E.ISSN.2614-6061
P.ISSN.2527-4295
DOI : 10.37081/ed.v13i2.7399
Vol. 13 No. 2 Edisi Mei 2025, pp.741-745

# PENERAPAN ALGORITMA KRIPTOGRAFI PADA SISTEM ENKRIPSI DAN DESKRIPSI PESAN BERBASIS WEB MENGGUNAKAN VISUAL STUDIO CODE

Oleh :
**Ermawita[1)], Rahmad Fauzi[2)], Meliza[3)]**
[1,2,3] Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Institut Pendidikan Tapanuli Selatan
[1]email: ermajuwita91@gmail.com
[2]email: udauzi@gmail.com
[3]email: melizamelisa1@gmail.com

**Informasi Artikel**
**Riwayat Artikel :**
Submit, 26 April 2025
Revisi, 4 Mei 2025
Diterima, 14 Mei 2025
Publish, 15 Mei 2025

**Kata Kunci :**
Kriptografi,
Enkripsi,
Deskripsi.

**ABSTRAK**
Keamanan data dalam komunikasi digital menjadi hal yang sangat penting, terutama pada sistem berbasis web. Penelitian ini membahas penerapan algoritma kriptografi untuk enkripsi dan deskripsi pesan dalam sebuah aplikasi berbasis web dengan menggunakan Visual Studio Code sebagai lingkungan pengembangan. Tujuan dari penelitian ini adalah untuk merancang dan membangun sistem yang mampu menjaga kerahasiaan informasi melalui proses enkripsi saat pengiriman pesan dan deskripsi saat penerimaan pesan. Sistem dikembangkan menggunakan bahasa pemrograman HTML, CSS, JavaScript, dan PHP. Algoritma kriptografi yang digunakan adalah Caesar cipher, Vigenere cipher, Affine Cipher dan Hill Cipher karena keamanannya yang tinggi dan efisiensinya dalam pengolahan data. Hasil implementasi menunjukkan bahwa sistem dapat mengenkripsi pesan secara efektif menjadi format yang tidak terbaca dan dapat mengembalikannya ke bentuk semula tanpa kehilangan informasi. Dengan demikian, sistem ini dapat meningkatkan keamanan komunikasi data pengguna dan mencegah akses tidak sah terhadap isi pesan.



***Corresponding Author:***
Nama: Ermawita
Afiliasi: Institut Pendidikan Tapanuli Selatan
Email: ermajuwita91@gmail.com

## 1. PENDAHULUAN

Dalam era digital yang semakin maju, pertukaran informasi melalui jaringan internet menjadi hal yang umum dan tak terhindarkan. Komunikasi berbasis web digunakan dalam berbagai sektor seperti pendidikan, bisnis, pemerintahan, dan sosial. Namun, seiring dengan meningkatnya penggunaan teknologi informasi, ancaman terhadap keamanan data juga semakin kompleks. Informasi yang dikirimkan secara terbuka melalui jaringan dapat dengan mudah disadap, dimanipulasi, atau disalahgunakan oleh pihak yang tidak bertanggung jawab.

Untuk mengatasi permasalahan tersebut, diperlukan suatu mekanisme pengamanan data yang dapat menjaga kerahasiaan isi pesan. Salah satu metode yang paling umum digunakan adalah kriptografi, yaitu ilmu yang berkaitan dengan pengamanan informasi melalui proses enkripsi (penyandian) dan dekripsi (pengembalian ke bentuk asli). Berbagai algoritma kriptografi klasik seperti Caesar Cipher, Vigenère Cipher, Affine Cipher, dan Hill Cipher telah dikenal luas dan masih digunakan sebagai dasar pembelajaran maupun dalam implementasi sistem pengamanan tingkat dasar.

Caesar Cipher merupakan algoritma sederhana yang mengenkripsi pesan dengan menggeser huruf-huruf dalam alfabet. Vigenère Cipher memperluas konsep ini dengan menggunakan kata kunci sebagai dasar pergeseran huruf. Affine Cipher mengkombinasikan operasi perkalian dan penjumlahan untuk memetakan karakter, sementara Hill Cipher menggunakan konsep matriks dalam proses enkripsi. Meskipun algoritma ini tergolong

klasik, penerapannya dalam sistem modern berbasis web tetap memberikan manfaat edukatif dan fungsional, terutama dalam memahami prinsip dasar pengamanan data.

Visual Studio Code dipilih sebagai alat pengembangan karena kemudahan penggunaannya serta dukungannya terhadap berbagai bahasa pemrograman web seperti HTML, CSS, JavaScript, dan PHP, yang memungkinkan pembuatan sistem enkripsi dan dekripsi secara efisien dan interaktif.

## 2. METODE PENELITIAN

Penelitian ini merupakan penelitian rekayasa perangkat lunak yang bersifat deskriptif kuantitatif sesuai dengan Tujuan dari penelitian ini adalah merancang dan mengimplementasikan sistem enkripsi dan deskripsi pesan berbasis web menggunakan algoritma kriptografi klasik. Penelitian ini menggunakan metode eksperimental, dengan tahapan pengembangan sistem dimulai dari analisis kebutuhan hingga pengujian fungsionalitas sistem.

**Alur Penelitian**

Berikut adalah tahapan dan alur yang digunakan dalam proses penelitian:

a. Identifikasi Masalah

Tahapan identifikasi masalah adalah dengan menentukan kebutuhan keamanan data dalam komunikasi berbasis web serta pentingnya penggunaan algoritma kriptografi.

b. Studi Literatur

Tahap studi literartur yang dilaksanakan adalah melakukan kajian terhadap teori dasar kriptografi dan algoritma klasik yang digunakan: Caesar Cipher, Vigenère Cipher, Affine Cipher, dan Hill Cipher.

c. Perancangan Sistem

Tahapan perancangan system dilakukan dengan tahapan merancang antarmuka pengguna (UI) berbasis web menggunakan HTML dan CSS, menyusun logika proses enkripsi dan deskripsi berdasarkan algoritma kriptografi serta menentukan struktur kode dan alur data dalam sistem.

d. Implementasi Sistem

Pada tahap implementasi sistem menggunakan Visual Studio Code sebagai lingkungan pengembangan., Mengembangkan sistem menggunakan HTML, CSS, JavaScript, dan PHP dan menerapkan masing-masing algoritma kriptografi sebagai fungsi dalam sistem yang dapat dipilih oleh pengguna.

e. Pengujian Sistem

Proses pengujian sistem dilakukan menggunakan metode black-box testing untuk mengevaluasi hasil enkripsi dan deskripsi dengan melibatkan skenario uji terhadap pesan teks dengan panjang dan karakteristik berbeda serta menilai keakuratan hasil dekripsi, kestabilan sistem, dan kecepatan proses.

f. Analisis Hasil

Tahapan analisiis hasil dimulai dari menganalisis keberhasilan sistem dalam mengembalikan pesan asli melalui proses dekripsi dan membandingkan kompleksitas dan efektivitas dari masing-masing algoritma yang digunakan.

g. Kesimpulan dan Saran

Tahapan terakhir yang dilaksanakan adalah menyimpulkan keberhasilan sistem dan memberikan saran untuk pengembangan lanjutan.

## 3. HASIL DAN PEMBAHASAN

Sistem enkripsi dan deskripsi pesan berbasis web berhasil dikembangkan menggunakan Visual Studio Code. Antarmuka sistem memungkinkan pengguna untuk memasukkan pesan teks, memilih salah satu dari empat algoritma kriptografi (Caesar, Vigenère, Affine, Hill), lalu mengenkripsi dan mendekripsi pesan sesuai algoritma yang dipilih. Sistem ini dibangun menggunakan HTML dan CSS untuk tampilan, JavaScript untuk validasi input, serta PHP untuk logika enkripsi dan deskripsi.

Hasil uji menunjukkan bahwa Aplikasi berhasil mengolah input dan menampilkan hasil tanpa error, Struktur file yang modular mempermudah pengembangan dan pemeliharaan dan Penggunaan function.php meningkatkan keterbacaan kode.

**a. Algoritma Caesar chipper**

Algoritma Caesar chipper merupakan teknik kriptografi yang mengganti tiap huruf dalam pasan dengan huruf lain yang berjarak tertentu dalam alphabet. Tiap huruf alphabet digeser n huruf ke kanan dan dalam perhitungan ini terdapat bagian deskripsi dan enkripsi.

Dimana enkripsi adalah proses penyandian pesan dari plainteks ke cipherteks sedangkan deskripsi adalah proses pengambilan pesan dari cipherteks ke plainteks. Dalam perhitungan ini kita dapat menggunakan persamaan sebagai berikut

Persamaan enkripsi :

$E(x) = (Pi + k) \bmod 26$

Persamaan Deskripsi :

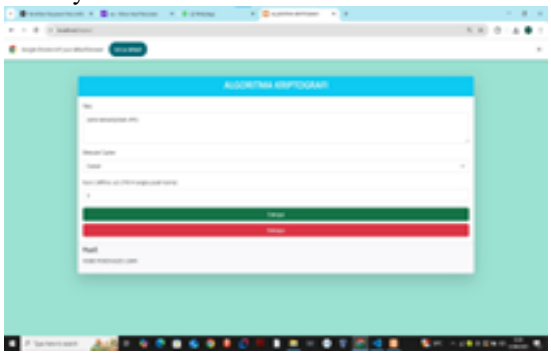
$D(x) = (Ci - k) \bmod 26$

Contoh Soal Proses Enkripsi dengan Algoritma Caesar Cipher

Soal : SAYA MAHASISWA VIF

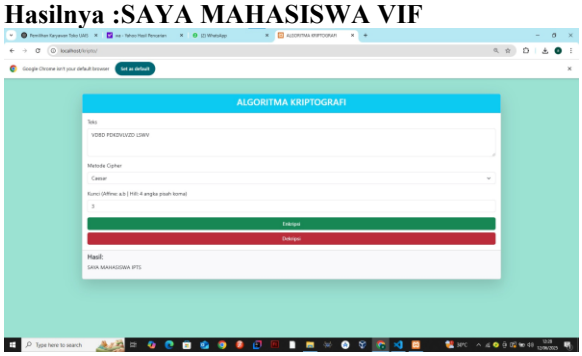
Key :3

Hasilnya : VDBD PDKDVLVZD LSWV



Gambar 1. Tampilan Antarmuka Aplikasi Algoritma Kriptografi perhitungan caisar bagian enkripsi.

Contoh Soal Proses Deskripsi dengan Algoritma Caesar Cipher
Soal : VDBD PDKDVLVZD LSWV
Key :3
**Hasilnya :SAYA MAHASISWA VIF**



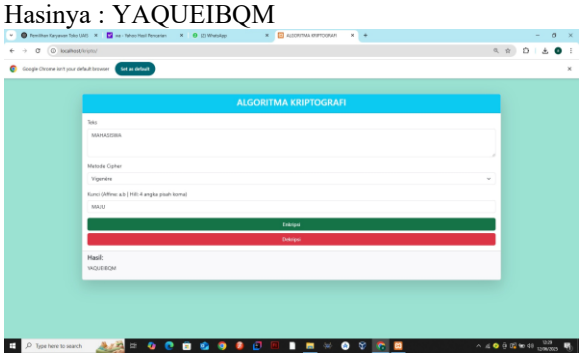

Gambar 2. Tampilan Antarmuka Aplikasi Algoritma Kriptografi perhitungan caisar bagian deskripsi.

**b. Algoritma Vigenere chiper**

Vigenere Chiper menggunakan tabel bujur sangkar dalam melakukan proser enkripsi. Algoritma Vigenere Chiper ditemukan oleh Blaise De Vigenere yang memiliki dua jenis perhitungan deskripsi dan enkripsi. Dimana enkripsi adalah proses penyandian pesan dari plainteks ke cipherteks sedangkan deskripsi adalah proses pengambilan pesan dari cipherteks ke plainteks. Vigenere chiper adalah metode menyandikan teks alpabet dengan menggunakan deretan sandı caesar berdasarkan huruf-huruf pada kata kunci. Seperti persamaan berikut

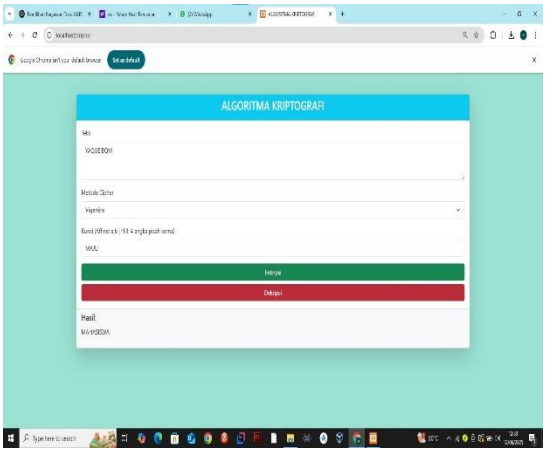
Persamaan enkripsi :
E(x) = (Pi + Ki) mod 26
Persamaan deskripsi :
D(x) = (Ci- Ki) mod 26

Contoh Soal Proses Enkripsi dengan Algoritma Vigenere Cipher
Soal : Mahasiswa
Key : Maju
Hasinya : YAQUEIBQM




Gambar 3. Tampilan Antarmuka Aplikasi Algoritma Kriptografi perhitungan vigenere bagian enkripsi

Contoh Soal Proses Deskripsi dengan Algoritma Vigenere Cipher.
Soal : YAQUEIBQM
Key : Maju
Hasinya : Mahasiswa




Gambar 4. Tampilan Antarmuka Aplikasi Algoritma Kriptografi perhitungan vigenere bagian deskripsi.

**c. Algoritma Afffine chiper**

Algoritma Affine Cipher merupakan perluasan dari caesar Chiper. Konsep dasar dari algoritma ini adalah mengalikan plainteks dengan sebuah kunci dan menimbulkan dengan sebuah pergeseran.

Rumus : E(x) = (a.x+b) mod m
dimana:
a = kunci utama
b = kunci kedua
m = Jumlah seluruh karakter yg akan digunakan dalam penyandian.
X = nilai plainteks yg akan disandikan

Pada perhitungan ini terdapat bagian deskripsi dan enkripsi. Dimana enkripsi adalah proses penyandian pesan dari plainteks ke cipherteks sedangkan deskripsi adalah proses pengambilan pesan dari cipherteks ke plainteks seperti pada gambar:

Contoh Soal Proses Enkripsi Menggunakan Affine Cipher
Rumus E(x) = (a.x+b) mod 26
Soal : IPTS
Key : 5,8
Hasinya : WFZU


Gambar 5. Tampilan Antarmuka Aplikasi Algoritma Kriptografi perhitungan affine bagian enkripsi.

Contoh Soal Proses Deskripsi Menggunakan Affine Cipher
Rumus D(x) = (a.x-b) mod 26
Soal : WFZU Key : 5,8
Hasinya : IPTS


Gambar 6. Tampilan Antarmuka Aplikasi Algoritma Kriptografi perhitungan affine bagian deskripsi.

**d. Algoritma Hill chipper**

Algoritma ini memanfaatkan perkalian antar matriks dan melakukan invers pada matriks. Algoritma ini menggunakan matrike berukuran MxM (Matriks persegi) sebagal kunci yang digunakan untuk melakukan proses enskripsi dan deskripsi. Dimana enkripsi adalah proses penyandian pesan dari plaintaks ke ciphertaks sedangkan deskripsi adalah proses pengambilan pesan dari ciphertaks ke plaintaks Proses enskripsi pada hill chiper dilakukan per blok Plainteks. Ukuran Blok x ukuran kunci.

Persamaan enkripsi :

$C = E(K^1 c) = K.\ P \bmod 26$

Persamaan deskripsi :

$P = D(K^{-1}.P) = K^{-1}.\ c \bmod 26$ dengan.

C= chiperteks

P= Plainteks

K =Kunci

seperti pada gambar:

Contoh Soal Proses Enkripsi Menggunakan Affine Hill Cipher

$C = E(K^{-1} c) = K.\ P \bmod 26$

Soal : KRIPTO

Key :2,1,3,4

Hasinya : LUFGAJ

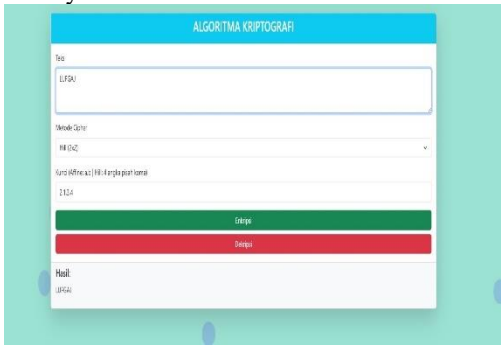

Gambar 7. Tampilan Antarmuka Aplikasi Algoritma Kriptografi perhitungan hill bagian enkripsi.

Contoh Soal Proses Deskripsi Menggunakan Hill Cipher

$P = D(K^{-1}P) = K^{-1}.\ c \bmod 26$

Soal : LUFGAJ Key :2,1,3,4

Hasinya : KRIPTO




Gambar 8. Tampilan Antarmuka Aplikasi Algoritma Kriptografi perhitungan hill bagian deskripsi.

## 4. KESIMPULAN

Berdasarkan hasil implementasi dan pengujian, dapat disimpulkan bahwa Sistem enkripsi dan deskripsi pesan berbasis web berhasil dikembangkan dengan baik dan dapat menjalankan fungsinya secara optimal menggunakan keempat algoritma kriptografi klasik. Setiap algoritma memiliki keunggulan dan kelemahan masing-masing, sehingga pemilihan algoritma sebaiknya disesuaikan dengan kebutuhan keamanan dan kompleksitas sistem: *Caesar Cipher* cocok untuk pemahaman dasar., *Vigenère Cipher* cocok untuk pengamanan tingkat menengah., *Affine Cipher* memberikan kombinasi matematis sederhana. Dan *Hill Cipher* memberikan keamanan lebih tinggi namun memerlukan pengolahan kunci yang tepat.

Penggunaan Visual Studio Code dan teknologi web (HTML, CSS, JS, PHP) mendukung pengembangan sistem secara fleksibel, interaktif, dan mudah digunakan oleh pengguna akhir. Sistem ini dapat dijadikan media pembelajaran kriptografi klasik sekaligus digunakan dalam konteks komunikasi sederhana yang tetap memperhatikan aspek keamanan pesan.

Secara keseluruhan, perbandingan keempat algoritma pada aplikasi web menunjukkan hierarki yang jelas. Caesar menawarkan kecepatan dan kemudahan, tetapi minim proteksi. Vigenère dan Affine memperkenalkan kompleksitas kunci dan keamanan yang lebih baik. Sementara Hill cipher mencapai ketahanan tertinggi di antara algoritma klasik. Selanjutnta, untuk proteksi keamanan yang lebih baik dalam penyandian pesan disarankan menggunakan pendekatan hybrid dengan menggunakan Caesar atau Vigenère untuk pesan ringan atau keperluan edukasi, dan Affine atau Hill untuk pesan sensitif atau panjang. Rekomendasi lebih lanjut menunjukkan perlunya integrasi dengan kriptografi modern seperti AES atau RSA dan pengamanan transport seperti TLS, guna membawa sistem ini menuju implementasi web aman di masa depan.

## 5. REFERENSI

Munir, R. (2015). *Kriptografi*. Bandung: Informatika.

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education.

Kurniawan, D. (2020). Implementasi Algoritma Caesar Cipher dalam Sistem Keamanan Informasi. *Jurnal Teknik Informatika*, 6(2), 110–118.

Siregar, A., & Prasetyo, H. (2021). Penerapan Algoritma Vigenère Cipher dalam Sistem Enkripsi Teks Berbasis Web. *Jurnal Teknologi Informasi dan Komputer*, 8(1), 45–52. https://doi.org/10.25126/jtik.v8i1.1234

Susanto, A., & Wijaya, H. (2019). Analisis Affine Cipher untuk Pengamanan Data Teks Menggunakan Bahasa Pemrograman PHP. *Jurnal Ilmiah Komputer dan Informatika (JIKI)*, 3(1), 22–30.

Rosita, E., & Putra, R. A. (2022). Implementasi Hill Cipher dalam Aplikasi Enkripsi Data Pesan. *Jurnal Sistem dan Teknologi Informasi*, 5(3), 134–140.

Pratama, R., & Nugroho, A. (2020). Perbandingan Kompleksitas Algoritma Kriptografi Klasik untuk Keamanan Pesan. *Jurnal Sistem Informasi*, 4(2), 78–85.

Kurniawan, A. (2018). *Belajar HTML, CSS, dan JavaScript untuk Pemula*. Jakarta: Elex Media Komputindo.

Mozilla Developer Network. (2023). *JavaScript Guide*. Retrieved from https://developer.mozilla.org/en-US/docs/Web/JavaScript/Guide

W3Schools. (2023). *PHP Tutorial*. Retrieved from https://www.w3schools.com/php/