JSI : Jurnal Sistem Informasi *(E-Journal), VOL. 17, NO.1, April 2025*
ISSN Print : 2085-1588
ISSN Online : 2355-4614
LINK: https://jsi.ejournal.unsri.ac.id/index.php/jsi/index

Kriptografi Klasik dan Keamanan Dasar : Implementasi Kasir Restoran dengan Pendekatan Metode Caesar Cipher

Yoga Pratama[1], Bayu Maulana Ayassy[2], Cahyo Hidayatullah[3], Frans Putra Sinaga[4], Ahmad Turmudi Zy[5]
[1,2,3,4] Teknik Informatika, Teknik, Universitas Pelita Bangsa
e-mail: yogapratama.312210042@mhs.pelitabangsa.ac.id, bayuayassy.312210166@mhs.pelitabangsa.ac.id, cahyo.312210079@mhs.pelitabangsa.ac.id, fransputrasinaga046mhs.pelitabangsa.ac.id

Abstrak

Penelitian ini membahas penerapan algoritma Caesar Cipher dalam meningkatkan keamanan data pada sistem kasir restoran berbasis web. Proses enkripsi dan dekripsi dilakukan dengan metode sederhana, yaitu menggeser huruf berdasarkan kunci tertentu. Algoritma ini diterapkan untuk mengenkripsi kata sandi pengguna sebelum disimpan di dalam basis data, memberikan lapisan keamanan tambahan. Namun, algoritma ini memiliki keterbatasan karena rentan terhadap serangan brute force dan analisis frekuensi akibat jumlah kunci yang terbatas. Penelitian ini mengilustrasikan penerapan Caesar Cipher dalam melindungi data pengguna, sekaligus mengidentifikasi kelemahan utamanya. Hasil penelitian menunjukkan bahwa algoritma ini lebih cocok digunakan pada aplikasi dengan kebutuhan keamanan rendah. Selain itu, penelitian ini menyoroti perlunya menggunakan algoritma yang lebih kuat, seperti AES atau metode hashing bcrypt dan SHA-256, untuk melindungi data secara lebih efektif. Temuan ini juga membuka peluang untuk mengombinasikan Caesar Cipher dengan metode enkripsi lainnya sebagai langkah inovatif dalam meningkatkan keamanan sistem informasi di masa depan.

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

Abstract

This research discusses the application of the Caesar Cipher algorithm in improving data security in web-based restaurant cashier systems. The encryption and decryption process is carried out in a simple way, namely shifting letters based on a certain key. This algorithm is implemented to encrypt user passwords before they are stored in the database, thereby providing an additional layer of security. However, this algorithm has limitations because it is vulnerable to brute force attacks and frequency analysis due to the limited number of keys. This research describes the application of Caesar Cipher in protecting user data, while identifying its main weaknesses. The research results show that this algorithm is more suitable for use in applications with low security requirements. Additionally, this research highlights the need to use stronger algorithms, such as AES or bcrypt and SHA-256 hashing methods, to protect data more effectively. This finding also opens up opportunities to combine Caesar Cipher with other encryption methods as an innovative step in improving the security of information systems in the future.

Keywords*: Caesar Cipher, Data Encryption, Web-Based Restaurant Cashier System, Password Security, Cryptographic Vulnerability*

1. PENDAHULUAN

Semakin maju teknologi, semakin meningkat pula risiko keamanannya. Dalam hal ini keamanan dan privasi adalah aspek yang sangat penting dalam hal data.[1] Keamanan data menjadi aspek yang harus diperhatikan didalam perkembangan teknologi, dimana

data yang diolah atau yang dikirim dalam suatu transmisi data bisa saja jatuh ke pihak-pihak yang tidak bertanggung jawab.[2] Dalam melakukan perjalanan bisnis, data merupakan salah satu bagian terpenting dalam lingkungan bisnis. Data yang memuat informasi, baik 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]

Pengamanan terhadap suatu data semakin hari juga semakin berkembang, hal ini dikarenakan banyak algoritma kriptografi telah dapat dipecahkan oleh perangkat lunak yang memang dibuat untuk memecahkan algoritma-algoritma kriptografi. Selain menerapkan algoritma kriptografi yang baru, biasanya banyak peneliti memodifikasi suatu algoritma kriptografi. Tentu saja hal ini bukanlah suatu pekerjaan yang mudah.[2]

Kriptografi merupakan bagian ilmu yang mempelajari tentang cara menjaga agar data atau pesan tetap aman.[5] 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.[6] 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.[7] 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).[8] 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.[9] 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.[10] 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.[11] Oleh karena itu, enkripsi Caesar Cipher menjadi salah satu pilihan yang populer untuk meningkatkan keamanan login pada website.[11] 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.[12]

Caesar Cipher adalah salah satu teknik kriptografi yang sederhana namun efektif dalam memperbaiki keamanan data.[13] Regular expression adalah sebuah urutan

karakter yang dapat mencari sebuah pola. Pola pencarian kata atau teks memerlukan sebuah algoritma yang diatur dalam regular expression itu sendiri, yang membedakan regex (regular expression) dengan string biasa yaitu meta characters atau token di mana terdapat karakter- karakter khusus yang memiliki sebuah arti atau maksud tersendiri dalam pola pencarian, karakter-karakter ini tidak akan di cocokan secara literal dengan karakter itu sendiri, tapi mewakili sekelompok karakter lain atau pola khusus tertentu.[14] 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 algoritme 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”.[15]

Pengirim pesan harus dapat memastikan bahwa pesan yang dikirim benar-benar terjaga keamanan, tidak ada informasi yang diganti atau dikurangi, sehingga informasi sampai kepada penerima sesuai dengan keadaan semula dari pengirim informasi. Proses pengaman informasi dapat dilakukan dengan beberapa algoritma kriptografi yang tersedia. Algoritma kriftografi terdiri dari dua era yaitu, algoritma klasik dan algoritma modern. sedangkan kunci pada kriptografi terdiri dari kunci private dan kunci publik.[16]

Dalam tinjauan literatur, Beberapa peneliti telah melakukan inovasi dengan memodifikasi algoritma kriptografi sehingga dapat menigkatkan kemanan pada penggunaan algoritma tersebut.[17] Sebagai contoh, penelitian yang dilakukan oleh Algoritma Caesar Cipher pada Pengenkripsian Pesan Teks, 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.[18] 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.[8]

Tujuan penulisan untuk laporan tugas akhir ini adalah mengimplementasikan enkripsi pada web kasir retoram dengan algoritme kriptografi Caesar Cipher, lalu data tersebut akan didekripsikan oleh client side dengan algoritme kriptografi Caesar Cipher.[15] penelitian ini dapat memberikan kontribusi penting dalam pengembangan sistem keamanan informasi yang lebih kokoh di masa depan.[19] Dengan memahami secara mendalam tentang cara kerja teknik-teknik kriptanalisis ini dapat memberikan wawasan yang berharga dalam mengembangkan sistem keamanan[20] 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.[19]

2. METODE

Penelitian dimulai dengan studi literatur untuk memahami prinsip kerja Caesar Cipher, kelemahannya, serta implementasi dalam Sebuah aplikasi. Beberapa referensi digunakan untuk mendalami pengamanan data, basis data, dan sistem informasi berbasis web. Studi ini juga dilakukan untuk menginplementasikan metode caesar chiper dalam menyelesaikan tugas mata kuliah kami.

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

2.1 Enkripsi dan Dekripsi Caesar Cipher

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

2.1.1 Enkripsi

Proses enkripsi menggunakan rumus berikut:

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

dimana:

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

Setiap huruf dalam plaintext digeser sebanyak k posisi di dalam alfabet untuk meng- hasilkan ciphertext.

2.1.2 Dekripsi

Proses dekripsi menggunakan rumus berikut:

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

dimana:

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

Proses dekripsi ini membalikkan pergeseran yang dilakukan pada enkripsi untuk mengem- balikan ciphertext menjadi plaintext.

2.2 Implementasi Algoritma

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

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

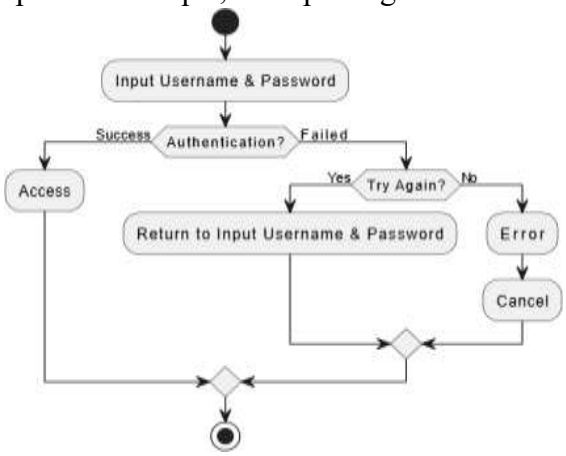
Dalam penelitian ini, implementasi dilakukan pada data simulasi berupa pesan teks dan data sederhana seperti nilai mahasiswa dan informasi pengguna.

2.3 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).

2.4 Visualisasi Proses

Visualisasi alur kerja Caesar Cipher ditampilkan dalam diagram autentikasi pengguna pada Gambar 1. Diagram ini menunjukkan langkah-langkah proses autentikasi 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

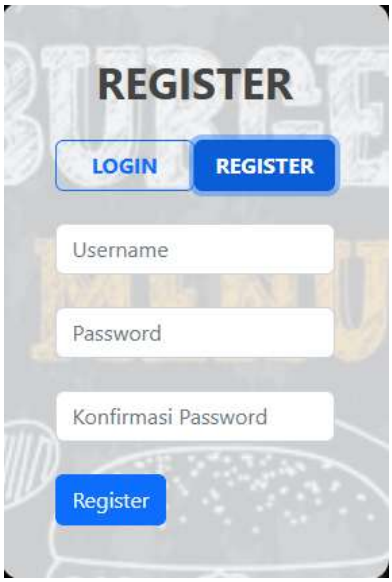
3. HASIL DAN PEMBAHASAN

Caesar Cipher memiliki karakteristik sederhana, sehingga sering digunakan untuk tujuan edukasi dan dalam aplikasi dengan tingkat keamanan rendah. Dalam implementasi prak- tis, Caesar Cipher digunakan untuk mengenkripsi teks pendek seperti password, pesan rahasia, atau data sementara dalam sistem informasi kecil. Namun, kelemahan utama al- goritma ini terletak pada sifat deterministiknya dan jumlah kunci yang terbatas, sehingga rentan terhadap serangan brute force dan analisis frekuensi.

JSI : Jurnal Sistem Informasi *(E-Journal), VOL. 17, NO.1, April 2025*
ISSN Print : 2085-1588
ISSN Online : 2355-4614
LINK: https://jsi.ejournal.unsri.ac.id/index.php/jsi/index

Untuk mengatasi kelemahan tersebut, beberapa penelitian mengusulkan modifikasi algoritma Caesar Cipher dengan menggabungkannya dengan metode kriptografi lain. Misalnya, kombinasi Caesar Cipher dengan Vigenere Cipher dapat meningkatkan kom- pleksitas enkripsi, sehingga lebih sulit dipecahkan oleh serangan brute force. Selain itu, penerapan algoritma dalam sistem berbasis teknologi modern seperti Java dan Android menunjukkan potensi penggunaannya dalam aplikasi sederhana.

3.1. Implementasi Website Kasir Restoran

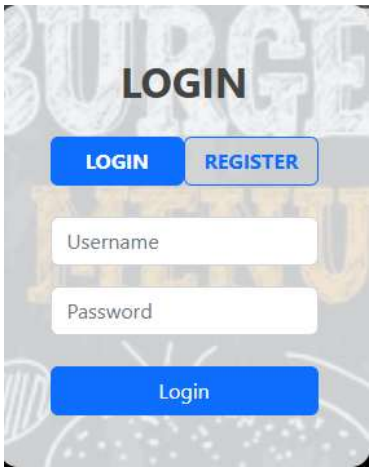


Gambar 2. Registrasi Website Kasir Restoran

Gambar 2 adalah halaman registrasi pada sistem website Kasir Resto Duo Saudara. Pada halaman ini, pengguna dapat mendaftarkan akun baru dengan mengisi informasi yang diperlukan, seperti username, password dan Konfirmasi Password. Setelah pengguna menekan tombol "Register" password yang dimasukkan akan dienkripsi menggunakan algoritma Caesar Cipher sebelum disimpan ke dalam basis data.

Gambar 3 adalah halaman login sistem website Kasir Resto Duo Saudara. 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.

JSI : Jurnal Sistem Informasi *(E-Journal), VOL. 17, NO.1, April 2025*
ISSN Print : 2085-1588
ISSN Online : 2355-4614
LINK: https://jsi.ejournal.unsri.ac.id/index.php/jsi/index



Gambar 3. Login Website Kasir Restoran

3.2. Hasil Plaintext Database

	id	username	password
Ubah Salin Hapus	1	yoga	ukcw
Ubah Salin Hapus	2	bayu	xwuq
Ubah Salin Hapus	3	cahyo	ywduk
Ubah Salin Hapus	4	frans	bnwjo

Gambar 4. Hasil Enkripsi Database

Gambar ini menunjukkan tabel basis data dengan kolom "ID", "Nama Pengguna", dan "Kata Sandi". Kolom kata sandi berisi hasil enkripsi menggunakan metode Caesar Chiper. Ini menunjukkan bahwa kata sandi asli dienkripsi sebelum disimpan dalam basis data, menggunakan algoritma seperti Caesar Cipher. Meskipun enkripsi ini menyediakan lapisan keamanan tambahan, skema seperti Caesar Cipher masih rentan terhadap serangan, jadi dalam aplikasi dunia nyata, algoritma hashing yang lebih kuat seperti bcrypt atau SHA-256 sering digunakan. Sebaiknya lakukan itu.

4. KESIMPULAN

Terlepas dari kelebihannya dalam kesederhanaan dan kemudahan implementasi, algoritma Caesar Cipher tidak lagi cocok untuk digunakan dalam sistem keamanan informasi modern karena kelemahan yang signifikan terhadap serangan brute force dan analisis frekuensi.

Pada penelitian ini implementasi Caesar Cipher pada sistem kasir restoran menunjukkan bahwa algoritma ini dapat digunakan untuk proses enkripsi sederhana,

seperti melindungi password pengguna sebelum disimpan dalam database.Namun, penelitian ini juga menyoroti perlunya algoritma enkripsi yang lebih kuat seperti AES dan algoritma hashing seperti bcrypt dan SHA-256 untuk memastikan keamanan data yang lebih tinggi.

Melalui penelitian ini, kami memperoleh pemahaman lebih dalam tentang cara kerja Caesar cipher, kelemahannya, dan potensi modifikasi untuk meningkatkan keamanannya. Penelitian ini juga memberikan wawasan bahwa aspek keamanan perlu dipertimbangkan secara holistik ketika mengintegrasikan algoritma kriptografi ke dalam aplikasi modern seperti sistem berbasis web.

Di masa depan, menggabungkan algoritma kriptografi Caesar dengan metode enkripsi lainnya dapat menjadi dasar eksperimen lebih lanjut guna membangun sistem yang lebih aman dan efisien.

REFERENCES

[1] 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

[2] S. Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti, P. Keamanan Kriptografi Caesar Cipher dengan Menerapkan Algoritma Kompresi, S. Codes, and S. Darma Nasution, “Terakreditasi SINTA Peringkat 2,” *masa berlaku mulai*, vol. 1, no. 3, pp. 1209–1215, 2017.

[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] R. Febrianingsih, A. Hafiz, and M. Informatikan, “Jurnal Informasi Dan Komputer Vol : 7 No : 2 Thn .: 2019 IMPLEMENTASI KRIPTOGRAFI BERBASIS CAESAR CHIPER UNTUK Jurnal Informasi Dan Komputer Vol : 7 No : 2 Thn .: 2019,” *Anal. Infrastruktur Teknol. Inf. Menggunakan Framew. Cobit 4.1*, vol. Vol :7, pp. 81–86, 2019.

[6] 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.

[7] 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

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

[9] 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

[10] 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

[11] 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.

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

[13] 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.

[14] S. Admissions, M. K. Fauzi, and A. Setiawan, "Implementasi Algoritma Vigenere Chiper dan Caesar Chiper Untuk Pengamanan Password Dalam Penerimaan Siswa Baru," no. 3, 2024.

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

[16] Noviyanti. P and Mira, "Analisa Algoritma Kriptografi Klasik Caesar Cipher Viginere Cipher dan Hill Cipher – Study Literature," *J. Inf. Technol.*, vol. 2, no. 1, pp. 23–30, 2022, doi: 10.46229/jifotech.v2i1.387.

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

[18] 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.

[19] 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.

[20] 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.