

Aplikasi Keamanan Data File Hasil Pemilihan Ketua Osis Menggunakan Metode Modifikasi Caesar Cipher Berbasis Web (Studi Kasus SMA Pab 8 Saentis)

Application of Student Council Chairperson Election Result File Data Security Using Web-Based Caesar Cipher Modification Method (Case Study of SMA Pab 8 Saentis)

Ayunda Lutfika^{a,1}, Wiwi Verina^{b,2}

^{a,b}Rekayasa Perangkat Lunak, Universitas Potensi Utama, Medan 20241, Sumatera Utara, Indonesia

Email: ayundalutfita@gmail.com¹, Email: wiwiverina.azzahra@gmail.com²

ABSTRAK

Keamanan data merupakan aspek penting dalam menjaga kerahasiaan dan integritas informasi, khususnya dalam lingkungan institusi pendidikan. SMA PAB 8 Saentis sebagai salah satu sekolah di Kabupaten Deli Serdang menyimpan data penting berupa hasil pemilihan Ketua OSIS secara terkomputerisasi. Namun, belum adanya sistem pengamanan file menyebabkan kerentanan data dan manipulasi tidak sah. Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan pembangunan aplikasi keamanan berkas berbasis web dengan menggunakan teknik kriptografi. Algoritma yang digunakan adalah modifikasi dari Caesar Cipher yang berfungsi untuk mengenkripsi dan mendekripsi file teks untuk mencegah otorisasi ilegal. Aplikasi ini diharapkan mampu melindungi file hasil pemilihan suara Ketua OSIS agar tetap aman dan terjaga kerahasiaannya. Dengan implementasi sistem ini, informasi vital di lingkungan sekolah dapat terlindungi dari ancaman eksternal maupun internal.

Kata Kunci : Keamanan data, kriptografi, Caesar Cipher, enkripsi, dekripsi, file pemilihan OSIS.

ABSTRACT

Data security is a crucial aspect in maintaining the confidentiality and integrity of information, especially within educational institutions. SMA PAB 8 Saentis, a high school located in Deli Serdang Regency, stores important data such as the results of the student council (OSIS) election in a computerized manner. However, the absence of a proper file security system raises the risk of data leakage and misuse by unauthorized parties. To address this issue, this study proposes the development of a web-based file protection application using cryptographic methods. The algorithm implemented is a modified Caesar Cipher, which functions to encrypt and decrypt text files so they cannot be accessed by unauthorized users. This application is expected to secure the student council election result files and maintain their confidentiality. With this system, vital information within the school environment can be protected from both external and internal threats.

Keywords : Data security, cryptography, Caesar Cipher, encryption, decryption, student council election file.

Disubmit:

Info Artikel :
Direview:

Diterima :

Copyright © 2024 – senadimu. All rights reserved.

1. PENDAHULUAN

Keamanan data merupakan proses penting yang bertujuan untuk melindungi informasi dari akses, pengungkapan, perubahan, atau penghancuran yang tidak sah oleh entitas internal maupun eksternal [1]. Dalam dunia teknologi informasi kontemporer, mekanisme keamanan data dirancang untuk memastikan integritas, kerahasiaan, dan ketersediaan data, sehingga mencegah penyalahgunaan oleh aktor jahat atau lalai [2]. Pada dasarnya, teknologi keamanan data mengintegrasikan prinsip dan praktik dari keamanan telekomunikasi dan keamanan komputer, yang bekerja secara sinergis untuk melindungi sistem informasi dari potensi ancaman [3].

Kerahasiaan informasi merupakan komponen fundamental dari keamanan data, terutama bagi organisasi atau lembaga yang dipercayakan dengan dokumen sensitif atau penting [4]. Pemanfaatan atau pengungkapan data kepemilikan yang tidak sah dapat mengakibatkan dampak finansial yang substansial dan kerusakan pada reputasi organisasi [5]. Oleh karena itu, sangat penting bagi semua entitas untuk menerapkan langkah-langkah yang kuat yang membatasi akses ke informasi sensitif hanya untuk individu yang berwenang. Sebagai aset organisasi yang vital, data harus dilindungi untuk menjaga integritasnya dan mencegah akses atau eksploitasi yang tidak sah [6].

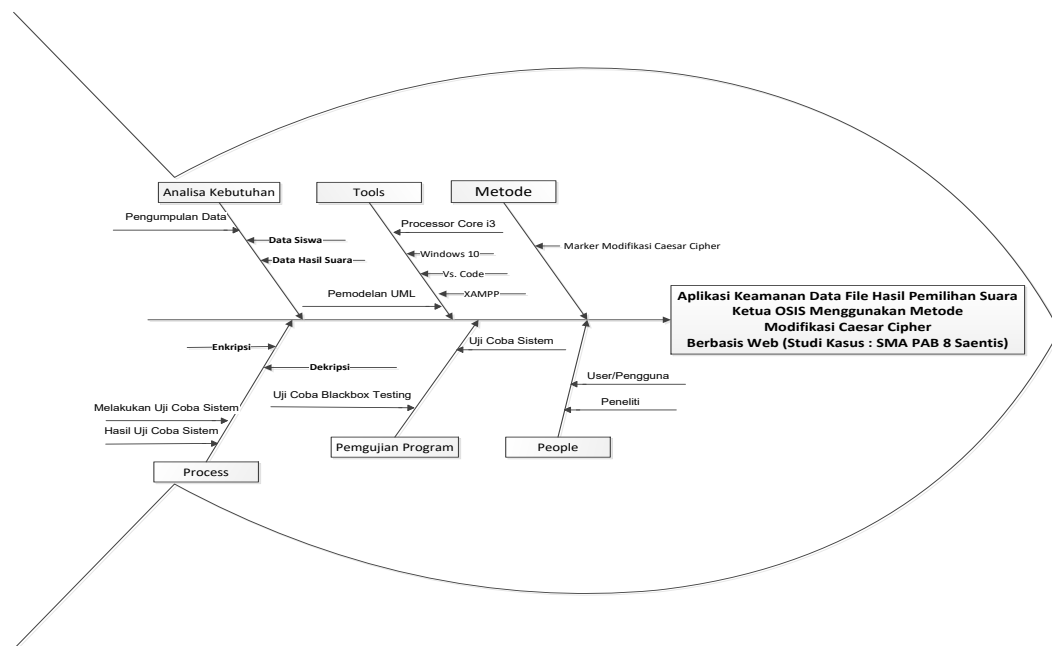
SMA PAB 8 Saentis, yang terletak di Jl. Kali Serayu Dusun 16, Saentis, Kecamatan Percut Sei Tuan, Kabupaten Deli Serdang, Sumatera Utara, merupakan salah satu lembaga pendidikan yang masih menyimpan data hasil pemilihan ketua OSIS secara manual dan terkomputerisasi tanpa sistem pengamanan file yang memadai. File hasil pemilihan ketua OSIS bersifat internal dan hanya boleh diakses oleh pihak sekolah yang berwenang. Namun, penyimpanan data penting seperti hasil pemilihan OSIS di satu folder komputer tanpa sistem keamanan yang tepat dapat menimbulkan risiko kebocoran maupun rekayasa data yang tidak etis [7].

Untuk mencegah risiko tersebut, dibutuhkan sebuah sistem keamanan yang mampu melindungi file dari akses tidak sah. Pendekatan metodologis yang dapat diimplementasikan dalam konteks ini adalah kriptografi, yaitu ilmu yang mempelajari teknik penyandian data agar tidak dapat dibaca oleh pihak lain selain yang memiliki kunci [8]. Kriptografi berfungsi untuk menjaga kerahasiaan dan keaslian data selama proses penyimpanan maupun transmisi [9]. Dalam penelitian ini, digunakan algoritma modifikasi *Caesar Cipher*, yaitu pengembangan dari algoritme klasik Caesar Cipher yang melakukan proses pergeseran karakter dengan kunci tertentu pada data teks [10]. Algoritma ini dipilih karena mudah diimplementasikan, efisien, dan cocok untuk kebutuhan pengamanan file berformat teks seperti hasil pemilihan ketua OSIS. Proses enkripsi dilakukan untuk mengubah isi file menjadi bentuk yang tidak dikenali, sedangkan proses dekripsi dilakukan untuk mengembalikannya ke bentuk semula dengan kunci yang sama [11].

Penelitian ini bertujuan untuk merancang dan mengimplementasikan aplikasi keamanan data berbasis web yang mampu melakukan enkripsi dan dekripsi file hasil pemilihan ketua OSIS di SMA PAB 8 Saentis. Dengan adanya sistem ini, diharapkan keamanan data dapat meningkat, risiko kebocoran informasi dapat diminimalisir, dan integritas file hasil pemilihan tetap terjaga [12]. Selain itu, penelitian ini juga diharapkan dapat menjadi sarana pembelajaran bagi siswa dan pihak sekolah mengenai penerapan dasar kriptografi dalam dunia nyata [13]. Penelitian "Modifikasi Algoritma *Caesar Cipher* Pada Kode ASCII Dalam Meningkatkan Keamanan Pesan Teks". Sistem ini mampu menghasilkan ciphertext yang kompleks dan sulit dibaca, menjadikannya solusi efektif untuk pengamanan data digital pada file [14]. Penelitian "Perancangan Keamanan Data Pesan Dengan Menggunakan Metode *Kriptografi Caesar Cipher*". Berdasarkan hasil pengujian aplikasi *enkripsi-dekripsi* berbasis *Caesar Cipher* yang mampu menjaga keamanan pesan teks sederhana, meskipun masih memiliki batasan panjang pesan dan belum menggabungkan teknik keamanan lain seperti

2. METODE

Gambar 1 *Diagram Fishbone*



Keterangan :

1. Analisis Kebutuhan

Pada tahap ini dilakukan proses identifikasi dan pemetaan kebutuhan sistem sebagai dasar dalam pengembangan aplikasi. Aktivitas ini bertujuan untuk memahami keterkaitan antarvariabel yang berperan dalam sistem serta menentukan komponen fungsional yang dibutuhkan agar aplikasi dapat beroperasi sesuai tujuan penelitian. Tahapan ini mencakup kegiatan pengumpulan informasi dan telaah literatur yang relevan, guna memperoleh landasan teoretis yang kuat tentang mekanisme kerja sistem yang akan dikembangkan. Melalui proses ini, diperoleh gambaran menyeluruh mengenai hubungan antarunsur penelitian yang nantinya menjadi dasar dalam perancangan struktur aplikasi berbasis web.

2. Desain Sistem

Tahapan ini mencakup perancangan sistem secara visual dan structural yaitu *Class Diagram*, *Use Case Diagram*, *Sequence Diagram*, serta *Activity Diagram*, yang merupakan alat bantu pemodelan UML untuk menggambarkan fungsionalitas sistem dan alur proses.

3. Penulisan Program

Tahapan ini merupakan fase implementatif di mana rancangan sistem yang telah dibuat pada tahap desain diterjemahkan ke dalam bentuk kode program yang dapat dijalankan secara fungsional.

- a. *Visual Studio Code : Editor* yang digunakan dalam penulisan kode.
- b. *XAMPP : Platform* untuk menjalankan server lokal (Apache, MySQL, PHP).
- c. *Google Chrome* : Digunakan untuk menguji tampilan dan fungsionalitas sistem berbasis web.

4. Penerapan Metode

Pada tahapan ini peneliti memilih berbasis *full coding* sesuai dengan pengumpulan data dalam Aplikasi Keamanan Data File Hasil Pemilihan Suara Ketua OSIS Menggunakan Metode Modifikasi *Caesar Cipher*.

5. Pengujian Program

Pengujian dilakukan untuk mengevaluasi apakah sistem bekerja sesuai harapan *Black Box Testing* teknik pengujian berdasarkan fungsionalitas sistem tanpa memperhatikan struktur internal kode.

6. Pemeliharaan Sistem

Setelah sistem diimplementasikan, dilakukan pemeliharaan untuk memastikan keberlanjutan SMA PAB 8 Saentis & Peneliti bertanggung jawab terhadap keberlangsungan sistem, perbaikan bila terjadi kesalahan, dan adaptasi terhadap kebutuhan baru.

3. HASIL DAN PEMBAHASAN

Metode *Modifikasi Caesar Cipher* merupakan salah satu algoritma substitusi klasik tertua yang melakukan proses *enkripsi* dan *dekripsi* untuk mengamankan data. Studi kasus ini akan membahas penerapan metode *Modifikasi Caesar Cipher* dalam mengamankan data hasil rekapan perhitungan suara pemilihan ketua osis, data diperoleh berdasarkan rekapan perolehan suara yang dilakukan secara manual dengan cara pencoblosan suara, setelah itu data direkap berdasarkan pencoblosan data suara keseluruhan. Dengan menggunakan data hasil rekapan, peneliti dapat membuat inferensi atau kesimpulan tentang proses pengamanan data. Adapun langkah-langkah penerapan metode *Modifikasi Caesar Cipher* dapat dijelaskan sebagai berikut :

1. Tabel Perhitungan

Tabel perhitungan *Caesar Cipher* berfungsi sebagai alat bantu untuk proses *enkripsi* dan *dekripsi* huruf dengan cara menggeser posisi huruf dalam alfabet berdasarkan nilai kunci tertentu. Adapun table perhitungan yang digunakan sebagai berikut :

Tabel 1. Perhitungan *Caesar Chipper*

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Keterangan:

Dalam proses enkripsi, setiap huruf dalam teks biasa disubstitusi sedemikian rupa sehingga huruf A digantikan oleh D, B oleh E, dan seterusnya. Hal ini dapat direpresentasikan dengan memberikan nilai integer pada setiap huruf, yang mana menggeser setiap huruf sebanyak tiga posisi dalam alfabet sama dengan melakukan operasi aritmatika modular pada teks biasa P . Secara spesifik, pergeseran ini setara dengan menerapkan operasi modulo untuk mengubah P menjadi teks sandi C .

2. Proses *Enkripsi* dan *Dekripsi*

Enkripsi merupakan teknik sistematis untuk mengubah data ke dalam format terenkripsi guna memastikan kerahasiaannya, sehingga informasi tersebut tidak dapat dipahami tanpa proses dekripsi selanjutnya. Sebaliknya, dekripsi melibatkan pembalikan transformasi ini untuk memulihkan data asli dari bentuk terenkripsinya. Mekanisme yang mendasari enkripsi dan dekripsi dapat dijelaskan sebagai berikut.

Tabel 2. Data Rekapitulasi Suara

No	Calon Ketua Osis	Calon Wakil Ketua Osis	Hasil Suara
1	Rio	Pandu	292
2	Febri	Cut	157
3	Sri W	Dinda	83

- a. *Enkripsi* dan *Dekripsi* I
Plaintext (x) : R I O
Kunci (n) : 6

Tabel 3. Tabel *Enkripsi*

PLAIN	Caesar Cipher	CIPHER
R	$E_1 = (17+6) \text{ modulus } 26 = 23$	X

I	$E_1 = (8+6) \text{ modulus } 26 = 14$	O
O	$E_1 = (14+6) \text{ modulus } 26 = 20$	U

Proses *dekripsi* diambil dari data *enkripsi* pada tabel 3 sebagai berikut:

Ciphertext (y) : X O U

Kunci (n) : 6

Tabel 4. Tabel *Dekripsi*

CIPHER	Caesar Cipher	PLAIN
X	$D_1 = (23-6) \text{ modulus } 26 = 17$	R
O	$D_2 = (14-6) \text{ modulus } 26 = 8$	I
U	$D_3 = (20-6) \text{ modulus } 26 = 14$	O

b. *Enkripsi dan Dekripsi II*

Proses *enkripsi* diambil sampel data nama hasil perhitungan suara pada tabel 2 sebagai berikut:

Plaintext (x) : P A N D U

Kunci (n) : 6

Tabel 5. Tabel *Enkripsi*

PLAIN	Caesar Cipher	CIPHER
P	$E_1 = (15+6) \text{ modulus } 26 = 21$	Y
A	$E_1 = (0+6) \text{ modulus } 26 = 6$	G
N	$E_1 = (13+6) \text{ modulus } 26 = 19$	T
D	$E_1 = (3+6) \text{ modulus } 26 = 9$	J
U	$E_1 = (20+6) \text{ modulus } 26 = 0$	A

Proses dekripsi diambil dari data enkripsi pada tabel 5 sebagai berikut:

Ciphertext (y) : Y G M W A

Kunci (n) : 6

Tabel 6. Tabel *Dekripsi*

CIPHER	Mod Caesar Cipher	PLAIN
Y	$E_1 = (21-6) \text{ modulus } 26 = 15$	P
G	$E_1 = (6-6) \text{ modulus } 26 = 0$	A
T	$E_1 = (19-6) \text{ modulus } 26 = 13$	N
J	$E_1 = (9-6) \text{ modulus } 26 = 3$	D
A	$E_1 = (0-6) \text{ modulus } 26 = 20$	U

c. *Enkripsi dan Dekripsi III*

Proses *enkripsi* diambil sampel data nama hasil perhitungan suara pada tabel 2 sebagai berikut:

Plaintext (x) : F E B R I

Kunci (n) : 6

Tabel 7. Tabel *Enkripsi*

PLAIN	Caesar Cipher	CIPHER
F	$E_1 = (5+6) \text{ modulus } 26 = 11$	L
E	$E_1 = (4+6) \text{ modulus } 26 = 10$	K
B	$E_1 = (1+6) \text{ modulus } 26 = 7$	H
R	$E_1 = (17+6) \text{ modulus } 26 = 23$	X
I	$E_1 = (8+6) \text{ modulus } 26 = 14$	O

Proses *dekripsi* diambil dari data enkripsi pada tabel 7 sebagai berikut:

Ciphertext (y) : L K H X O

Kunci (n) : 6

Tabel 8. Tabel *Dekripsi*

CIPHER	Mod Caesar Cipher	PLAIN
L	$E_1 = (11-6) \text{ modulus } 26 = 5$	F
K	$E_1 = (10-6) \text{ modulus } 26 = 6$	E
H	$E_1 = (7-6) \text{ modulus } 26 = 1$	B
X	$E_1 = (23-6) \text{ modulus } 26 = 17$	R
O	$E_1 = (14-6) \text{ modulus } 26 = 8$	I

d. *Enkripsi dan Dekripsi IV*

Proses *enkripsi* diambil sampel data nama hasil perhitungan suara pada tabel 2 sebagai berikut:

Plaintext (x) : C U T

Kunci (n) : 6

Tabel 9. Tabel *Enkripsi*

PLAIN	Caesar Cipher	CIPHER
C	$E_1 = (2+6) \text{ modulus } 26 = 8$	I
U	$E_1 = (20+6) \text{ modulus } 26 = 0$	A
T	$E_1 = (19+6) \text{ modulus } 26 = 25$	Z

Proses *dekripsi* diambil dari data enkripsi pada tabel 9 sebagai berikut:

Ciphertext (y) : X O U

Kunci (n) : 6

Tabel 10. Tabel *Dekripsi*

CIPHER	Caesar Cipher	PLAIN
I	$D_1 = (8-6) \text{ modulus } 26 = 2$	C
A	$D_2 = (0-6) \text{ modulus } 26 = 20$	U
Z	$D_3 = (25-6) \text{ modulus } 26 = 19$	T

Proses *enkripsi* diambil sampel data nama hasil perhitungan suara pada table 2 sebagai berikut:

Plaintext (x) : S R I

Kunci (n) : 6

Tabel 11. Tabel *Enkripsi*

PLAIN	Caesar Cipher	CIPHER
S	$E_1 = (18+6) \text{ modulus } 26 = 24$	Y
R	$E_1 = (17+6) \text{ modulus } 26 = 23$	X
I	$E_1 = (8+6) \text{ modulus } 26 = 14$	O

e. *Enkripsi dan Dekripsi V*

Proses *dekripsi* diambil dari data *enkripsi* pada tabel 12 sebagai berikut:

Ciphertext (y) : Y X O

Kunci (n) : 6

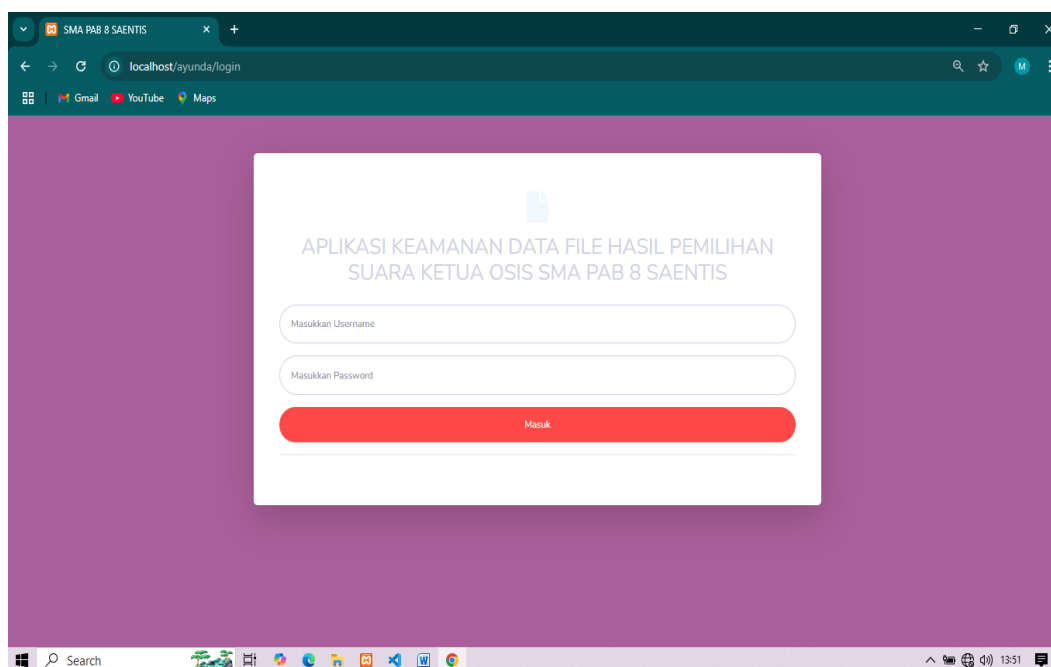
Tabel 13. Tabel *Dekripsi*

CIPHER	Caesar Cipher	PLAIN
Y	$D_1 = (24-6) \text{ modulus } 26 = 18$	S
X	$D_2 = (23-6) \text{ modulus } 26 = 17$	R
O	$D_3 = (14-6) \text{ modulus } 26 = 8$	I

Setelah tahapan enkripsi dan dekripsi direalisasikan secara menyeluruh, langkah berikutnya berfokus pada penyajian hasil implementasi dari rancangan sistem yang telah dikembangkan. Bagian ini berfungsi sebagai representasi visual dari sistem, guna memperlihatkan bagaimana rancangan konseptual yang telah dirumuskan diterjemahkan ke dalam bentuk antarmuka pengguna yang operasional. Visualisasi hasil perancangan ini memberikan gambaran konkret terhadap interaksi pengguna dengan sistem serta validasi atas kesesuaian rancangan dengan kebutuhan fungsional yang telah diidentifikasi sebelumnya:

1. Tampilan *Login*

Gambar 2. Tampilan *Login*

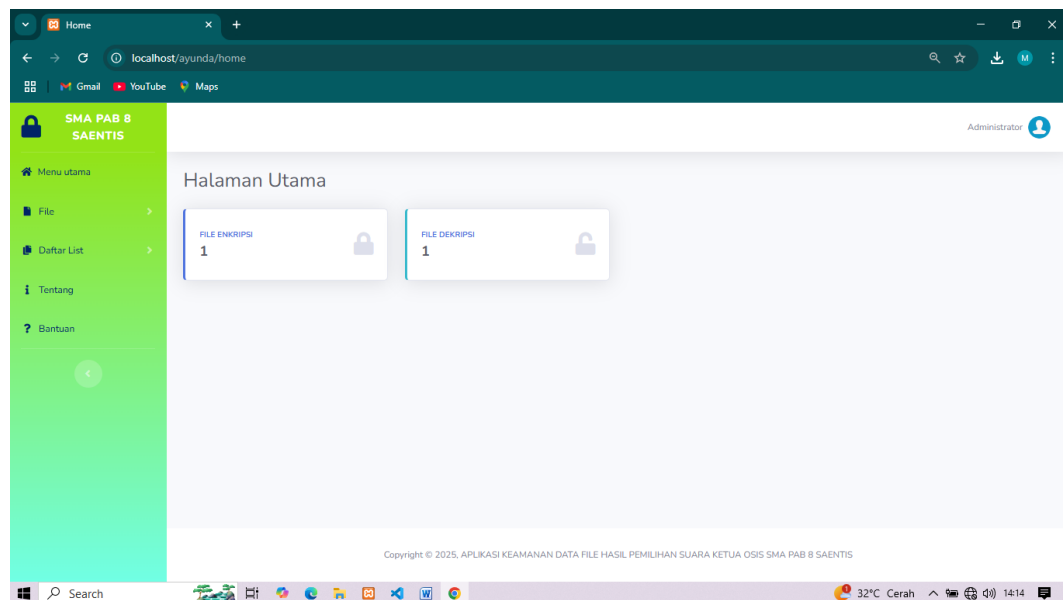


Halaman Tampilan Login berfungsi sebagai gerbang utama bagi pengguna untuk mengakses sistem yang telah dikembangkan. Pada tahap operasional ini, sistem mengimplementasikan mekanisme autentikasi yang berorientasi pada keamanan dengan menyediakan dua komponen input, yaitu username dan password, serta satu tombol aksi Login sebagai pemicu proses verifikasi kredensial. Prosedur login tersebut dirancang agar hanya dapat diakses oleh administrator sistem, sehingga hak akses pengguna biasa secara otomatis dibatasi demi menjaga integritas serta keamanan data. Ketika data autentikasi divalidasi dengan benar, sistem akan menavigasikan pengguna menuju halaman dashboard sesuai dengan level otoritas masing-masing. Desain antarmuka pada halaman ini mengedepankan prinsip kesederhanaan dan fungsionalitas, dengan tata letak yang intuitif untuk memastikan pengalaman pengguna berlangsung efisien sekaligus aman secara sistemik.

2. Tampilan *Form* Utama

Tampilan *Form* Utama pada sistem terlihat pada gambar berikut.

Gambar 3. Tampilan *Form* Utama



Tampilan Form Utama merepresentasikan antarmuka inti dari aplikasi kriptografi yang berfungsi sebagai pusat navigasi untuk seluruh aktivitas sistem. Melalui halaman ini, pengguna dapat mengoperasikan berbagai fungsi aplikasi yang telah dirancang secara terintegrasi. Form utama menjadi jembatan utama antara pengguna dan logika kriptografi di balik sistem, di mana seluruh proses interaktif mulai dari pemanggilan fitur hingga eksekusi algoritma dapat dijalankan secara langsung.

Pada form ini disajikan sejumlah elemen menu yang diorganisasikan secara hierarkis untuk memudahkan penggunaan. Terdapat menu File yang berfungsi sebagai pengelola dasar dokumen, serta menu Program yang menjadi pusat operasional proses kriptografi. Di dalam menu Program, tersedia dua submenu fungsional, yaitu Enkripsi dan Dekripsi, yang masing-masing mengakomodasi kebutuhan pengguna dalam mengubah plaintext menjadi ciphertext maupun mengembalikannya ke bentuk semula. Struktur antarmuka dirancang agar tetap sederhana namun memiliki tingkat keterbacaan dan efisiensi tinggi, sehingga seluruh proses pemanfaatan sistem dapat dijalankan secara intuitif tanpa mengesampingkan pendekatan akademis terhadap implementasi metode kriptografi.

3. Tampilan *Form* Enkripsi

Tampilan *Form* Enkripsi pada sistem terlihat pada gambar berikut.

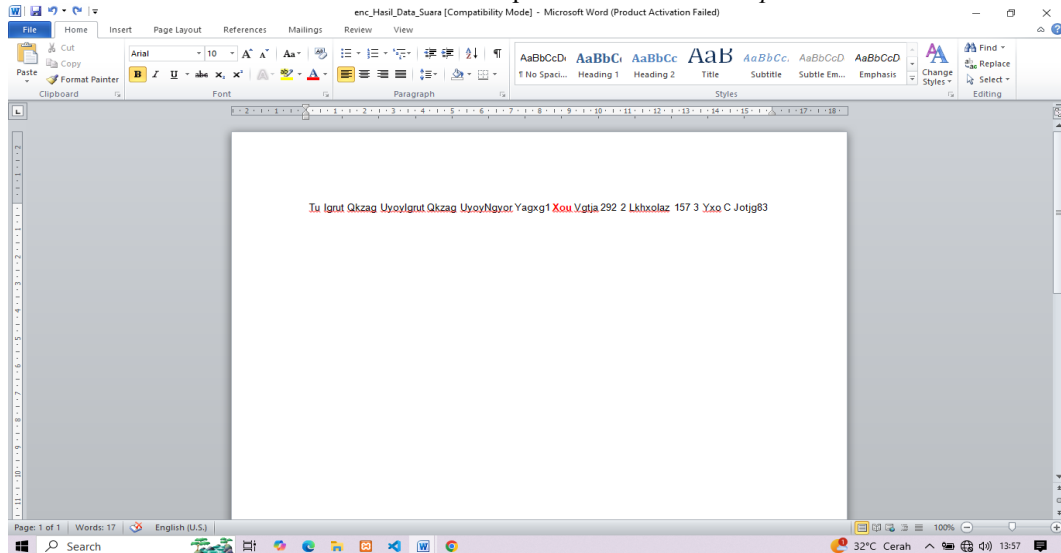
Gambar 4. Tampilan *Form* Enkripsi

Tampilan Form Enkripsi berfungsi sebagai komponen utama dalam proses konversi data dari bentuk terbaca (plaintext) menjadi bentuk tersandi (ciphertext), sehingga informasi yang terkandung di dalamnya tidak dapat diinterpretasikan tanpa akses terhadap kunci enkripsi yang sah. Melalui antarmuka ini, pengguna memiliki kendali penuh terhadap operasi penyandian, dengan beberapa fitur fungsional yang mendukung efisiensi serta keamanan proses.

Pada form ini, pengguna dapat melakukan sejumlah tindakan seperti memilih atau mengunggah berkas dengan ekstensi tertentu (misalnya .doc), menentukan lokasi penyimpanan hasil enkripsi, serta mengeksport data yang telah dikonversi menjadi ciphertext. Selain itu, tersedia pula opsi untuk keluar dari form setelah seluruh prosedur selesai dilaksanakan. Tujuan utama dari rancangan form ini adalah memastikan keotentikan proses perlindungan data dengan antarmuka yang minimalis namun informatif, sehingga proses enkripsi berlangsung terstruktur, mudah dioperasikan, dan tetap menjamin kerahasiaan data secara menyeluruh.

4. Tampilan *Form Hasil Enkripsi*
Tampilan *Form Hasil Enkripsi* pada sistem terlihat pada gambar berikut.

Gambar 5. Tampilan *Form Hasil Enkripsi*



Fungsi dari setiap tombol yang terdapat pada *Form Enkripsi* dirancang untuk memfasilitasi pengguna dalam menjalankan proses pengolahan data secara sistematis dan aman. Setiap tombol memiliki peran spesifik yang berkontribusi dalam tahapan enkripsi, mulai dari pemilihan berkas hingga penyimpanan hasil penyandian

Browse : Tombol ini digunakan untuk menelusuri dan memilih berkas (file) yang akan diproses ke dalam sistem untuk dilakukan enkripsi. Ketika tombol ini diaktifkan, sistem akan menampilkan jendela Open File Dialog yang memungkinkan pengguna memilih dokumen dengan ekstensi yang sesuai, seperti .txt atau .doc. Setelah file dipilih, informasi lokasi serta nama file akan ditampilkan otomatis di kolom input untuk proses berikutnya.

Enkripsi File : Fungsi utama tombol ini adalah mengonversi data dari bentuk plaintext menjadi ciphertext dengan menerapkan algoritma kriptografi sesuai kunci yang diberikan oleh pengguna. Setelah perintah enkripsi dijalankan, sistem akan menampilkan hasil proses berupa file terenkripsi yang tidak dapat dibaca oleh pihak tidak berwenang. Operasi ini juga memastikan bahwa struktur data tetap utuh meskipun isi informasinya telah disandikan secara matematis.

5. Tampilan *Form Dekripsi*
Tampilan *Form Dekripsi* pada sistem terlihat pada gambar berikut :

Gambar 6. Tampilan *Form Dekripsi*

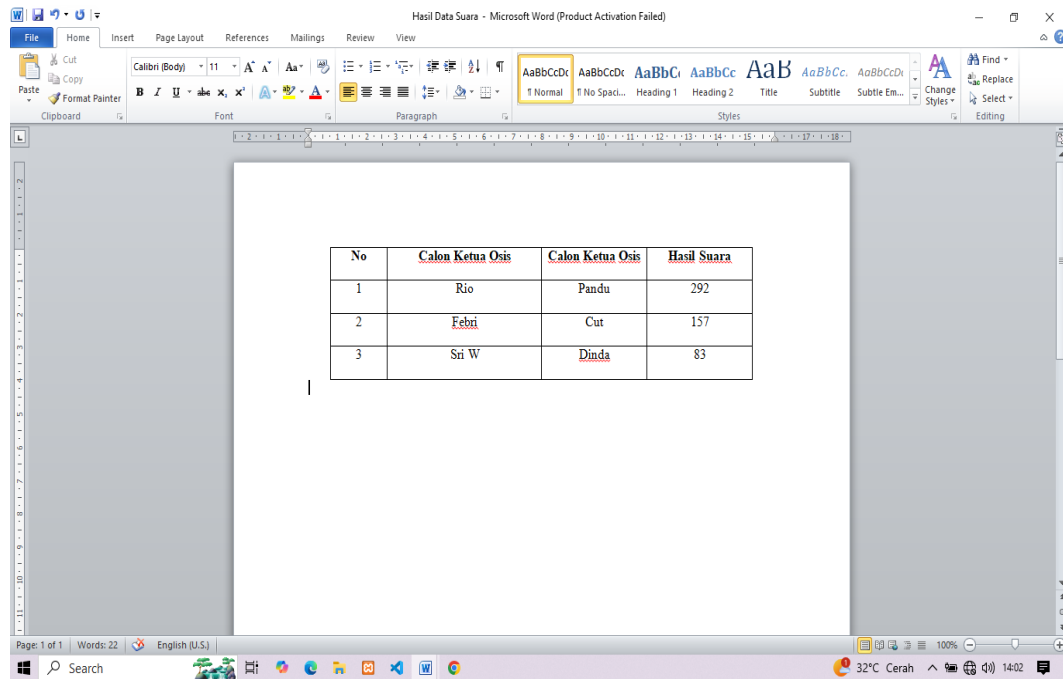
Tampilan Form Dekripsi berperan sebagai komponen operasional yang digunakan untuk mengubah data hasil enkripsi (ciphertext) kembali menjadi bentuk awalnya (plaintext). Melalui form ini, sistem melakukan proses pemulihan informasi berdasarkan kunci yang dimasukkan oleh pengguna, sehingga hanya pihak berotoritas dengan kunci sah yang dapat mengakses isi data secara utuh.

Fitur-fitur yang tersedia pada form ini dirancang untuk mempermudah pengguna dalam menjalankan proses dekripsi secara sistematis. Di antaranya, pengguna dapat memilih berkas terenkripsi yang ingin dikonversi, menentukan lokasi penyimpanan hasil dekripsi, serta menutup form setelah proses selesai. Proses dekripsi ini menggunakan prinsip kebalikan dari enkripsi, di mana algoritma melakukan operasi matematis yang mengembalikan struktur data ke kondisi semula. Dengan demikian, form ini memastikan keberlangsungan siklus pengelolaan data terenkripsi—dari penyandian hingga pengembalian informasi—tetap terjaga secara autentik dan aman secara metodologis.

6. Tampilan *Form Hasil Dekripsi*

Tampilan *Form Hasil Dekripsi* pada sistem terlihat pada gambar berikut :

Gambar 7. Tampilan *Form Hasil Dekripsi*



No	Calon Ketua Osis	Calon Ketua Osis	Hasil Suara
1	Rio	Pandu	292
2	Febii	Cut	157
3	Sri W	Dinda	83

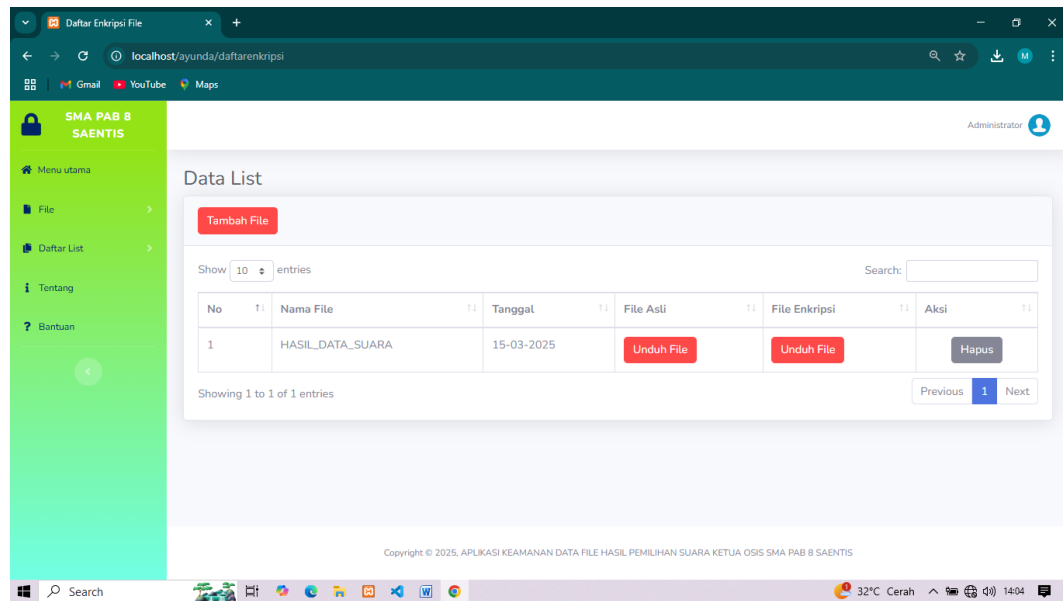
Fungsi dari setiap tombol yang terdapat dalam Form Dekripsi memiliki peranan yang saling terintegrasi dalam memastikan proses pemulihan data dari bentuk terenkripsi (ciphertext) menjadi teks asli (plaintext) dapat berjalan dengan efisien dan aman:

Browse : Tombol ini berfungsi untuk membuka jendela direktori sistem guna menelusuri serta memilih file yang akan diproses dalam tahap dekripsi. Ketika tombol diaktifkan, sistem akan menampilkan file explorer yang memungkinkan pengguna memilih file terenkripsi yang sesuai format, seperti .txt atau .doc, untuk kemudian dimuat ke dalam form dekripsi.

Dekripsi File : Tombol ini berperan dalam menjalankan proses inti dekripsi, yaitu mengubah data file yang masih berupa ciphertext menjadi bentuk plaintext. Mekanisme dekripsi dijalankan berdasarkan kunci yang telah dimasukkan oleh pengguna; sistem akan memverifikasi keabsahan kunci dan selanjutnya melakukan rekonstruksi data agar dapat dibaca kembali seperti semula. Setelah proses selesai, hasil dekripsi dapat disimpan pada direktori yang ditentukan, memastikan data telah berhasil dikembalikan ke bentuk aslinya tanpa kehilangan integritas informasi.

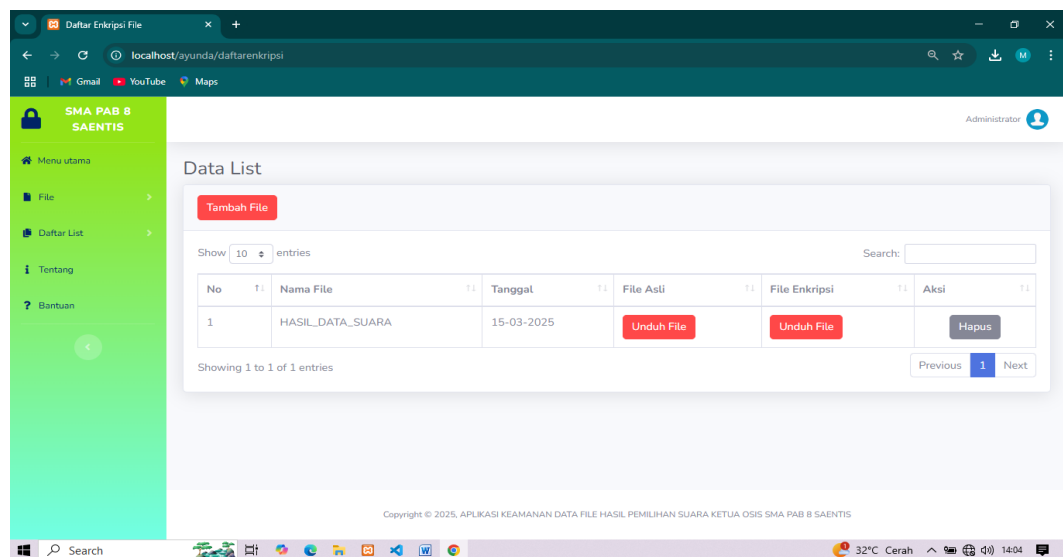
7. Tampilan Form List Enkripsi

Tampilan Form List Enkripsi pada sistem ini terlihat pada gambar berikut :

Gambar 8. Tampilan *Form List Enkripsi*

Tampilan *Form* daftar list ini berfungsi untuk melihat data *file* yang terenkripsi dalam bentuk *file*.

8. Tampilan *Form List Dekripsi*
Tampilan *Form List Dekripsi* pada sistem ini terlihat pada gambar berikut :

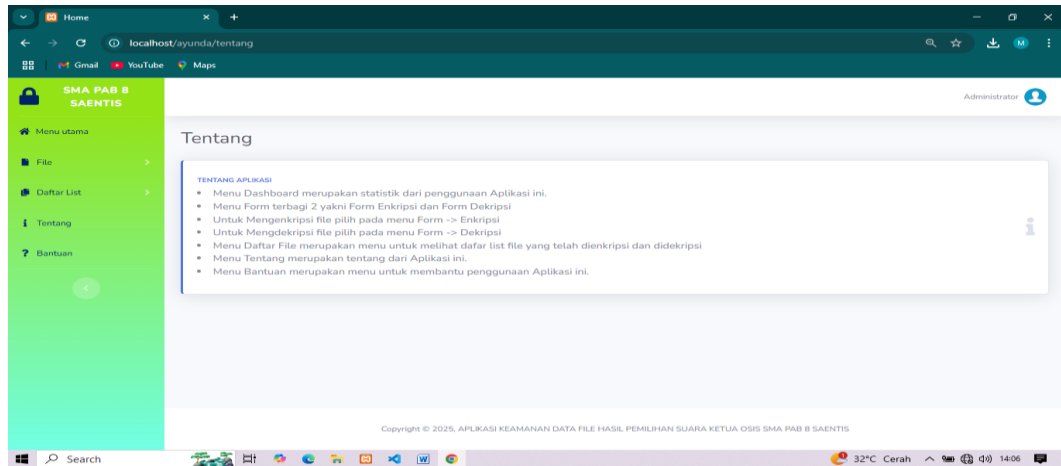
Gambar 9. Tampilan *Form List Dekripsi*

Tampilan *Form* daftar list ini berfungsi untuk melihat data *file* yang terdekripsi dalam bentuk *file*.

9. Tampilan *Form* Tentang

Tampilan *Form* Tentang pada sistem ini terlihat pada gambar berikut :

Gambar 10. Tampilan *Form* Tentang

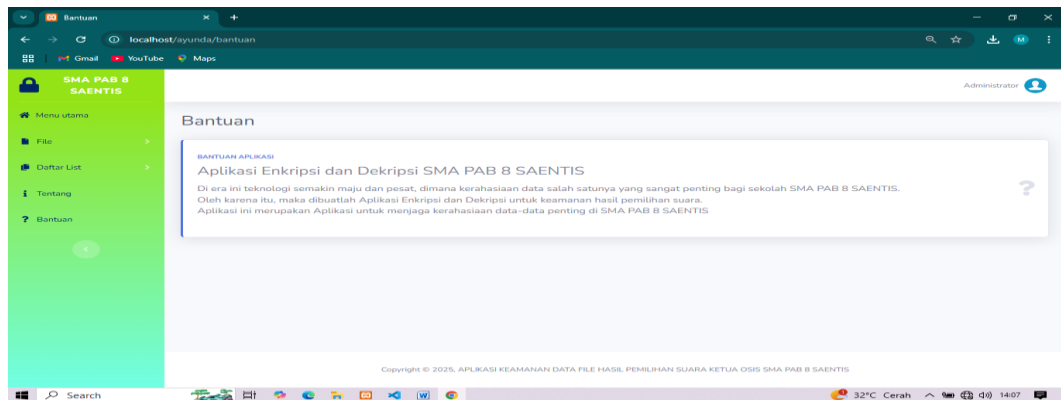


Tampilan *Form* tentang ini berfungsi untuk melihat informasi tentang aplikasi yang dirancang.

10. Tampilan *Form* Bantuan

Tampilan *Form* Bantuan pada sistem ini terlihat pada gambar berikut :

Gambar 11. Tampilan *Form* Bantuan



Tampilan *Form* bantuan ini berfungsi untuk melihat informasi bantuan penggunaan aplikasi yang dirancang.

4. KESIMPULAN

1. Didalam melakukan proses *enkripsi file* aplikasi harus dapat membaca isi dari sebuah *file* dan menuliskan kembali hasil proses *dekripsi* pada *file* yang sama.
2. Proses *enkripsi* dengan menggunakan algoritma Modifikasi *Caeser Cipher* dengan menggunakan Bahasa pemrograman *PHP* dan *Database MySQL*.
3. Aplikasi Metode Modifikasi *Caeser Cipher* melakukan proses *enkripsi* dengan menggunakan Modifikasi *Caeser Cipher* dan kunci yang dipergunakan akan dikonversi terlebih dahulu menjadi bilangan-bilangan *hexadecimal*.

UCAPAN TERIMA KASIH

Sebagai penutup, penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah memberikan kesempatan dan dukungan dalam penyelesaian Karya Tulis Ilmiah (KTI) ini.

REFERENSI

- [1] Abdillah, R. (2021). Pemodelan Uml Untuk Sistem Informasi Persewaan Alat Pesta. *Jurnal Fasilkom*, 11(2), 79–86. <https://doi.org/10.37859/jf.v11i2.2673>
- [2] Aranski, A. R. W. , F. A. , F. K. I. S. , M. T. (2023). Implementasi Algoritma Caesar Cipher Untuk Keamanan Data Anggota Perpustakaan Di Universitas Xyz. *Jurnal SITEBA*, 2(1), 34–41.
- [3] Asmara, R., Fajri, A. F., Novinaldi, N., Iswandy, E., & Nanda, A. P. (2024). Membangun Pengelolaan Aplikasi Web Berbasis Docker pada Kominfo Padang Panjang. *Jurnal Pustaka Data (Pusat Akses Kajian Database, Analisa Teknologi, Dan Arsitektur Komputer)*, 4(1), 17–21. <https://doi.org/10.55382/jurnalpustakadata.v4i1.666>
- [4] Dalam, M., Nomor, M., & Kendaraan, P. (2023). Pemanfaatan Jaringan Saraf Tiruan Hamming dan. 7(1), 84–95.
- [4] Harmayani, Apdilah Dicky, Mapilindo, Oktopanda, & Hutahaeen Jeperson. (2021). FullBook+Aplikasi+Komputer-dikompresi.
- [5] Meriska Hamni, Khairul Amri, M., Sherly Rezeky, & Adnan Buyung Nasution. (2022). Penerapan Keamanan Data Dengan Menggunakan Metode Caesar Chiper Untuk Mengamankan Database Mysql. *Jurnal Informatika Teknologi Dan Sains*, 4(4), 472–477. <https://doi.org/10.51401/jinteks.v4i4.2196>.
- [6] Mira, Purnomo, H. D., & Sembiring, I. (2022). Modifikasi Algoritma Caesar Cipher pada Kode ASCII dalam Meningkatkan Keamanan Pesan Teks. *Journal of Information Technology*, 2(1), 16–22. <https://doi.org/10.46229/jifotech.v2i1.293>.
- [7] Mohammad Harun Alfirdaus, Muhlis Tahir, Nabilla Enno Dewanti, Riki Ardianto, Nela Nur Azurah, & Nanang Firman Cahyono. (2023). Perancangan Aplikasi Enkripsi Deskripsi Menggunakan Metode Caesar Chiper Berbasis Web. *Jurnal Teknik Mesin, Industri, Elektro Dan Informatika*, 2(2), 64–76. <https://doi.org/10.55606/jtmei.v2i2.1628>.
- [8] Munawar, Z., Iswanto, Widhiantoro, D., & Putri, N. I. (2022). Analisis Sentimen Covid-19 Pada Media Sosial Dengan Model Neural Machine Translation. *Tematik*, 9(1), 15–20. <https://doi.org/10.38204/tematik.v9i1.899>

- [9] Nasution, S. D. (2024). Modifikasi Algoritma Caesar Cipher Menggunakan Linear Congruent Method Untuk Mengamankan Data. *Jurnal Informatika*, 01(03), 95–101.

- [10] 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)*, 3(4), 367–373. <https://doi.org/10.47065/bit.v3i4.420>.