Jurnal Teknologi Sistem Informasi dan Aplikasi **ISSN: 2654-3788**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2654-4229**
Vol. 6, No. 3, Juli 2023 (262-268) **DOI: 10.32493/jtsi.v6i3.30118**

Kombinasi Algoritma Vigenere dan Beaufort Cipher dalam Mengamankan Script Coding

Ilham[1], Abdul Halim Hasugian[2]

[12]Ilmu Komputer, Universitas Islam Negeri Sumatera Utara, Jl. William Iskandar Ps. V, Medan Estate, Kec. Percut Sei Tuan, Kabupaten Deli Serdang, Sumatera Utara 20371
e-mail: [1]ilhamavira@gmail.com,[2] abdulhasugian12@gmail.com

Submitted Date: May 22nd, 2023 Reviewed Date: June 03rd, 2023
Revised Date: June 12th, 2023 Accepted Date: June 16th, 2023

Abstract

Cryptography has become an essential aspect in ensuring the security of information and data, especially in the context of script coding that contains secret codes that need to be kept confidential. The problem faced is securing script coding so that it cannot be accessed or modified by unauthorized parties. In this research, we propose the use of a combination of the Vigenere and Beaufort Cipher algorithms to secure script coding. The proposed method involves encrypting and decrypting script coding using both cryptographic algorithms simultaneously. The Vigenere Cipher algorithm is used to protect the integrity and confidentiality of script coding, while the Beaufort Cipher is used as an additional layer to enhance security and prevent attacks. This method is implemented and evaluated using a number of script coding samples that include sensitive secret codes. The results of the method implementation show that the combination of the Vigenere and Beaufort Cipher algorithms successfully improves the security level of script coding. Script coding encrypted using both algorithms becomes difficult to read and modify by unauthorized parties. Additionally, the encryption and decryption processes of script coding run quickly and efficiently, without impeding system performance. This research makes an important contribution to the field of information security, particularly in securing script coding. The combination of the Vigenere and Beaufort Cipher algorithms can be considered an effective solution in maintaining the confidentiality and integrity of sensitive script coding..

Keywords: Cryptography; Vigenere Algorithm; Beaufort Algorithm; Security

Abstrak

Kriptografi telah menjadi aspek penting dalam menjaga keamanan informasi dan data, terutama dalam konteks script coding yang mengandung kode-kode rahasia yang harus dijaga kerahasiaannya. Masalah yang dihadapi adalah mengamankan script coding agar tidak dapat diakses atau dimodifikasi oleh pihak yang tidak berwenang. Dalam penelitian ini, kami mengusulkan penggunaan kombinasi algoritma Vigenere dan Beaufort Cipher untuk mengamankan script coding. Metode yang diusulkan melibatkan enkripsi dan dekripsi script coding menggunakan kedua algoritma kriptografi tersebut secara bersamaan. Algoritma Vigenere Cipher digunakan untuk melindungi integritas dan kerahasiaan script coding, sementara Beaufort Cipher digunakan sebagai lapisan tambahan untuk memperkuat keamanan dan mencegah serangan. Metode ini diimplementasikan dan dievaluasi dengan menggunakan sejumlah script coding yang mencakup kode-kode rahasia yang sensitif. Hasil penerapan metode menunjukkan bahwa kombinasi algoritma Vigenere dan Beaufort Cipher berhasil meningkatkan tingkat keamanan script coding. Script coding yang dienkripsi menggunakan kedua algoritma tersebut menjadi sulit untuk dibaca dan dimodifikasi oleh pihak yang tidak berwenang. Selain itu, proses enkripsi dan dekripsi script coding berjalan dengan cepat dan efisien, sehingga tidak menghambat kinerja sistem. Penelitian ini memberikan kontribusi penting dalam bidang keamanan informasi, khususnya dalam mengamankan script coding.

Kombinasi algoritma Vigenere dan Beaufort Cipher ini dapat dijadikan sebagai solusi yang efektif dalam menjaga kerahasiaan dan integritas script coding yang sensitif.

Kata kunci: Kriptografi; Algoritma Vigenere; Algoritma Beaufort; Keamanan

1 Pendahuluan

Dalam era digital saat ini, keamanan informasi dan perlindungan data sensitif menjadi sangat penting (Maya et al., 2022). Script coding, yang berisi kode-kode rahasia yang digunakan dalam pengembangan perangkat lunak dan aplikasi, merupakan salah satu aspek yang perlu dijaga kerahasiaannya. Namun, seringkali script coding rentan terhadap serangan dan akses oleh pihak yang tidak berwenang. Oleh karena itu, penting untuk memiliki metode yang efektif dalam mengamankan script coding agar dapat melindungi integritas dan kerahasiaannya (Buulolo & Sindar, 2020).

Dalam sistem saat ini, script coding seringkali hanya dilindungi oleh penggunaan metode enkripsi sederhana atau tidak dilindungi sama sekali. Hal ini meninggalkan celah bagi pihak yang tidak berwenang untuk mengakses, membaca, atau bahkan mengubah script coding. Meskipun beberapa metode enkripsi seperti AES (Advanced Encryption Standard) digunakan, namun mereka mungkin kurang efektif dalam melindungi script coding secara khusus (Maya et al., 2022).

Masalah yang dihadapi dalam sistem saat ini adalah kurangnya tingkat keamanan yang memadai untuk melindungi script coding (Rachmadsyah et al., 2020). Script coding yang tidak dienkripsi atau hanya dilindungi oleh metode enkripsi sederhana rentan terhadap serangan dan manipulasi (Triansyah, 2019). Serangan yang berhasil dapat mengakibatkan hilangnya integritas script coding, pencurian kode rahasia, atau pengungkapan informasi sensitif yang dapat merugikan organisasi atau individu.

Untuk menyelesaikan masalah ini, kami mengusulkan penggunaan kombinasi algoritma Vigenere dan Beaufort Cipher sebagai metode yang efektif dalam mengamankan script coding. Kombinasi ini akan memperkuat tingkat keamanan script coding melalui proses enkripsi dan dekripsi yang kompleks. Algoritma Vigenere Cipher akan digunakan untuk melindungi integritas dan kerahasiaan script coding, sementara Beaufort Cipher akan memberikan lapisan tambahan keamanan (Rachmadsyah et al., 2020).

Untuk menerapkan metode ini, akan dilakukan implementasi algoritma Vigenere dan Beaufort Cipher dalam proses enkripsi dan dekripsi script coding. Script coding sensitif akan dienkripsi menggunakan kedua algoritma ini sehingga menjadi sulit untuk dibaca atau dimodifikasi oleh pihak yang tidak berwenang (Rachmadsyah et al., 2020). Selain itu, rencana pelaksanaan juga mencakup evaluasi dan pengujian terhadap tingkat keamanan, efisiensi, dan kecepatan metode ini dalam mengamankan script coding. Hasil evaluasi dan pengujian akan digunakan untuk mengukur keberhasilan metode ini dalam menyelesaikan masalah yang ada.

2 Metodologi penelitian

2.1 Analisis Data

Setelah melakukan perencanaan, langkah berikutnya adalah menganalisis kebutuhan untuk merancang aplikasi, termasuk kebutuhan perangkat lunak. Dalam pengembangan aplikasi, diperlukan perangkat keras seperti komputer atau laptop, serta lingkungan pengembangan seperti Visual Studio Code, untuk membuat aplikasi berbasis website.

2.2 Perancangan

Dalam tahap ini, digunakan kombinasi Vigenere dan Beaufort Cipher untuk meningkatkan keamanan Sript Codingan. Beberapa desain antarmuka telah disusun. Setelah menyelesaikan proses peninjauan desain aplikasi, langkah selanjutnya adalah memulai implementasi desain tersebut ke dalam kode pemrograman.

2.3 Pengujian

Di tahap ini, tengah dilakukan uji coba aplikasi menggunakan kombinasi metode kriptografi Vigenere dan Beaufort. Uji coba ini bertujuan untuk memverifikasi keamanan data secara menyeluruh dan mengatasi masalah kinerja serta operasional aplikasi. Selain itu, juga dilakukan uji coba fungsional untuk memastikan bahwa aplikasi berjalan sesuai dengan perencanaan. Uji coba ketahanan juga sangat penting untuk memastikan aplikasi dapat beroperasi dengan baik pada berbagai perangkat.

2.4 Penerapan Penggunaan

Di tahap ini, rencananya akan dilakukan penyempurnaan dan pengembangan aplikasi berdasarkan kebutuhan yang teridentifikasi selama tahap pengujian. Penyempurnaan akan dilakukan untuk mengatasi kesalahan yang terungkap selama proses pengujian. Selanjutnya, akan dilakukan pengembangan untuk meningkatkan kinerja aplikasi agar dapat memberikan manfaat maksimal dalam proses enkripsi dan dekripsi.

3 Hasil dan Pembahasan

3.1 Pembahasan

Algoritma Vigenere Cipher adalah salah satu algoritma kriptografi yang digunakan untuk mengenkripsi dan mendekripsi pesan dengan menggunakan kunci enkripsi yang terdiri dari sebuah kata atau frasa (Afandi & Nurhayati, 2021). Algoritma ini termasuk dalam jenis algoritma substitusi polyalphabetic, di mana setiap karakter dalam pesan terenkripsi dihasilkan dari beberapa karakter dalam kunci enkripsi. Algoritma ini pertama kali ditemukan oleh seorang kriptografer Prancis, Blaise de Vigenere, pada tahun 1586.

Algoritma Vigenere Cipher bekerja dengan cara mengubah setiap karakter dalam pesan menjadi karakter lain dalam alfabet, yang bergantung pada nilai karakter dalam kunci enkripsi (Setyawati1 et al., 2021). Untuk melakukan pengenkripsian pesan, setiap karakter dalam pesan diubah menjadi nilai numerik dalam alfabet. Selanjutnya, nilai numerik tersebut ditambahkan dengan nilai numerik karakter kunci enkripsi yang sesuai, dalam urutan yang sama dengan karakter pesan. Akhirnya, hasil penjumlahan tersebut dikonversi kembali menjadi karakter dalam alfabet menggunakan rumus (1) dan gambar 1 yang telah ditentukan.

$$Ci = (Pi + Ki) \bmod 26 \quad (1)$$

Huruf	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 1. Tabel Vigenere Cipher

Vigenere Cipher adalah metode enkripsi yang menggunakan karakter pada kunci secara berulang-ulang untuk mengubah setiap karakter pada plainteks. Untuk mengenkripsi pesan "hello world" dengan kunci "ilham", berikut adalah langkah-langkah yang dilakukan:

a. Atur kunci pada baris pertama, dan tuliskan plainteks pada baris di bawahnya.
b. Konversi setiap karakter alfabet pada pesan terenkripsi dan kunci ke dalam bilangan bulat antara 0 hingga 25. Misalnya, plainteks "hello world" dapat diubah menjadi bilangan bulat sebagai berikut:
   h = 7, e = 4, l = 11, l = 11, o = 14, (spasi) = 32, w = 22, o = 14, r = 17, l = 11, d = 3, i = 8, l = 11, h = 7, a = 0, m = 12.
c. Lakukan operasi enkripsi dengan menjumlahkan setiap karakter plainteks dengan karakter pada kunci, kemudian hitung hasil mod 26 dari jumlah tersebut. Rumus enkripsi Vigenere Cipher (1):
   dimana:
   Ci = karakter terenkripsi
   Pi = karakter plainteks
   Ki = karakter kunci
d. Lakukan operasi enkripsi pada setiap karakter plainteks dengan karakter pada kunci yang sesuai. Misalnya, enkripsi karakter pertama "h" dengan karakter pertama kunci "i" adalah sebagai berikut:
   Ci = (Pi + Ki) mod 26
   Ci = (7 + 8) mod 26
   Ci = 15
   Karakter terenkripsi dari "h" adalah "P".
e. Lakukan operasi yang sama pada setiap karakter plainteks dengan karakter pada kunci yang sesuai hingga seluruh pesan terenkripsi. Dengan menggunakan kunci "ilham", pesan terenkripsi dari "hello world" adalah "PNZPMBGKNT".

Untuk mendekripsi pesan yang telah dienkripsi dengan algoritma Vigenere Cipher, langkah-langkah yang dilakukan adalah kebalikan dari proses pengenkripsian (Tampubolon, 2021). Pertama-tama, setiap karakter dalam pesan terenkripsi diubah menjadi nilai numerik dalam alfabet, kemudian dikurangi dengan nilai numerik karakter kunci dekripsi yang sesuai (dalam urutan yang sama dengan karakter pesan), dan hasilnya diubah kembali menjadi karakter dalam alfabet menggunakan rumus (2):

$$Ci = (Pi - Ki) \bmod 26 \quad (2)$$

Proses dekripsi Vigenere Cipher dilakukan dengan mengubah setiap karakter pada pesan terenkripsi menggunakan karakter pada kunci secara berulang-ulang. Berikut ini adalah cara kerja dekripsi Vigenere Cipher secara lengkap:

a. Pertama, tuliskan kunci pada suatu baris, dan pesan terenkripsi pada baris di bawahnya.
b. Konversi setiap karakter alfabet yang terdiri dari 26 karakter pada pesan terenkripsi dan kunci ke dalam bilangan bulat dari 0 hingga 25. Misalnya, pesan terenkripsi "PNZPMBGKNT" dengan kunci "ilham" akan diubah ke dalam bilangan bulat sebagai berikut:
   P = 15, N = 13, Z = 25, P = 15, M = 12, B = 1, G = 6, K = 10, N = 13, T = 19 i = 8, l = 11, h = 7, a = 0, m = 12
c. Lakukan operasi dekripsi dengan menghitung hasil pengurangan setiap karakter pesan terenkripsi dengan karakter pada kunci, kemudian hitung hasil mod 26 dari selisih tersebut menggunakan rumus dekripsi Vigenere Cipher (2):
   Pi = (Ci - Ki) mod 26
   di mana:
   Pi = karakter plainteks
   Ci = karakter terenkripsi
   Ki = karakter kunci
d. Lakukan operasi dekripsi pada setiap karakter pesan terenkripsi dengan karakter pada kunci yang sesuai. Misalnya, dekripsi karakter pertama "P" dengan karakter pertama kunci "i" adalah sebagai berikut:
   Pi = (Ci - Ki) mod 26
   Pi = (15 - 8) mod 26
   Pi = 7
   Karakter plainteks dari "P" adalah "h".
e. Lakukan operasi yang sama pada setiap karakter pesan terenkripsi dengan karakter pada kunci yang sesuai, hingga seluruh pesan terdekripsi.
f. Pesan terdekripsi dari "PNZPMBGKNT" dengan kunci "ilham" adalah "HELLO WORLD".

Algoritma Beaufort Cipher merupakan teknik kriptografi yang berguna untuk mengamankan pesan dengan cara mengenkripsi plainteks menggunakan sebuah kunci (Rachmadsyah et al., 2020). Mirip dengan Vigenere Cipher, algoritma ini juga menggunakan kunci, tetapi dengan pengulangan yang berbeda. Algoritma ini diciptakan oleh Sir Francis Beaufort, seorang insinyur Angkatan Laut Inggris pada tahun 1840. Seperti Vigenere Cipher, Beaufort Cipher juga mengubah karakter dalam pesan menggunakan kunci. Namun, kelemahan dari Beaufort Cipher adalah mudahnya diprediksi karena pola perulangan pada plaintext (Ginting, 2020) (Rachmadsyah et al., 2020). Oleh karena itu, analisis frekuensi dapat dilakukan pada teks sandi untuk menemukan pola perulangan plaintext.

Untuk mengenkripsi pesan "hello world" dengan key "ilham" menggunakan Beaufort Cipher, gunakan gambar 2 dan rumus (3) berikut:

$$Ci = (Pi + Ki) \bmod 26 \quad (3)$$

Huruf	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Gamabr 2. Tabel Beaufort Cipher

Langkah-langkah untuk mengenkripsi pesan menggunakan Algoritma Beaufort Cipher sebagai berikut:

a. Pertama-tama, plainteks dan key akan diubah menjadi angka berdasarkan urutan alfabetnya. Misalnya, "hello world" menjadi "7 4 11 11 14 22 14 17 11 3 3" dan "ilham" menjadi "8 11 7 0 12".
b. Selanjutnya, untuk setiap huruf dalam plainteks, cari huruf ke-n dalam key yang sesuai (n adalah indeks huruf dalam plainteks, dimulai dari 0). Jika indeks huruf dalam plainteks lebih besar dari panjang key, mulai lagi dari awal key. Misalnya, huruf pertama dalam plainteks "h" akan mencari huruf ke-0 dalam key, yaitu "i".
c. Kurangkan angka indeks huruf dalam plainteks dengan angka indeks huruf dalam key. Jika hasil pengurangan kurang dari 0, tambahkan 26. Misalnya, untuk huruf pertama dalam plainteks "h" dan huruf pertama dalam key "i", indeks huruf "h" adalah 7 dan indeks huruf "i" adalah 8. Hasil pengurangan 8-7=1, sehingga indeks huruf yang dienkripsi adalah 1.
d. Hasil pengurangan di atas akan menjadi indeks huruf dalam alfabet. Ubah hasil tersebut menjadi huruf sesuai dengan alfabetnya. Misalnya, indeks huruf yang dienkripsi adalah 1, maka huruf yang dihasilkan adalah "F".
e. Ulangi langkah-langkah di atas untuk setiap huruf dalam plainteks.

Dengan menggunakan cara di atas, seluruh pesan "hello world" dengan key "ilham" akan dienkripsi menjadi "FVYDZIQGZG". Pesan tersebut menjadi lebih aman dalam pengirimannya karena tidak dapat dengan mudah dibaca oleh orang yang tidak memiliki key. Namun, perlu diingat bahwa Beaufort Cipher memiliki kelemahan mudahnya ditembus karena pola perulangan pada plaintext, sehingga perlu dilakukan pengamanan tambahan untuk memperkuat keamanannya.

Untuk melakukan dekripsi pada Beaufort Cipher, langkah-langkah yang dilakukan mirip dengan proses enkripsi. Namun, rumus yang digunakan adalah rumus (4) sebagai berikut:

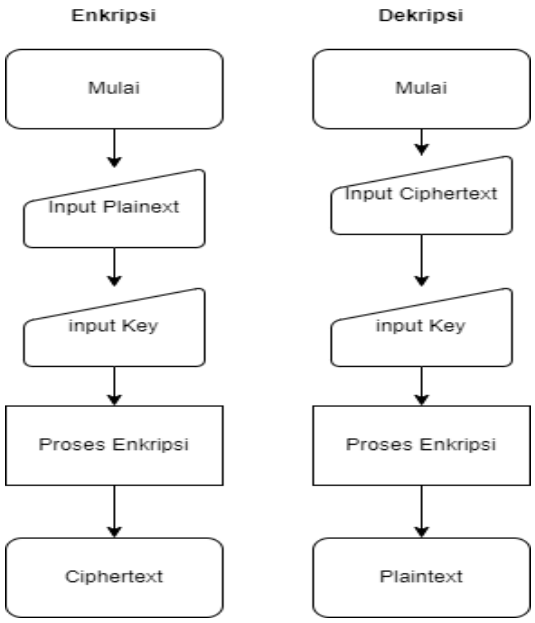
$$Pi = (Ki - Ci) \bmod 26 \quad (4)$$

Berikut adalah cara untuk mendekripsi pesan "FVYDZIQGZG" menggunakan Beaufort Cipher dengan key "ilham":

a. Ubah pesan terenkripsi dan key menjadi angka berdasarkan urutan alfabetnya. Contohnya, "FVYDZIQGZG" menjadi "5 21 24 3 25 8 16 6 25 6" dan "ilham" menjadi "8 11 7 0 12".
b. Untuk setiap huruf dalam pesan terenkripsi, cari huruf ke-n dalam key yang sesuai (n adalah indeks huruf dalam pesan terenkripsi, dimulai dari 0). Jika indeks huruf dalam pesan terenkripsi lebih besar dari panjang key, mulailah lagi dari awal key. Sebagai contoh, huruf pertama dalam pesan terenkripsi "F" akan mencari huruf ke-0 dalam key, yaitu "i".
c. Kurangkan angka indeks huruf dalam key dengan angka indeks huruf dalam pesan terenkripsi. Jika hasil pengurangan kurang dari 0, tambahkan 26. Contohnya, untuk huruf pertama dalam pesan terenkripsi "F" dan huruf pertama dalam key "i", indeks huruf "F" adalah 5 dan indeks huruf "i" adalah 8. Hasil pengurangan 8-5=3, sehingga indeks huruf yang didekripsi adalah 3.
d. Hasil pengurangan di atas akan menjadi indeks huruf dalam alfabet. Ubah hasil tersebut menjadi huruf sesuai dengan alfabetnya. Misalnya, indeks huruf yang didekripsi adalah 3, maka huruf yang dihasilkan adalah "C".
e. Ulangi langkah-langkah di atas untuk setiap huruf dalam pesan terenkripsi. Sebagai contoh, untuk huruf kedua dalam pesan terenkripsi "V" dan huruf kedua dalam key "l", indeks huruf "V" adalah 21 dan indeks huruf "l" adalah 11. Hasil pengurangan 11-21=16, sehingga indeks huruf yang didekripsi adalah 16. Huruf yang dihasilkan adalah "Q".
f. Teruskan langkah-langkah di atas untuk seluruh pesan terenkripsi "FVYDZIQGZG" dengan key "ilham". Hasilnya akan menjadi "HELLOWORLD". Pesan tersebut dapat dengan mudah dibaca oleh penerima yang memiliki key yang sama dengan pengirim.

3.2 Hasil

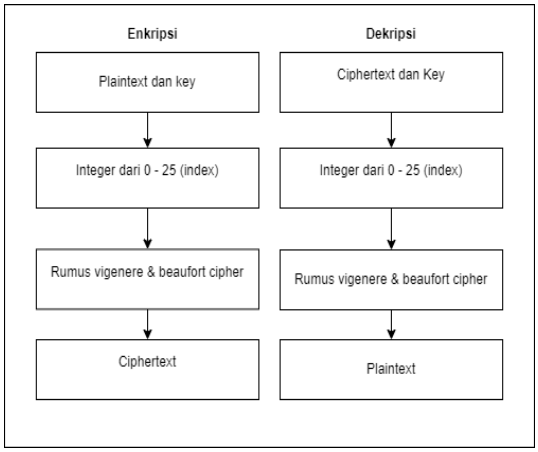
Untuk mencapai sistem yang optimal, perencanaan yang baik juga diperlukan. Oleh karena itu, berikut adalah tahapan yang harus diikuti dalam proses enkripsi dan dekripsi teks menggunakan algoritma Vigenere dan Beaufort Cipher pada aplikasi berbasis website.



Gamabr 3. Flowchart system aplikasi

Berikut adalah tahapan yang perlu diikuti untuk menyelesaikan algoritma ini, yang dijelaskan dalam Gambar 4.

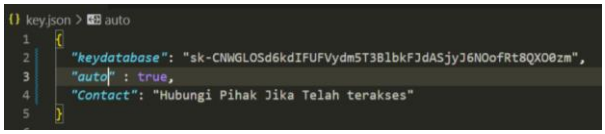
Jurnal Teknologi Sistem Informasi dan Aplikasi **ISSN: 2654-3788**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2654-4229**
Vol. 6, No. 3, Juli 2023 (262-268) **DOI: 10.32493/jtsi.v6i3.30118**



Gamabr 4. Enkripsi dan Dekripsi Vigenere dan Beaufort Cipher

Enkripsi merupakan proses transformasi data asli atau informasi (plaintext) menjadi bentuk yang tidak dapat dibaca atau dimengerti (ciphertext). Sedangkan dekripsi adalah proses mengembalikan data yang telah dienkripsi (ciphertext) menjadi bentuk asli atau data yang dapat dimengerti (plaintext) dengan menggunakan kunci yang sesuai dengan algoritma enkripsi yang digunakan sebelumnya.

Sebagai contoh kasus, akan di lakukan pengamanan isi dari file json pada API (Applicaion Programing Interface) pada Gambar 5:



Gambar 5. Contoh Codingan JSON (Javascript Obect Notation)

Application Programming Interface (API) adalah kumpulan aturan dan protokol yang memungkinkan perangkat lunak berkomunikasi dengan perangkat lunak lainnya (Leo et al., 2022). API bertindak sebagai perantara antara berbagai aplikasi atau komponen perangkat lunak yang berbeda, memungkinkan mereka saling berinteraksi dan berbagi data dengan cara yang terstruktur dan terstandarisasi. Secara keseluruhan, API memainkan peran penting dalam pengembangan perangkat lunak modern, memfasilitasi interaksi dan integrasi antara aplikasi yang berbeda, serta memberikan cara yang terstruktur dan efisien untuk berbagi data dan fungsionalitas di antara sistem yang berbeda(Tedyyana et al., 2021) (Alyahi et al., 2015).

Key pada API di atas akan dienkripsi agar menjaga keamanan untuk memastikan hanya orang tertentu yang memiliki akses yang dapat mengaksesnya. Perhatikan pada Gambar 6.

Gambar 6. Proses Enkripsi

Setelah memasukan plaintext dan key nya, lanjut ke proses enkripsi sehingga menghasilkan output ciphertext seperti Gambar 7.

Gambar 7. Output Ciphertext

Untuk mendapatkan plaintext nya Kembali, user hanya perlu memasukan key nya dan ciphertext nya, maka plainext akan di dapatkan. Untuk mengkombinasikan dari kedua algortima user hanya perlu mengenkripsi ciphertext dari vigenere cipher ke dalam beaufort cipher supaya lebih aman.

4 Kesimpulan dan Saran

Gabungan teknik kriptografi Vigenere dan Beaufort Cipher telah berhasil diimplementasikan dengan sukses dalam proses enkripsi dan dekripsi. Hal ini menunjukkan bahwa kedua teknik kriptografi ini dapat bekerja bersama secara harmonis dan menghasilkan hasil yang diinginkan.

Dengan menggunakan gabungan teknik ini, keamanan pesan teks dapat ditingkatkan secara signifikan. Proses enkripsi yang dilakukan dua kali menggunakan metode kriptografi yang berbeda memberikan lapisan keamanan tambahan, sehingga pesan menjadi lebih sulit untuk dipahami oleh pihak yang tidak berwenang.

Selain itu, penting juga untuk dicatat bahwa kombinasi teknik kriptografi Vigenere dan Beaufort Cipher dapat diterapkan dalam bahasa pemrograman JavaScript. Hal ini memberikan

fleksibilitas dan kemudahan bagi pengembang perangkat lunak untuk mengimplementasikan dan menggunakan teknik ini dalam pengembangan aplikasi berbasis web.

Secara keseluruhan, gabungan teknik kriptografi Vigenere dan Beaufort Cipher adalah solusi yang efektif untuk meningkatkan keamanan pesan teks dan dapat diaplikasikan dengan mudah dalam bahasa pemrograman JavaScript.

Referensi

Afandi, M. I., & Nurhayati, N. (2021). Implementasi Algoritma Vigenere Cipher Dan Atbash Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Berbasis Android. *It (Informatic Technique) Journal*, *8*(1), 30. https://doi.org/10.22303/it.8.1.2020.30-41

Alyahi, A. S., Nugroho, S., & Utomo, D. (2015). Aplikasi Mobile Learning Berbasis Web Service Menggunakan Sistem Operasi Android (Studi Kasus Fakultas Teknik Elektronika dan Komputer UKSW). *Techné : Jurnal Ilmiah Elektroteknika*, *14*(02), 137–146. https://doi.org/10.31358/techne.v14i02.132

Buulolo, N., & Sindar, A. (2020). Analisis dan Perancangan Keamanan Data Teks Menggunakan Algoritma Kriptografi DES (Data Encryption Standard). *Respati*, *15*(3), 61. https://doi.org/10.35842/jtir.v15i3.373

Ginting, V. S. (2020). Penerapan Algoritma Vigenere Cipher dan Hill Cipher Menggunakan Satuan Massa. *Jurnal Teknologi Informasi*, *4*(2), 241–246. https://doi.org/10.36294/jurti.v4i2.1365

Leo, L. P., Ambarwari, A., & Putra, S. D. (2022). Rancang Bangun Web Service Api Dan Dokumentasi Rest Api Web Portal Unit Kegiatan Mahasiswa Di Politeknik Negeri Lampung. *ROUTERS: Jurnal Sistem Dan Teknologi Informasi*, *1*(1), 9–18. https://doi.org/10.25181/rt.v1i1.2700

Maya, W. R., Azanuddin, A., & Elfitriani, E. (2022). Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer)*, *21*(1), 1. https://doi.org/10.53513/jis.v21i1.4764

Rachmadsyah, A., Perdana, A., & Budiman, A. (2020). Kombinasi Algoritma Beaufort Cipher dan Vigenere Cipher untuk Pengamanan Pesan Teks Berbasis Mobile Application. *Jurnal Minfo Polgan*, *9*(2), 12–17.

Setyawati1, N. Y., Khofid2, A. N. R., U.BWati, A., & Vera. (2021). *Modifikasi Kriptografi Klasik Kombinasi Metode Vigenere Cipher dan Caesar Cipher (Modification of Classical Cryptography Combination of the Vigenere Cipher and Caesar Cipher Methods)*. *1*(1), 1–8.

Tampubolon, A. (2021). Implementasi Kombinasi Algoritma RSA dan Algoritma DES Pada Aplikasi Pengaman Pesan Teks. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer)*, *20*(1), 38. https://doi.org/10.53513/jis.v20i1.2598

Tedyyana, A., Fauzi, M., & Ratnawati, F. (2021). Revamp Keamanan Web Service Milik PT XYZ Menggunakan REST API. *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*, *12*(1), 1–10. https://doi.org/10.31849/digitalzone.v12i1.6378

Triansyah, H. (2019). Kombinasi Kriptografi Algoritma Vigenere Cipher dan Algoritma AES Untuk Pengamanan Pesan Teks. *TECHSI - Jurnal Teknik Informatika*, *11*(3), 408. https://doi.org/10.29103/techsi.v11i3.1874