PROSES ENKRIPSI BERLAPIS MENGGUNAKAN TEKNIK KRIPTOGRAFI VIGENERE DAN CAESAR

Muhammad Fauzan Gifari, Muhammad Azwa Dipani, Syahbarudin Abdillah, Ahmad Turmudi Zy
Teknik Informatika, Universitas Pelita Bangsa
Jl. Inspeksi Kalimalang Tegal Danas Arah Deltamas, Cibatu, Cikarang, Indonesia
syahbarabdillah@gmail.com

ABSTRAK

Dengan meningkatnya kebutuhan akan mekanisme perlindungan data yang sederhana namun efektif untuk mencegah akses tidak sah dan modifikasi data sensitive.Teknik kriptografi klasik dipilih karena sifatnya yang mudah diterapkan dan kompatibel dengan berbagai sistem berbasis teks.Penelitian ini mengusulkan pendekatan enkripsi berlapis dengan menggabungkan Vigenere Cipher dan Caesar Cipher untuk meningkatkan keamanan data berbasis teks.Dengan mengeksplorasi efektivitas teknik kriptografi klasik dalam memberikan perlindungan dasar terhadap akses tidak sah dan modifikasi data sensitif dengan menggabungkan dua teknik kriptografi klasik. Proses enkripsi dilakukan dalam dua tahap: pertama, data akan dienkripsi menggunakan Vigenere Cipher, kemudian dienkripsi kembali menggunakan Caesar Cipher. Proses dekripsi dilakukan secara terbalik, dimulai dengan Caesar Cipher dan diikuti dengan Vigenere Cipher. Dari Hasil pengujian menunjukkan bahwa metode ini efektif untuk memberikan perlindungan dasar pada data seperti kata sandi dan informasi sederhana. Namun, metode ini tetap memiliki kelemahan, seperti rentannya Caesar Cipher terhadap serangan brute-force dan potensi analisis frekuensi pada Vigenere Cipher jika kunci yang digunakan terlalu pendek. Oleh karena itu, metode enkripsi berlapis memberikan perlindungan tambahan, metode ini lebih cocok untuk aplikasi dengan kebutuhan keamanan dasar. Untuk kebutuhan keamanan yang lebih tinggi, disarankan untuk menggunakan algoritma enkripsi yang lebih kuat seperti AES atau RSA, guna memastikan perlindungan data yang lebih aman dan lebih terjamin.

Kata Kunci : *Vigenere Cipher, Caesar Cipher, keamanan data, kriptografi, perlindungan data*

1. PENDAHULUAN

Dalam era di mana informasi yang ada dinilai sangat berharga, pihak-pihak yang tidak bertanggung jawab dapat memanfaatkan informasi tersebut dengan tujuan yang buruk [10][19].

Serangan terhadap data, seperti pencurian, modifikasi, dan penyadapan, menjadi ancaman serius yang dapat merugikan individu maupun organisasi. Ancaman ini semakin meningkat seiring dengan bertambahnya jumlah data yang ditransmisikan melalui jaringan, baik itu data pribadi, transaksi keuangan, hingga informasi sensitif lainnya. Oleh karena itu, diperlukan metode perlindungan data yang tidak hanya efektif tetapi juga efisien dalam penggunaannya [3][5].

Salah satu solusi yang telah digunakan secara luas adalah kriptografi [11].

Kriptografi adalah ilmu yang digunakan untuk mentransfer informasi secara aman antara dua pihak tanpa intervensi dari pihak luar [18].

Dalam dunia digital saat ini, ancaman seperti pencurian data, modifikasi, dan penyadapan semakin sering terjadi [2],maka dari itu kriptografi digunakan sebagai langkah pencegahan. Secara garis besar, kriptografi dibedakan menjadi dua jenis yaitu kriptografi klasik dan kriptografi modern [8][15].

Dalam kriptografi terdapat dua prinsip yaitu deksripsi dan enkripsi, dimana dekripsi merupakan proses mengubah bentuk cipher text menjadi aslinya, sedangkan enkripsi adalah proses penggunaan algoritma khusus untuk mengubah data atau informasi menjadi bentuk yang hampir mustahil untuk dikenali [9][14].

Kriptografi klasik, seperti Vigenere Cipher dan Caesar Cipher, menawarkan metode sederhana namun efektif untuk enkripsi data [10].

Vigenere Cipher adalah teknik kriptografi klasik yang menggunakan substitusi polialfabetik dengan memanfaatkan kata kunci untuk menentukan pola enkripsi [7][17], sedangkan Caesar Cipher mengandalkan pergeseran huruf berdasarkan kunci tertentu [20].

Meskipun memiliki keunggulan, kedua algoritma ini rentan terhadap serangan seperti analisis frekuensi dan brute-force.

Untuk mengatasi kelemahan seperti yang disebutkan di atas, penelitian ini mengusulkan pendekatan enkripsi berlapis dengan menggabungkan Vigenere Cipher dan Caesar Cipher. Pendekatan ini bertujuan untuk meningkatkan keamanan data dengan memanfaatkan keunggulan dari kedua algoritma tersebut [2][13].

2. TINJAUAN PUSTAKA

Kandungan dalam tinjauan pustaka bisa berupa landasan teori yang relevan dengan topik skripsi yang akan dibahas, di mana landasan teori ini menjadi panduan pertama dalam penyusunan skripsi.

2.1. Kriptografi

Kriptografi adalah ilmu yang digunakan untuk mentransfer informasi secara aman antara dua pihak tanpa intervensi dari pihak luar [16].

Dalam dunia digital saat ini, ancaman seperti pencurian data, dan penyadapan semakin sering terjadi [1].

Salah satu teknik yang terkenal dalam kriptografi adalah *Vigenere Cipher*, yang merupakan metode substitusi polialfabetik. Penelitian oleh Nacira et al. menunjukkan bahwa Vigenere Cipher dapat diperluas untuk menyertakan data numerik, sehingga angka juga dapat dienkripsi [2].

2.2. Caesar Cipher

Caesar Cipher merupakan salah satu algoritma yang paling sederhana dan banyak digunakan [20]. Dalam teknik Caesar cipher setiap huruf digeser ke beberapa tempat, pola dalam teks sandi sama dengan panjang kata kunci yang digunakan. Formula matematika untuk enkripsi dan dekripsi dapat dilihat pada formula (1) dan formula (2).

$$C_i = (P_i + k)\ mod\ 26 \quad (1)$$

$$P_i = (C_i - k)\ mod\ 26 \quad (2)$$

Di mana Ci merupakan ciphertext posisi ke-i, Pi adalah posisi plaintext ke-i, k merupakan besar dari nilai pergeseran.

2.3. Vigenere Cipher

Teknik Vigenere Cipher mengenkripsi teks abjad dengan bantuan berbagai sandi Caesar berdasarkan huruf dari beberapa key. Vigenere cipher terdiri dari banyak Caesar cipher dengan nilai pergeseran yang berbeda.Vigenere Cipher juga dikenal sebagai cipher substitusi alfabet yang merupakan matriks pergeseran sandi 26 x 26 Caesar[10].

Formula matematika untuk enkripsi dan dekripsi Vigenere dapat dilihat pada formula (3) dan (4).

$$C_i = (P_i + k_i)\ mod\ 26 \quad (3)$$

$$P_i = (C_i - k_i)\ mod\ 26 \quad (4)$$

Di mana Ci merupakan ciphertext posisi ke-i, Pi adalah posisi plaintext ke-i, ki adalah posisi key ke-i.

2.4. Kombinasi Vigenere dan Caesar Cipher

Menggabungkan proses enkripsi dari Vigenere dan Caesar Cipher untuk menghasilkan ciphertext dari plaintext dan kunci yang diberikan. Kombinasi kedua algoritma ini bertujuan untuk meningkatkan keamanan dengan memanfaatkan keunggulan masing-masing teknik sambil mengurangi kelemahan yang ada [1].

Meskipun metode ini menawarkan peningkatan keamanan, masih ada risiko terhadap serangan analisis frekuensi dan brute-force. Oleh karena itu, penulis merekomendasikan penggunaan algoritma yang lebih kuat seperti AES atau RSA untuk aplikasi yang memerlukan tingkat keamanan lebih tinggi [2].

Formula matematika untuk gabungan dari enkripsi dan dekripsi Vigenere dan Caesar dapat dilihat pada formula (5) dan (6).

$$C_i = (\left(P_i + k(i\ mod\ len(k))\right) + s)\ mod\ 26 \quad (5)$$

$$C_i = (C_i - s) - k(i\ mod\ len(k))\ mod\ 26 \quad (6)$$

Di mana Ci merupakan posisi karakter ciphertext yang telah dienkripsi dengan kedua algoritma (Caesar dan Vigenère) pada posisi ke-i, S adalah nilai pergeseran Caesar yang digunakan saat enkripsi, $k(i\ mod\ len(k))$ adalah posisi karakter kunci yang digunakan dalam algoritma Vigenère pada posisi ke-i, $len(k)$ adalah panjang kunci Vigenère yang digunakan untuk enkripsi, dan Pi adalah posisi karakter plaintext yang terdekripsi setelah langkah dekripsi gabungan (menggunakan dekripsi Caesar dan Vigenère) pada posisi ke-i.

2.5. Implementasi Sistem Enkripsi

Dalam pengembangan sistem enkripsi ini, PHP digunakan sebagai bahasa pemrograman, dengan fitur pengunggahan file dan proses enkripsi/dekripsi yang efisien. Hasil pengujian menunjukkan bahwa sistem berhasil mengenkripsi data secara efektif, meskipun tetap ada kerentanan terhadap metode serangan tertentu [1].

Penelitian ini memberikan wawasan tentang bagaimana kombinasi teknik kriptografi klasik dapat diterapkan dalam konteks modern untuk meningkatkan perlindungan data sensitif.

2.6. Pentingnya Adaptasi Teknik Kriptografi

Sistem ini juga menyoroti pentingnya pemahaman tentang algoritma kriptografi klasik dan potensi penerapannya dalam sistem keamanan data saat ini. Dengan mengadaptasi teknik-teknik lama seperti Vigenere dan Caesar Cipher, peneliti berusaha menciptakan solusi yang lebih kuat dan relevan untuk tantangan keamanan informasi di era digital [2].

3. METODE PENELITIAN

Penelitian ini menggunakan metode kombinasi yang melibatkan studi literatur untuk memahami konsep dasar dan kelemahan algoritma kriptografi klasik, serta implementasi algoritma untuk menguji pendekatan enkripsi berlapis yang diusulkan. Metode ini terdiri dari dua tahapan utama: studi literatur dan implementasi algoritma.

3.1. Studi literatur

Studi literatur dilakukan untuk mengidentifikasi dan menganalisis algoritma kriptografi klasik yang relevan, yaitu Vigenere Cipher dan Caesar Cipher. Literatur yang digunakan meliputi buku, jurnal, artikel, dan publikasi daring. Berikut adalah langkah-langkah dalam studi literatur:

a. Identifikasi Algoritma Dasar: Penelusuran sumber terkait konsep dan prinsip kerja Vigenere Cipher dan Caesar Cipher. Literatur yang digunakan mencakup analisis kelemahan kedua algoritma, seperti kerentanan terhadap analisis frekuensi dan brute-force.
b. Kajian Kelebihan dan Kekurangan: Mengidentifikasi keunggulan dan keterbatasan

dari masing-masing algoritma, terutama dalam konteks keamanan data.

c. Pencarian Solusi: Mengkaji metode-metode yang telah diusulkan dalam literatur untuk mengatasi kelemahan algoritma klasik, seperti penggabungan teknik enkripsi.

Hasil dari studi literatur ini kemudian menjadi dasar untuk merancang pendekatan enkripsi berlapis yang menggabungkan kedua algoritma tersebut.

3.2. Implementasi Algoritma dengan PHP

Implementasi algoritma enkripsi berlapis dilakukan menggunakan PHP. PHP dipilih karena fleksibilitasnya untuk membangun aplikasi berbasis web yang mendukung manipulasi teks, serta kompatibilitasnya dengan server dan database untuk menyimpan data hasil enkripsi. Detail Implementasi Algoritma dengan PHP

3.3. Perancangan Sistem

Sistem ini dirancang untuk memiliki dua fungsi utama:

a. Enkripsi Berlapis: Menggabungkan algoritma Vigenere dan Caesar untuk mengenkripsi file atau teks.
b. Dekripsi Berlapis: Membalikkan proses enkripsi untuk mendapatkan kembali plaintext.

Sistem mendukung pengunggahan file (file upload), sehingga file teks yang akan dienkripsi dapat langsung diproses oleh server.

3.4. Struktur Folder Sistem

a. index.php: Halaman utama untuk antarmuka pengguna.
b. encrypt.php: Berisi logika enkripsi (menggunakan Vigenere dan Caesar Cipher).
c. decrypt.php: Berisi logika dekripsi.
d. uploads/: Folder untuk menyimpan file yang diunggah pengguna.
e. results/: Folder untuk menyimpan hasil enkripsi.

3.5. Fitur Utama

a. Input Data: Pengguna dapat memasukkan teks atau mengunggah file teks.
b. Input Kunci: Pengguna memasukkan dua kunci, satu untuk Vigenere Cipher dan satu untuk Caesar Cipher.

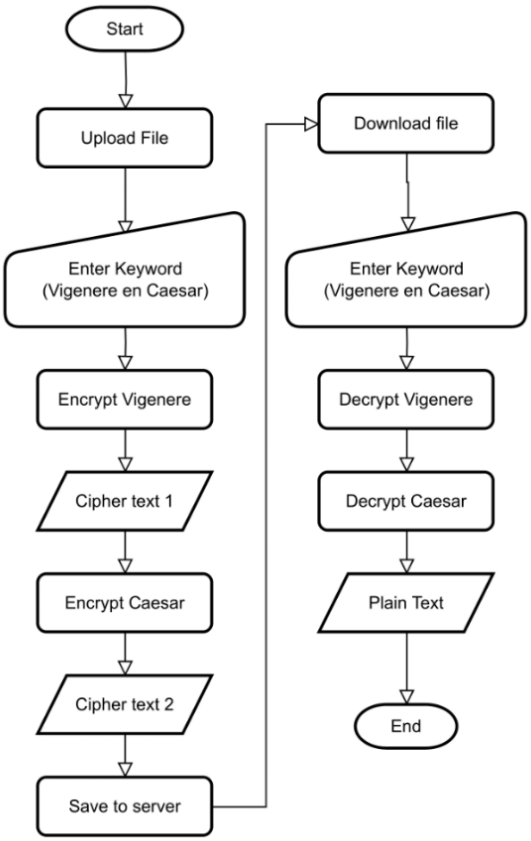
3.6. Proses Enkripsi

a. File atau teks yang diunggah dienkripsi menggunakan Vigenere Cipher.
b. Hasil enkripsi pertama (Ciphertext 1) dienkripsi ulang menggunakan Caesar Cipher.
c. Hasil akhir (Ciphertext 2) disimpan di server.

3.7. Proses Dekripsi

a. Ciphertext 2 didekripsi menggunakan Caesar Cipher untuk mendapatkan Ciphertext 1.
b. Ciphertext 1 didekripsi menggunakan Vigenere Cipher untuk mendapatkan plaintext asli.
c. Unduh File Hasil: Pengguna dapat mengunduh hasil enkripsi atau dekripsi.

3.8. Flowchart Proses Enkripsi



Gambar 1. Flowchart Proses Enkripsi dan Dekripsi

Penjelasan pada flowchart diatas, sebagai berikut :
Pada bagian Enkripsi

a. Start: Proses dimulai.
b. Upload File: Pengguna mengunggah file yang ingin dienkripsi.
c. Enter Keyword (Vigenere dan Caesar): Pengguna memasukkan kata kunci yang digunakan untuk enkripsi dengan algoritma Vigenere dan Caesar.
d. Encrypt Vigenere: File dienkripsi menggunakan algoritma Vigenere berdasarkan kata kunci yang dimasukkan. Hasilnya adalah *Cipher Text 1*.
e. Encrypt Caesar: Hasil enkripsi Vigenere (*Cipher Text 1*) dienkripsi kembali menggunakan algoritma Caesar, menghasilkan *Cipher Text 2*.
f. Save to Server: *Cipher Text 2* disimpan di server.

Pada bagian Dekripsi

a. Download File: Pengguna dapat mengunduh file terenkripsi (*Cipher Text 2*) dari server.
b. Enter Keyword (Vigenere dan Caesar): Pengguna memasukkan kata kunci yang sama seperti saat enkripsi.
c. Decrypt Caesar: *Cipher Text 2* didekripsi menggunakan algoritma Caesar untuk mendapatkan kembali *Cipher Text 1*.

d. Decrypt Vigenere: *Cipher Text 1* didekripsi menggunakan algoritma Vigenere untuk mendapatkan *Plain Text* (teks asli).
e. End: Proses selesai.

Pengujian dilakukan untuk memastikan bahwa sistem enkripsi berlapis yang menggabungkan algoritma Vigenere Cipher dan Caesar Cipher dapat diterapkan dengan benar pada berbagai jenis data, baik itu teks biasa maupun file yang diunggah oleh pengguna. Evaluasi juga mencakup kemudahan penggunaan sistem serta efektivitas algoritma dalam melindungi informasi dari akses yang tidak sah.

Hasil dari pengujian menunjukkan bahwa algoritma ini berhasil mengenkripsi data dengan baik, menghasilkan Ciphertext yang aman dan tidak dapat dibaca tanpa kunci yang tepat. Proses enkripsi dua lapis, pertama dengan Vigenere Cipher dan kemudian dengan Caesar Cipher, terbukti efektif dalam meningkatkan tingkat keamanan data dibandingkan dengan penggunaan satu algoritma saja. Meskipun demikian, kombinasi algoritma ini tetap rentan terhadap serangan brute force, terutama jika kunci yang digunakan tidak cukup kuat atau mudah ditebak.

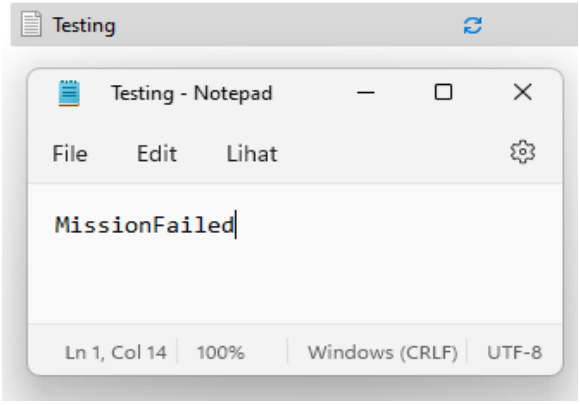
Kombinasi antara metode studi literatur untuk memahami kelemahan masing-masing algoritma dan implementasi praktis dari enkripsi berlapis menggunakan PHP ini memungkinkan penelitian ini memberikan kontribusi nyata dalam meningkatkan perlindungan data pada aplikasi berbasis web. Meskipun Vigenere Cipher dan Caesar Cipher tergolong algoritma kriptografi klasik yang relatif sederhana, penerapannya cukup efektif untuk aplikasi dengan tingkat keamanan dasar, seperti pada sistem ini. Sistem ini memberikan lapisan perlindungan yang cukup untuk data sensitif, seperti file teks atau informasi pribadi yang diunggah pengguna, namun tetap membutuhkan penguatan lebih lanjut dalam hal manajemen kunci dan perlindungan terhadap serangan yang lebih kompleks.

4. HASIL DAN PEMBAHASAN

Caesar Cipher dan Vigenere Cipher adalah algoritma kriptografi klasik yang dikenal karena kesederhanaannya. Caesar Cipher sering digunakan untuk mengenkripsi teks pendek seperti password atau pesan rahasia dalam sistem kecil, tetapi kelemahan Caesar cipher sendiri ada pada jumlah kunci yang terbatas dan sifat deterministik yang membuatnya rentan terhadap serangan brute force. Di sisi lain, Vigenere Cipher menawarkan kerumitan lebih tinggi, meskipun pola berulang pada kuncinya tetap menjadi celah bagi analisis kriptografi.

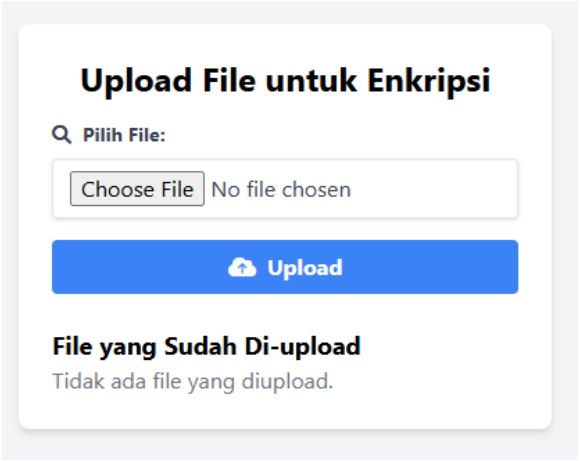
Untuk mengatasi kelemahan ini, kombinasi Caesar dan Vigenere Cipher muncul sebagai solusi. Pendekatan ini meningkatkan tingkat keamanan dengan memanfaatkan kekuatan kedua algoritma. Selain itu, implementasinya dalam pengembangan website menggunakan php menunjukkan bahwa enkripsi berlapis ini dapat menjadi pilihan sederhana namun efektif untuk aplikasi sehari-hari.

4.1. Implementasi PHP



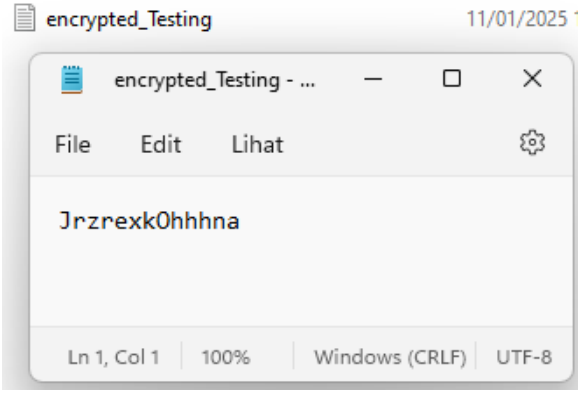
Gambar 2. Plaintext yang akan diuji coba

Gambar diatas merupakan plaintext yang akan digunakan dalam uji coba dengan menggunakan enkripsi berlapis dengan menggabungkan Vigenere Cipher dan Caesar Cipher.



Gambar 3. Tampilan Antarmuka

Gambar diatas merupakan tampilan antarmuka sistem. Pada halaman ini kita memasukan file plaintext yang ingin dienkripsi menggunakan algoritma Vigenere dan Caesar Cipher sebelum disimpan ke dalam server.



Gambar 4. Hasil file enkripsi didalam Sever

Gambar diatas merupakan hasil dari enkripsi enkripsi berlapis dengan menggabungkan Vigenere Cipher dan Caesar Cipher. Dalam pengujian ini juga dilakukan dengan Empat jenis data yang berbeda, dengan hasil sebagai berikut:

Tabel 1. Hasil Enkripsi

Input (Plaintext)	Vigenere Cipher (Key = "SECURE")	Caesar Cipher (Shift = 5)	Ciphertext (Final)
FileTransferComplete	XmnyKvsruzvvUsojcili	CrsdPaxwzeaaZxtohnqn	CrsdPaxwzeaaZxtohnqn
DatabaseBackup	VevusekiDutomt	AjazxjpnIzytry	AjazxjpnIzytry
ServerErrorNotFound	KitpvvWvtiiRgxHilrv	PnyuaaBaynnWlcMnqwa	PnyuaaBaynnWlcMnqwa
JumpScare	ByojJgsvg	GdtoOlxal	GdtoOlxal

Tabel 2. Hasil Dekripsi

Ciphertext (Final)	Dekripsi (Caesar)	Dekripsi (Vigenere)	Output (Plaintext)
CrsdPaxwzeaaZxtohnqn	XmnyKvsruzvvUsojcili	FileTransferComplete	FileTransferComplete
AjazxjpnIzytry	VevusekiDutomt	DatabaseBackup	DatabaseBackup
PnyuaaBaynnWlcMnqwa	KitpvvWvtiiRgxHilrv	ServerErrorNotFound	ServerErrorNotFound
GdtoOlxal	ByojJgsvg	JumpScare	JumpScare

Penjelasan Proses Enkripsi dan Dekripsi dengan Data File

1. Proses Enkripsi Menggunakan Vigenere Cipher
   a. Input: "FileTransferComplete"
   b. Kunci: "SECURE"
   Langkah-langkah:
   a. Setiap karakter dalam teks asli digantikan dengan karakter yang berada pada posisi yang digeser sesuai dengan kunci yang ditentukan.
   b. Misalnya, untuk huruf pertama 'F', menggunakan kunci 'S' yang menggeser 'F' sebanyak 18 posisi, menghasilkan 'X'.
   c. Huruf kedua 'i' menggunakan kunci 'E' yang menggeser 'i' sebanyak 4 posisi, menghasilkan 'm'.
   d. Proses ini dilakukan untuk setiap karakter, menghasilkan teks terenkripsi.
   Hasil Enkripsi Vigenere: "XmnyKvsruzvvUsojcili"
2. Proses Enkripsi Menggunakan Caesar Cipher
   a. Input: "XmnyKvsruzvvUsojcili"
   b. Shift: 5
   Langkah-langkah:
   a. Huruf pertama 'X' digeser sebanyak 5 posisi dalam alfabet, menghasilkan 'C'.
   b. Huruf kedua 'm' digeser sebanyak 5 posisi, menghasilkan 'r'.
   c. Proses ini dilakukan untuk setiap karakter pada ciphertext.
   Hasil Enkripsi Caesar: "CrsdPaxwzeaaZxtohnqn"
3. Proses Dekripsi Menggunakan Caesar Cipher
   a. Input: "CrsdPaxwzeaaZxtohnqn"
   b. Shift: -5 (menggeser mundur sebanyak 5 posisi)
   Langkah-langkah:
   a. Huruf pertama 'C' digeser kembali sebanyak 5 posisi, menghasilkan 'X'.
   b. Huruf kedua 'r' digeser kembali sebanyak 5 posisi, menghasilkan 'm'.
   c. Proses ini dilanjutkan untuk seluruh huruf pada ciphertext.
   Hasil Dekripsi Caesar: "XmnyKvsruzvvUsojcili"
4. Proses Dekripsi Menggunakan Vigenere Cipher
   a. Input: "XmnyKvsruzvvUsojcili"
   b. Kunci: "SECURE"
   Langkah-langkah:
   a. Huruf pertama 'X' digeser kembali oleh kunci 'S' (posisi 18), menghasilkan 'F'.
   b. Huruf kedua 'm' digeser kembali oleh kunci 'E' (posisi 4), menghasilkan 'i'.
   c. Proses ini dilakukan untuk setiap karakter sesuai dengan pola kunci.
   Hasil Dekripsi Vigenere: "FileTransferComplete"

4.2. Kelemahan pada Proses Enkripsi danDekripsi dengan menggabungan Vigenere Cipher dan Caesar Cipher

Dalam implementasi ini, proses enkripsi dimulai dengan menggunakan Vigenere Cipher untuk mengenkripsi pesan terlebih dahulu, lalu melanjutkan dengan enkripsi menggunakan Caesar Cipher. Setelah pesan terenkripsi, dekripsi dilakukan dengan langkah terbalik: pertama, ciphertext didekripsi menggunakan Caesar Cipher, baru kemudian menggunakan Vigenere Cipher. Meskipun menambah lapisan keamanan, gabungan kedua cipher ini memiliki beberapa kelemahan yang perlu diperhatikan, seperti

a. Kerentanannya terhadap Serangan Frekuensi pada Vigenere Cipher: Jika kunci Vigenere yang digunakan terlalu pendek atau berulang, penyerang bisa dengan mudah mendeteksi pola dalam ciphertext dan menebak kunci. Ini mengurangi efektivitas lapisan pertama enkripsi, meskipun menggunakan Vigenere Cipher yang lebih kompleks daripada Caesar Cipher.
b. Rentan terhadap Serangan Brute Force pada Caesar Cipher: Setelah pesan melalui Vigenere Cipher, lapisan kedua yang menggunakan Caesar Cipher masih memiliki kelemahan. Dengan hanya 25 kemungkinan pergeseran, penyerang bisa dengan mudah mencoba semua pergeseran untuk menemukan plaintext asli. Ini membuat Caesar Cipher cukup mudah untuk ditembus jika serangan brute force diterapkan.

c. Kombinasi yang Tidak Sepenuhnya Efektif: Meskipun menambahkan dua lapisan enkripsi, gabungan antara Vigenere dan Caesar Cipher tetap rentan jika kunci atau pergeseran yang digunakan terlalu sederhana. Keamanan enkripsi ini bisa terancam jika penyerang tahu cara memanfaatkan kelemahan pada masing-masing cipher.
d. Kesulitan dalam Mengelola Kunci: Baik Vigenere maupun Caesar Cipher memerlukan pengelolaan kunci yang baik. Jika kunci Vigenere terlalu pendek atau terlalu mudah ditebak (misalnya, menggunakan kata sederhana seperti "SECURE"), atau pergeseran Caesar yang dipilih tidak cukup kompleks, maka kedua lapisan enkripsi menjadi kurang efektif. Pengelolaan kunci yang buruk bisa membiarkan data rentan terhadap serangan.
e. Pola yang Terbentuk dalam Enkripsi Berlapis: Kombinasi antara Caesar Cipher yang menggeser karakter secara statis dan Vigenere yang menggunakan pergeseran berdasarkan kunci, bisa membentuk pola yang dapat dikenali oleh penyerang. Meskipun Vigenere memberikan lapisan perlindungan pertama, pola ini bisa tetap muncul setelah proses dekripsi pertama dengan Caesar Cipher.

5. KESIMPULAN DAN SARAN

Penelitian ini berhasil mengimplementasikan dan menguji enkripsi berlapis menggunakan kombinasi Vigenere Cipher dan Caesar Cipher dalam PHP untuk melindungi data pada website berbasis teks. Dari Hasil pengujian diatas menunjukkan bahwa metode ini efektif memberikan perlindungan dasar pada data seperti kata sandi dan informasi sederhana, dengan enkripsi dan dekripsi yang berjalan lancar. Namun, penelitian ini juga mengidentifikasi kelemahan penting, terutama Caesar Cipher yang rentan terhadap serangan brute-force, serta Vigenere Cipher yang bisa dieksploitasi jika kunci yang digunakan terlalu pendek atau berulang. Kontribusi dari penelitian ini adalah memberikan wawasan tentang penerapan enkripsi berlapis di PHP, meskipun terbatas pada aplikasi dengan kebutuhan keamanan dasar. Untuk penggunaan dengan skala yang lebih besar, disarankan untuk melakukan kombinasi menggunakan algoritma enkripsi yang lebih kuat seperti AES atau RSA, guna memastikan perlindungan data yang lebih aman dan lebih terjamin.

DAFTAR PUSTAKA

[1] Putra, M. A., Rustan, F., Liwe, L. M., & Suryaningrum, K. M. (2023). Securing Text File Using Combination of Vigenere and One - Time Pad Cipher Algorithm. *Procedia Computer Science*, *227*, 1030–1038. https://doi.org/10.1016/j.procs.2023.10.612

[2] Saraswat, A., Khatri, C., Sudhakar, Thakral, P., & Biswas, P. (2016). An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication. *Procedia Computer Science*, *92*, 355–360. https://doi.org/10.1016/j.procs.2016.07.390

[3] Abed, H. H., Shaeel, A. S., & Annoze, R. S. A. (2023). Hiding algorithm based fused images and Caesar cipher with intelligent security enhancement. *International Journal of Electrical and Computer Engineering*, *13*(6), 6797–6805. https://doi.org/10.11591/ijece.v13i6.pp6797-6805

[4] Chemlal, A., Tabti, H., El Bourakkadi, H., Hicham, R., Jarjar, A., & Benazzi, A. (2024). DNA-Level Enhanced Vigenère Encryption for Securing Color Images. *Acadlore Transactions on AI and Machine Learning*, *3*(2), 119–136. https://doi.org/10.56578/ataiml030205

[5] Hameed, T. H., & Sadeeq, H. T. (2022). Modified Vigenère cipher algorithm based on new key generation method. *Indonesian Journal of Electrical Engineering and Computer Science*, *28*(2), 954–961. https://doi.org/10.11591/ijeecs.v28.i2.pp954-961

[6] Hammad, R., Latif, K. A., Amrullah, A. Z., Hairani, Subki, A., Irfan, P., Zulfikri, M., Lalu Zazuli Azhar, M., Innuddin, M., & Marzuki, K. (2022). Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message. *Journal of Physics: Conference Series*, *2279*(1). https://doi.org/10.1088/1742-6596/2279/1/012006

[7] Hasnain, N., Shoukat, N., & Azam, M. (2022). An Improved Method of Vigenere Cipher to Securely Compress the Text by using Relative Frequency. *International Journal of Innovative Science and Research Technology*, *7*(10). https://www.researchgate.net/publication/365823032

[8] Imam Riadi, Abdul Fadlil, & Fahmi Auliya Tsani. (2022). Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *7*(1), 33–45. https://doi.org/10.14421/jiska.2022.7.1.33-45

[9] Imanda, R., Nasution, H., Gumanti, U., Sinambela, R. G., Sima, B. A., Arista, C., Bangun, B., Sitepu, B. K., & Fauzi, A. (2023). *Journal of Artificial Intelligence and Engineering Applications Development Of Hybrid Encryption Method Using Affine Cipher, Vigenere Cipher, And Elgamal Algorithm To Secure Text Messages In Data Communication System*. *2*(2). https://ioinformatic.org/

[10] Intani, K., Wulandari, G., Hasanah, H., Syarifudin, I. L., & Brillian, E. M. C. (2023). Meningkatkan Keamanan Pesan Rahasia pada Vigenere Cipher Menggunakan Kombinasi

Caesar Cipher dan Multiple-Key. *J I M P - Jurnal Informatika Merdeka Pasuruan*, *8*(1), 28. https://doi.org/10.51213/jimp.v8i1.847

[11] Irianti, E., Surianto, D. F., Ainun Zahra Adistia, Muh. Juharman, & Jumadil Ahmad Safi'i. (2023). Implementasi Kriptografi Vigenere Cipher untuk Keamanan Data Informasi Desa. *Progressive Information, Security, Computer, and Embedded System*, *1*(1), 8–15. https://doi.org/10.61255/pisces.v1i1.24

[12] JARJAR, M., ABDELLAH, A., Qobbi, Y., kaddouhi, S. El, JarJar, A., & Benazzi, A. (2023). *Image Encryption Using a Reworked Vigenere Network That Incorporates Bitwise Genetic Crossover*. https://doi.org/10.21203/rs.3.rs-2625919/v1

[13] Khaled Khalel Alregabo, A., & Hikmat Ismail, Y. (2023). Eximia Journal Proposed Method for Efficient Block Cipher Cryptography. *Eximia Journal*, *9*, 11–24. www.eximiajournal.com

[14] Maulana, D. K., Tanjung, S. M., Ritonga, R. S., & Ikhwan, A. (2023). Penerapan Kriptografi Vigenere Cipher Pada Kekuatan Kata Sandi. *Jurnal Sains Dan Teknologi (JSIT)*, *3*(1), 47–52. https://doi.org/10.47233/jsit.v3i1.483

[15] Murad, S. H., & Rahouma, K. H. (2022). Hybrid Cryptography for Cloud Security: Methodologies and Designs. In *Lecture Notes in Networks and Systems* (Vol. 224). Springer Singapore. https://doi.org/10.1007/978-981-16-2275-5_7

[16] Noviyanti. P, & Mira. (2022). Analisa Algoritma Kriptografi Klasik Caesar Cipher Viginere Cipher dan Hill Cipher – Study Literature. *Journal of Information Technology*, *2*(1), 23–30. https://doi.org/10.46229/jifotech.v2i1.387

[17] Purwanti, Nurcahya, S. D., & Nazelliana, D. (2024). Message Security in Classical Cryptography Using the Vigenere Cipher Method. *International Journal Software Engineering and Computer Science (IJSECS)*, *4*(1), 350–357. https://doi.org/10.35870/ijsecs.v4i1.2263

[18] Putra, N. B., Andika, B. C., Bagas, A. D. P., & Ridwan, M. (2023). *Implementasi sandi vigenere Cipher dalam mengenrkipsi pesan*. *1*(1), 42–50. https://jurnal.ittc.web.id/index.php/jct/article/view/25/46

[19] Qowi, Z., & Hudallah, N. (2021). Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm. *Journal of Physics: Conference Series*, *1918*(4). https://doi.org/10.1088/1742-6596/1918/4/042009

[20] Tan, C. M. S., Arada, G. P., Abad, A. C., & Magsino, E. R. (2021). A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher. *Journal of Physics: Conference Series*, *1997*(1). https://doi.org/10.1088/1742-6596/1997/1/012021