Digital Transformation Technology (Digitech) | e-ISSN: 2807-9000
Volume 5, **Number** 1, Maret 2025
https://doi.org/10.47709/digitech.v5i1.5984

Analysis dan Implementasi Algoritma Caesar Chiper Dalam Pengamanan Pesan Teks Berbasis Web di Desa

Eka Aprianti[1*],Ahmad Marsehan[2]
[1,2]Universitas PGRI Silampari, Indonesia
[1]ekaafrnt@gmail.com, [2]ahmadmarsehan @gmail.com

open access
Histori Artikel:
Diajukan: 30 Mei 2025
Disetujui: 18 Juni 2025
Dipublikasi: 22 Juni 2025
Kata Kunci:
Caesar Chiper; Algoritma Caesar Chiper; Vigenere Cipher; Kiptografi klasik; Algoritma Modern

Abstrak
Dalam era digital, kebutuhan akan keamanan informasi menjadi sangat krusial, terutama dalam komunikasi berbasis web. Desa-desa dengan infrastruktur teknologi yang masih terbatas sering kali menjadi target rawan kebocoran data akibat lemahnya sistem keamanan. Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan algoritma Caesar Cipher sebagai salah satu bentuk pengamanan pesan teks berbasis web yang sederhana namun fungsional. Caesar Cipher merupakan algoritma kriptografi klasik yang bekerja dengan metode pergeseran huruf dalam alfabet untuk menyandikan pesan. Meskipun tergolong lemah terhadap serangan brute-force dan analisis frekuensi, algoritma ini tetap relevan untuk aplikasi dasar dan edukasi mengenai konsep enkripsi. Penelitian dilakukan dengan membangun sistem web sederhana yang mengintegrasikan algoritma Caesar Cipher dalam proses pengiriman dan penerimaan pesan. Hasil implementasi menunjukkan bahwa algoritma ini mampu memberikan tingkat pengamanan dasar yang cukup efektif untuk skala penggunaan terbatas di desa. Selain itu, penelitian ini juga membuka peluang pengembangan lebih lanjut dengan mengombinasikan Caesar Cipher dengan metode keamanan lainnya guna meningkatkan ketahanan terhadap serangan siber.

PENDAHULUAN

Penelitian-penelitian sebelumnya telah membahas berbagai pendekatan dalam menjaga keamanan pesan teks, baik melalui metode kriptografi klasik maupun modern. Ramadhan et al. (2020) menunjukkan bahwa algoritma Caesar Cipher masih efektif digunakan untuk kebutuhan enkripsi dasar karena sifatnya yang sederhana dan mudah diimplementasikan. Sari dan Nugroho (2021) membandingkan Caesar Cipher dengan algoritma lain dari sisi kecepatan proses dan tingkat kompleksitas. Penelitian oleh Andika (2019) lebih menyoroti penerapan Caesar Cipher dalam aplikasi desktop, sehingga belum menyentuh aspek implementasi berbasis web yang lebih relevan untuk kebutuhan komunikasi desa digital. Sementara itu, Lestari dan Prasetyo (2020) mengkaji keamanan pesan dalam aplikasi populer seperti WhatsApp, namun belum secara khusus membahas penerapannya dalam konteks lokal seperti pelayanan publik di desa. Handayani et al. (2022) menekankan pentingnya sistem komunikasi yang aman dalam penyelenggaraan layanan publik desa, tetapi tidak secara rinci membahas implementasi algoritma enkripsi tertentu.

Tujuan penelitian ini adalah untuk menganalisis dan mengimplementasikan algoritma Caesar Cipher dalam sistem pengiriman pesan berbasis web yang sederhana dan mudah diadopsi oleh perangkat desa**.** Penelitian ini diharapkan dapat memberikan solusi enkripsi dasar yang ringan, praktis, dan relevan untuk meningkatkan keamanan komunikasi digital di lingkungan pemerintahan desa, tanpa memerlukan sumber daya teknologi maupun keahlian teknis yang tinggi.

STUDI LITERATUR

Penelitian ini dilakukan tidak terlepas dari kajian penelitian terdahulu yang dijadikan sebagai dasar pembanding dan landasan teori. Kajian penelitian terdahulu adalah penelitian-penelitian yang telah dilakukan sebelumnya dan digunakan sebagai referensi untuk mendukung pengembangan sistem pengamanan pesan berbasis web menggunakan algoritma Caesar Cipher.Berdasarkan penelitian yang dilakukan oleh Ramadhan et al. (2020) dalam jurnalnya yang berjudul "Penerapan Algoritma Caesar Cipher untuk Pengamanan Pesan Teks pada Aplikasi Sederhana", algoritma Caesar Cipher dinilai efektif untuk enkripsi dasar karena kemudahannya dalam implementasi dan kecepatannya dalam proses enkripsi serta dekripsi. Hal ini menjadi landasan awal dalam pemilihan algoritma Caesar Cipher untuk skala sistem sederhana. Selanjutnya, Sari dan Nugroho (2021) dalam penelitiannya yang membandingkan Caesar Cipher dengan algoritma kriptografi lainnya seperti Vigenère Cipher menunjukkan bahwa Caesar Cipher unggul dari sisi kecepatan namun memiliki kelemahan dari sisi keamanan. Penelitian ini relevan untuk menunjukkan posisi Caesar Cipher dalam konteks algoritma klasik dan memberikan justifikasi bahwa algoritma ini cocok untuk sistem dengan kebutuhan keamanan dasar seperti pada perangkat desa. Penelitian lain yang dilakukan oleh Andika (2019) meneliti implementasi Caesar Cipher dalam aplikasi desktop.

Penelitian ini menunjukkan bahwa algoritma Caesar Cipher cukup fleksibel untuk diintegrasikan ke dalam aplikasi, meskipun belum dikembangkan untuk sistem berbasis web. Hal ini membuka peluang untuk mengadopsi algoritma tersebut dalam bentuk aplikasi web sederhana seperti yang dilakukan dalam penelitian ini. Sementara itu, Lestari dan Prasetyo (2020) membahas aspek keamanan pesan dalam aplikasi WhatsApp, yang menunjukkan urgensi perlindungan data pada media komunikasi. Namun, fokus penelitiannya tidak secara spesifik menyasar pengamanan data di tingkat lokal seperti perangkat desa, sehingga konteks desa masih menjadi celah yang belum banyak dibahas.Terakhir, Handayani et al. (2022) dalam jurnalnya menekankan pentingnya pengembangan sistem komunikasi yang aman dalam layanan publik desa, tetapi belum membahas secara rinci tentang implementasi algoritma tertentu seperti Caesar Cipher. Penelitian ini memperkuat urgensi keamanan informasi di lingkungan desa yang mulai terdigitalisasi. Berdasarkan kajian literatur di atas, dapat disimpulkan bahwa meskipun algoritma Caesar Cipher telah banyak diteliti, masih terdapat celah dalam hal implementasinya pada sistem web sederhana yang dapat digunakan oleh perangkat desa. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan sistem pengiriman pesan berbasis web dengan pengamanan menggunakan algoritma Caesar Cipher yang sederhana, mudah dipahami, dan relevan dengan kondisi teknologi di desa.

METODE PENELITIAN

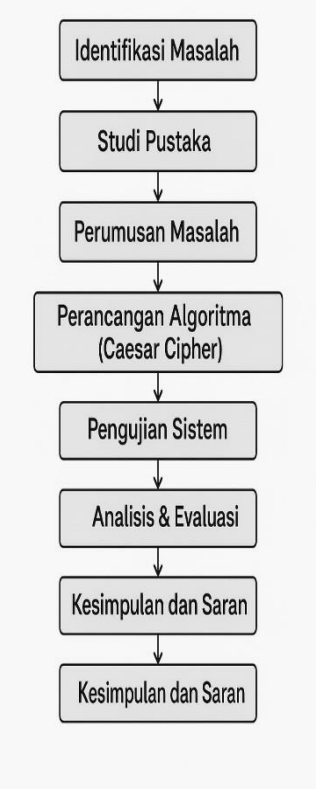
Penelitian ini menggunakan metode rekayasa perangkat lunak (Software Engineering Method) dengan pendekatan pengembangan sistem berbasis pengamatan kebutuhan pengguna (user need analysis) dan pengujian fungsionalitas aplikasi**.** Model pendekatan yang digunakan adalah Waterfall Model**,** yaitu model pengembangan sistem berurutan dari tahap analisis kebutuhan hingga tahap implementasi.

Metode ini dipilih karena sesuai untuk pengembangan aplikasi dengan spesifikasi yang sudah jelas dan tidak banyak mengalami perubahan selama proses pengembangan.
Penelitian ini dilakukan melalui beberapa tahapan berikut:

1. Desain Penelitian : Tahap awal ini bertujuan untuk menyusun kerangka kerja penelitian secara sistematis agar pelaksanaan berjalan terarah dan terstruktur (Mulyadi, 2013). Desain ini meliputi penentuan objek penelitian, tujuan, serta pendekatan pengumpulan data.
2. Identifikasi Masalah :Peneliti menganalisis permasalahan utama, yaitu lemahnya keamanan dalam proses pengiriman pesan berbasis web di lingkungan perangkat desa. Banyak pesan dikirim tanpa enkripsi, sehingga mudah disadap atau diubah isinya.
3. Perumusan Masalah : Masalah dirumuskan dalam bentuk pertanyaan: Bagaimana mengamankan pesan teks berbasis web dengan metode Caesar Cipher yang sederhana namun efektif untuk digunakan oleh perangkat desa?
4. Studi Pustaka dan Teori Pendukung : Mengkaji literatur dan penelitian terdahulu yang berkaitan dengan kriptografi, Caesar Cipher, serta penerapan sistem keamanan informasi.
5. Perancangan Algoritma Caesar Cipher : Algoritma Caesar Cipher dirancang dengan metode substitusi karakter, di mana setiap huruf pada pesan digeser sejumlah nilai tertentu (kunci). Algoritma ini akan diintegrasikan ke dalam program desktop.
6. Perancangan dan Pengembangan Aplikasi**:** Aplikasi dirancang berbasis desktop menggunakan Visual Basic. Fitur utama aplikasi meliputi:

    1. Menu Login dan Logout
    2. Menu Enkripsi (untuk mengubah pesan asli menjadi terenkripsi)
    3. Menu Dekripsi (untuk mengubah pesan terenkripsi kembali ke bentuk semula)

7. Pengujian dan Evaluasi Sistem : Aplikasi diuji menggunakan skenario pengiriman dan penerimaan pesan, untuk mengukur efektivitas fungsi enkripsi dan dekripsi. Evaluasi dilakukan dari segi fungsi, kecepatan proses, dan kemudahan penggunaan oleh pengguna non-teknis. Dalam penelitian ini, proses pengembangan sistem dilakukan secara bertahap melalui beberapa tahapan yang sistematis. Setiap tahapan saling berkaitan dan bertujuan untuk menghasilkan sistem enkripsi pesan teks yang efektif menggunakan algoritma Caesar Cipher. Adapun alur metodologi penelitian yang digunakan dapat dilihat pada Gambar 1 berikut:



Gambar 1. Tahapan Metodologi Penelitian Menggunakan Algoritma Caesar Cipher

Gambar 1 menunjukkan alur metodologi penelitian yang dimulai dari identifikasi masalah, studi pustaka, hingga perancangan algoritma dan pengujian sistem. Setelah sistem diuji, dilakukan analisis serta evaluasi hasil untuk mengetahui efektivitas metode yang digunakan. Langkah akhir berupa penyusunan kesimpulan dan saran menjadi bagian penting sebagai refleksi terhadap hasil yang telah diperoleh, serta sebagai dasar rekomendasi untuk penelitian selanjutnya.

HASIL

Tampilan Antar Muka Dan Hasil Implementasi

Sistem enkripsi-dekripsi berbasis Caesar Cipher yang dikembangkan ditujukan untuk memenuhi kebutuhan komunikasi internal yang aman di lingkungan pemerintahan desa. Untuk memastikan kemudahan penggunaan, antarmuka sistem dirancang dengan pendekatan sederhana, ringan, dan intuitif, sehingga dapat dioperasikan oleh pengguna awam sekalipun. Tampilan utama sistem terdiri dari tiga menu utama, yaitu Enkripsi, Dekripsi, dan Tentang Sistem, yang terletak di bagian atas halaman. Navigasi yang rapi dan tata letak elemen yang minimalis mendukung kenyamanan pengguna dalam menjelajahi aplikasi. Pada halaman utama, pengguna akan menemukan deskripsi singkat mengenai fungsi sistem dan cara kerjanya. Ini penting sebagai pengantar, terutama bagi pengguna baru yang belum familiar dengan konsep enkripsi. Saat pengguna memilih menu *Enkripsi*, sistem menampilkan sebuah form interaktif yang terdiri dari kolom input untuk memasukkan pesan asli yang ingin dienkripsi dan kolom kunci pergeseran (*shift key*) sebagai parameter utama dalam algoritma Caesar Cipher. Setelah pengguna menekan tombol “Enkripsi”, hasil pesan yang telah dikodekan akan muncul di bawah form secara otomatis. Proses ini memungkinkan pengguna memahami bagaimana teks dapat diubah menjadi format yang tidak mudah dibaca tanpa kunci yang sesuai. Begitu pula pada halaman *Dekripsi*, pengguna diberikan form untuk memasukkan pesan terenkripsi serta kunci pergeseran yang digunakan sebelumnya. Dengan menekan tombol “Dekripsi”, sistem akan memproses pesan dan menampilkan hasil pesan asli secara langsung. Desain halaman ini menekankan pengalaman yang efisien dan minim gangguan visual, sehingga pengguna dapat fokus pada fungsi utama sistem.

Berikut ditampilkan dokumentasi visual dari antarmuka halaman utama sistem:

Gambar 2. Tampilan Antarmuka Sistem Enkripsi-Dekripsi Berbasis Caesar Cipher

Gambar 2 menunjukkan antarmuka dari halaman enkripsi dan dekripsi pada sistem enkripsi-dekripsi berbasis algoritma Caesar Cipher yang dikembangkan untuk mendukung keamanan komunikasi internal di lingkungan pemerintahan desa. Bagian Atas (Halaman Enkripsi) Antarmuka halaman enkripsi menyediakan dua kolom input utama. Kolom pertama bertuliskan "Pesan", yang digunakan untuk memasukkan teks asli yang akan dienkripsi. Kolom kedua adalah "Kunci Pergeseran" (Shift Key), yang berfungsi sebagai parameter algoritma Caesar Cipher dalam menentukan seberapa jauh pergeseran huruf dilakukan. Setelah pengguna mengisi kedua kolom ini dan menekan tombol "Enkripsi", sistem akan secara otomatis menghasilkan pesan terenkripsi dan menampilkannya di bawah form tersebut. Bagian Bawah (Halaman Dekripsi) Antarmuka halaman dekripsi menampilkan dua kolom input pula. Kolom "Pesan Terenkripsi" ditujukan untuk memasukkan teks yang sebelumnya telah dienkripsi menggunakan metode Caesar Cipher. Kolom "Kunci Pergeseran" harus diisi dengan nilai pergeseran yang sama seperti saat proses enkripsi. Setelah tombol "Dekripsi" ditekan, sistem akan memproses data dan menampilkan hasil berupa teks asli secara langsung.Tampilan yang sederhana dan konsisten antara halaman enkripsi dan dekripsi mencerminkan desain yang ramah pengguna dan mudah dioperasikan oleh perangkat desa, termasuk mereka yang tidak memiliki latar belakang teknis. Gambar ini sekaligus merupakan dokumentasi visual dari hasil implementasi sistem pada tahap pengujian.

Halaman Tentang Sistem berfungsi sebagai sarana edukatif. Di dalamnya terdapat penjelasan mengenai tujuan pembuatan sistem ini, yakni untuk mendukung keamanan komunikasi digital skala kecil di desa. Selain itu, dijelaskan pula prinsip kerja algoritma Caesar Cipher yang hanya menggeser karakter huruf dengan sejumlah nilai tertentu. Penjelasan ini disampaikan dengan bahasa yang sederhana, agar mudah dipahami oleh pengguna non-teknis. Hal ini menunjukkan bahwa sistem tidak hanya berfungsi sebagai alat bantu teknis, tetapi juga sebagai media pembelajaran keamanan informasi dasar.Keunggulan utama sistem ini terletak pada kesederhanaan dan keringanannya. Aplikasi dapat dijalankan melalui browser tanpa memerlukan instalasi atau konfigurasi tambahan. Bahkan, sistem ini dapat dioperasikan secara offline**,** yang sangat berguna bagi wilayah pedesaan dengan keterbatasan akses internet. Penggunaan algoritma Caesar Cipher yang mudah dipahami membuat sistem ini ideal untuk digunakan oleh perangkat desa dalam mengamankan pesan-pesan singkat seperti catatan internal, pengingat rapat, atau instruksi antar staf. Namundemikian, sistem ini memiliki beberapa keterbatasan yang penting untuk dicatat. Dari sisi keamanan, Caesar Cipher merupakan algoritma klasik yang mudah dipecahkan jika diketahui

metodenya. Hal ini menjadikannya tidak cocok untuk mengamankan data yang bersifat sangat sensitif, seperti informasi pribadi penduduk atau data keuangan desa. Selain itu, sistem ini belum mendukung enkripsi dengan kunci rahasia yang kompleks karena hanya mengandalkan pergeseran huruf antara 0 hingga 25, sehingga jumlah kombinasi sangat terbatas. Fitur manajemen pengguna seperti sistem login juga belum tersedia, sehingga sistem belum dapat membedakan antara pengguna yang berwenang dan umum, yang pada akhirnya menurunkan kontrol akses terhadap data dan fitur.

Untuk memastikan bahwa sistem berfungsi sebagaimana mestinya, dilakukan pengujian terhadap fitur-fitur utama yang ada. Hasil pengujian menunjukkan bahwa seluruh komponen berjalan dengan baik tanpa kendala berarti. Tabel berikut menyajikan ringkasan hasil pengujian terhadap fungsi dasar sistem:

Tabel 1. Performance

Test	Activity	Status
Login	Website	Success
Logout	Website	Success
Login	Website	Success

Dari hasil tersebut, dapat disimpulkan bahwa sistem sudah layak digunakan untuk kebutuhan komunikasi internal berskala kecil di lingkungan desa. Namun, untuk pengembangan selanjutnya, sistem perlu diperkuat dari segi keamanan dan akses kontrol agar dapat digunakan secara lebih luas dan aman.

PEMBAHASAN

Berdasarkan hasil implementasi, Hasil implementasi sistem menunjukkan bahwa aplikasi enkripsi pesan berbasis Caesar Cipher ini memiliki beberapa keunggulan yang sangat relevan dan sesuai dengan kebutuhan komunikasi di lingkungan pedesaan. Salah satu kelebihan utama adalah kesederhanaannya dalam penggunaan. Sistem ini dirancang agar dapat dijalankan langsung melalui browser, tanpa perlu melakukan proses instalasi atau konfigurasi tambahan. Hal ini tentu sangat membantu perangkat desa yang umumnya tidak memiliki latar belakang teknis atau perangkat keras dengan spesifikasi tinggi. Selain itu, algoritma Caesar Cipher yang digunakan dalam sistem ini memiliki karakteristik yang mudah dipahami. Pengguna hanya perlu memasukkan pesan dan nilai kunci pergeseran tertentu untuk mengenkripsi maupun mendekripsi data. Kesederhanaan ini sangat menguntungkan bagi pengguna awam karena mereka dapat memahami logika dasar enkripsi tanpa perlu pengetahuan mendalam tentang kriptografi. Keterlibatan langsung pengguna dalam proses ini turut memberikan edukasi dasar mengenai pentingnya menjaga keamanan informasi. Keunggulan lain dari sistem ini adalah kemampuannya untuk berjalan secara offline. Dalam konteks wilayah pedesaan yang belum sepenuhnya terjangkau oleh jaringan internet yang stabil, kemampuan sistem untuk dijalankan secara lokal tanpa koneksi internet menjadi nilai tambah yang signifikan.

Hal ini memungkinkan perangkat desa untuk tetap menjaga kerahasiaan komunikasi internal, seperti pengiriman pesan antar staf atau catatan penting, tanpa ketergantungan pada konektivitas digital. Efisiensi sistem dalam menangani pesan-pesan pendek juga membuatnya sangat cocok sebagai solusi pengamanan komunikasi sehari-hari yang ringan namun fungsional. Meskipun memiliki kelebihan tersebut, sistem ini juga menghadirkan beberapa keterbatasan penting yang perlu dicermati, terutama jika ingin digunakan dalam jangka panjang atau diperluas penggunaannya. Dari sisi keamanan, algoritma Caesar Cipher sebenarnya tergolong sebagai metode kriptografi klasik yang sudah banyak diketahui dan mudah dipecahkan. Sifat algoritma ini memungkinkan siapa saja yang mengetahui pola pergeserannya untuk dengan cepat membongkar isi pesan, sehingga sistem ini kurang cocok untuk mengamankan informasi yang bersifat rahasia atau sensitif. Lebih lanjut, sistem ini hanya mendukung penggunaan kunci dalam bentuk angka 0–25 untuk pergeseran huruf, sehingga jumlah kombinasi yang tersedia sangat terbatas. Hal ini menjadikan sistem rentan terhadap serangan brute force karena kunci yang digunakan mudah ditebak. Untuk data seperti informasi pribadi warga, dokumen keuangan, atau surat keputusan resmi, sistem ini belum dapat memberikan tingkat keamanan yang memadai. Keterbatasan lainnya terletak pada belum tersedianya fitur login atau manajemen pengguna. Saat ini, sistem masih bersifat terbuka, artinya siapa saja yang mengaksesnya dapat langsung menggunakan semua fiturnya tanpa ada proses otentikasi terlebih dahulu. Hal ini mengurangi aspek keamanan dan kontrol, karena tidak ada pembeda antara pengguna umum dan pengguna yang memiliki wewenang resmi dalam penggunaan sistem. Dalam konteks pemerintahan desa, fitur autentikasi akan sangat penting untuk memastikan bahwa hanya pihak berwenang yang dapat mengakses atau memproses

informasi penting. Oleh karena itu, meskipun sistem ini telah berhasil memenuhi sebagian besar kebutuhan komunikasi internal perangkat desa secara sederhana dan efisien, pengembangan lebih lanjut sangat diperlukan. Khususnya pada aspek keamanan dan pengelolaan akses pengguna, agar sistem ini dapat digunakan secara lebih luas dan andal dalam mendukung digitalisasi layanan desa.

KESIMPULAN

Sistem pengamanan pesan teks berbasis web menggunakan algoritma Caesar Cipher mampu menjawab rumusan masalah terkait kebutuhan akan sistem komunikasi internal yang aman, mudah digunakan, dan sesuai untuk lingkungan pemerintahan desa dengan keterbatasan infrastruktur teknologi. Sistem ini berhasil dikembangkan dengan antarmuka yang sederhana dan intuitif, memungkinkan pengguna awam mengoperasikannya tanpa pelatihan khusus, serta dapat dijalankan secara offline sehingga cocok diterapkan di wilayah pedesaan. Selain itu, penggunaan algoritma Caesar Cipher memberikan nilai edukatif dalam memperkenalkan konsep dasar keamanan informasi kepada pengguna non-teknis. Sistem ini efektif untuk mengenkripsi dan mendekripsi pesan-pesan pendek yang tidak bersifat rahasia tinggi, seperti pengingat, catatan internal, atau instruksi operasional antar staf desa. Meski demikian, keterbatasan dari sisi keamanan masih menjadi catatan penting, karena algoritma Caesar Cipher mudah dipecahkan dan sistem belum mendukung enkripsi kompleks maupun fitur otentikasi pengguna. Oleh karena itu, untuk pengembangan lebih lanjut, disarankan agar sistem menggunakan algoritma kriptografi yang lebih kuat seperti Vigenère Cipher atau AES, dilengkapi dengan sistem login dan pengaturan hak akses untuk membatasi penggunaan hanya kepada pihak yang berwenang, serta dilakukan pengembangan antarmuka yang lebih informatif dan responsif agar sistem lebih adaptif terhadap beragam tingkat literasi digital pengguna desa. Selain itu, penyediaan modul pelatihan atau dokumentasi panduan sangat dianjurkan guna meningkatkan pemahaman pengguna terhadap prinsip keamanan informasi, serta evaluasi keamanan berkala dan simulasi serangan sederhana perlu dilakukan untuk memastikan ketahanan sistem terhadap potensi ancaman. Dengan mengakomodasi saran-saran tersebut, sistem ini memiliki potensi untuk berkembang menjadi solusi komunikasi internal desa yang tidak hanya praktis dan edukatif, tetapi juga aman, terjangkau, dan berkelanjutan dalam jangka panjang

REFERENSI

Andika, R. (2019). Implementasi Caesar Cipher Dalam Aplikasi Desktop Untuk Pengamanan Pesan. *Jurnal Teknologi Informasi, 7*(2), 45–56.

Handayani, S., Rahayu, D., & Purnama, L. (2022). Sistem Komunikasi Aman Dalam Layanan Publik Desa: Studi Kasus Di Kecamatan X. *Jurnal Pemerintahan Desa, 3*(1), 12–25.

Hidayat, T., Nugraha, A., & Wibowo, H. (2022). Penguatan Literasi Digital Dan Keamanan Informasi Desa Berbasis Web. *Jurnal Transformasi Digital, 1*(1), 33–47.

Lestari, N., & Prasetyo, E. (2020). Analisis Keamanan Pesan Di Aplikasi Whatsapp: Implikasi Untuk Pengamanan Lokal. *Jurnal Kriptografi dan Keamanan, 5*(3), 78–89.

Mulyadi, D. (2013). *Metodologi Penelitian Kuantitatif Dan Komunikasi*. Remaja Rosdakarya.

Rahman, I., & Sari, F. (2021). Transformasi Digital Dalam Pengelolaan Desa: Tantangan Dan Peluang. *Jurnal Administrasi Desa, 2*(2), 100–115.

Ramadhan, A., Sucipto, S., & Wulandari, R. (2020). Penerapan Caesar Cipher Untuk Pengamanan Pesan Teks Pada Aplikasi Sederhana. *Jurnal Informatika, 8*(4), 123–131.

Setiawan, B. (2020). Akses Internet Dan Digitalisasi Layanan Publik Di Desa Terpencil. *Jurnal Ilmu Komunikasi, 10*(1), 27–40.

Sari, F., & Nugroho, A. (2021). Perbandingan Caesar Cipher Dan Vigenère Cipher Dari Sisi Kecepatan Dan Kompleksitas. *Jurnal Kriptografi, 6*(2), 55–66.

Santoso, R., & Malik, A. (2018). *Pengantar Kriptografi dan Algoritma Klasik*. Andi Offset.

Sunaryo, P. (2022). Kriptografi Ringan Berbasis Javascript Untuk Edukasi Dan Aplikasi Dasar. *Jurnal Teknologi Terapan, 4*(1), 88–97.

Susanti, E., & Pramana, B. (2019). Evaluasi Model Waterfall Dalam Pengembangan Aplikasi Desa Berbasis Web. *Jurnal Rekayasa Perangkat Lunak, 2*(1), 15–26.

Utami, P., & Wijaya, Y. (2021). Alternatif Enkripsi Untuk Komunikasi Desa Digital: Tinjauan Algoritma Klasik Dan Modern. *Jurnal Sistem Informasi, 9*(3), 145–158.

Wahyudi, M. (2020). Keamanan Pesan Teks: Pendekatan Kriptografi Sederhana Untuk Pendidikan. *Jurnal Pendidikan Informatika, 11*(2), 72–81.

Yulianto, A., Suryani, M., & Pratama, D. (2021). Pengembangan Modul Pelatihan Kriptografi Untuk Perangkat Desa. *Jurnal Pengabdian Kepada Masyarakat, 1*(2), 30–42.