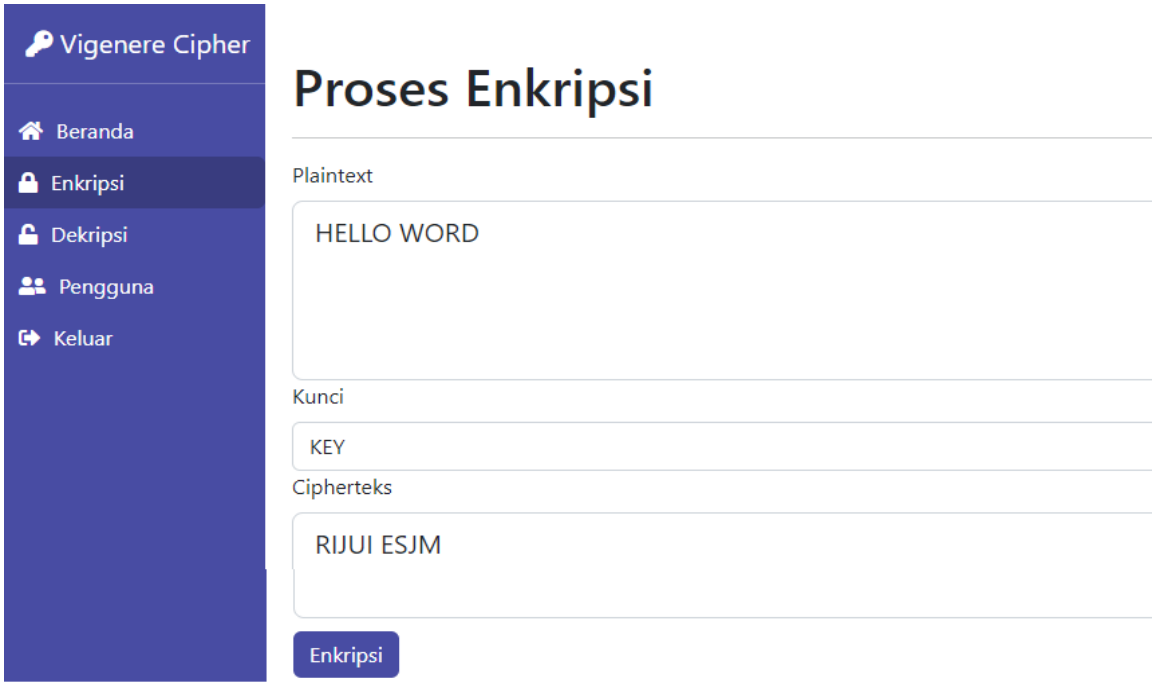


Gambar 2. Halaman Login

Jika pengguna berhasil login maka sistem akan melanjutkan ke halaman beranda. Pada halaman tersebut terlihat judul penelitian yang penulis lakukan dan identitas penulis sendiri. Pada tampilan beranda ini juga pengguna dapat melihat menu-menu yang terdapat dalam aplikasi yakni emkripsi, deskripsi, pengguna dan keluar. Adapun tampilan halaman beranda dapat dilihat pada gambar 3 berikut.

Gambar 3. Halaman Beranda

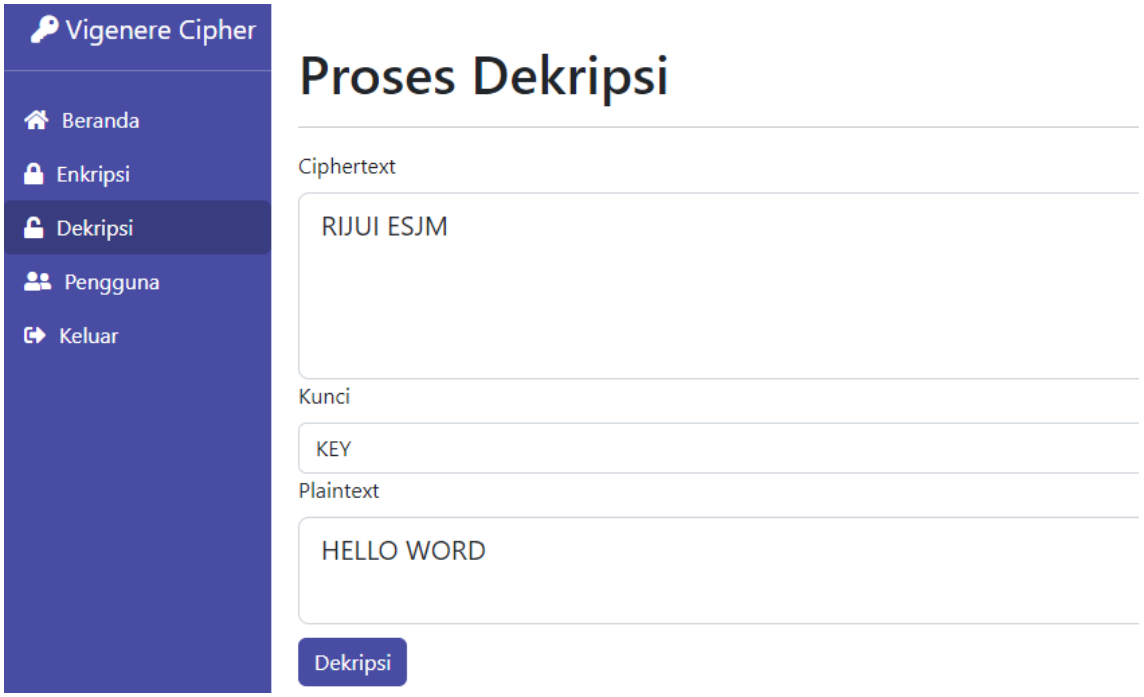
Jika pengguna mengklik menu enkripsi, sistem akan membuka halaman enkripsi. Halaman enkripsi merupakan halaman yang digunakan untuk melakukan proses pengamanan teks menggunakan vigenere cipher dengan kunci dinamis. Adapun tampilan dari halaman enkripsi dapat dilihat pada gambar 4 berikut.



Gambar 4. Halaman Enkripsi

Jika dilihat dari tampilan diatas terlihat proses ekripsi yang dilakukan dengan menginputkan plaintext "HELLO WORD" dan kunci "KEY". Hasil dari proses ini akan tampil saat diklik tombol enkripsi dan menghasilkan cipherteks "RIJUI ESJM".

Halaman selanjutnya yaitu halaman dekripsi, halaman ini digunakan untuk mengembalikan teks yang sudah dienkripsi menjadi teks asli menggunakan vigenere cipher dengan kunci dinamis. Adapun tampilan dari halaman dekripsi dapat dilihat pada gambar 5 berikut.



Gambar 5. Halaman Dekripsi

4. KESIMPULAN

Dari penelitian yang telah dilakukan dapat disimpulkan beberapa hal sebagai berikut:

1. Kesimpulan dari penelitian ini menunjukkan bahwa implementasi kunci dinamis dalam metode Vigenère Cipher secara signifikan meningkatkan keamanan pesan teks. Dengan mengubah kunci secara periodik dan berdasarkan karakteristik pesan, metode ini dapat mengurangi risiko serangan kriptanalisis. Penelitian ini menegaskan bahwa kunci dinamis merupakan langkah penting dalam memperkuat keamanan komunikasi, menjadikannya sebagai solusi yang lebih andal dalam era digital.
2. Kesimpulan dari penelitian ini juga menegaskan bahwa penerapan kunci dinamis dalam metode Vigenère Cipher secara efektif meningkatkan keamanan pesan teks. Dengan memanfaatkan kunci yang berubah-ubah, sistem ini mampu mengurangi potensi serangan kriptanalisis dan memperkuat perlindungan terhadap data sensitif. Penelitian ini menunjukkan bahwa inovasi dalam penggunaan kunci dinamis adalah kunci untuk menciptakan metode enkripsi yang lebih aman, menjawab tantangan keamanan informasi di era digital saat ini.
3. Untuk pengembangan penelitian berikutnya, kriptografi hybrid ini dapat diaplikasikan langsung ke dalam pengamanan database ataupun file untuk meningkatkan keamanan data yang disimpan.

DAFTAR PUSTAKA

[1] A. Z. Hasibuan, M. S. Asih, and H. Harahap, "Penerapan QR Code dan Vigenere Cipher Dalam Sistem Pelaporan Juru Parkir Ilegal," *QUERY*, vol. 3, no. 1, pp. 53–61, 2019, [Online]. Available:

https://jurnal.uinsu.ac.id/index.php/query/article/view/4460/2199

[2] R. R. J. Putra and I. N. Anisa, *Kriptografi Penerapan dalam Keamanan Transaksi Komersial*. Indonesia Emas Group, 2024.

[3] M. S. Dairi, M. S. Asih, and Khairunnisa, "Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan," *JIRSI*, vol. 2, no. 1, pp. 214–223, 2023, [Online]. Available: https://jurnal.unity-academy.sch.id/index.php/jirsi/article/view/44/35

[4] R. Rahman *et al.*, *Buku Ajar Keamanan Jaringan Komputer*. Jambi: PT. Sonpedia Publishing Indonesia, 2024.

[5] Z. Arif and A. Nurokhman, "Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi," *JTSI*, vol. 4, no. 2, pp. 394–405, 2023, [Online]. Available: https://jurnal.mdp.ac.id/index.php/jtsi/article/download/6077/1616

[6] K. A. Saputra and G. A. J. Saskara, "Kriptografi Simetris RC4 pada Transaksi Online Booking Engine System," *J. Teknol. dan Kejuru.*, vol. 17, no. 2, pp. 286–295, 2020, [Online]. Available: https://ejournal.undiksha.ac.id/index.php/JPTK/article/download/27096/15812/53402

[7] M. R. Andani, "Kenali Kriptografi dari Penjelasan Sampai Teknis Pengembangannya.," 19 April 2021. [Online]. Available: https://www.sekawanmedia.co.id/: https://www.sekawanmedia.co.id/blog/pengertian-kriptografi/

[8] Yusfrizal, "RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE CHIPER DAN RSA BERBASIS ANDROID," *JTIK*, vol. 3, no. 2, p. 29, 2019.

[9] A. Z. Hasibuan, "Implementasi Kriptografi Hybrid Menggunakan Caesar Cipher dan Affine Cipher Untuk Kemanan Teks," *JUREKSI*, vol. 2, no. 3, pp. 2240–2250, 2024, [Online]. Available: https://kti.potensi-utama.org/index.php/JUREKSI/article/view/2045/937

[10] A. S. E. Gunadhi, "PENGAMANAN DATA REKAM MEDIS PASIEN MENGGUNAKAN KRIPTOGRAFI VIGÈNERE CIPHER," *Algoritma*, vol. 13, no. 2, p. 295, 2016.