

Aplikasi Simulasi Enkripsi Menggunakan Metode Caesar Cipher Berbasis Website

Fiqri Dian Priyatna Sinaga, Khoiratul Azmi, Afri Yunda Nasution, Rivaldi Prima Nanda, Ibnu Rusydi

¹⁻⁵Fakultas Sains dan Teknologi, Program Studi Ilmu Komputer, Universitas Islam Negeri Sumatera Utara Medan

E-mail: ¹fiqridpss@gmail.com, ²miiiazmiirpan@gmail.com, ³afriyundanasution@gmail.com,
⁴rivaldiprimanandaxtkj2@gmail.com, ⁵ibnurusydi@dharmawangsa.ac.id
Korespondensi : fiqridpss@gmail.com

Abstrak

Kriptografi merupakan bidang fundamental dalam keamanan data, namun sering dianggap sulit dipahami oleh mahasiswa pemula karena sifatnya yang abstrak dan matematis. Penelitian terdahulu menunjukkan bahwa pembelajaran Caesar Cipher umumnya masih bersifat teoritis atau berbasis aplikasi desktop yang kurang interaktif dan memiliki keterbatasan aksesibilitas. Oleh karena itu, penelitian ini bertujuan mengembangkan aplikasi simulasi enkripsi Caesar Cipher berbasis website sebagai media pembelajaran interaktif. Pengembangan sistem dilakukan menggunakan metode prototype, sedangkan pengujian fungsional menerapkan metode black box. Evaluasi efektivitas aplikasi dilakukan melalui pengumpulan data primer menggunakan kuesioner kepada mahasiswa. Hasil penelitian menunjukkan bahwa sebelum menggunakan aplikasi, sebanyak 82,4% mahasiswa berada pada tingkat pemahaman rendah hingga sedang, sedangkan setelah menggunakan aplikasi, 100% mahasiswa berada pada tingkat pemahaman tinggi. Temuan ini membuktikan bahwa aplikasi simulasi enkripsi Caesar Cipher berbasis website efektif dalam meningkatkan pemahaman mahasiswa terhadap konsep fundamental kriptografi sebagai dasar sebelum mempelajari algoritma keamanan data yang lebih lanjut.

Kata kunci: Kriptografi, Caesar Cipher, Simulasi Enkripsi, Media Pembelajaran, Aplikasi Website.

Abstract

Cryptography is a fundamental field in data security; however, it is often considered difficult for beginner students due to its abstract and mathematical nature. Previous studies indicate that learning Caesar Cipher is commonly conducted through theoretical approaches or desktop-based applications with limited interactivity and accessibility. Therefore, this study aims to develop a web-based Caesar Cipher encryption simulation application as an interactive learning medium. The system was developed using the prototype method, while functional testing was conducted using the black box testing approach. The effectiveness of the application was evaluated through primary data collected through questionnaires distributed to students. The results show that before using the application, 82.4% of students were at low to moderate levels of understanding, whereas after using the application, 100% of students reached a high level of understanding. These findings indicate that the web-based Caesar Cipher simulation application is effective in improving students' understanding of fundamental cryptographic concepts prior to studying more advanced data security algorithms.

Keywords: Cryptography, Caesar Cipher, Encryption Simulation, Learning Media, Web Application.

1. PENDAHULUAN

Di tengah pesatnya transformasi digital, keamanan data telah menjadi disiplin ilmu yang *fundamental* [1]. Namun, bagi mahasiswa awam yang baru mengenal dunia teknologi informasi, memahami konsep abstrak kriptografi seringkali menjadi tantangan besar. Kriptografi bukan

sekadar tentang penyandian pesan, melainkan melibatkan logika matematika yang menjadi fondasi keamanan siber *modern* [2]. Untuk menjembatani pemahaman tersebut, diperlukan pengenalan melalui metode kriptografi klasik sebagai langkah awal pembelajaran. Salah satu metode yang paling efektif untuk memperkenalkan prinsip dasar enkripsi adalah algoritma Caesar Cipher. Sebagai algoritma substitusi monoalfabetik, Caesar Cipher menawarkan logika sederhana mengenai bagaimana sebuah karakter diubah menjadi karakter lain melalui pergeseran posisi berdasarkan kunci (*key*) tertentu [3]. Meskipun sederhana, algoritma ini merupakan instrumen pedagogis terbaik untuk mengajarkan konsep aritmatika modulo dan enkripsi simetris kepada mahasiswa sebelum mereka menghadapi algoritma *modern* yang lebih kompleks [4].

Beberapa penelitian terdahulu telah mencoba mengimplementasikan metode ini sebagai sarana belajar, namun masih memiliki batasan pada sisi interaktivitas dan aksesibilitas. Sebagai contoh, penelitian oleh Pratiwi et al., (2022) berfokus pada implementasi Caesar Cipher menggunakan Visual Basic 2010 berbasis desktop yang memerlukan instalasi *environment* tertentu, sehingga kurang praktis untuk pembelajaran mandiri yang cepat. Selain itu, penelitian dari Sinaga dan Frangk, (2023) lebih menekankan pada analisis keamanan algoritmanya secara teoritis tanpa menyediakan media visualisasi yang menunjukkan proses pergeseran karakter secara *real time* [5,6]. Akibatnya, pemahaman mahasiswa seringkali hanya terbatas pada menghafal rumus matematis, tanpa memahami secara intuitif bagaimana setiap karakter bertransformasi di balik layar. Melihat celah tersebut, penelitian ini bertujuan untuk mengembangkan “Aplikasi Simulasi Enkripsi Menggunakan Metode Caesar Cipher Berbasis Website”. Berbeda dengan penelitian sebelumnya, aplikasi ini dirancang secara khusus sebagai media visualisasi edukatif yang interaktif. Fokus utama aplikasi ini adalah menyajikan proses pergeseran alfabet pada metode Caesar Cipher secara jelas dan sistematis. Dengan memanfaatkan *platform* berbasis website, mahasiswa dapat mengakses simulasi ini secara langsung melalui peramban tanpa memerlukan proses instalasi. Melalui pendekatan ini, diharapkan mahasiswa, khususnya yang masih awam, dapat memperoleh gambaran visual yang lebih jelas mengenai logika dasar kriptografi, sehingga mempermudah proses transisi dalam mempelajari sistem keamanan data yang lebih lanjut.

2. METODE PENELITIAN

2.1 Analisis Permasalahan

Permasalahan utama dalam pembelajaran kriptografi bagi mahasiswa pemula adalah sulitnya memahami konsep algoritma yang bersifat abstrak [7]. Caesar Cipher, sebagai algoritma kriptografi klasik, memiliki peran penting sebagai *fundamental* awal untuk memahami konsep enkripsi sebelum mempelajari algoritma kriptografi modern yang lebih kompleks [8]. Namun, proses pembelajarannya masih didominasi oleh pendekatan teoritis dan perhitungan manual tanpa visualisasi pergeseran alfabet yang jelas, sehingga menyulitkan pemahaman konseptual mahasiswa. Oleh karena itu, diperlukan sebuah sistem berbasis website yang mampu memvisualisasikan proses enkripsi Caesar Cipher secara interaktif dan mudah dipahami, sehingga mahasiswa dapat memahami logika dasar kriptografi secara bertahap sebagai bekal untuk mempelajari sistem keamanan data pada tahap selanjutnya [9].

2.2 Pengembangan Sistem

Penelitian ini menggunakan metode *Prototype* dalam pengembangan sistem. Metode ini dipilih karena memungkinkan pengembangan aplikasi dilakukan secara bertahap dan berulang sesuai kebutuhan pengguna [10]. Tahapan pengembangan meliputi analisis kebutuhan, perancangan dan pembuatan *prototype* aplikasi simulasi enkripsi Caesar Cipher berbasis

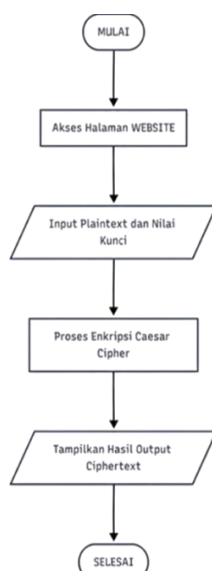
website, evaluasi serta penyempurnaan *prototype* berdasarkan umpan balik pengguna, hingga implementasi sistem *final* sebagai media pembelajaran interaktif [11].



Gambar 1. Metode Prototype

2.2 Desain Flowchart

Alur dari aplikasi ini dirancang untuk membantu pengguna memahami cara kerja enkripsi klasik dengan pergeseran karakter (*shift*) secara sederhana dan interaktif. Pengguna dapat memasukkan *teks* asli (*plaintext*) serta nilai pergeseran kunci, kemudian sistem akan memproses data tersebut menggunakan rumus Caesar Cipher untuk menghasilkan *teks* terenkripsi (*ciphertext*). Dari sisi fungsional, sistem berfokus pada proses enkripsi. Hal ini menjadikan aplikasi lebih sesuai sebagai media pembelajaran kriptografi dasar, khususnya untuk memahami konsep substitusi karakter pada Caesar Cipher.



Gambar 2. Flowchart Enkripsi Caesar Cipher

3. HASIL DAN PEMBAHASAN

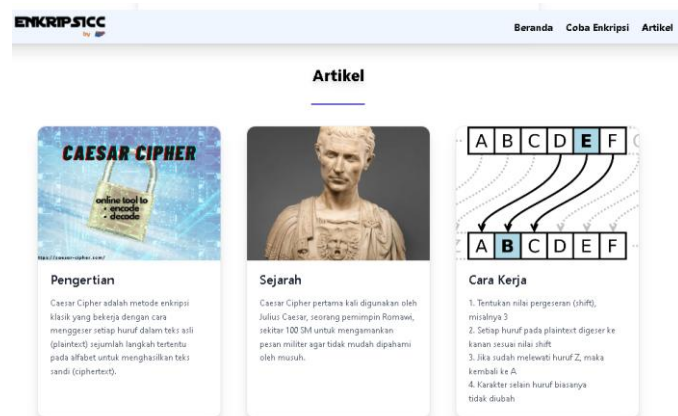
3.1 Implementasi dan Pengujian

Aplikasi simulasi enkripsi Caesar Cipher berbasis website diimplementasikan berdasarkan hasil pengembangan *prototype* yang telah disempurnakan. Aplikasi ini memungkinkan pengguna memasukkan *teks* dan nilai pergeseran (*key*) serta menampilkan hasil enkripsi secara interaktif dengan visualisasi pergeseran alfabet.









Gambar 3. Halaman Utama

Gambar 4. Halaman Simulasi Enkripsi



Gambar 6. Halaman Seputar Enkripsi Caesar Cipher

Pengujian dilakukan menggunakan metode *Black Box* untuk memastikan fungsi *input*, proses enkripsi, dan tampilan hasil berjalan dengan baik. Hasil pengujian menunjukkan bahwa aplikasi berfungsi sesuai tujuan dan layak digunakan sebagai media pembelajaran dasar kriptografi sebelum mempelajari algoritma keamanan data yang lebih lanjut.

Tabel 1. Pengujian Simulasi Enkripsi Caesar Cipher				
Skenario	Test Case	Keinginan Hasil	Hasil Pengujian	Kesimpulan
Tidak melakukan <i>input teks</i>		Sistem menampilkan notifikasi bahwa <i>teks</i> masukan tidak ada		Valid
<i>Input teks</i> tanpa pergeseran Caesar Cipher		Sistem menghasilkan <i>teks</i> keluaran yang identik dengan <i>teks</i> masukan		Valid
<i>Input teks</i> dengan pergeseran Caesar Cipher sebesar 2		Sistem menghasilkan teks terenkripsi dengan pergeseran alfabet sebanyak dua karakter		Valid

Dapat dilihat dari pengujian proses enkripsi Caesar Cipher menggunakan pemetaan alfabet ke bilangan numerik dengan ketentuan:

$$A = 0, B = 1, \dots, Z = 25 \tag{1}$$

Rumus enkripsi Caesar Cipher dinyatakan sebagai:

$$C_i = (P_i + K) \bmod 26 \tag{2}$$

Dengan:

- P_i = nilai numerik *plainteks* ke- i
- K = nilai kunci (*key*)
- C_i = nilai numerik *ciphertext* ke- i

Diketahui:

$$Plainteks = Belajar, K = 2 \tag{3}$$

Maka proses enkripsi setiap karakter adalah sebagai berikut:

$$B = 1 \rightarrow (1 + 2) \bmod 26 = 3 \rightarrow D \tag{4}$$

$$e = 4 \rightarrow (4 + 2) \bmod 26 = 6 \rightarrow g \tag{5}$$

$$l = 11 \rightarrow (11 + 2) \bmod 26 = 13 \rightarrow n \tag{6}$$

$$a = 0 \rightarrow (0 + 2) \bmod 26 = 2 \rightarrow c \tag{7}$$

$$j = 9 \rightarrow (9 + 2) \bmod 26 = 11 \rightarrow l \tag{8}$$

$$a = 0 \rightarrow (0 + 2) \bmod 26 = 2 \rightarrow c \tag{9}$$

$$r = 17 \rightarrow (17 + 2) \bmod 26 = 19 \rightarrow t \tag{10}$$

Sehingga diperoleh hasil ciphertext:

$$Chipertext = Dgnclct \tag{11}$$

3.2 Hasil

Pengumpulan data dalam penelitian ini menggunakan data primer yang diperoleh melalui kuesioner berbasis Google Form. Kuesioner disebarkan kepada mahasiswa sebagai responden untuk mengetahui tingkat pengetahuan awal mengenai kriptografi, khususnya Caesar Cipher, serta mengevaluasi dampak penggunaan aplikasi simulasi enkripsi berbasis website terhadap pemahaman mereka.

Kuesioner awal diikuti oleh 45 responden. Hasil pengumpulan data ditunjukkan pada Tabel 2.

Tabel 2. Tingkat Pengetahuan Awal Mahasiswa terhadap Kriptografi

Pilihan	Ya	Tidak	Ragu-ragu
Responden	14	25	6

Berdasarkan Tabel 2, dapat diketahui bahwa hanya 14 mahasiswa yang telah mengetahui konsep kriptografi, sementara 31 mahasiswa belum memiliki pemahaman yang jelas mengenai kriptografi. Data ini menunjukkan bahwa sebagian besar responden atau mahasiswa masih berada pada tahap awal dalam mengenal sebuah konsep keamanan data.

Selanjutnya, dilakukan pengumpulan data terhadap mahasiswa yang belum memahami kriptografi terkhususnya dibagian fundamental awal Caesar Cipher untuk mengetahui minat mereka dalam mempelajari kriptografi setelah diberikan penjelasan singkat mengenai algoritma atau metode Caesar Cipher. Jumlah responden atau mahasiswa pada tahap ini adalah 31 mahasiswa, sebagaimana ditunjukkan pada bagian Tabel 3.

Tabel 3. Minat Mahasiswa Mempelajari Kriptografi Dasar

Pilihan	Ya	Tidak	Ragu-ragu
Responden	17	10	4

Dari data tersebut, sebanyak 17 mahasiswa menunjukkan ketertarikan untuk mempelajari kriptografi dasar, sedangkan 14 mahasiswa belum menunjukkan minat yang kuat. Hal ini mengindikasikan bahwa pengenalan awal terhadap konsep kriptografi dapat meningkatkan ketertarikan mahasiswa.

Evaluasi tingkat pemahaman mahasiswa terhadap Caesar Cipher sebelum menggunakan aplikasi simulasi dilakukan terhadap 17 mahasiswa yang bersedia mengikuti uji coba. Hasilnya disajikan pada Tabel 4.

Tabel 4. Tingkat Pemahaman Mahasiswa Sebelum Menggunakan Aplikasi

Tingkat Pemahaman	Jumlah Responden
1	5
2	4
3	5
4	2
5	1

Data menunjukkan bahwa sebagian besar mahasiswa berada pada tingkat pemahaman rata-rata ke bawah, sehingga diperlukan media pembelajaran yang mampu membantu meningkatkan pemahaman secara bertahap.

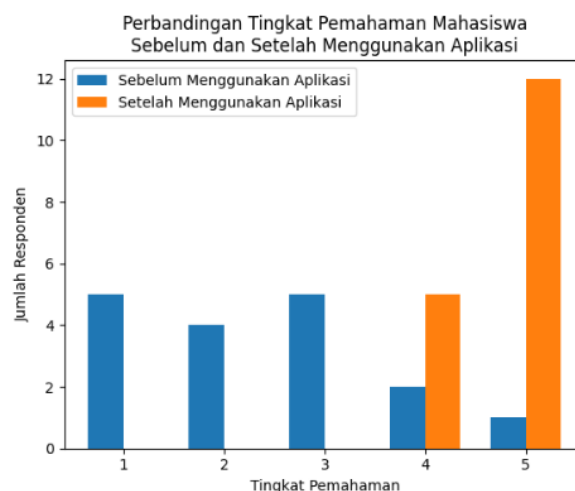
Setelah menggunakan aplikasi simulasi enkripsi Caesar Cipher berbasis website, dilakukan pengukuran ulang tingkat pemahaman mahasiswa. Hasilnya ditunjukkan pada Tabel 5.

Tabel 5. Tingkat Pemahaman Mahasiswa Setelah Menggunakan Aplikasi

Tingkat Pemahaman	Jumlah Responden
1	0
2	0
3	0
4	5
5	12

Berdasarkan Tabel 5, terlihat adanya peningkatan signifikan pada tingkat pemahaman mahasiswa. Jumlah mahasiswa dengan pemahaman tinggi (tingkat 4 dan 5) meningkat secara signifikan dibandingkan sebelum menggunakan aplikasi.

Data tingkat pemahaman mahasiswa sebelum dan sesudah penggunaan aplikasi simulasi Caesar Cipher divisualisasikan dalam bentuk diagram untuk menunjukkan perubahan dan peningkatan pemahaman secara komparatif.



Gambar 7. Perbandingan Tingkat Pemahaman Mahasiswa Sebelum dan Sesudah Pemakaian Aplikasi Simulasi

4. KESIMPULAN

Aplikasi simulasi enkripsi Caesar Cipher berbasis website yang dikembangkan dengan metode *prototype* berhasil diimplementasikan sebagai media pembelajaran kriptografi dasar dan telah diuji menggunakan metode *black box* dengan hasil seluruh fungsi berjalan sesuai perancangan. Berdasarkan evaluasi pengguna, sebelum menggunakan aplikasi sebanyak 82,4% mahasiswa berada pada tingkat pemahaman rendah hingga sedang (tingkat 1–3), sedangkan hanya 17,6% yang memiliki pemahaman tinggi (tingkat 4–5). Setelah menggunakan aplikasi,

terjadi peningkatan signifikan, di mana 100% mahasiswa berada pada tingkat pemahaman tinggi (tingkat 4–5). Hasil ini menunjukkan bahwa aplikasi simulasi efektif dalam meningkatkan pemahaman mahasiswa terhadap konsep *fundamental* Caesar Cipher sebagai dasar sebelum mempelajari algoritma keamanan data yang lebih lanjut. Pengembangan selanjutnya disarankan untuk menambahkan algoritma kriptografi lain sebagai perbandingan, fitur dekripsi, serta evaluasi pembelajaran yang lebih mendalam. Selain itu, pengujian dengan jumlah responden yang lebih besar dan integrasi materi pendukung diharapkan dapat meningkatkan efektivitas aplikasi sebagai media pembelajaran.

DAFTAR PUSTAKA

- [1] Lutfika, A., Verina, W., 2025, Aplikasi Keamanan Data File Hasil Pemilihan Ketua Osis Menggunakan Metode Modifikasi Caesar Cipher (Studi Kasus MA PAB 8 Saentis), *Prosiding Seminar Nasional Multi Disiplin Ilmu (Senadimu)*, No.1, Vol.2, 98-114, <https://senadimu.potensi-utama.org/index.php/home/article/view/437>.
- [2] Saragih, J. G. G., 2025, Penerapan Kriptografi untuk Pengamanan Data Nilai Siswa dengan Algoritma Super Enkripsi. *ADA Journal of Information System Research*, No.2, Vol.2, 77-85, <https://doi.org/10.64366/adajisr.v2i2.78>.
- [3] Aprianti, E., Marsehan, A., 2025, Analisis dan Implementasi Algoritma Caesar Cipher Dalam pengamanan Pesan Teks berbasis Web di Desa. *Digital Transformation Technology*, No.1, Vol.5, 191-196, <https://doi.org/10.47709/digitech.v5i1.5984>.
- [4] Kurnia, S. P., Ndruru, S., Tambunan, N. P., Hasbially, M., Turmudi, A., 2025, Analisis Performa Beaufort Cipher Dan ROT13 Dalam Proses Enkripsi Dan Dekripsi Pada Data Teks. *Jurnal Media Informatika*, No.2, Vol.6, 1058-1065, <https://doi.org/10.55338/jumin.v6i2.5363>.
- [5] Pratiwi, R., Utami, L. C., Bima Sakti, R., Triase., 2022, Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher. *Bulletin of Information Technology (BIT)*, No.4, Vol.3, 367-373, <https://doi.org/10.47065/bit.v3i4.420>.
- [6] Sinaga, R., Frangk., 2023, Modifikasi Algoritma Caesar Cipher Dengan Menambahkan Key Untuk Peningkatan Keamanan. *CSRID (Computer Science Research and Its Development Journal)*, No.2, Vol.15, 156-166, <https://doi.org/10.22303/csr-id.15.2.2023.156-166>.
- [7] Raja, R., Nainggolan, A., Naibaho, D., Kartika, D., 2025, Pengembangan Permainan Edukasi Kriptografi Menggunakan Rpg Maker Mz. *Jurnal Mathedu (Mathematic Education Journal)*, No.1, Vol.8, 19-30, <https://doi.org/10.37081/mathedu.v8i1.6768>.
- [8] Vebby., Ahmad, S., Van, L. L., 2023, Penerapan Algoritma Caesar Cipher Dalam Metode Kriptografi Klasik Pada Panic Button. *Zonasi: Jurnal Sistem Informasi*, No.1, Vol.5, 126-136, <https://doi.org/10.31849/zn.v5i1.13075>.
- [9] Ardiyanto. M. A. R., 2025, Membangun Fondasi Pemahaman Tentang Caesar Cipher Bagi Siswa SMA. *Journal of Cyber Community Services*, No.1, Vol.1, 21-25, <https://doi.org/10.64163/joccs.v1i1.29>.
- [10] Martantoh. E., Harahap, J. A., 2023, Perancangan Sistem Informasi Data Nilai Siswa Di Sman 2 Padang Bolak Sumatera Utara Menggunakan Metode Prototyping. *Journal of Innovation and Future Technology (IFTECH)*, No.2, Vol.5, 24-33, <https://doi.org/10.47080/ifttech.v5i2.2694>.
- [11] Kustanto, P., Ramadhan, B. K., Noeman, A., 2024, Penerapan Metode Prototype dalam Perancangan Media Pembelajaran Interaktif. *Journal of Students Research in Computer Science*, No.1, Vol.5, 83-94, <https://doi.org/10.31599/6x0dfz47>.