PENERAPAN SUPER ENKRIPSI ALGORITMA AFFINE CIPHER, VERNAM CIPHER DAN RAIL FENCE CIPHER PADA PENGAMANAN DATA

Azzuhra Althaf Alfarabbi[1], Achmad Fauzi[2], Ratih Puspadini[3]
Teknik Informatika, Sekolah Tinggi Manajemen dan Informatika Kaputama Binjai
azzuhraalthafalfarabbi@gmail.com, fauzyrivai88@gmail.com, puspadini.ratih@gmail.com

ABSTRACT

Advancements in information technology have transformed library data management from manual to digital systems. While this shift facilitates data management, it also heightens information security risks—such as theft, manipulation, and unauthorized access—associated with library data. Consequently, a security mechanism capable of safeguarding data confidentiality and integrity is required. This study aims to implement a "super-encryption" method by combining the Affine Cipher, Vernam Cipher, and Rail Fence Cipher algorithms within a web-based library data security system. The research employs the Waterfall methodology, encompassing requirements analysis, system design, implementation, testing, and maintenance. The resulting system, "Perpus Secure," is a PHP and MySQL-based application designed to manage library data while protecting sensitive information, such as book records, member details, collection descriptions, and PDF e-book files. Security is achieved through a three-stage layered encryption process: the Affine Cipher for character substitution, the Vernam Cipher for key-based encryption, and the Rail Fence Cipher for character transposition using a zig-zag pattern. Implementation results demonstrate the successful integration of the Affine, Vernam, and Rail Fence ciphers into the web-based library information system. Encrypted data is stored as ciphertext, rendering it unreadable to unauthorized parties. The system also incorporates additional security measures, including user authentication, access control, CSRF protection, prepared statements, audit logs, and SHA-256 hash verification to ensure e-book file integrity. Testing confirms that the system effectively performs encryption, ciphertext storage, and data decryption in accordance with the established design

Keywords: Super-encryption, Affine Cipher, Vernam Cipher, Rail Fence Cipher, Cryptography, Data Security, Library Information System.

Article History
Received: Agustus 2026
Reviewed:Agustus 2026
Published: Agustus 2026

Plagiarism Checker No 237.u873247.fh8374

Copyright : Author
Publish by : Kohesi

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

ABSTRAK

Perkembangan teknologi informasi menyebabkan pengelolaan data perpustakaan mengalami perubahan dari sistem manual menjadi sistem digital. Perubahan tersebut memberikan kemudahan dalam pengelolaan data, namun juga meningkatkan risiko terhadap keamanan informasi seperti pencurian, manipulasi, dan akses tidak sah terhadap data perpustakaan. Oleh karena itu, diperlukan suatu mekanisme pengamanan yang mampu menjaga kerahasiaan dan integritas data. Penelitian ini bertujuan untuk menerapkan metode super enkripsi dengan mengombinasikan algoritma Affine Cipher, Vernam Cipher, dan Rail Fence Cipher pada sistem pengamanan data perpustakaan berbasis web. Metode penelitian yang digunakan adalah metode waterfall yang meliputi tahapan analisis kebutuhan, perancangan sistem, implementasi, pengujian, serta pemeliharaan sistem. Sistem yang dibangun berupa aplikasi Perpus Secure berbasis PHP dan MySQL yang mampu melakukan pengelolaan data perpustakaan serta memberikan perlindungan terhadap data sensitif seperti data buku, data anggota, deskripsi koleksi, dan file e-book PDF. Proses pengamanan dilakukan melalui tiga tahapan enkripsi berlapis, yaitu Affine Cipher sebagai proses substitusi karakter, Vernam Cipher sebagai proses enkripsi berbasis kunci, dan Rail Fence Cipher sebagai proses transposisi karakter menggunakan pola zig-zag. Hasil implementasi menunjukkan bahwa metode super enkripsi Affine Cipher, Vernam Cipher, dan Rail Fence Cipher berhasil diterapkan pada sistem informasi perpustakaan berbasis web. Data yang telah melalui proses enkripsi disimpan dalam bentuk ciphertext sehingga tidak dapat dibaca secara langsung oleh pihak yang tidak memiliki hak akses. Sistem juga dilengkapi dengan mekanisme keamanan tambahan berupa autentikasi pengguna, pembatasan hak akses, perlindungan CSRF, prepared statement, audit log, serta verifikasi hash SHA-256 untuk menjaga integritas file e-book. Berdasarkan hasil pengujian, sistem mampu menjalankan proses enkripsi, penyimpanan ciphertext, dan dekripsi data sesuai dengan rancangan yang telah dibuat.

Kata Kunci: **Super Enkripsi, Affine Cipher, Vernam Cipher, Rail Fence Cipher, Kriptografi, Keamanan Data, Sistem Informasi Perpustakaan.**

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi sistem perpustakaan dari pengelolaan secara manual menjadi sistem digital. Data perpustakaan seperti data anggota, koleksi buku, transaksi peminjaman, pengembalian, serta data petugas kini disimpan dalam basis

data yang dapat diakses melalui jaringan komputer. Digitalisasi tersebut memberikan kemudahan dalam pengelolaan informasi, namun di sisi lain juga meningkatkan risiko terhadap ancaman keamanan data seperti pencurian, penyadapan, manipulasi, maupun akses oleh pihak yang tidak berwenang. Oleh karena itu, diperlukan mekanisme pengamanan yang mampu menjaga kerahasiaan, integritas, dan keaslian data perpustakaan.

Keamanan informasi merupakan salah satu aspek penting dalam pengelolaan sistem informasi perpustakaan. Apabila data penting dapat diakses atau dimodifikasi oleh pihak yang tidak memiliki hak akses, maka akan menimbulkan berbagai kerugian, seperti hilangnya data, kesalahan informasi, hingga terganggunya pelayanan kepada pengguna perpustakaan. Salah satu teknik yang banyak digunakan untuk melindungi data adalah kriptografi, yaitu ilmu yang mempelajari metode penyandian informasi sehingga hanya pihak yang memiliki kunci tertentu yang dapat membaca isi data tersebut. Dengan menerapkan kriptografi, data yang tersimpan maupun dikirimkan melalui jaringan dapat terlindungi dari berbagai bentuk ancaman keamanan.

Salah satu algoritma kriptografi klasik yang masih banyak digunakan sebagai media pembelajaran dan penelitian adalah Affine Cipher. Algoritma ini merupakan pengembangan dari Caesar Cipher dengan menggunakan fungsi matematika linear sehingga menghasilkan proses substitusi karakter yang lebih kompleks. Meskipun memiliki tingkat keamanan yang lebih baik dibandingkan Caesar Cipher, Affine Cipher masih memiliki kelemahan apabila digunakan secara tunggal karena pola substitusinya masih dapat dianalisis menggunakan teknik kriptoanalisis, terutama jika jumlah ciphertext yang diperoleh cukup banyak.

Selain Affine Cipher, algoritma Vernam Cipher juga dikenal memiliki mekanisme enkripsi yang kuat karena menggunakan operasi XOR antara plaintext dan kunci. Jika panjang kunci sama dengan panjang pesan dan digunakan hanya satu kali, metode ini dikenal sebagai One-Time Pad yang secara teori memiliki tingkat keamanan yang sangat tinggi. Namun, dalam implementasinya terdapat kendala pada pengelolaan dan distribusi kunci, sehingga apabila digunakan secara mandiri masih memiliki keterbatasan dalam penerapan sistem pengamanan data sehari-hari (Mulder, 2022).

Algoritma Rail Fence Cipher merupakan teknik transposisi yang bekerja dengan mengubah posisi karakter tanpa mengubah nilai karakter tersebut. Metode ini menghasilkan ciphertext dengan menyusun karakter dalam pola zig-zag sesuai jumlah rail yang digunakan. Walaupun sederhana dan mudah diimplementasikan, Rail Fence Cipher memiliki kelemahan apabila diterapkan sebagai algoritma tunggal karena pola penyusunannya masih dapat diprediksi oleh pihak yang memahami metode transposisi. Oleh sebab itu, diperlukan kombinasi beberapa algoritma agar kelemahan masing-masing metode dapat saling melengkapi dan menghasilkan sistem pengamanan yang lebih baik.

Salah satu pendekatan yang dapat diterapkan adalah super enkripsi, yaitu teknik yang menggabungkan dua atau lebih algoritma kriptografi secara berurutan sehingga menghasilkan lapisan keamanan yang lebih tinggi dibandingkan penggunaan satu algoritma saja. Dalam penelitian ini, proses enkripsi dilakukan menggunakan kombinasi Affine Cipher, Vernam Cipher,

dan Rail Fence Cipher. Affine Cipher berfungsi melakukan substitusi karakter, Vernam Cipher memberikan lapisan enkripsi menggunakan operasi XOR, sedangkan Rail Fence Cipher melakukan transposisi terhadap hasil enkripsi sebelumnya. Kombinasi ketiga algoritma tersebut dapat meningkatkan kompleksitas ciphertext sehingga lebih sulit dianalisis maupun dipecahkan oleh pihak yang tidak berwenang.

2. METODE PENELITIAN

Metode yang digunakan dalam penelitian "Penerapan Super Enkripsi Algoritma Affine Cipher, Vernam Cipher dan Rail Fence Cipher Pada Pengamanan Data" terdiri dari tiga metode kriptografi, yaitu Affine Cipher, Vernam Cipher, dan Rail Fence Cipher yang dikombinasikan menjadi suatu metode super enkripsi. Metode super enkripsi merupakan teknik pengamanan data yang dilakukan dengan menerapkan beberapa algoritma kriptografi secara bertahap atau berlapis sehingga menghasilkan tingkat keamanan yang lebih baik dibandingkan dengan penggunaan satu algoritma saja.

Pada tahap pertama, algoritma Affine Cipher digunakan sebagai metode substitusi karakter yang berfungsi untuk mengubah plaintext menjadi ciphertext berdasarkan perhitungan matematis menggunakan nilai kunci tertentu. Proses ini bertujuan untuk mengganti karakter asli dengan karakter hasil penyandian sehingga informasi awal tidak dapat dibaca secara langsung oleh pihak yang tidak memiliki kunci.

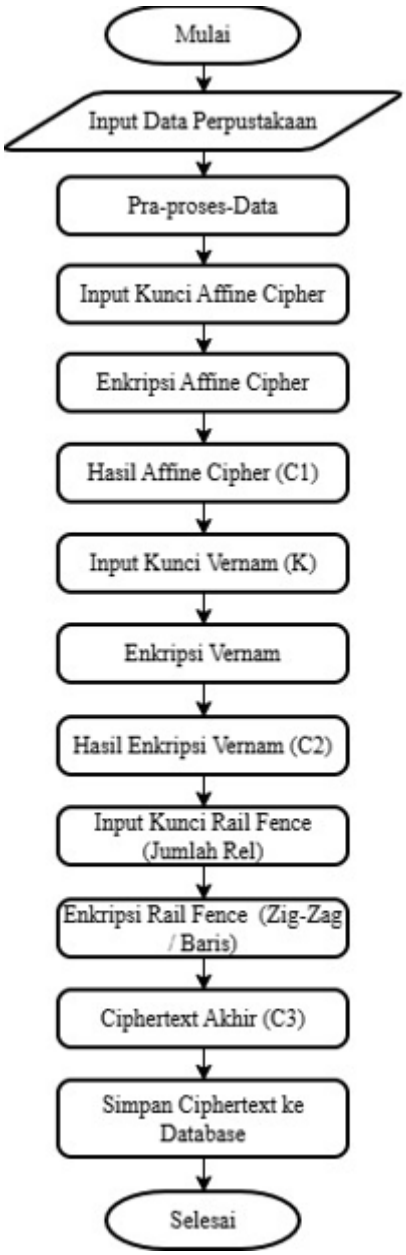
Tahap kedua menggunakan algoritma Vernam Cipher yang berfungsi memberikan lapisan keamanan tambahan melalui proses kombinasi antara plaintext atau ciphertext hasil tahap sebelumnya dengan kunci yang telah ditentukan. Algoritma ini bekerja menggunakan operasi berbasis karakter sehingga menghasilkan ciphertext yang memiliki pola berbeda dari hasil enkripsi sebelumnya dan meningkatkan tingkat kerahasiaan data.

Tahap terakhir menggunakan algoritma Rail Fence Cipher sebagai metode transposisi yang melakukan perubahan posisi karakter berdasarkan pola zig-zag sesuai jumlah rail yang digunakan. Proses ini tidak mengubah nilai karakter, tetapi mengacak susunan karakter sehingga ciphertext akhir menjadi lebih sulit dianalisis dan dikembalikan ke bentuk aslinya tanpa mengetahui parameter yang digunakan.

Ketiga algoritma tersebut diterapkan secara berurutan, dimana hasil enkripsi dari algoritma pertama akan menjadi masukan bagi algoritma berikutnya hingga menghasilkan ciphertext akhir. Dengan mengombinasikan metode substitusi dan transposisi, penerapan super enkripsi ini diharapkan mampu meningkatkan keamanan data perpustakaan dengan menjaga aspek kerahasiaan (confidentiality) dan integritas data (integrity) dari akses yang tidak berwenang.

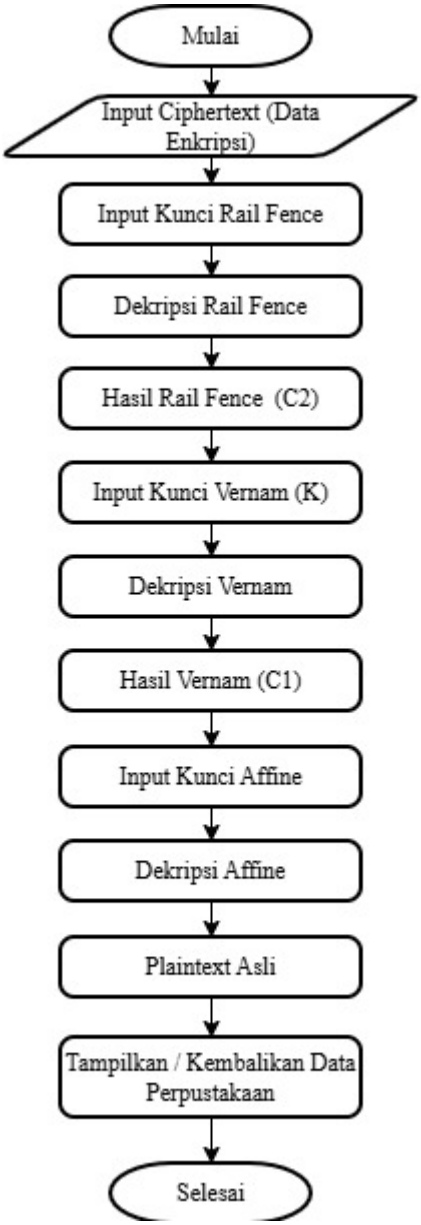
2.1 Flowchart

a. Flowchart Enkripsi



Gambar 1. Flowcharat Enkripsi

b. Flowchart Dekripsi



Gambar 2. Flowchart Dekripsi

2.2 Penerapan Metode Super Enkripsi

a. Tahap Enkripsi

Tahap pertama dari metode Super Enkripsi adalah melakukan enkripsi menggunakan algoritma Alfine Cipher. Algoritma ini merupakan teknik kriptografi klasik yang menggunakan fungsi matematika untuk mengubah setiap karakter plaintext menjadi ciphertext.

Parameter yang digunakan adalah

Nilai a = 5

Nilai b = 8

Plaintext

Plaintext yang akan di enkripsi adalah ;

ALGORITMADANPEMROGRAMAN

Alfine chiper menggunakan representasi huruf menjadi angka sebagai berikut.

A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8
J	K	L	M	N	O	P	Q	R
9	10	11	12	13	14	15	16	17
S	T	U	V	W	X	Y	Z	
18	19	20	21	22	23	24	25	

Enkripsi

Rumus alfine chiper

$C = (aP + b) \bmod 26$

Dengan

C = chipertext

P = Plaintext

a = 5

b = 8

Karakter 1 = A

P = 0

C = (5 x 0 + 8) mod 26

= 0 + 8 = 8

Nilai 8 = I

Perhitungan Kata ALGORITMA dapat dilihat pada tabel dibawah ini

Tabel 1 Perhitungan Kata ALGORITMA

Huruf	P	Perhitungan	C	Chipertext
A	0	(5 x 0 + 8) = 8 mod 26	8	I
L	11	(5 x 11 + 8) = 63 mod 26	11	L
G	6	(5 x 6 + 8) = 38 mod 26	12	M
O	14	(5 x 14 + 8) = 78 mod 26	0	A
R	17	(5 x 17 + 8) = 93 mod 26	15	P
I	8	(5 x 8 + 8) = 48 mod 26	22	W
T	19	(5 x 19 + 8) = 103 mod 26	25	Z
M	12	(5 x 12 + 8) = 68 mod 26	16	Q
A	0	(5 x 0 + 8) = 8 mod 26	8	I

Tabel 2 Perhitungan Kata DAN

Huruf	P	Perhitungan	C	Chipertext
D	3	(5 x 3 + 8) = 23 mod 26	23	X
A	0	(5 x 0 + 8) = 8 mod 26	8	I

Huruf	P	Perhitungan	C	Chipertext
N	13	(5 x 13 + 8) = 73 mod 26	12	V

Tabel 3 Perhitungan Kata PEMROGRAMAN

Huruf	P	Perhitungan	C	Chipertext
P	15	(5 x 15 + 8) = 83 mod 26	5	F
E	4	(5 x 4 + 8) = 28 mod 26	2	C
M	12	(5 x 12 + 8) = 68 mod 26	16	Q
R	17	(5 x 17 + 8) = 93 mod 26	15	P
O	14	(5 x 14 + 8) = 78 mod 26	0	A
G	6	(5 x 6 + 8) = 38 mod 26	12	M
R	17	(5 x 17 + 8) = 93 mod 26	15	P
A	0	(5 x 0 + 8) = 8 mod 26	8	I
M	12	(5 x 12 + 8) = 68 mod 26	16	Q
A	0	(5 x 0 + 8) = 8 mod 26	8	I
N	13	(5 x 13 + 8) = 73 mod 26	12	V

Sehingga didapatkan hasil chiphertext

ILMAPWZQIXIPFCQPAMPIQIV

Enkripsi dengan metode Vernam Chiper

Plainttaxt : ILMAPWZQIXIPFCQPAMPIQIV

Kuci : KRIFTOGRAFI

Rumus vernam chipher

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

I = 8

Kunci K = 10

Ci = (8 + 10) mod 26

= 18 mod 26

= S

Tabel 4. Hasil Perhitungan Enkropsi Vernam Chiper

No	Plaintext	Nilai P	Key	Nilai K	(P+K) Mod 26	cipher
1	I	8	K	10	18	S
2	L	11	R	17	2	C
3	M	12	I	8	20	U
4	A	0	F	5	5	F
5	P	15	T	19	8	I
6	W	22	O	14	10	K
7	Z	25	G	6	5	F
8	Q	16	R	17	7	H
9	I	8	A	0	8	I
10	X	23	F	5	2	C
11	I	8	I	8	16	Q
12	P	15	K	10	25	Z
13	F	5	R	17	22	W
14	C	2	I	8	10	K
15	Q	16	F	5	21	V
16	P	15	T	19	8	I
17	A	0	O	14	14	O
18	M	12	G	6	18	S
19	P	15	R	17	6	G
20	I	8	A	0	8	I
21	Q	16	F	5	21	V
22	I	8	I	8	16	Q

No	Plaintext	Nilai P	Key	Nilai K	(P+K) Mod 26	cipher
23	V	21	K	10	5	F

Hasil ciphetext Vernam Chiper

SCUFIKFHICQZWKVIOGIVQF

Enkripsi dengan metode rail chiper

Plaintext : SCUFIKFHICQZWKVIOGIVQF

Rel (Key) = 3

Rel 1 = S . . . I . . . I . . . W . . . O . . . V . .

Rel 2 = . C . F . K . H . C . Z . K . S . I . Q .

Rel 3 = . . U . . . F . . . F . . . Q . . . V . . . G . . . F

Membaca tiap rel

Rel 1 = SIIWOV

Rel 2 = CFKHZKSIQ

Rel 3 = UFFQVGF

Gabungkan semua rel

SIIWOVCFKHZKSIQUFFQVGF

b. Proses Dekripsi

Setelah proses Super Enkripsi yang terdiri dari Affine Cipher, Vernam Cipher, Rail Fence Cipher, plaintext "ALGORITMA DAN PEMROGRAMAN" berhasil dienkripsi menjadi ciphertext akhir lakukan dekripsi.

Rail Cipher

Chiphertext = SIIWOVCFKHZKSIQUFFQVGF

Jumlah karakter = 23

Jumlah rel = 3

Rel 1 = 6 karakter

Rel 2 = 11 karakter

Rel 3 = 6 karakter

Sehingga pembagiannya menjadi

Rel	**Isi**
Rel 1	SIIWOV
Rel 2	CFKHCZKISIQ
Rel 3	UFQVGF

Kemudian karakter dikembalikan mengikuti pola Zig-Zag

Tabel 5. Pola Zig-Zag Re

No	Rel	Huruf
1	1	S
2	2	C
3	3	U
4	2	F
5	1	I
6	2	K
7	3	F
8	2	H
9	1	I
10	2	C
11	3	Q
12	2	Z
13	1	W
14	2	K
15	3	V
16	2	I
17	1	O

No	Rel	Huruf
18	2	S
19	3	G
20	2	I
21	1	V
22	2	Q
23	3	F

Sehingga hasil dekripsi diatas adalah

SCUFIKFHICQZWKVIOSGIVQF

Vernam Cipher

Cipher : SCUFIKFHICQZWKVIOSGIVQF

Kunci : KRIFTOGRAFIKRIFTOGRAFIK

Rumus : $P = (C_i - K_i) \bmod 26$

Chipher = S = 18

Key = K = 10

= (18 - 10) mod 26

= 8 = I

Tabel 6. Dekripsi Vernam Cipher

No	Cipher	Nilai C	Key	Nilai K	(C-K) Mod 26	Plain
1	S	18	K	10	8	I
2	C	2	R	17	11	L
3	U	20	I	8	12	M
4	F	5	F	5	0	A
5	I	8	T	19	15	P
6	K	10	O	14	22	W
7	F	5	G	6	25	Z
8	H	7	R	17	16	Q

No	Cipher	Nilai C	Key	Nilai K	(C-K) Mod 26	Plain
9	I	8	A	0	8	I
10	C	2	F	5	23	X
11	Q	16	I	8	8	I
12	Z	25	K	10	15	P
13	W	22	R	17	5	F
14	K	10	I	8	2	C
15	V	21	F	5	16	Q
16	I	8	T	19	15	P
17	O	14	O	14	0	A
18	S	18	G	6	12	M
19	G	6	R	17	15	P
20	I	8	A	0	8	I
21	V	21	F	5	16	Q
22	Q	16	I	8	8	I
23	F	5	K	10	21	V

Sehingga Plaintext : ILMAPWZQIXIPFCQPAMPIQIV

Affine Cipher

Ciphertext : ILMAPWZQIXIPFCQPAMPIQIV

Rumus

$P = a^{-1} (C - b) \bmod 26$ / $P = 21 (C-8) \bmod 26$

Cipher = I = 8

= 21 (8-8) mod 26

= 21 (0) mod 26

= 0 (A)

Tabel 7 Dekripsi Affine Cipher

No	Cipher	Nilai C	(C-8) Mod 26	Nilai P	Plain
1	I	8	21(8–8) mod 26	0	A
2	L	11	21(11–8) mod 26	11	L
3	M	12	21(12–8) mod 26	6	G
4	A	0	21(0–8) mod 26	14	O
5	P	15	21(15–8) mod 26	17	R
6	W	22	21(22–8) mod 26	8	I
7	Z	25	21(25–8) mod 26	19	T
8	Q	16	21(16–8) mod 26	12	M
9	I	8	21(8–8) mod 26	0	A
10	X	23	21(23–8) mod 26	3	D
11	I	8	21(8–8) mod 26	0	A
12	P	15	21(15–8) mod 26	17	R
13	F	5	21(5–8) mod 26	15	P
14	C	2	21(2–8) mod 26	4	E
15	Q	16	21(16–8) mod 26	12	M
16	P	15	21(15–8) mod 26	17	R
17	A	0	21(0–8) mod 26	14	O
18	M	12	21(12–8) mod 26	6	G
19	P	15	21(15–8) mod 26	17	R
20	I	8	21(8–8) mod 26	0	A
21	Q	16	21(16–8) mod 26	12	M
22	I	8	21(8–8) mod 26	0	A
23	V	21	21(21–8) mod 26	13	N

Sehingga Plaintext : ALGORITMA DAN PEMROGRAMAN

3. HASIL DAN PEMBAHASAN

Berdasarkan hasil penelitian “Penerapan Super Enkripsi Algoritma Affine Cipher, Vernam Cipher dan Rail Fence Cipher Pada Pengamanan Data”, telah berhasil dibangun aplikasi Perpus Secure

sebagai sistem informasi perpustakaan berbasis web yang dilengkapi dengan mekanisme pengamanan data. Sistem ini mampu mengelola data perpustakaan seperti data buku, anggota, transaksi peminjaman, serta koleksi digital e-book dengan menerapkan proses enkripsi untuk melindungi informasi penting.

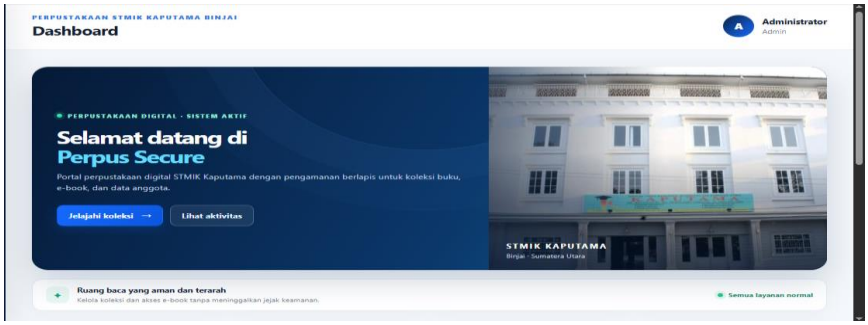
Hasil implementasi menunjukkan bahwa metode super enkripsi berhasil diterapkan melalui tiga tahapan, yaitu algoritma Affine Cipher sebagai proses substitusi karakter, Vernam Cipher sebagai proses enkripsi berbasis kunci, dan Rail Fence Cipher sebagai proses transposisi karakter menggunakan pola zig-zag. Kombinasi ketiga algoritma tersebut menghasilkan ciphertext yang lebih kompleks sehingga data tidak dapat dibaca secara langsung oleh pihak yang tidak memiliki kunci.

Pada proses pengamanan data, sistem mampu mengenkripsi informasi perpustakaan seperti judul buku, pengarang, penerbit, deskripsi koleksi, serta file e-book PDF sebelum disimpan. File PDF yang diunggah akan melalui proses validasi, enkripsi, dan penyimpanan dalam bentuk ciphertext pada lokasi yang tidak dapat diakses langsung melalui browser, sehingga keamanan data menjadi lebih terjaga.

Selain penerapan algoritma kriptografi, sistem juga dilengkapi dengan fitur keamanan tambahan seperti autentikasi pengguna, pembatasan hak akses, perlindungan CSRF, prepared statement, audit log, serta verifikasi hash SHA-256 untuk memastikan integritas file. Mekanisme tersebut mampu mencegah akses tidak sah dan memastikan file hasil dekripsi tetap sesuai dengan data asli.

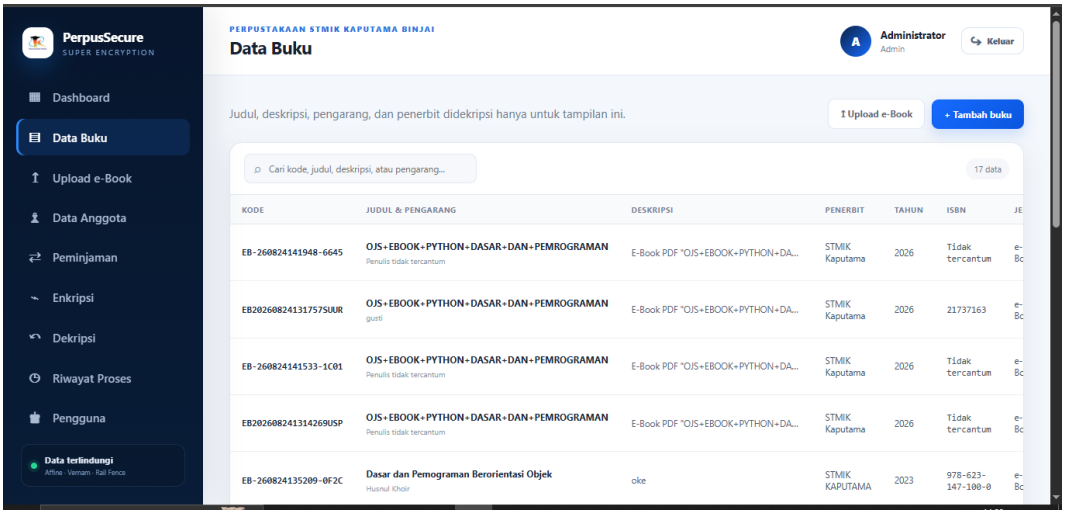
Berdasarkan hasil pengujian menggunakan metode Black Box Testing, seluruh fitur utama sistem berjalan sesuai dengan rancangan. Proses login, pengelolaan data perpustakaan, enkripsi dan dekripsi file PDF, serta mekanisme keamanan berhasil dijalankan dengan baik. Dengan demikian, penerapan super enkripsi algoritma Affine Cipher, Vernam Cipher, dan Rail Fence Cipher dapat digunakan sebagai solusi dalam meningkatkan keamanan data perpustakaan berbasis web. Berikut ini merupakan interface keamanan data perpustakaan

a. Menu Utama



Gambar 3. Dashboard / menu utama

b. Data E-Book



Gambar 4. Data E-Book

KESIMPULAN

Kesimpulan: kesimpulan penelitian menyatakan bahwa penerapan super enkripsi menggunakan algoritma Affine Cipher, Vernam Cipher, dan Rail Fence Cipher berhasil diterapkan pada sistem pengamanan data perpustakaan berbasis web. Kombinasi ketiga algoritma tersebut mampu menghasilkan ciphertext melalui proses enkripsi berlapis sehingga data sensitif seperti data buku, anggota, deskripsi koleksi, dan file e-book PDF tidak tersimpan dalam bentuk teks asli. Sistem Perpus Secure juga mampu menjaga kerahasiaan dan integritas data melalui dukungan mekanisme keamanan tambahan seperti autentikasi pengguna, pembatasan hak akses, perlindungan CSRF, prepared statement, audit log, serta verifikasi hash SHA-256.

Saran: Saran untuk pengembangan penelitian selanjutnya adalah sistem dapat dikembangkan dengan menambahkan metode kriptografi atau kombinasi algoritma keamanan lain agar tingkat keamanan semakin meningkat. Selain itu, penelitian berikutnya dapat membandingkan metode super enkripsi Affine Cipher, Vernam Cipher, dan Rail Fence Cipher dengan algoritma kriptografi modern, serta mengembangkan mekanisme manajemen kunci yang lebih aman seperti pembangkitan kunci otomatis dan penyimpanan kunci terenkripsi. Pengembangan aplikasi juga dapat diperluas dengan mendukung berbagai format dokumen, platform mobile, serta pengujian pada jumlah data yang lebih besar untuk mengetahui performa sistem pada lingkungan yang lebih kompleks.

DAFTAR PUSTAKA

Agustina, L., Sujarwo, I., & Khudzaifah, M. (2023). Membangun super enkripsi untuk mengamankan pesan. *Jurnal Riset Mahasiswa Matematika, 2(5), 195-200.* *https://doi.org/10.18860/jrmm.v2i5.21036*

Anwar, A. Q. H., & Amrulloh, M. F. (2025). Implementasi Rail Fence Cipher & DES untuk Meningkatkan Keamanan Data Pribadi Siswa Sekolah Luar Biasa. *Digital Transformation Technology*, *5*(2), 31–42. *https://itscience.org/jurnal/index.php/digitech/article/view/6710*

Bahri, S., Jihan, F., & Rudianto, B. (2023). Implementasi algoritma super enkripsi Vigenere Cipher dan Route Cipher pada penyandian pesan teks. *Jurnal Matematika UNAND, 12(2), 168–175. https://doi.org/10.25077/jmua.12.2.168-175.2023*

Basyarahil, F. A., Astuti, H. M., & Hidayanto, B. C. (2017). Evaluasi manajemen keamanan informasi menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO/IEC 27001:2013 Pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya. *Jurnal Teknik ITS, 6(1), A123-A128.*

Budiyanto, Primananda, R., & Bakhtiar, F. A. (2021). Implementasi Enkripsi Vernam Cipher dan Distribusi Kunci Three-Pass Protocol untuk Mengamankan Data Chatting pada ATmega328. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *5*(3), 1119–1125. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/8744

Diana, I. N. (2022). Algoritma Affine Cipher dan Modifikasi Affine Cipher, serta Kombinasinya dengan Cipher Transposisi Grup Simetri untuk Mengamankan Pesan Teks. *KUBIK: Jurnal Publikasi Ilmiah Matematika*, *7*, 39–48.

Eko Siswanto. (2021). *Kupas Tuntas Pemrograman PHP*. Semarang: Yayasan Prima Agus Teknik

Elwahdiyah, A., & Hartono. (2025). Jenis data dan skala pengukuran: Mengenal klasifikasi data, skala pengukuran dan implikasinya dalam analisis. Didaktik: *Jurnal Ilmiah PGSD STKIP Subang, 11(4), 223-238.*

Farhan Saputra. (2025). Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Data. *Jurnal: Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia*

Jonny, J., Ambarwati, A., & Darujati, C. (2021). Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005. Sistemasi: *Jurnal Sistem Informasi, 10(1), 1-10. https://doi.org/10.32520/stmsi.v10i1.995*

Joseph Teguh Santoso & Migunani. (2023). Disain & Analisis Sistem Berorientasi Obyek Dengan UML.

Indra Ava Dianta. (2021). *Logika dan Algoritma Untuk Merancang Aplikasi Komputer*. Semarang: Yayasan Prima Agus Teknik

Lestari, A., Tami, N. P., Saputra, F. D., & Widarti, E. (2025). Combination of Rail Fence and

Route Cipher: Dual Encryption Strategy in Digital Messages. *Journal of Software Engineering and Multimedia (JASMED)*, *3*(2), 75–85. *https://doi.org/10.20895/jasmed.v3i2.10097*

Mantra, I., Rahman, A. A., & Saragih, H. (2020). Maturity Framework Analysis ISO 27001:2013 on Indonesian Higher Education. *International Journal of Engineering and Technology, 9(2), 429–436. https://doi.org/10.14419/ijet.v9i2.30581*

Munir, R. (2006). *Kriptografi*. Bandung: Informatika.

Vansuri, R., Fauzi, A., Prasetyo, E. T., Negara, R., Ramadhan, R., Restu, A. M., & Firmansyah, R. R. (2023). Peran CIA (Confidentiality, Integrity, Availability) terhadap manajemen keamanan informasi. Jurnal Ilmu Multidisiplin, 2(1), 106–113. https://doi.org/10.38035/jim.v2i1.234

Velentin Mulder. (2022). *Trends Data Protection and Encription Technologies*. Switzerland: Quentin Ladetto

Yusuf Ramadhan Nasution, Heri Santoso, & Amalia, S. W. (2023). Penerapan Algoritma Vernam Dalam Mengamankan Dokumen Pdf. *Jurnal Informatika Dan Rekayasa Elektronik*, *6*(1), 37–46. https://doi.org/10.36595/jire.v6i1.804