REALISASI KRIPTOGRAFI KLASIK MENGGUNAKAN CAESAR CIPHER DAN VIGENÈRE CIPHER PADA PLATFORM APLIKASI WEB

Rizka Alfinatul Umam, Muhlis Tahir, Ika Maulidia, Zidan Zam Zami
Pendidikan Informatika, Universitas Trunojoyo Madura
Jl. Raya Telang, Perumahan Telang Inda, Telang, Kec. Kamal, Kabupaten Bangkalan, Jawa Timur 69162
220631100063@student.trunojoyo.ac.id

ABSTRAK

Perkembangan teknologi informasi yang pesat telah membuka banyak peluang bagi pertukaran data melalui platform web, namun juga meningkatkan risiko keamanan data. Penelitian ini bertujuan untuk mengembangkan dan menguji simulasi keamanan data pada platform web menggunakan teknik kriptografi klasik Caesar Cipher dan Vigenère Cipher. Metode penelitian yang diterapkan adalah penelitian terapan dengan fokus pada pengembangan aplikasi berbasis web menggunakan HTML, CSS, PHP, dan MySQL. Aplikasi ini dirancang dengan tiga fitur utama yaitu enkripsi, dekripsi, dan pencatatan riwayat aktivitas. Hasil penelitian menunjukkan bahwa implementasi kedua algoritma kriptografi berhasil mengenkripsi dan mendekripsi pesan dengan akurat sesuai dengan perhitungan manual. Algoritma Vigenère Cipher menunjukkan tingkat kompleksitas yang lebih tinggi dalam penyamaran pola teks dibandingkan Caesar Cipher, yang mengindikasikan keamanan yang lebih baik. Aplikasi web yang dikembangkan berhasil melakukan proses enkripsi dan dekripsi secara responsif, serta menyimpan hasil prosesnya ke dalam basis data. Penelitian ini memberikan kontribusi terhadap pemahaman mekanisme perlindungan data menggunakan kriptografi klasik dan dapat menjadi dasar pengembangan sistem keamanan yang lebih tangguh di masa depan.

Kata kunci : *kriptografi; enkripsi; dekripsi; Caesar Cipher; Vigenère Cipher; aplikasi web*

1. PENDAHULUAN

Perkembangan teknologi informasi telah mengubah berbagai aspek kehidupan secara signifikan, terutama dalam hal penggunaan platform web untuk pertukaran data. Dengan meningkatnya aktivitas berbasis web, risiko terhadap keamanan data pun semakin tinggi. Ancaman seperti peretasan, pencurian data, dan serangan siber lainnya menjadi tantangan serius bagi para pengembang platform web. Oleh karena itu, penting untuk menerapkan metode perlindungan data yang efektif, salah satunya melalui penggunaan teknik kriptografi [1].

Kriptografi adalah sebuah teknik yang digunakan untuk melindungi data dengan cara mengubah informasi menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang, kecuali dengan menggunakan kunci tertentu. Dengan penerapan teknik ini, kerahasiaan, keaslian, dan integritas data yang dikirimkan melalui platform web dapat terjamin. Oleh karena itu, simulasi penerapan teknik ini pada platform web menjadi penting guna menguji ketahanan sistem terhadap kemungkinan serangan.

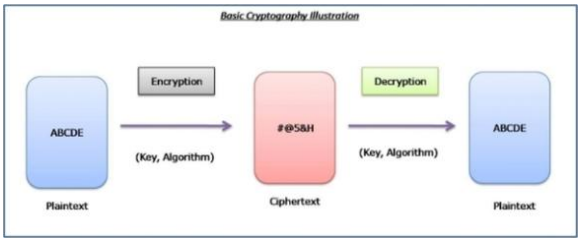
Dalam praktiknya, simulasi keamanan data yang berbasis kriptografi dilakukan dengan mengimplementasikan algoritma enkripsi dalam skenario nyata di *platform* web. Kemudian, efektivitas algoritma tersebut diukur terhadap berbagai jenis ancaman yang mungkin muncul. Hasil dari simulasi ini tidak hanya berperan dalam memahami mekanisme perlindungan data, tetapi juga menjadi acuan penting dalam merancang sistem keamanan yang lebih tangguh di masa depan [2]. Melalui pengujian yang sistematis, para pengembang dapat mengevaluasi kekuatan dan kelemahan dari metode kriptografi yang diterapkan.

Melalui penelitian tentang simulasi keamanan data pada *platform* web menggunakan teknik kriptografi ini, diharapkan dapat diperoleh gambaran yang lebih jelas mengenai efektivitas teknologi enkripsi dalam menjaga keamanan data pengguna. Selain itu, penelitian ini juga bertujuan untuk memberikan kontribusi nyata terhadap pengembangan teknologi keamanan informasi di Indonesia, khususnya dalam konteks meningkatnya kebutuhan akan perlindungan data pribadi di era digital saat ini.

2. TINJAUAN PUSTAKA

2.1. Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu "*kryptos*" dan "*graphein*". *Kryptos* memiliki arti tersembunyi, sedangkan *graphein* berarti menulis. Seperti yang dikemukakan oleh Nuryanto dalam Sari [3], kriptografi adalah ilmu dan seni untuk memastikan keamanan pesan. Algoritma kriptografi terdiri dari tiga fungsi dasar: enkripsi, dekripsi, dan kunci. Kriptografi tidak hanya menyembunyikan pesan, namun dengan kriptografi dipastikan terjaminnya integritas pesan agar sampai ke penerima dalam keadaan utuh. Menurut Azhari [4] terdapat dua proses dalam kriptografi, yaitu enkripsi dan dekripsi. Untuk gambaran mengenai ilustrasi kriptografi dapat dilihat dari gambar 1.



Gambar 1. Ilustrasi kriptografi

Adapun istilah-istilah yang digunakan di dunia kriptografi, yaitu:

a. *Plaintext*, merupakan pesan asli yang akan dijaga kerahasiaan isi pesannya.
b. *Ciphertext*, merupakan hasil pesan asli yang sudah dikodekan.
c. Enkripsi, merupakan proses pengkodean dari *plaintext* menjadi *ciphertext*.
d. Dekripsi, merupakan proses dekode dari *ciphertext* menjadi *plaintext* sehingga pesan dapat terbaca dengan jelas.
e. Kunci, merupakan input rahasia yang digunakan oleh algoritma kriptografi untuk mengenkripsi atau mendekripsi data.

Ilmu kriptografi diciptakan bukannya tanpa alasan. Ada 5 tujuan dari kriptografi yaitu sebagai berikut [5]:

a. *Privacy/Confidentially*. *Privacy*, artiny kriptografi bersifat rahasia, sedangkan *confidentially* adalah hubungan antara data yang diberikan ke pihak laik untuk keperluan tertentu dan hanya diizinkan apabila untuk keperluan tertentu.
b. *Integrity*, kriptografi menekankan bahwa isi pesan tidak boleh diubah tanpa seizin dari pemilik pesan. Pesan yang diterima harus sampai dengan isi yang sesuai dan sama persis saat informasi dikirim.
c. *Authenticity*, Aspek ini berhubungan dengan ketersediaan data dan informamsi. Data dan informasi yang berbeda dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak.
d. *Availability*, kriptografi dapat menghindari terjadinya penyangkalan, yang mana pengirim pesan akan menyangkal bahwa ia telah mengirim pesan pun sebaliknya penerima pesan akan menyangkal bahwa telah menerima pesan.
e. *Access control*, hal ini berhubungan dengan klasisfikasi data, mekanisme autentikasi dan juga privasi. *Access control* sering digunakan untuk melakukan kombinasi *user id/password* atau dengan menggunakan mekanisme lain.

2.2. Enkripsi dan Dekripsi

Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (encryption). Sedangkan sebaliknya, mengubah *ciphertext* menjadi *plaintext* merupakan definisi dekripsi. Pada sebuah keamanan jaringan, enkripsi adalah proses mengubah *plaintext* menjadi *ciphertext* sehingga pesan yang dikirim tidak dapat dikenali. Sedangkan, dekripsi merupakan proses dekode *ciphertext* menjadi *plaintext* kembali seperti semula sehingga pesan dapat dengan mudah dibaca [6].

2.3. Caesar Cipher dan Vigenère Cipher

Caesar Cipher diambil dari nama Julius Caesar, seorang kaisar Roma yang menggunakan cipher substitusi untuk mengirim pesan ke Marcus Tullius Cicero. Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Dalam Caesar cipher, untuk mengubah *plaintext* menjadi *ciphertext*, dilakukan berdasarkan kunci digunakan. Enkripsi pada Caesar Cipher dilakukan dengan menggeser huruf dalam jumlah tertentu berdasarkan kunci yang digunakan [6].

Vigenère Cipher adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Vigenère Cipher menggunakan kunci dalam bentuk kata atau frasa, yang kemudian diulang sepanjang teks. Enkripsi dilakukan dengan menambahkan nilai huruf dari kunci ke huruf teks asli, sementara dekripsi dilakukan dengan pengurangan.

Caesar Cipher dan Vigenère Cipher keduanya merupakan teknik dari kriptografi klasik yang dapat digunakan untuk mengamankan isi pesan dengan melakukan metode substitusi huruf [7]. Caesar Cipher merupakan metode sederhana yang menggantikan huruf dari *plaintext* ke *ciphertext* dengan melakukan pergeseran huruf. Sedangkan Vigenère Cipher memiliki algoritma yang lebih kompleks dengan menerapkan serangkaian Caesar Cipher berdasarkan huruf-huruf dalam kata kunci. Setiap huruf dalam *plaintext* dienkripsi dengan pergeseran yang ditentukan oleh huruf yang ada pada kata kunci. Hal ini yang membuat Vigenère Cipher lebih susah untuk dipecahkan.

2.4. Aplikasi Berbasis Web

Untuk membangun sebuah aplikasi berbasis web yang dapat berfungsi, HTML dan CSS sangat berperan penting untuk tujuan tersebut. HTML dapat digunakan untuk membangun struktur halaman web, sedangkan CSS digunakan untuk mengatur tampilan dan tata letak [8]. Selain itu, PHP juga sering digunakan sebagai bahasa pemrograman untuk memproses logika, serta MySQL berperan sebagai sistem manajemen basis data relasional untuk menyimpan dan mengelola data [9].

Beberapa penelitian telah mengintegrasikan kriptografi klasik, termasuk Caesar Cipher dan Vigenère Cipher, dengan aplikasi berbasis web untuk pengamanan data. Syahputra [10] mengembangkan aplikasi tabungan berbasis web dengan mengenkripsi data pengguna dengan menggunakan algoritma Vigenère Cipher dan disimpan ke dalam *database*

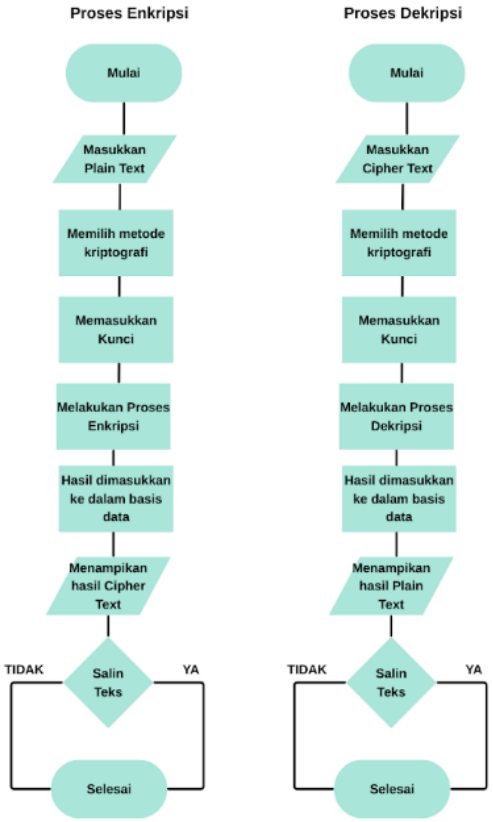
dalam bentuk *ciphertext* dan dapat didekripsi kembali. Demikian pula penelitian oleh Azura dkk [11] yang membuat aplikasi web kriptografi berbasis PHP untuk enkripsi teks dengan vignere cipher.

3. METODE PENELITIAN

Penelitian ini menggunakan metode terapan, yaitu penelitian yang berfokus pada penyelesaian masalah secara langsung dan praktis. Penelitian terapan ini tidak berfokus pada pengembangan sebuah ide, teori, atau gagasan tapi lebih berfokus penerapan penelitian tersebut dalam kehidupan sehari-hari, dimana ciri utama dari penelitian ini adalah tingkat abstraksi yang rendah, dan manfaat atau dampaknya dapat dirasakan secara langsung. Ciri khas dari penelitian terapan adalah tingkat abstraksinya yang rendah serta manfaat atau dampak nyata yang dapat dirasakan secara langsung oleh pengguna [12].

Penelitian ini menerapkan algoritma kriptografi klasik Caesar Cipher dan Vigenère Cipher melalui pengembangan aplikasi berbasis web. Pemilihan kedua algoritma tersebut didasari pada beberapa pertimbangan bahwa algoritma kriptografi klasik ini dapat memberikan konsep dasar kriptografi, dasar pengembangan kriptografi modern, dan dapat memahami potensi-potensi kelemahan sistem [7].

3.1. Desain Sistem



Gambar 2. Diagram alir proses enkripsi dan dekripsi

Pada penelitian ini, sistem yang dikembangkan merupakan aplikasi berbasis web. Aplikasi ini dapat memproses langkah-langkah enkripsi maupun dekripsi terhadap teks yang dimasukkan pengguna. Aplikasi ini menyediakan dua fitur yang diambil dari metode kriptografi klasik, yaitu Caesar Cipher dan Vigenère Cipher. Setelah pengguna memilih salah satu metode yang tersedia dan memasukkan kunci, aplikasi akan memproses hasilnya sesuai metode yang dipilih dan menampilkan hasilnya. Pengguna juga diberi fitur untuk langsung menyalin hasil enkripsi dan dekripsi. *Flowchart* sistem ditampilkan pada Gambar 2 berikut, yang menggambarkan proses enkripsi dan dekripsi dari input pengguna hingga penyimpanan ke basis data.

Setelah dilakukannya proses enkripsi dan dekripsi, beberapa data akan dimasukkan ke dalam database. Adapun beberapa data yang dimasukkan adalah teks asli, metode, kunci, hasil enkripsi/dekripsi, dan tanggal dilakukannya proses. Data-data ini dimunculkan pada tab Riwayat.

3.2. Desain Basis Data

Basis data yang digunakan adalah MySQL dengan nama *database* "db_enkripsi_dekripsi" dan memiliki satu tabel yaitu "enkripsi_dekripsi". Tabel tersebut menyimpan berbagai informasi yang didapat dari setiap proses enkripsi ataupun dekripsi yang dilakukan.

Adapun struktur tabel "enkripsi_dekripsi adalah sebagai berikut :

a. id (Primary Key): Kode unik otomatis untuk setiap entri.
b. teks_asli: Teks yang dimasukkan oleh pengguna.
c. hasil: Teks hasil proses enkripsi atau dekripsi.
d. metode: Metode yang digunakan, yaitu *Caesar* atau *Vigenère*.
e. kunci: Kunci yang digunakan dalam proses enkripsi atau dekripsi.
f. tanggal: Tanggal ketika proses enkripsi atau dekripsi dilakukan

Desain basis data ini bersifat sederhana dan digunakan untuk mencatat setiap aktivitas pengguna dalam sistem secara sistematis.

3.3. Teknologi yang Digunakan

Pengembangan aplikasi ini menggunakan beberapa teknologi sebagai berikut.

a. *Front End*
   - HTML : Html digunakan pada pengembangan ini untuk mengatur struktur dasar pada laman web.
   - CSS : CSS digunakan untuk mendesain laman web agar terlihat lebih menarik dan *user-friendly.*
b. *Back End*
   - PHP : PHP digunakan untuk memproses enkripsi dan dekripsi serta sebagai jembatan untuk berinteraksi dengan database.
   - MySQL : Untuk menyimpan data hasil enkripsi dan dekripsi.

c. Server Lokal
   - XAMPP : Digunakan sebagai platform pengembangan lokal yang menyediakan server Apache dan MySQL secara terintegrasi.

3.4. Prosedur Implementasi

Langkah-langkah yang dilakukan dalam pengembangan sistem ini dilakukan melalui tahapan berikut.

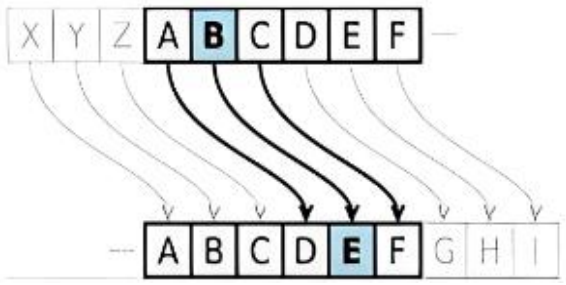
3.5. Pengembangan Antar Muka

Penerapan rancangan antarmuka pengguna menggunakan HTML sebagai struktur dasar dan CSS digunakan untuk mendesain laman web. Pada halaman web terdapat tiga tab, yaitu tab Enkripsi, Dekripsi, dan Riwayat. Pada halaman Enkripsi dan Dekripsi masing-masing terdapat form input untuk memasukkan teks yang akan dienkripsi/dekripsi, lalu pilihan metode enkripsi/dekripsi. Hasil proses ditampilkan secara langsung di bagian bawah.

3.6. Implementasi Algoritma Caesar Cipher

Adapun proses Caesar Cipher adalah sebagai berikut [13] :

a. Tentukan berapa besar pemindahan karakter yang dipakai untuk membuat cipherteks ke plainteks.
b. Tukar posisi karakter plainteks menjadi cipherteks berdasarkan pemindahan yang telah ditentukan sebelumnya. Contoh, pemindahan = 3. Jadi huruf A digeser menjadi huruf D, huruf B menjadi huruf E, dan berikutnya



Gambar 3. Proses perpindahan huruf Caesar Cipher

Formula yang digunakan untuk enkripsi adalah:

$$E(x) = (x + k) \mod 26 \quad (1)$$

Sedangkan untuk dekripsi:

$$D(x) = (x - k) \mod 26 \quad (2)$$

Pada formula x adalah posisi huruf dalam alfabet (0–25) dan k adalah nilai kunci. Berikut merupakan satuan huruf dalam alfabet yang digunakan sebagai dasar dalam penerapan Caesar Cipher[14].

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 4. Indeks susunan huruf alfabet

3.7. Implementasi Algoritma Vignere Cipher

Algoritma Vigenere Cipher ialah salah satu algoritma kriptografi klasik yang menggunakan prinsip bujur sangkar vigenere untuk melaksanakan enkripsi [15]. Contoh bujur sangkar Vigenere bisa dilihat pada Gambar 5.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 5. Tabula recta

Vigenere Cipher merupakan hasil pengembangan lebih lanjut dari Caesar Cipher dan termasuk dalam kategori polyalphabetic substitution cipher [16]. Vigenere Cipher dapat dilakukan dengan dua cara yaitu dengan cara manual memakai bujur sangkar vigenere (tabula recta) seperti pada Gambar 5 maupun dengan cara substitusi angka (matematis) [17]. Secara matematis, enkripsi menggunakan Vigenère Cipher dapat menggunakan formula :

$$C_i = (P_i + K_i) \mod 26 \quad (1)$$

Sedangkan untuk dekripsi :

$$P_i = (C_i - K_i + 26) \mod 26 \quad (2)$$

Di mana *Mi* adalah huruf ke-i dari *plaintext*, *Ki* adalah huruf ke-i dari kunci (diulang jika lebih pendek dari *plaintext*), dan *Ci* adalah huruf ke-i dari *ciphertext*, dengan i adalah posisi huruf dalam alfabet seperti yang sudah dijabarkan pada gambar 4.

3.8. Integrasi dengan Basis Data

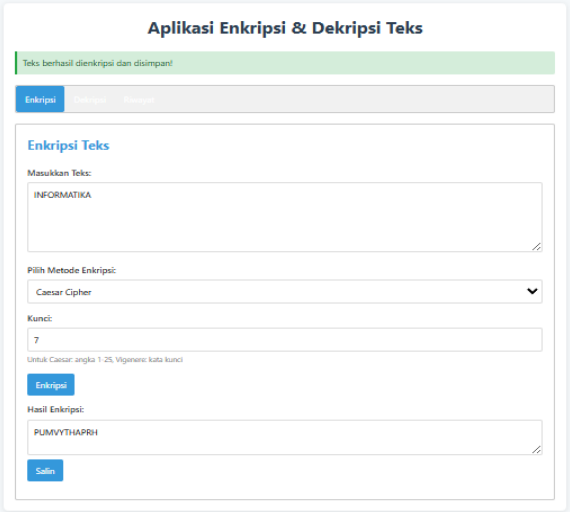
Front End dan Back End dikoneksikan dengan menggunakan bahasa pemrograman PHP agar dapat saling terhubung. Setelah proses enkripsi atau dekripsi selesai, hasilnya disimpan dalam tabel "enkripsi_teks". Data yang disimpan mencakup teks asli, teks hasil enkripsi/dekripsi, metode yang digunakan, kunci, serta tanggal dilakukannya proses enkripsi dan dekripsi.

4. HASIL DAN PEMBAHASAN

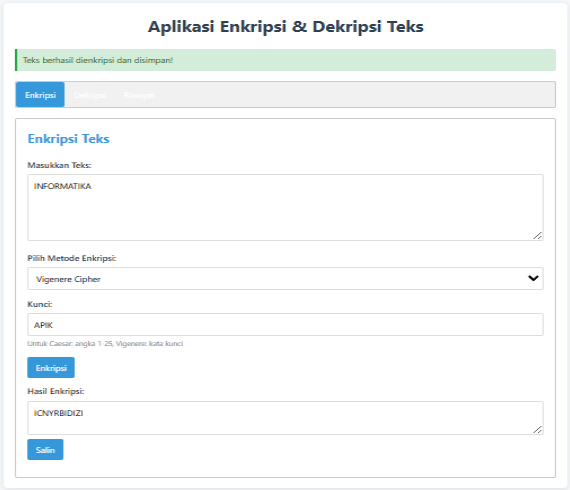
4.1. Hasil Enkripsi dan Dekripsi

Pengujian dilakukan dengan percobaan dengan menggunakan beberapa contoh. Untuk menguji enkripsi, akan dimasukkan plain text "INFORMATIKA" dengan kunci 7 untuk metode Caesar Cipher dan APIK sebagai kunci untuk metode Vigenère Cipher.

Proses enkripsi "INFORMATIKA" secara manual dengan kunci 7 dan "APIK" untuk metode Caesar Cipher dan Vigenère Cipher:

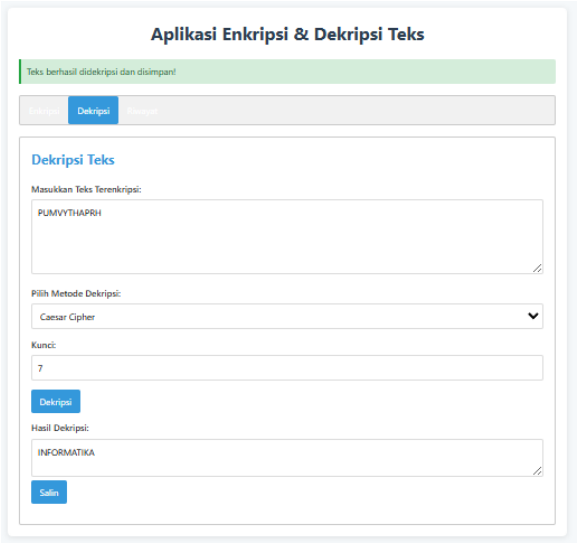


Gambar 6. Pengujian enkripsi Caesar Cipher dengan web

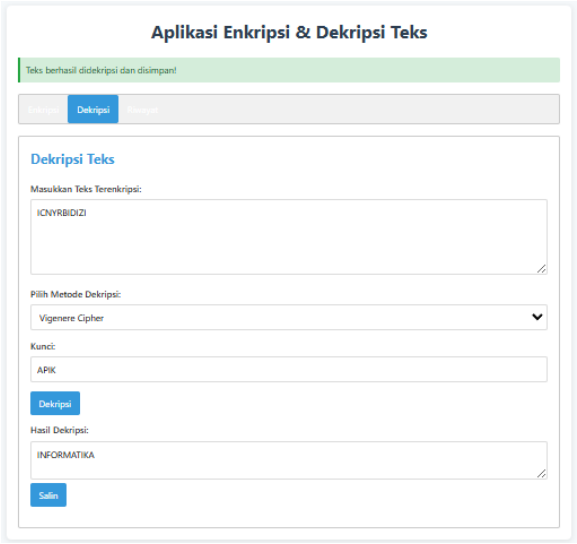


Gambar 7. Pengujian enkripsi Vigenère Cipher dengan web

Melalui gambar 6 dan 7, didapatkan hasil pengujian enkripsi dari *plaintext* "INFORMATIKA" dengan kunci 7 untuk metode Caesar Cipher dan kunci "APIK" untuk metode Vigenère Cipher. Bentuk *ciphertext* dari hasil enkripsi Caesar Cipher adalah "PUMVYTHAPRH" dan dengan metode Vigenère Cipher adalah "ICNYRBIDIZI". Adapun pengujian dekripsi :



Gambar 8. Pengujian dekripsi Caesar Cipher dengan web

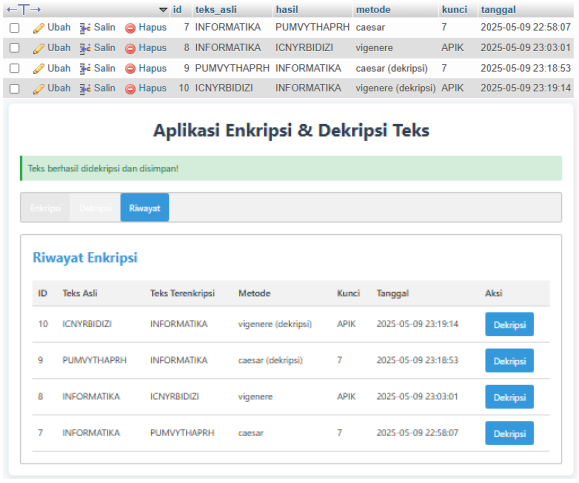


Gambar 9. Pengujian dekripsi Vigenère Cipher dengan web

Melalui gambar 8 dan 9, didapatkan hasil pengujian dekripsi dari *ciphertext* "PUMVYTHAPRH" dengan kunci 7 untuk metode Caesar Cipher dan *cipertext* "ICNYRBIDIZI" untuk metode Vigenère Cipher dengan kunci "APIK" memiliki hasil dekripsi yang sama yaitu "INFORMATIKA". Hal ini menunjukkan bahwa proses yang dilakukan pada aplikasi web memiliki hasil yang akurat.

4.2. Penyimpanan ke Basis Data

Setiap hasil proses enkripsi maupun dekripsi disimpan ke dalam tabel "enkripsi_dekripsi" pada database. Berikut adalah contoh isi tabel setelah beberapa proses dijalankan:



Gambar 10. Riwayat proses di database dan web

Hasil pengujian sistem menunjukkan keberhasilan dalam menjalankan proses enkripsi dan dekripsi terhadap input teks secara akurat, baik dengan menggunakan algoritma Caesar Cipher maupun Vigenère Cipher. Pada algoritma Caesar Cipher, transformasi karakter dilakukan dengan pergeseran alfabet berdasarkan nilai kunci yang bersifat tetap dan linear. Sebagai ilustrasi, teks "INFORMATIKA" yang dienkripsi dengan kunci 7 menghasilkan *ciphertext* "PUMVYTHAPRH. Sementara itu, algoritma Vigenère Cipher memberikan hasil enkripsi yang lebih kompleks, karena setiap huruf pada *plaintext* dienkripsi menggunakan karakter yang berbeda-beda dari kunci yang diulang. Sebagai contoh, teks yang sama "INFORMATIKA" dengan kunci "APIK" menghasilkan *ciphertext* "ICNYRBIDIZI".

Kompleksitas ini menjadikan Vigenère Cipher lebih efektif dalam menyamarkan pola karakter karena tidak terjadi pengulangan pola seperti pada Caesar Cipher. Proses dekripsi pada kedua algoritma juga berjalan sesuai dengan yang diharapkan, yaitu dapat mengembalikan *ciphertext* ke bentuk *plaintext* secara tepat, selama kunci yang digunakan identik dengan kunci saat proses enkripsi. Dari sisi kinerja aplikasi berbasis web, sistem mampu menangani input teks dan kunci secara responsif, dengan proses enkripsi dan dekripsi yang berlangsung cepat. Hal ini dimungkinkan karena kedua algoritma bersifat ringan dan tidak memerlukan komputasi yang kompleks. Antarmuka pengguna yang sederhana dan intuitif turut menunjang kemudahan dalam pengoperasian sistem.

Aplikasi juga dapat menerima input teks dengan panjang yang bervariasi serta mampu menghindari terjadinya error saat input kosong atau kunci tidak sesuai. Meskipun demikian, sistem belum sepenuhnya mendukung karakter non-alfabet seperti tanda baca atau angka. Seluruh hasil dari proses enkripsi dan dekripsi tercatat secara sistematis dalam basis data melalui tabel "enkripsi_teks" yang menyimpan informasi penting berupa teks asli, hasil enkripsi atau dekripsi, metode algoritma yang digunakan, dan nilai kunci. Penyimpanan ini tidak hanya menjamin transparansi data, tetapi juga membuka peluang untuk dikembangkan menjadi fitur riwayat aktivitas pengguna secara historis. Keakuratan data yang tersimpan mengindikasikan bahwa sistem telah mampu melakukan integrasi antara logika pemrosesan dengan penyimpanan data dalam basis data secara konsisten dan andal.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian yang telah dipaparkan pada Bab 4. Hasil dan Pembahasan, dapat disimpulkan bahwa penerapan algoritma kriptografi klasik Caesar Cipher dan Vigenère Cipher pada aplikasi berbasis web mampu melakukan proses enkripsi dan dekripsi secara akurat dan efisien, serta sistem berhasil menyimpan data hasil proses ke dalam basis data dengan baik. Penggunaan kedua algoritma ini memberikan pemahaman dasar tentang keamanan data, meskipun masih memiliki keterbatasan seperti belum mendukung karakter non-alfabet secara menyeluruh. Oleh karena itu, disarankan untuk pengembangan lebih lanjut agar aplikasi mendukung format input yang lebih kompleks serta mempertimbangkan penggunaan algoritma kriptografi modern untuk meningkatkan tingkat keamanan dan ketahanan sistem terhadap serangan yang lebih canggih.

DAFTAR PUSTAKA

[1] A. A. Winata, M. Syafrullah, and I. Irawan, "Implementasi Algoritme Kriptografi Advanced Encryption Standard (AES-128) untuk Pengamanan Data Berbasis Web pada McDonald's Cabang TB Simatupang," *Jurnal Ticom: Technology of Information and Communication*, vol. 12, no. 3, pp. 91–96, 2024.

[2] S. Hadi and F. Fachri, "IMPLEMENTASI RANCANG BANGUN APLIKASI KRIPTOGRAFI BERBASIS WEB MENGGUNAKAN METODE ENKRIPSI BASE-64," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 2, pp. 2026–2031, 2025.

[3] M. Sari, H. D. Purnomo, and I. Sembiring, "Algoritma Kriptografi Sistem Keamanan SMS di Android," *Journal of Information Technology*, vol. 2, no. 1, pp. 11–15, 2022.

[4] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *JPSK*, vol. 2, no. 01, pp. 163–171, Mar. 2022, doi: 10.47709/jpsk.v2i01.1390.

[5] D. Widyawan and I. Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional

Keselamatan Transportasi," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 4, no. 1, pp. 15–22, 2021.

[6] R. Hammad *et al.*, "Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message," in *Journal of Physics: Conference Series*, IOP Publishing, 2022, p. 012006.

[7] V. M. Hidayah, D. I. Mulyana, and Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks," *joe*, vol. 5, no. 3, pp. 8563–8573, Feb. 2023, doi: 10.31004/joe.v5i3.1647.

[8] M. R. Ramadhan and T. Sutabri, "SISTEM INFORMASI PEMESANAN MENU MAKANAN BERBASIS WEB," *Cross-border*, vol. 6, no. 1, pp. 350–359, 2023.

[9] I. Y. Daeli and A. Nur, "Pengembangan Rekayasa Perangkat Lunak Online Sistem E-Recruitment pengawai PT. FM Global Logistics Berbasisi web," *Journal Of Informatics And Busisnes*, vol. 2, no. 3, pp. 468–479, 2024.

[10] R. Syahputra, "Penerapan Algoritma Vigenere Cipher Pada Aplikasi Tabungan Siswa Berbasis Web," *KETIK: Jurnal Informatika*, vol. 1, no. 06, pp. 19–23, 2024.

[11] S. Azura *et al.*, "Penerapan Kemanan Data Text menggunakan Metode Kriptografi Vigener Chiper Berbasis Web," *Digital Transformation Technology (Digitech)| E*, vol. 3, no. 1, pp. 20–28, 2023.

[12] N. W. Hidayatulloh, M. Tahir, H. Amalia, N. A. Basyar, A. F. Prianggara, and M. Yasin, "Mengenal Advance Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data," *digitech*, vol. 3, no. 1, pp. 1–10, May 2023, doi: 10.47709/digitech.v3i1.2293.

[13] Fachrul Dhika Ardiansyah, Alfina Damayanti, Clarizza Azzahra Mudya Putri, Ayu Fitria Dinda Rany, Syaidin Joyo Biroso, and Muhlis Tahir, "IMPLEMENTASI KRIPTOGRAFI CAESAR CHIPER PADA APLIKASI ENKRIPSI DAN DEKRIPSI," *JUISIK*, vol. 3, no. 1, pp. 105–112, May 2023, doi: 10.55606/juisik.v3i1.438.

[14] M. Hidayat, M. Tahir, A. Sukriyadi, A. Sulton, C. A. S. A, and S. A. F, "PENERAPAN KRIPTOGRAFI CAESAR CHIPER DALAM PENGAMANAN DATA," *JUKIM*, vol. 2, no. 03, pp. 35–41, May 2023, doi: 10.56127/jukim.v2i03.619.

[15] N. B. Putra, B. C. Andika, A. D. Purba, and M. Ridwan, "Implementasi Sandi Vigenere Cipher dalam Mengenkripsikan Pesan," *JOCITIS-Journal Science Infomatica and Robotics*, vol. 1, no. 1, pp. 42–50, 2023.

[16] E. Wahyudi *et al.*, "Peningkatan Keamanan Data Melalui Teknik Super Enkripsi Menggunakan Algoritma Vigenere dan Caesar," *JIP*, vol. 10, no. 3, pp. 315–322, May 2024, doi: 10.33795/jip.v10i3.5131.

[17] Imam Riadi, Abdul Fadlil, and Fahmi Auliya Tsani, "Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher," *JISKa*, vol. 7, no. 1, pp. 33–45, Jan. 2022, doi: 10.14421/jiska.2022.7.1.33-45.