Polygon: Jurnal Ilmu Komputer dan Ilmu Pengetahuan Alam
Volume. 4 Nomor. 1 Januari 2026
e-ISSN: 3046-5419; p-ISSN: 3032-6249, Hal 32-41
DOI: https://doi.org/10.62383/polygon.v4i1.925
Tersedia: https://journal.arimsi.or.id/index.php/Polygon

Implementasi Algoritma *Caesar Cipher* untuk Enkripsi dan Dekripsi Pesan

Siti Fadiyah Nabila[1*], Maisyarah[2], Zahara Vonna[3], Salsabila Arifa Hasibuan[4], Silfia Rahmadani Sitorus[5], Aninda Evioni[6], Ibnu Rusydi[7]
[1-7]Fakultas Sains dan Teknologi, Prodi Ilmu Komputer, Universitas Islam Negeri Sumatera Utara, Indonesia
**Penulis Korespondensi: fadiyahnabila20@gmail.com*

Abstract. *Information security is an essential aspect of digital communication, particularly in the exchange of text-based messages through open networks. Messages transmitted without protection are vulnerable to interception and unauthorized modification. One classical cryptographic technique that remains relevant as a foundational learning tool is the Caesar Cipher algorithm. This study aims to implement the Caesar Cipher algorithm for message encryption and decryption and to analyze its effectiveness and security level. The research method employed is a descriptive approach through literature review and a case study by applying character-shift techniques to text messages. The results indicate that the Caesar Cipher algorithm successfully transforms plaintext into ciphertext and restores it back to its original form through the decryption process. Although the algorithm is simple and easy to implement, it has significant limitations in terms of security due to its small key space and vulnerability to brute-force attacks. Therefore, Caesar Cipher is not suitable for protecting sensitive data but remains valuable as an introductory model for understanding basic cryptographic concepts.*

Keywords: *Caesar Cipher; Cryptography; Decryption; Encryption; Information Security.*

Abstrak. Keamanan informasi merupakan aspek penting dalam komunikasi digital, khususnya pada pertukaran pesan berbasis teks melalui jaringan terbuka. Pesan yang dikirim tanpa perlindungan berisiko mengalami penyadapan dan perubahan oleh pihak yang tidak berwenang. Salah satu teknik kriptografi klasik yang masih relevan sebagai dasar pembelajaran adalah algoritma Caesar Cipher. Penelitian ini bertujuan untuk mengimplementasikan algoritma Caesar Cipher dalam proses enkripsi dan dekripsi pesan serta menganalisis efektivitas dan tingkat keamanannya. Metode penelitian yang digunakan adalah metode deskriptif melalui studi literatur dan studi kasus dengan menerapkan teknik pergeseran karakter pada pesan teks. Hasil penelitian menunjukkan bahwa algoritma Caesar Cipher mampu mengubah pesan asli menjadi pesan tersandi dan mengembalikannya kembali ke bentuk semula melalui proses dekripsi. Meskipun sederhana dan mudah diimplementasikan, algoritma ini memiliki keterbatasan dari sisi keamanan karena ruang kunci yang kecil dan mudah dipecahkan dengan serangan brute force. Oleh karena itu, Caesar Cipher kurang sesuai untuk pengamanan data rahasia, namun tetap bermanfaat sebagai media pembelajaran konsep dasar kriptografi.

Kata kunci: Caesar Cipher; Dekripsi; Enkripsi; Keamanan Informasi; Kriptografi.

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam cara manusia berinteraksi dan bertukar informasi. Penggunaan media digital seperti aplikasi pesan instan, surat elektronik, dan sistem berbasis web semakin meningkat seiring dengan kemudahan akses internet (Olanrewaju et al., 2025). Kondisi ini menyebabkan volume data dan pesan yang dipertukarkan menjadi semakin besar dan beragam, mulai dari informasi pribadi hingga data yang bersifat rahasia (Thakkar, 2025). Di sisi lain, kemajuan tersebut juga diiringi dengan meningkatnya ancaman keamanan informasi yang dapat membahayakan kerahasiaan dan keutuhan pesan (Utomo et al., 2025).

Ancaman terhadap keamanan pesan digital umumnya berupa penyadapan, pencurian data, serta manipulasi isi pesan oleh pihak yang tidak berwenang (Menggunakan et al., 2021). Pesan yang dikirim tanpa mekanisme perlindungan yang memadai sangat rentan terhadap

Naskah Masuk: 07 Desember 2025; Revisi: 01 Januari 2026; Diterima: 20 Januari 2026;
Terbit: 22 Januari 2026

serangan tersebut, terutama ketika melewati jaringan terbuka (Alfirdaus et al., 2023). Oleh karena itu, aspek keamanan informasi menjadi faktor penting yang harus diperhatikan dalam sistem komunikasi digital (Noviyanti et al., 2022). Keamanan pesan tidak hanya bertujuan untuk melindungi isi informasi, tetapi juga untuk menjamin kepercayaan pengguna terhadap sistem komunikasi yang digunakan (Balamurugan et al., 2021).

Salah satu pendekatan yang umum digunakan untuk menjaga keamanan pesan adalah kriptografi (Siregar et al., 2024). Kriptografi merupakan teknik pengamanan informasi dengan cara mengubah pesan asli (plaintext) menjadi pesan tersandi (ciphertext) sehingga tidak dapat dipahami oleh pihak yang tidak berhak (Ramadhan & Rahman, 2024). Metode ini telah digunakan sejak lama dan terus berkembang seiring dengan kemajuan teknologi. Melalui proses enkripsi dan dekripsi, kriptografi berperan penting dalam menjaga kerahasiaan data, baik pada sistem komunikasi sederhana maupun sistem informasi berskala besar (Ziliwu et al., 2022).

Caesar Cipher merupakan salah satu algoritma kriptografi klasik yang menggunakan teknik substitusi dengan cara menggeser setiap karakter pada pesan berdasarkan nilai kunci tertentu (Rahma et al., 2025). Algoritma ini dikenal sebagai metode enkripsi yang paling sederhana dan mudah dipahami. Meskipun tingkat keamanannya relatif rendah jika dibandingkan dengan algoritma kriptografi modern, Caesar Cipher memiliki nilai historis yang penting dalam perkembangan ilmu kriptografi (Pramudya & Suhardi, 2025). Selain itu, algoritma ini sering digunakan sebagai media pembelajaran untuk memperkenalkan konsep dasar enkripsi, dekripsi, dan penggunaan kunci dalam sistem keamanan informasi (Caesar et al., 2023).

Berdasarkan latar belakang tersebut, penelitian ini difokuskan pada implementasi algoritma Caesar Cipher dalam proses enkripsi dan dekripsi pesan teks (Purnamasari et al., 2022). Penelitian ini bertujuan untuk memahami mekanisme kerja Caesar Cipher serta menganalisis kelebihan dan keterbatasannya sebagai metode pengamanan data (Informasi, 2025). Diharapkan hasil penelitian ini dapat memberikan gambaran awal mengenai konsep dasar kriptografi serta menjadi referensi bagi penelitian selanjutnya yang membahas pengembangan atau penerapan algoritma kriptografi yang lebih kompleks dan aman (Uci Julya Ningsih et al., 2024).

2. KAJIAN TEORITIS

Keamanan informasi merupakan upaya sistematis untuk melindungi data dari berbagai ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaannya. Kerahasiaan berkaitan dengan perlindungan data agar hanya dapat diakses oleh pihak yang berwenang, integritas berfokus pada keutuhan data agar tidak mengalami perubahan yang tidak sah, sedangkan ketersediaan memastikan data dapat diakses saat dibutuhkan (Siagian & Indra, 2025). Ketiga prinsip tersebut menjadi dasar utama dalam perancangan sistem keamanan informasi, khususnya pada sistem komunikasi digital yang melibatkan pertukaran pesan melalui jaringan terbuka. Tanpa penerapan mekanisme keamanan yang tepat, informasi berpotensi disalahgunakan sehingga dapat menimbulkan kerugian bagi individu maupun organisasi (Teknik et al., 2025).

Kriptografi merupakan salah satu teknik fundamental dalam keamanan informasi yang berfungsi untuk menjaga kerahasiaan pesan melalui proses enkripsi dan dekripsi. Proses enkripsi mengubah pesan asli (plaintext) menjadi pesan tersandi (ciphertext) menggunakan algoritma dan kunci tertentu, sedangkan dekripsi berfungsi untuk mengembalikan ciphertext ke bentuk semula. Dalam kajian kriptografi, algoritma dibedakan menjadi kriptografi klasik dan kriptografi modern. Kriptografi klasik umumnya menggunakan teknik substitusi dan transposisi yang relatif sederhana, namun memiliki peran penting dalam perkembangan awal ilmu kriptografi. Konsep-konsep dasar yang diperkenalkan dalam kriptografi klasik menjadi landasan bagi pengembangan algoritma kriptografi modern yang lebih kompleks dan aman (Aprianti & Marsehan, 2025).

Caesar Cipher termasuk dalam kategori kriptografi klasik dengan teknik substitusi monoalfabetik, di mana setiap karakter pada plaintext digeser berdasarkan nilai kunci tertentu dalam urutan alfabet. Beberapa penelitian sebelumnya menunjukkan bahwa Caesar Cipher mudah diimplementasikan dan efektif untuk menjelaskan konsep dasar enkripsi dan dekripsi, terutama dalam konteks pembelajaran keamanan informasi. Namun, penelitian-penelitian tersebut juga menegaskan bahwa algoritma ini memiliki kelemahan signifikan dari sisi keamanan karena ruang kunci yang terbatas, sehingga rentan terhadap serangan brute force. Meskipun demikian, Caesar Cipher tetap relevan sebagai dasar teoritis dan praktis dalam penelitian yang bertujuan untuk memahami mekanisme kerja kriptografi sebelum mengkaji algoritma pengamanan data yang lebih kompleks (Ardiansyah et al., 2023).

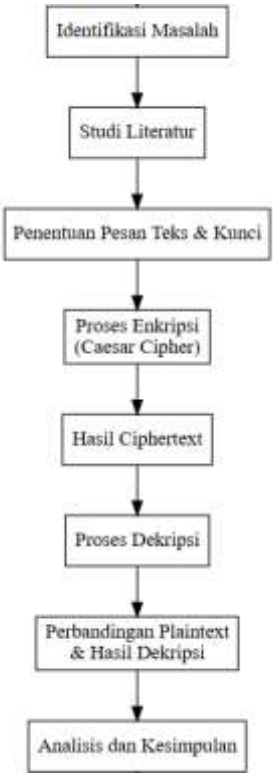
3. METODE PENELITIAN

Penelitian ini menggunakan desain penelitian deskriptif dengan pendekatan studi literatur dan studi kasus. Pendekatan deskriptif dipilih untuk menggambarkan secara sistematis proses implementasi algoritma Caesar Cipher dalam enkripsi dan dekripsi pesan teks tanpa melakukan pengujian hipotesis statistik. Fokus penelitian diarahkan pada pemahaman mekanisme kerja algoritma serta analisis hasil transformasi pesan sebelum dan sesudah proses enkripsi dan dekripsi.

Populasi dalam penelitian ini berupa seluruh bentuk pesan teks yang dapat direpresentasikan dalam karakter alfabet, sedangkan sampel penelitian berupa beberapa pesan teks sederhana yang digunakan sebagai objek uji. Pemilihan sampel dilakukan secara purposive, dengan mempertimbangkan kemudahan observasi perubahan pesan pada setiap tahapan proses enkripsi dan dekripsi. Data yang digunakan merupakan data sekunder berupa pesan teks yang dirancang oleh peneliti, sehingga tidak melibatkan responden secara langsung.

Teknik pengumpulan data dilakukan melalui studi literatur untuk memperoleh landasan teori terkait keamanan informasi dan algoritma Caesar Cipher, serta studi kasus dengan menerapkan algoritma Caesar Cipher pada pesan teks. Instrumen penelitian berupa skema algoritma Caesar Cipher yang digunakan untuk melakukan proses pergeseran karakter berdasarkan nilai kunci tertentu. Alat analisis data yang digunakan adalah analisis deskriptif dengan membandingkan plaintext, ciphertext, dan hasil dekripsi untuk menilai keberhasilan algoritma dalam menjaga kerahasiaan pesan.

Model penelitian disusun dalam bentuk alur proses yang menggambarkan tahapan enkripsi dan dekripsi pesan menggunakan algoritma Caesar Cipher. Analisis dilakukan dengan mengamati perubahan karakter pada pesan setelah proses enkripsi serta kemampuan algoritma dalam mengembalikan pesan ke bentuk semula melalui proses dekripsi. Keberhasilan algoritma dinilai berdasarkan kesesuaian antara plaintext awal dan hasil dekripsi, serta tingkat keterbacaan ciphertext tanpa mengetahui nilai kunci.



Gambar 1. Alur Metode.

4. HASIL DAN PEMBAHASAN

```
ALGORITMA Caesar_Cipher
INPUT: plaintext, kunci
OUTPUT: ciphertext, hasil_dekripsi
PROSEDUR Enkripsi_Caesar(plaintext, kunci)
   ciphertext ← string kosong
   UNTUK setiap karakter char dalam plaintext LAKUKAN
      JIKA char adalah huruf kapital MAKA
         ciphertext ← ciphertext +
                  karakter( (kodeASCII(char) - 65 + kunci) mod 26 + 65 )
      JIKA char adalah huruf kecil MAKA
         ciphertext ← ciphertext +
                  karakter( (kodeASCII(char) - 97 + kunci) mod 26 + 97 )
      JIKA char bukan huruf MAKA
         ciphertext ← ciphertext + char
   AKHIR UNTUK
   KEMBALIKAN ciphertext
```

```
END PROSEDUR
PROSEDUR Dekripsi_Caesar(ciphertext, kunci)
  plaintext ← string kosong
  UNTUK setiap karakter char dalam ciphertext LAKUKAN
    JIKA char adalah huruf kapital MAKA
      plaintext ← plaintext +
            karakter( (kodeASCII(char) - 65 - kunci) mod 26 + 65 )
    JIKA char adalah huruf kecil MAKA
      plaintext ← plaintext +
            karakter( (kodeASCII(char) - 97 - kunci) mod 26 + 97 )
    JIKA char bukan huruf MAKA
      plaintext ← plaintext + char
  AKHIR UNTUK
  KEMBALIKAN plaintext
END PROSEDUR
PROGRAM UTAMA
  TAMPILKAN "Program Caesar Cipher"
  INPUT plaintext
  INPUT kunci
  ciphertext ← Enkripsi_Caesar(plaintext, kunci)
  hasil_dekripsi ← Dekripsi_Caesar(ciphertext, kunci)
  TAMPILKAN plaintext
  TAMPILKAN ciphertext
  TAMPILKAN hasil_dekripsi
  JIKA plaintext = hasil_dekripsi MAKA
    TAMPILKAN "Dekripsi berhasil"
  JIKA TIDAK MAKA
    TAMPILKAN "Dekripsi gagal"
SELESAI
```

```
=== Program Caesar Cipher ===
Masukkan pesan teks (plaintext): Ilmu Komputer Jaya
Masukkan nilai kunci pergeseran: 3

--- Hasil Proses ---
Plaintext          : Ilmu Komputer Jaya
Ciphertext         : Lopx Nrpsxwhu Mdbd
Hasil Dekripsi     : Ilmu Komputer Jaya

Analisis:
Dekripsi berhasil, pesan asli dapat dikembalikan dengan benar.

=== Proses Selesai ===
```

Gambar 2. Output.

Hasil Implementasi Algoritma Caesar Cipher

Implementasi algoritma Caesar Cipher dilakukan menggunakan bahasa pemrograman Python dengan menerapkan fungsi enkripsi dan dekripsi berbasis pergeseran karakter. Pengujian dilakukan terhadap pesan teks “Ilmu Komputer Jaya” dengan nilai kunci pergeseran sebesar 3. Berdasarkan hasil eksekusi program, diperoleh output berupa ciphertext “Lopu Nrpsxwhu Mbdb”. Hasil tersebut menunjukkan bahwa setiap karakter alfabet pada plaintext berhasil digeser tiga posisi ke depan sesuai dengan aturan algoritma Caesar Cipher, sementara spasi tetap dipertahankan tanpa perubahan.

Proses dekripsi dilakukan dengan menggunakan nilai kunci yang sama, yaitu 3, namun dengan arah pergeseran karakter yang berlawanan. Hasil dekripsi menunjukkan bahwa ciphertext “Lopu Nrpsxwhu Mbdb” berhasil dikembalikan ke bentuk plaintext awal, yaitu “Ilmu Komputer Jaya”. Kesamaan antara plaintext awal dan hasil dekripsi menandakan bahwa proses enkripsi dan dekripsi berjalan dengan benar dan konsisten sesuai dengan prinsip kerja algoritma Caesar Cipher.

Keberhasilan proses dekripsi juga ditunjukkan melalui analisis program yang secara otomatis membandingkan plaintext awal dengan hasil dekripsi. Sistem menyatakan bahwa dekripsi berhasil karena pesan asli dapat dikembalikan secara utuh tanpa mengalami perubahan karakter. Hal ini membuktikan bahwa algoritma Caesar Cipher mampu menjaga integritas pesan selama proses enkripsi dan dekripsi, selama nilai kunci yang digunakan tetap sama.

Pembahasan

Berdasarkan hasil implementasi, algoritma Caesar Cipher terbukti mampu mengamankan pesan teks dengan cara mengubah plaintext menjadi ciphertext yang tidak dapat dipahami secara langsung tanpa mengetahui nilai kunci pergeseran. Ciphertext yang dihasilkan

tidak memiliki keterbacaan makna secara linguistik, sehingga pihak yang tidak mengetahui kunci akan mengalami kesulitan dalam memahami isi pesan. Kondisi ini menunjukkan bahwa Caesar Cipher mampu memenuhi aspek kerahasiaan informasi pada tingkat dasar.

Namun demikian, dari sisi keamanan, algoritma Caesar Cipher memiliki keterbatasan yang cukup signifikan. Ruang kunci yang terbatas, yaitu hanya 26 kemungkinan pergeseran, menyebabkan algoritma ini rentan terhadap serangan brute force. Pihak yang tidak berwenang dapat mencoba seluruh kemungkinan kunci dalam waktu yang relatif singkat untuk memperoleh pesan asli. Oleh karena itu, meskipun Caesar Cipher efektif dalam memperkenalkan konsep dasar kriptografi, algoritma ini tidak direkomendasikan untuk pengamanan data yang bersifat sensitif atau rahasia.

Secara keseluruhan, hasil penelitian menunjukkan bahwa algoritma Caesar Cipher lebih sesuai digunakan sebagai media pembelajaran dan pemahaman awal mengenai mekanisme enkripsi dan dekripsi pesan. Implementasi yang sederhana serta hasil yang mudah diamati menjadikan algoritma ini relevan untuk tujuan edukatif. Untuk kebutuhan keamanan data yang lebih kompleks, diperlukan penerapan algoritma kriptografi modern dengan tingkat keamanan yang lebih tinggi.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil implementasi dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa algoritma Caesar Cipher berhasil diimplementasikan untuk proses enkripsi dan dekripsi pesan teks dengan cara menggeser setiap karakter sesuai dengan nilai kunci yang ditentukan. Hasil pengujian menunjukkan bahwa ciphertext yang dihasilkan tidak dapat dipahami secara langsung dan proses dekripsi mampu mengembalikan pesan ke bentuk semula secara utuh, sehingga membuktikan bahwa algoritma ini bekerja sesuai dengan prinsip dasar kriptografi. Meskipun demikian, algoritma Caesar Cipher memiliki keterbatasan dari sisi keamanan karena ruang kunci yang terbatas dan mudah dipecahkan menggunakan metode brute force, sehingga kurang sesuai untuk pengamanan data yang bersifat sensitif. Oleh karena itu, penelitian selanjutnya disarankan untuk mengembangkan atau mengombinasikan algoritma Caesar Cipher dengan algoritma kriptografi lain yang lebih kompleks guna meningkatkan tingkat keamanan informasi.

DAFTAR REFERENSI

Alfirdaus, M. H., Tahir, M., & Dewanti, N. E. (2023). Perancangan aplikasi enkripsi deskripsi menggunakan metode Caesar cipher berbasis web. *Jurnal Teknologi Multimedia dan Informatika, 2*(2), 1–8. https://doi.org/10.55606/jtmei.v2i2.1628

Aprianti, E., & Marsehan, A. (2025). Analisis dan implementasi algoritma Caesar cipher dalam pengamanan pesan teks berbasis web di desa. *Digitech Journal, 5*(1), 191–196. https://doi.org/10.47709/digitech.v5i1.5984

Ardiansyah, F. D., Damayanti, A., Azzahra, C., Putri, M., Fitria, A., Rany, D., Biroso, S. J., & Tahir, M. (2023). Implementasi kriptografi Caesar cipher pada aplikasi enkripsi dan dekripsi. *Jurnal UISIK, 3*(1), 1–9. https://doi.org/10.55606/juisik.v3i1.438

Balamurugan, C., Singh, K., Ganesan, G., & Rajarajan, M. (2021). Post-quantum and code-based cryptography: Some prospective research directions. *Cryptography, 5*(4), Article 38, 1–30. https://doi.org/10.3390/cryptography5040038

Caesar, K., Cipher, H., Sylviani, S., Kartiwa, A., Permana, F. C., Hadi, A. N., & Kadir, M. P. (2023). Aplikasi matriks untuk meningkatkan keamanan proses kriptografi Caesar, Vernam, dan Hill cipher. *Jurnal Sains dan Teknologi Undiksha, 12*(2), 502–515. https://doi.org/10.23887/jstundiksha.v12i2.52801

Informasi, J. T. (2025). Penerapan algoritma Caesar cipher pada aplikasi pengaman pesan berbasis website. *Jurnal Teknologi Informasi, 15*(2), 92–98. https://doi.org/10.36382/jti-tki.v15i2.530

Menggunakan, E., Vigenere, A., & Caesar, D. A. N. (2021). Peningkatan keamanan data melalui teknik super enkripsi. *Prosiding Seminar Nasional Teknologi Informasi*, 315–322.

Noviyanti, P., & Bhuana, I. S. (2022). Analisa algoritma kriptografi klasik Caesar cipher, Vigenere cipher, dan Hill cipher: Studi literatur. *JIFOTECH, 2*(1), 23–29. https://doi.org/10.46229/jifotech.v2i1.387

Olanrewaju, S. B., Eguavoen, O. V., Okunade, A., & Adekunle, O. (2025). A modified Caesar cipher encryption technique for secured information sharing. *Fountain Journal of Science, 9*(5), 180–186. https://doi.org/10.33003/fjs-2025-0905-3494

Pramudya, F. A., & Suhardi. (2025). Analisis keamanan komparatif Caesar cipher dan DES dalam konteks teknik kriptografi modern. *Jurnal Sistem Informasi dan Keamanan, 2*(3), 96–105.

Purnamasari, D., Dewi, A. K., & Trisetiyanto, A. N. (2022). Analisis performansi kriptografi berbasis Caesar cipher untuk keamanan data menggunakan Python pada tembang macapat. *Jurnal SITEe, 1*(2), 50–54. https://doi.org/10.31331/jsitee.v1i2.2079

Rahma, S. A., Putri, T., Novitasari, A., Djawas, F. W. S., & Zy, A. T. (2025). Implementasi keamanan data dalam sistem informasi manajemen. *Jurnal Sistem Informasi, 30*, 92–98.

Ramadhan, S. S., & Rahman, R. (2024). Implementasi enkripsi dan keamanan kriptografi. *Digibe Journal, 2*(2), 110–117. https://doi.org/10.25134/digibe.v2i2.46

Siagian, A. A., & Indra, Z. (2025). Analisis teknik Playfair dan shift cipher sebagai metode kriptografi klasik untuk keamanan data. *Jurnal Komputer dan Teknologi, 4*(1), 13–19. https://doi.org/10.58290/jukomtek.v4i1.315

Siregar, M., Jinan, A., Muhammad, T., & Gunung, R. (2024). Disguising text using Caesar cipher, reverse cipher, and least significant bit (LSB) algorithms in video. *Journal of Computer Networks, Architecture and High Performance Computing, 6*(3), 1134–1144. https://doi.org/10.47709/cnahpc.v6i3.4217

Teknik, F., Informasi, S., Utama, U. P., Yos, A. K. L., Medan, S., & Utara, S. (2025). Implementasi kriptografi dengan Caesar cipher pada fitur pesan di WhatsApp untuk keamanan. *MARS Journal, 3*(4), 1–8. https://doi.org/10.61132/mars.v3i4.978

Thakkar, B. (2025). A comprehensive study of substitution and transposition techniques in cryptographic systems. *International Journal of Cryptography Studies, 13*(2), 15–19.

Uci Julya Ningsih, Salsabila, S., Hutapea, I., Santika, D., & Gunawan, I. (2024). Pendekripsian Caesar cipher dengan menggunakan teknik-teknik kriptanalisis. *Jurnal Ilmu Komputer dan Multimedia, 1*(1), 11–15. https://doi.org/10.46510/ilkomedia.v1i1.10

Utomo, R., Syafaat, M., Widiatmoko, D., & Maulana, R. (2025). Cryptographic security analysis of the shift password method using the Google Colab application. *Jurnal Tekno, 12*(1), 104–109. https://doi.org/10.37373/tekno.v12i1.1231

Ziliwu, K. B., Maslan, A., & Kremer, H. (2022). Implementasi Caesar cipher pada algoritma kriptografi dalam penyandian pesan WhatsApp. *Jurnal Informatika, 2*, 117–125.