KRIPTOGRAFI KLASIK DAN KEAMANAN DASAR : IMPLEMENTASI KASIR RESTORAN DENGAN PENDEKATAN METODE CAESAR CIPHER

Yoga Pratama, Bayu Maulana Ayassy, Cahyo Hidayatullah, Frans Putra Sinaga, Ahmad Turmudi Zy
Teknik Informatika, Universitas Pelita Bangsa
Jl. Inspeksi Kalimalang No.9, Cibatu, Cikarang Selatan, Indonesia
yogapratama.312210042@mhs.pelitabangsa.ac.id

ABSTRAK

Keamanan data menjadi perhatian utama di era digital, terutama pada sistem POS berbasis web restoran yang sering kali menyimpan informasi sensitif seperti kata sandi pengguna. Dalam penelitian ini, algoritma Caesar Cipher digunakan sebagai metode enkripsi untuk meningkatkan keamanan data pada sistem kasir berbasis web. Algoritma ini menawarkan solusi sederhana namun memiliki keterbatasan pada jumlah kunci yang rentan terhadap serangan brute force dan analisis frekuensi. Hasil penelitian menunjukkan bahwa Caesar Cipher dapat memberikan perlindungan dasar dalam lingkungan dengan kebutuhan keamanan rendah. Selain itu, studi ini mengusulkan pengembangan lebih lanjut dengan kombinasi algoritma modern seperti AES dan hashing SHA-256 untuk meningkatkan keamanan. Penemuan ini memberikan wawasan baru dalam menciptakan sistem keamanan informasi yang lebih kuat di masa mendatang.

Kata kunci : *Caesar Cipher, Enkripsi Data, Sistem Kasir Restoran Berbasis Web, Keamanan Kata Sandi, Kerentanan Kriptografi*

1. PENDAHULUAN

Pada internet untuk melakukan kegiatan sehari-hari, termasuk penggunaan website untuk berkomunikasi, berbelanja, atau bahkan melakukan transaksi keuangan. Namun, keamanan informasi pengguna menjadi isu penting dalam penggunaan website ini. Salah satu cara untuk meningkatkan keamanan login pada website adalah dengan menggunakan enkripsi Caesar Cipher. Enkripsi Caesar Cipher adalah salah satu metode enkripsi sederhana yang dapat membantu melindungi informasi login dari serangan hacker atau pencurian identitas.[1]

Dalam hal ini keamanan dan privasi adalah aspek yang sangat penting dalam hal data.[2]

Data merupakan salah satu bagian terpenting dalam dunia binis, terutama dalam sistem kasir restoran berbasis web yang mencankup informasi seperti identitas seseorang, produk, maupun penjualan merupakan hal privasi baik bagi pebisnis maupun konsumen. Data yang seharusnya bersifat rahasia, menjadi target utama bagi penjahat cyber dan juga kompetitor bisnis.[3]

Untuk melindungi dan menjaga kerahasiaan data agar terhindar dari orang yang tidak berhak mendapatkan informasi tersebut, yaitu menggunakan metode kriptografi.[4]

Kriptografi dapat juga disebut salah satu ilmu dalam menjaga pengiriman pesan dan data dengan cara mengganti pesan atau data yang ingin di sampaikan menjadi satu kode yang di tentukan oleh pengirim dan selanjutnya di kirim ke tujuan yaitu penerima yang berhak dan zag dapat diterapkan dalam penyandian teks yang bersifat rahasia.[5]

Kriptografi dikenal dan dipakai cukup lama sejak kurang lebih tahun 1900 sebelum masehi.Kriptografi sendiri berasal dari kata “Crypto” yang berarti rahasia dan “graphy” yang berarti tulisan.[6]

Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi sebuah kode yang tidak dapat dimengerti pihak lain Kriptografi klasik beroperasi dalam mode karakter, yakni menggunakan huruf abjad (A - Z).[7]

Kriptografi adalah ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan data seperti keamanan data, akurasi data, integritas data, dan otentikasi data. Namun, tidak semua aspek keamanan informasi dapat diatasi dengan kriptografi.[8]

Oleh karena itu, perlindungan data dalam sistem informasi perlu mencakup aspek-aspek perlindungan yang komprehensif. Dalam upaya melindungi integritas dan kerahasiaan data, metode enkripsi dan deskripsi menjadi salah satu pilihan yang penting. Enkripsi adalah proses konversi data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Salah satu metode enkripsi yang sederhana namun efektif adalah Caesar Cipher.[9]

Metode ini dianggap sangat sederhana namun cukup efektif untuk mengamankan informasi login pada website. Dalam enkripsi Caesar Cipher, pesan yang dienkripsi dapat dengan mudah di-dekripsi dengan mengetahui jarak pergeseran dan alfabet yang digunakan. Oleh karena itu, enkripsi Caesar Cipher menjadi salah satu pilihan yang populer untuk meningkatkan keamanan login pada website.[1] sedangkan merupakan kebalikan dari proses enkripsi.

Pada tahapan ini, susunan karakter atau simbol acak yang dihasilkan dari proses enkripsi dapat disusun kembali ke bentuk teks asli agar dapat dibaca oleh penerima yang berhak. Tujuan dari proses dekripsi adalah untuk mengembalikan pesan yang

telah diubah oleh proses enkripsi menjadi bentuk aslinya.[10]

Caesar Cipher adalah salah satu teknik kriptografi yang sederhana namun efektif dalam memperbaiki keamanan data.[11].

Secara garis besar ada dua jenis kriptografi,yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik adalah kriptografi yang berbasis karakter (enkripsi dan dekripsi dilakukan pada setiap karakter). Sedangkan kriptografi modern adalah kriptografi yang beroperasi dalam mode bit (dinyatakan dalam 0 dan 1). Pada penelitian ini akan dibangun sistem keamanan dengan menggunakan kriptografi klasik dengan algoritma Caesar Cipher yang diimplementasikan pada web service, dimana Caesar Cipher merupakan salah satu enkripsi paling sederhana dengan menggantikan angka di mana setiap huruf dalam plaintext diganti dengan huruf dengan posisi tetap dipisahkan oleh nilai numerik yang digunakan sebagai "kunci".[12]

Algoritma Caesar Cipher dapat digunakan dalam pengamanan login website dengan cara mengenkripsi password yang dimasukkan oleh pengguna sebelum dikirim ke server. Dalam hal ini, password yang dimasukkan akan diubah menjadi teks acak yang hanya dapat dibaca oleh sistem yang memiliki kunci enkripsi yang tepat. Ketika pengguna melakukan login, password yang dimasukkan akan dienkripsi dan kemudian dibandingkan dengan password yang tersimpan di server yang juga telah dienkripsi menggunakan algoritma yang sama. Jika kedua password yang telah dienkripsi cocok, maka pengguna diizinkan untuk mengakses akun mereka. Pada proses login website, pengguna biasanya diminta untuk memasukkan username dan password sebagai langkah verifikasi identitas. Namun, masalah keamanan dapat timbul ketika data yang dikirimkan antara pengguna dan server dapat disadap oleh pihak yang tidak bertanggung jawab. Untuk mengatasi hal ini, algoritma Caesar Cipher dapat digunakan sebagai metode pengamanan untuk melindungi password yang dimasukkan oleh pengguna.[1]

Dalam tinjauan literatur, Beberapa peneliti telah melakukan inovasi dengan memodifikasi algoritma kriptografi sehingga dapat menigkatkan kemanan pada penggunaan algoritma tersebut.[13]

Sebagai contoh, penelitian yang dilakukan oleh Algoritma Caesar Cipher pada Pengenkripsian login pada sistem kasir restoran berbasis web, sementara penelitian yang dilakukan membahas tentang tinjauan pustaka terkait kriptografi dan Caesar Cipher. Selain itu, melakukan implementasi Caesar Cipher dengan menggunakan metode enkripsi pada teks.[14]

Namun algoritma kripografi klasik saat ini tidak banyak lagi digunakan karena sudah dianggap tidak aman. Kriptografi klasik memberikan konsep dasar pemahaman kriptografi dan dijadikan sebagai dasar algoritma kriptografi modern.[7]

Tujuan penulisan untuk laporan tugas akhir ini adalah mengimplementasikan enkripsi pada sistem kasir restoran berbasis web dengan algoritma kriptografi Caesar Cipher, lalu data tersebut akan didekripsikan oleh client side dengan algoritma kriptografi Caesar Cipher.[12]

Penelitian ini dapat memberikan kontribusi penting dalam pengembangan sistem keamanan informasi yang lebih kokoh di masa depan.[15] Dengan memahami secara mendalam tentang cara kerja teknik-teknik kriptanalisis ini dapat memberikan wawasan yang berharga dalam mengembangkan sistem keamanan[16]

Informasi yang lebih kokoh di masa depan. Melalui eksperimen dan analisis yang dilakukan dalam jurnal ini. Pemahaman yang lebih baik tentang kelemahan dan potensi solusi untuk meningkatkan keamanan sistem enkripsi akan didapatkan. Dengan demikian, upaya-upaya untuk melindungi informasi sensitif dari ancaman yang berkembang terus menerus dapat ditingkatkan secara signifikan.[15]

2. TINJAUAN PUSTAKA

2.1. Pentingnya Keamanan Data

Keamanan data menjadi aspek penting dalam perkembangan teknologi, terutama untuk melindungi data dari akses pihak yang tidak berwenang. Pengamanan login web kasir restoran menggunakan algoritma Caesar Cipher dapat menjadi langkah awal dalam memahami konsep dasar enkripsi data[2]

2.2. Penggunaan Algoritma Caesar Cipher

Algoritma Caesar Cipher sering digunakan untuk aplikasi dengan tingkat keamanan rendah karena kesederhanaannya. Misalnya, penelitian oleh Ramadhan menunjukkan bahwa metode ini dapat diterapkan dalam Sistem Kasir Restoran berbasis Java .[4]

Selain itu,mengaplikasikan algoritma ini pada sistem informasi akademik berbasis Android, yang menunjukkan fleksibilitasnya dalam berbagai platform teknologi.[9]

2.3. Kelemahan dan Modifikasi Algoritma Caesar Cipher

Caesar Cipher memiliki kelemahan mendasar, yaitu jumlah kunci yang terbatas, yang membuatnya rentan terhadap serangan brute force dan analisis frekuensi. Untuk mengatasi hal ini, Nasution memodifikasi algoritma menggunakan metode Linear Congruent untuk meningkatkan keamanan.[11]

Penelitian lain oleh Farhansyah juga menunjukkan bahwa kombinasi Caesar Cipher dengan algoritma lain dapat meningkatkan ketahanan enkripsi terhadap serangan.[14]

2.4. Aplikasi Praktis pada Sistem Informasi

Implementasi Caesar Cipher pada sistem informasi berbasis web telah diterapkan dalam berbagai kasus. Contohnya, penelitian ini menggunakan algoritma ini untuk mengenkripsi dan mendekripsi data berbasis web, menunjukkan relevansinya dalam skenario dunia nyata[10]

3. METODE PENELITIAN

Penelitian ini diawali dengan studi literatur untuk memahami prinsip dasar kerja Caesar Cipher, mengidentifikasi kelemahannya, serta mengeksplorasi implementasinya dalam sistem kasir restoran berbasis web. Berbagai referensi dimanfaatkan untuk memperdalam pengetahuan tentang keamanan data, pengelolaan basis data, dan pengembangan sistem informasi berbasis web. Studi ini juga dilakukan sebagai upaya untuk menerapkan metode Caesar Cipher dalam menyelesaikan tugas mata kuliah.

Dalam penelitian ini, metode yang digunakan meliputi beberapa tahapan, yaitu:

3.1. Prinsip Enkripsi dan Dekripsi Caesar Cipher

Caesar Cipher mengenkripsi teks dengan menggantikan setiap huruf dalam plaintext dengan huruf lain yang berada pada posisi tertentu di dalam alfabet. Posisi penggantian ini ditentukan oleh sebuah kunci berupa angka yang menunjukkan jumlah pergeseran huruf.

Biasanya proses enkripsi dan dekripsi memerlukan penggunaan kunci, yaitu sejumlah informasi rahasia. Beberapa mekanisme enkripsi menggunakan kunci yang sama untuk enkripsi dan dekripsi, sementara mekanisme lain menggunakan kunci yang berbeda untuk kedua proses tersebut. Dua tipe dasar dari teknologi kriptografi adalah symmetric (secret/private key) cryptography dan *asymmetric (public key) cryptography*. Pada *symmetric key cryptography* (kriptografi kunci simetris), baik pengirim maupun penerima memiliki kunci rahasia yang umum. Pada *asymmetric key cryptography* (kriptografi kunci asimetris), pengirim dan penerima masing-masing berbagi kunci publik dan privat.

Dalam penelitian ini, pendekatan Caesar Cipher termasuk kategori kriptografi simetris.

3.2. Proses Enkripsi

Enkripsi adalah teknik yang digunakan untuk mengamankan informasi dengan cara mengubahnya menjadi bentuk yang tidak dapat dibaca atau dimengerti oleh pihak yang tidak berwenang. Dengan enkripsi, meskipun informasi tersebut jatuh ke tangan yang salah, informasi tersebut tidak akan bisa dipahami tanpa kunci yang benar untuk mendekripsi atau mengembalikannya ke bentuk aslinya.

Proses enkripsi menggunakan rumus berikut:

$$Ci = (Pi + k)26$$

dimana:

a. Ci adalah huruf ciphertext ke-i,
b. Pi adalah huruf plaintext ke-i yang diubah menjadi angka $(A = 0, B = 1, C = 2, \ldots, Z = 25)$,
c. k adalah kunci pergeseran (jumlah posisi pergeseran),
d. 26 adalah jumlah huruf dalam alfabet.

3.3. Proses Dekripsi

Dekripsi merupakan suatu kegiatan yang bertujuan untuk mengembalikan suatu pesan yang telah dikodekan atau dienkripsi ke dalam pesan aslinya atau plaintext. Proses pemulihan isi pesan terenkripsi menggunakan kode tertentu. Dekripsi adalah kebalikan dari enkripsi. Ini adalah proses mengubah pesan asli menjadi pesan terenkripsi atau ciphertext. Proses mengubah teks biasa menjadi teks sandi disebut enkripsi, sedangkan proses mengubah teks sandi menjadi teks biasa disebut dekripsi.

Proses dekripsi menggunakan rumus berikut:

$$Pi = (Ci - k + 26)26$$

dimana:

a. P_i adalah huruf plaintext ke-i,
b. C_i adalah huruf ciphertext ke-i,
c. k adalah kunci pergeseran,
d. 26 adalah jumlah huruf dalam alfabet.

Proses dekripsi ini membalikkan pergeseran yang dilakukan pada enkripsi untuk mengembalikan ciphertext menjadi plaintext.

3.4. Penerapan dan Implementasi Algoritma

Pada aplikasi sistem kasir berbasis web ini, Caesar Cipher digunakan untuk mengamankan data pengguna, seperti password. Meskipun metode ini memberikan perlindungan dasar, penting untuk dicatat bahwa tingkat keamanannya relatif rendah dibandingkan dengan metode lain seperti hashing yang lebih kuat. Penggunaan Caesar Cipher dalam sistem ini bertujuan untuk menjaga kerahasiaan data dalam skenario yang lebih sederhana.

Implementasi algoritma Caesar Cipher dilakukan dengan menggunakan bahasa pemrograman Python dan Java. Proses implementasi mencakup dua tahap utama:

a. Enkripsi: Teks asli diubah menjadi teks terenkripsi (ciphertext) menggunakan pergeseran huruf yang ditentukan oleh kunci.
b. Dekripsi: Teks terenkripsi dikembalikan menjadi teks asli dengan membalik proses pergeseran huruf.

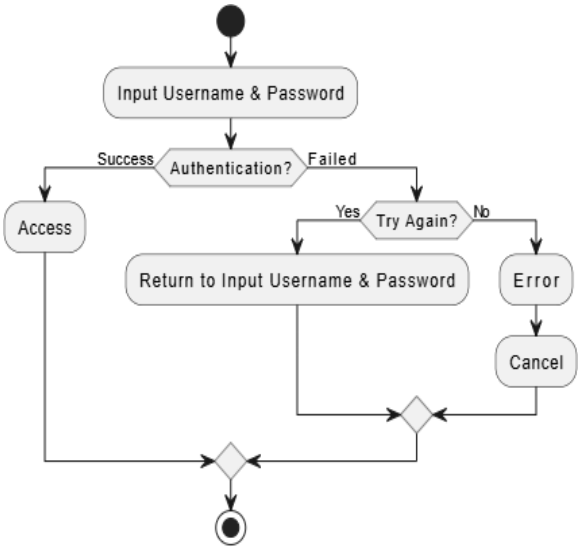
Penelitian ini menggunakan metode Caesar Cipher dengan pergeseran mundur sebanyak 4 langkah dalam proses register dan login pada sistem kasir restoran berbasis web, dengan ketentuan bahwa password sama dengan username.

3.5. Analisis Keamanan

Analisis keamanan dilakukan dengan menguji algoritma Caesar Cipher terhadap serangan brute force dan analisis frekuensi. Dalam serangan brute force, semua kemungkinan kunci diuji hingga teks asli ditemukan. Sementara itu, analisis frekuensi memanfaatkan distribusi kemunculan huruf dalam bahasa tertentu untuk menebak kunci enkripsi. Hasil analisis menunjukkan bahwa Caesar Cipher sangat rentan terhadap kedua jenis serangan ini, terutama karena jumlah kunci yang terbatas (hanya 25 kemungkinan pergeseran huruf).

3.6. Visualisasi Proses

Visualisasi alur kerja Caesar Cipher ditampilkan dalam diagram autentikasi pengguna pada Gambar 1. Diagram ini menunjukkan langkah-langkah proses autentikasi login pengguna menggunakan algoritma Caesar Cipher, termasuk input username dan password, proses enkripsi dan dekripsi, serta penanganan kesalahan autentikasi.



Gambar 1. Diagram Autentikasi dengan Caesar Cipher

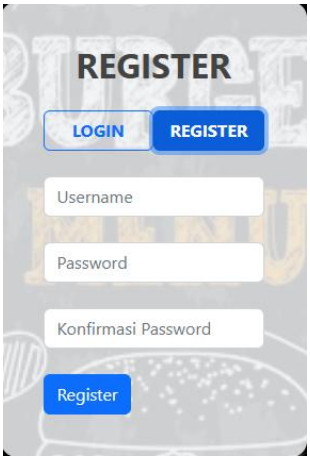
4. HASIL DAN PEMBAHASAN

Hasil penerapan algoritma Caesar Cipher dalam sistem kasir berbasis web ini menunjukkan efektivitas metode ini untuk mengenkripsi data sementara, seperti password. Meskipun efektif dalam konteks tertentu, metode ini memiliki beberapa kelemahan yang perlu diperhatikan, seperti yang telah dijelaskan dalam bagian metode penelitian.

Caesar Cipher dikenal dengan kesederhanaannya, yang menjadikannya pilihan populer untuk tujuan edukasi dan aplikasi dengan tingkat keamanan rendah. Dalam implementasi pada sistem kasir restoran berbasis web ini, algoritma tersebut digunakan untuk mengenkripsi data singkat, seperti password dibagian register dan login sementara dalam sistem informasi yang lebih kecil. Namun, kelemahan utama dari algoritma ini terletak kunci yang terbatas, yang menjadikan sitem kasir restoran berbasis web rentan terhadap serangan brute force dan analisis frekuensi.

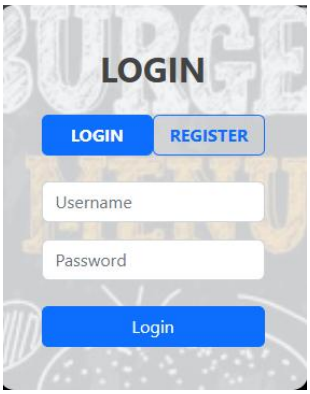
Untuk mengatasi masalah ini, beberapa penelitian mengusulkan untuk memodifikasi algoritma Caesar Cipher dengan menggabungkannya dengan metode kriptografi lain. Salah satu contohnya adalah mengombinasikan Caesar Cipher dengan Vigenère Cipher, yang dapat meningkatkan kerumitan enkripsi dan membuatnya lebih sulit dipecahkan oleh serangan brute force. Di samping itu, penggunaan algoritma ini dalam sistem yang berbasis pada teknologi modern seperti Java dan Android menunjukkan potensi aplikasinya dalam aplikasi yang lebih sederhana.

4.1. Implementasi Website Kasir Restoran



Gambar 2. Halaman Register

Gambar 2 menggambarkan halaman registrasi pada sistem website Kasir Restoran. Di halaman ini, pengguna dapat membuat akun baru dengan mengisi data yang diperlukan, seperti username, password, dan konfirmasi password. Setelah tombol "Register" ditekan, password yang dimasukkan akan dienkripsi menggunakan Caesar Cipher sebelum disimpan di basis data.



Gambar 3. Halaman Login

Gambar 3 menggambarkan halaman login sistem Kasir Restoran berbasis website. Di halaman ini, Anda dapat memasukkan informasi seperti nama pengguna dan kata sandi untuk masuk ke akun terdaftar Anda. Ketika pengguna mengklik tombol "Login", kata sandi yang dimasukkan dienkripsi menggunakan algoritma kriptografi Caesar dan dicocokkan dengan kata sandi terenkripsi di database.

4.2. Hasil Proses Visual data yang Terenkripsi

Dalam penelitian ini, digunakan metode Caesar Cipher dengan teknik enkripsi menggunakan pergeseran mundur sebanyak 4 langkah. Berikut adalah hasil perhitungan angka yang diperoleh dari

proses tersebut. Keterangan password sama dengan username

Y	O	G	A
U	K	C	W

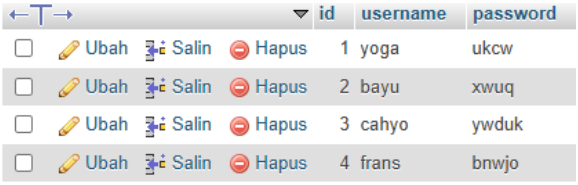
B	A	Y	U
X	W	U	X

C	A	H	Y	O
Y	W	D	U	K

F	R	A	N	S
B	N	W	J	O

Gambar 4. Hasil enkripsi caesar chiper

Pada Gambar 4 ini password di enkripsi menggunakan metode Caesar Chiper.



Gambar 5. Hasil Enkripsi Database (Password sama dengan username)

Gambar 5 menggambarkan proses enkripsi password yang dimasukkan pada halaman registrasi dan login menggunakan algoritma Caesar Cipher dengan pergeseran mundur 4 langkah. Sebagai contoh, kata 'yoga' dienkripsi menjadi 'ukcw' setelah pergeseran tersebut. Meskipun enkripsi ini memberikan lapisan perlindungan dasar, penggunaan algoritma hashing yang lebih aman seperti bcrypt atau SHA-256 sangat disarankan untuk aplikasi dunia nyata.

4.3. Analisis Keamanan pada Implementasi Login Sistem Kasir Restoran Berbasis Web

Algoritma Caesar Cipher yang diterapkan dalam sistem kasir restoran berbasis web memiliki beberapa kelemahan mendasar dalam hal keamanan data. Dengan hanya menyediakan 25 kemungkinan kunci pergeseran, algoritma ini sangat rentan terhadap serangan brute force, di mana seluruh kemungkinan kunci dapat diuji dalam waktu singkat untuk mengungkap kata sandi yang terenkripsi. Selain itu, metode ini tidak menggunakan teknik *salting*, yaitu penyisipan data acak sebelum enkripsi, sehingga kata sandi yang sama akan menghasilkan ciphertext yang identik. Hal ini membuat serangan analisis frekuensi menjadi lebih efektif, karena pola kemunculan karakter tetap terlihat jelas dalam ciphertext. Oleh karena itu, meskipun metode ini mampu memberikan perlindungan dasar dengan mencegah penyimpanan teks asli dalam database, disarankan untuk menggantinya dengan algoritma yang lebih kuat seperti AES atau metode hashing bcrypt yang dilengkapi dengan *salting* untuk meningkatkan keamanan data pengguna secara signifikan.

5. KESIMPULAN DAN SARAN

Algoritma Caesar Cipher berhasil diterapkan pada sistem kasir berbasis web untuk mengenkripsi dan mendekripsi data pengguna seperti password. Hasil penelitian menunjukkan bahwa metode ini melindungi aplikasi dengan kebutuhan keamanan rendah dengan baik. Namun, kelemahan utama algoritma ini adalah jumlah kunci yang terbatas. Ini membuatnya rentan terhadap serangan brute force dan analisis frekuensi. Oleh karena itu, untuk meningkatkan keamanan data, penelitian harus menggabungkan algoritma Caesar Cipher dengan algoritma kriptografi modern seperti AES atau hashing SHA-256. Selain itu, teknik salting harus diterapkan pada proses enkripsi untuk mencegah pola kemunculan data yang identik. Ini dapat menghasilkan sistem keamanan yang lebih kuat dan andal, terutama untuk aplikasi yang memiliki kebutuhan keamanan yang lebih tinggi.

DAFTAR PUSTAKA

[1] F. N. Faqih, M. Tahir, Z. Ashfarina, and ..., “Efektivitas Peningkatan Keamanan Login Pada Website Menggunakan Enkripsi Caesar Chipper,” *J. Adijaya ...*, vol. 01, no. 02, pp. 354–362, 2023.

[2] N. Aulia Putri *et al.*, “RESISTOR Journal | 61 Pengamanan Data Nilai Mahasiswa Menggunakan Algoritma Caesar Chiper dan RSA Berbasis Web”, [Online]. Available: https://s.id/jurnalresistor

[3] D. S. Data *et al.*, “Rancang Bangun Aplikasi Keamanan Data Penjualan Berbasis Web Menggunakan Metode Caesar Cipher Dan Base64 Pada Pabrik Tahu SS,” no. 3, pp. 952–964, 2024.

[4] G. I. Ramadhan and S. Alfarisi, “Penerapan Caesar Cipher Pada Absensi Dan Cuti Karyawan PT. Datacomindo Mitrausaha Berbasis Java,” *JRKT (Jurnal Rekayasa Komputasi Ter.*, vol. 1, no. 04, pp. 247–255, 2021, doi: 10.30998/jrkt.v1i04.6158.

[5] P. G. Pamungkas and A. H. Muhammad, “Modifikasi Algoritma Kriptografi Caesar Chiper pada Deretan Simbol dan Huruf di Smarphone dan Laptop,” *J. Inf. Technol.*, vol. 2, no. 1, pp. 1–5, 2022, doi: 10.46229/jifotech.v2i1.234.

[6] F. Harris and R. E. Sari, “Meningkatkan Keamanan Source Code Web Melalui Teknik Enkripsi dan Dekripsi Dengan Metode Reverse Cipher dan Caesar Cipher Improving Web Source Code Security Through Encryption and Decryption Techniques Using Reverse Cipher and Caesar Cipher Methods,” *Januari*, no. 2, p. 405, 2024, [Online]. Available: http://kti.potensi-utama.ac.id/index.php/JID

[7] J. Pendidikan and P. Jpp, "CHIPER DAN PLAYFAIR CIPHER PADA SISTEM KEAMANAN Jurnal Pendidikan dan," vol. 6, pp. 61–71, 2024.

[8] R. Ridho, C. Bisri, and A. M. Harahap, "Penerapan Kriptografi Enkripsi Dan Deskripsi Dalam Pendataan Pasien Klinik Mama Harfas Tembung Menggunakan Visual Basic," *J. Penelit. Dan …*, vol. 2, no. 1, pp. 30–33, 2023, [Online]. Available: http://www.jurnal.unidha.ac.id/index.php/jppie/article/view/676

[9] A. A. Amsyari and B. Gunawan, "Perancangan Dan Implementasi Caesar Chiper Untuk Meningkatkan Keamanan Sistem Informasi Akademik Sekolah Berbasis Android," *… J. Teknol. dan …*, no. 3, pp. 151–161, 2024, [Online]. Available: https://journal.arteii.or.id/index.php/Saturnus/article/view/205%0Ahttps://journal.arteii.or.id/index.php/Saturnus/article/download/205/350

[10] M. Harun Alfirdaus *et al.*, "Perancangan Aplikasi Enkripsi Deskripsi Mengunakan Metode Caesar Chiper Berbasis Web," *Jtmei)*, vol. 2, no. 2, pp. 64–76, 2023.

[11] S. Darma Nasution, "Pengamanan Perintah Koneksi ke Database MySQL Menggunakan Algoritma Caesar Cipher dan Algoritma Stout Codes," *Bull. Inf. Technol.*, vol. 5, no. 1, pp. 9–16, 2024, doi: 10.47065/bit.v5i1.1149.

[12] B. G. & R. P. Ritwiyan, "Implementasi Kriptografi Pada Web Service Dengan Metode Caesar Cipher," *Skanika*, vol. 4, no. 1, pp. 39–44, 2021.

[13] S. D. Nasution, "Modifikasi Algoritma Caesar Cipher Menggunakan Linear Congruent Method Untuk Mengamankan Data," vol. 01, no. 03, pp. 95–101, 2024.

[14] F. Farhansyah, M. F. Atila, A. Ridho, and M. Aldrin, "Implementasi Kriptografi Caesar Chiper dalam Mengubah Pesan Teks Terenkripsi," vol. 3, no. 1, pp. 62–68, 2024.

[15] Uci Julya Ningsih, Sophia Salsabila, Isniar Hutapea, Dewi Santika, and Indra Gunawan, "Pendekripsian Caesar Chiper Dengan Menggunakan Teknik-Teknik Kriptanalisis," *J. Ilmu Komput. dan Multimed.*, vol. 1, no. 1, pp. 11–15, 2024, doi: 10.46510/ilkomedia.v1i1.10.

[16] N. A. Nanda, S. M. S. Silalahi, D. Fatricia Nasution, M. Sari, and I. Gunawan, "Kriptografi dan Penerapannya Dalam Sistem Keamanan Data," *J. Media Inform.*, vol. 4, no. 2, pp. 90–93, 2023, doi: 10.55338/jumin.v4i2.428.