Implementasi Keamanan Data File Dokumen Menggunakan Modifikasi Algoritma Hill Cipher

Imay kurniawan[1*], Purwadi Budi Santoso[2]
[1,]Teknik Informatika, Teknik, Sekolah Tinggi Teknologi Wastukanca, Purwakarta, Indonesia
[2]Teknik Informatika, Teknik, Sekolah Tinggi Teknologi Mandala, Bandung, Indonesia
[1]Imaykurniawan@wastukancana.ac.id, [2]purwadiugm87@gmail.com
*Penulis Korespondensi
(Imay Kurniawan, Sekolah Tinggi Teknologi Wastukancana, Imaykurniawan@wastukancana.ac.id)

ABSTRAK

Keamanan data dokumen elektronik menjadi aspek krusial seiring dengan meningkatnya pertukaran informasi secara digital. Algoritma Hill Cipher merupakan salah satu teknik kriptografi kunci simetris berbasis matriks yang dikenal efisien, namun memiliki kerentanan terhadap *Known Plaintext Attack* (KPA) karena sifatnya yang linier. Penelitian ini bertujuan untuk meningkatkan keamanan algoritma Hill Cipher dengan menerapkan modifikasi teknik rotasi tiga kunci. Metode yang diusulkan melibatkan penggunaan tiga buah matriks kunci persegi yang berbeda. Proses enkripsi tidak hanya mengandalkan perkalian matriks standar, tetapi menerapkan perputaran atau rotasi kunci secara dinamis untuk setiap blok karakter yang diproses. Hasil pengujian menunjukkan bahwa modifikasi ini mampu menghasilkan nilai entropi yang lebih tinggi dan sebaran karakter yang lebih acak dibandingkan Hill Cipher standar. Penggunaan tiga kunci dengan mekanisme rotasi secara signifikan menyulitkan upaya kriptanalisis tanpa menambah beban komputasi yang berlebihan. Dengan demikian, sistem ini efektif dalam mengamankan file dokumen sensitif dari akses yang tidak sah.

Kata kunci: Kriptografi, Hill Cipher, Matriks, Rotasi Kunci, Enkripsi Dokumen.

ABSTRACT

The security of electronic document data has become crucial with the increasing digital exchange of information. The Hill Cipher algorithm is a matrix-based symmetric key cryptography technique known for its efficiency, but it is vulnerable to Known Plaintext Attacks (KPA) due to its linear nature. This research aims to improve the security of the Hill Cipher algorithm by implementing a modified three-key rotation technique. The proposed method involves the use of three different square key matrices. The encryption process, instead of relying solely on standard matrix multiplication, dynamically rotates the keys for each processed block of characters. Test results show that this modification produces higher entropy and a more random character distribution than the standard Hill Cipher. The use of three keys with a rotation mechanism significantly complicates cryptanalysis efforts without increasing excessive computational burden. Thus, this system is effective in securing sensitive document files from unauthorized access.

Keywords: *Cryptography, Hill Cipher, Matrix, Key Rotation, Document Encryption.*

1. PENDAHULUAN

Di era transformasi digital saat ini, pertukaran informasi melalui media elektronik telah menjadi kebutuhan primer [1]. Namun, kemudahan akses ini berbanding lurus dengan tingginya risiko keamanan, seperti penyadapan, pencurian data, hingga manipulasi berkas oleh pihak yang tidak bertanggung jawab [2]. Oleh karena itu, diperlukan mekanisme perlindungan data yang mumpuni untuk menjaga aspek kerahasiaan (confidentiality) dan integritas (integrity) pada file sensitif [3]. Kriptografi menjadi solusi utama dalam mengamankan data dengan cara menyamarkan pesan asli (*plaintext*) menjadi pesan acak (*ciphertext*) [4]. Salah satu algoritma klasik yang berbasis matriks adalah Hill Cipher [5]. Algoritma ini dikenal efisien karena melakukan enkripsi secara blok dan memiliki kecepatan pemrosesan yang relatif cepat.Meskipun memiliki keunggulan dalam teknik perkalian matriks, Hill Cipher standar memiliki kelemahan mendasar. Karena bersifat simetris dan menggunakan kunci yang sama untuk seluruh blok data, algoritma ini rentan terhadap serangan *Known Plaintext Attack* (KPA) [6]. Jika penyerang berhasil mendapatkan sebagian pasangan *plaintext* dan *ciphertext*, mereka dapat melakukan analisis linear untuk menemukan kunci matriks yang digunakan.Untuk mengatasi kelemahan tersebut, penelitian ini mengusulkan sebuah rancang bangun sistem keamanan file menggunakan Modifikasi Algoritma Hill Cipher. Inovasi utama dalam modifikasi ini adalah penggunaan 3 Kunci Berbeda.

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti [7]. Secara umum, proses kriptografi melibatkan dua fungsi utama: 1) Enkripsi : Proses mengubah data asli (*plaintext*) menjadi kode rahasia (*ciphertext*), 2) Dekripsi : Proses mengembalikan kode

rahasia (*ciphertext*) menjadi data asli (*plaintext*) menggunakan kunci yang sesuai [8]. Hill Cipher merupakan algoritma kriptografi kunci simetris yang ditemukan oleh Lester S. Hill pada tahun 1929. Algoritma ini termasuk dalam kategori *polygraphic substitution cipher* yang berbasis pada aljabar linear. Keamanan utamanya terletak pada penggunaan matriks sebagai kunci enkripsi dan dekripsi [9]. Proses enkripsi pada *Hill Cipher* dilakukan dengan mengalikan matriks kunci (K) dengan matriks plaintext (P) dalam modulo 26 (untuk teks) atau modulo 256 (untuk file/ASCII), yang dirumuskan sebagai berikut:

$$C = (K \cdot P)(mod\ m) \qquad (1)$$

Sedangkan untuk proses dekripsi, digunakan invers dari matriks kunci (K_{-1}):

$$P = (K_{-1} \cdot C)(mod\ m) \qquad (2)$$

Dalam Hill Cipher, kunci yang digunakan harus berupa matriks persegi berukuran n×n. Syarat utama agar sebuah matriks dapat dijadikan kunci adalah matriks tersebut harus memiliki invers. Sebuah matriks memiliki invers jika dan hanya jika determinannya tidak nol dan determinan tersebut harus relatif prima dengan nilai modulo yang digunakan (misalnya 256 untuk data file) [10]. Data dalam sebuah file komputer disimpan dalam bentuk biner atau byte (0-255). Pengamanan file menggunakan Hill Cipher mengharuskan sistem untuk membaca setiap byte data, mengelompokkannya ke dalam blok sesuai ukuran matriks kunci, dan melakukan operasi aritmatika matriks terhadap nilai desimal dari byte tersebut [11]. Dalam penelitian ini menggunakan matriks kunci berordo 3x3.

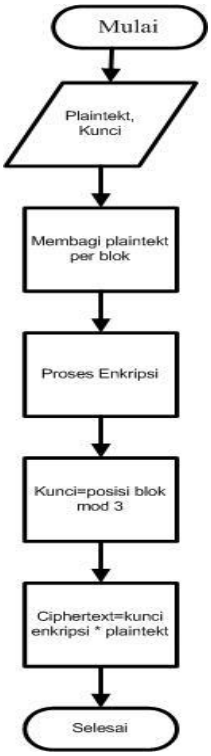
Penggunaan metode Hill Cipher telah dilakukan oleh beberapa peneliti sebelumnya namun dalam kasus yang berbeda, termasuk penelitian yang menggunakan algoritma Hill Cipher untuk keamanan rekam medis di puskemas Pematang Raya. Hasil penelitian menunjukkan berhasil mengamankan data rekam medis pesan [12]. Kelemahan dari penelitian ini adalah menggunakan modulo 93 sehingga tidak dapat mengenkripsi semua kode ascii (0-255). Penelitian selanjutnya, menerapkan algoritma Hill Cipher untuk mengamankan file digital menggunakan kunci matriks secara acak [13]. Hasil penelitian menunjukkan ada peningkatan keamanan karena menggunakan kunci matriks secara acak dari proses pembangkitan kunci. Kelemahan dari penelitian ini menggunakan 1 kunci matriks untuk semua blok. Penelitian selanjutnya Menerapkan algoritma HillCipher untuk keamanan data dengan menggunakan kunci matriks 5x5. Kesimpulan penelitian ini menunjukkan bahwa kompleksitas operasi invers matriks akan meningkatkan kesulitan bagi entitas yang tidak berwenang untuk mendekripsi pesan asli. Kelemahan dari dari penelitian ini tidak melakukan modifikasi algoritma Hill Cipher sehingga rentan terhadap serangan *Known Plaintext Attack* (KPA). Modifikasi algoritma Hill Cipher dengan rotasi tiga kunci untuk menutupi kelemahan Hill Cipher standar terhadap serangan *Known Plaintext Attack*. Dengan menggunakan lebih dari satu kunci yang bekerja secara bergantian (rotasi), pola frekuensi pada ciphertext akan menjadi lebih acak.Siklus rotasi kunci yang diusulkan dalam penelitian ini menggunakan fungsi modulo 3 untuk menentukan penggunaan kunci pada setiap indeks blok (*i*)

2. METODOLOGI PENELITIAN

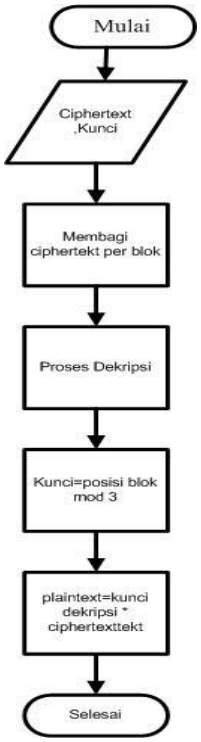
Metodologi penelitian menggunakan Waterfall. Waterfall adalah model pengembangan perangkat lunak klasik yang bersifat linier, sekuensial, dan terstruktur, di mana setiap tahapan (analisis, desain, implementasi, pengujian, pemeliharaan) harus diselesaikan sepenuhnya sebelum berpindah ke tahap berikutnya. Dalam penelitian ini hanya sampai tahap pengujian. Sebab jika hasil pengujian tidak sesuai ekspektasi, Waterfaal sulit untuk kembali ke tahap perencanaan untuk melakukan perubahan.

2.1 Analisis Sistem

Tahap awal dimulai dengan menganalisis cara kerja Hill Cipher standar yang bersifat statis. Fokus utama dalam tahap ini adalah merancang algoritma distribusi blok agar sinkron dengan rotasi tiga kunci (*K*1,*K*2,*K*3) sehingga tidak terjadi tumpang tindih saat proses dekripsi.
Diagram flowchart proses enkripsi dan dekripsi modifikasi Hill Cipher dengan rotasi 3 kunci,dapat dilihat pada gambar 3.1 dan 3.2:



Gambar 3.1 Flochart Enkripsi

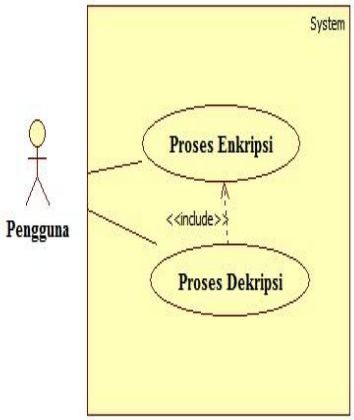


Gambar 3.2 Flowchart Dekripsi

3.2 Perancangan Sistem

3.2.1. Use Case Diagram

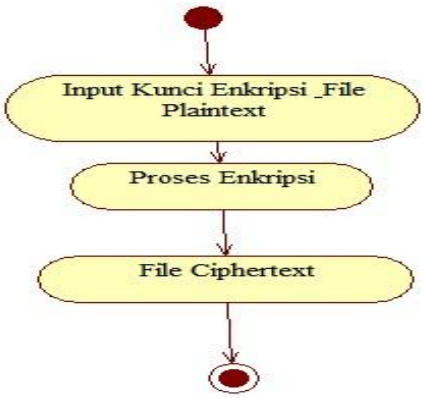
Use case diagram menggambarkan interaksi antara aktor (pengguna) dan sistem secara visual. Gambar use case diagram dapat dilihat pada gambar 3.3



Gambar 3.3 Use Case Diagram

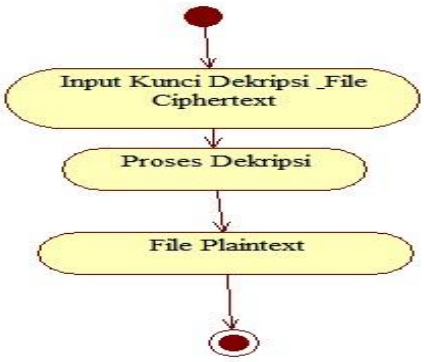
3.2.2 Activity Diagram Enkripsi

Activity diagram enkripsi adalah memodelkan proses-proses yang terjadi pada sebuah sistem untuk menggambarkan proses enkripsi. Activity diagram dapat dilihat pada gambar 3.4 :



Gambar 3.4 Activity Diagram Dekripsi

Activity diagram dekripsi adalah memodelkan proses-proses yang terjadi pada sebuah sistem untuk menggambarkan proses enkripsi. Activity diagram dapat dilihat pada gambar 3.5 :



Gambar 3.5 Activity Diagram Dekripsi

.

3. HASIL DAN PEMBAHASAN

3.1 Perhitungan Manual Proses Enkripsi

3.1.1Contoh Proses Enkripsi Hill Cipher Satu Kunci

Diketahui data plaintext = Algoritma, akan dilakukan proses enkripsi dengan satu kunci untuk memperoleh data ciphertext. Matriks kunci menggunakan matriks berordo 3x3, Syarat matriks kunci memiliki matriks nvers nilai determinan tidak sama dengan nol [11]. Disini dipilih matriks kunci dengan nilai determinan sama dengan satu:

$$K = \begin{vmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 1 & 3 & 3 \end{vmatrix}$$

karena matriks kunci 3x3 maka data plaintext dikelompokkan ke dalam kelipatan 3. P1=Alg, P2=ori,P3=tma. Selanjutnya konversi plaintext ke desimal dalam bentuk matriks :

$$\text{P1}=\begin{vmatrix} 65 \\ 108 \\ 103 \end{vmatrix}, \text{P2} = \begin{vmatrix} 111 \\ 114 \\ 105 \end{vmatrix}, \text{P3} = \begin{vmatrix} 116 \\ 109 \\ 97 \end{vmatrix}$$

Berdasarkan persamaan 1, rumus ciphertext diperoleh :

C = K x P mod 256

Untuk Kelompok 1

C1 = K x P1

$$= \begin{vmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 1 & 3 & 3 \end{vmatrix} \text{x} \begin{vmatrix} 65 \\ 108 \\ 103 \end{vmatrix} \text{ mod } 256 = \begin{vmatrix} 173 \\ 384 \\ 698 \end{vmatrix} \text{ mod } 256 = \begin{vmatrix} 173 \\ 128 \\ 186 \end{vmatrix}$$

Selanjutnya hasil enkripsi dikonversi ke karakter :
173=- , 128=€, 186=º

Untuk kelompok 2
C2 = K x P1
$= \begin{vmatrix}1 & 1 & 0\\1 & 2 & 1\\1 & 3 & 3\end{vmatrix} \text{ x } \begin{vmatrix}111\\114\\105\end{vmatrix} \text{ mod } 256 = \begin{vmatrix}225\\444\\768\end{vmatrix} \text{ mod } 256 = \begin{vmatrix}225\\188\\0\end{vmatrix}$
Selanjutnya hail enkripsi dikonversi ke karakter :
225=á , 188=¼, 0=NUL
Untuk kelompok 3 :
C3 = K x P3
$= \begin{vmatrix}1 & 1 & 0\\1 & 2 & 1\\1 & 3 & 3\end{vmatrix} \text{ x } \begin{vmatrix}116\\109\\97\end{vmatrix} \text{ mod } 256 = \begin{vmatrix}225\\431\\734\end{vmatrix} \text{ mod } 256 = \begin{vmatrix}225\\175\\222\end{vmatrix}$

Selanjutnya hasil enkripsi dionversi ke karakter :
225=á , 175=¯, 222=Þ

Selanjutnya gabungkan C1,C2, dan C3, hasil proses enkripsi data ciphertext sebagai berikut :
C=-€ º á¼NUL á¯ Þ

3.1.2 Contoh Proses Dekripsi Hill Cipher Satu Kunci

Diketahui ciphertext =-€ º` SI ô v þ û , kelompokkan data ciphertext ke dalam kelipatan tiga :
C1==-€ º, C2=` SI ô, C3= v þ û kemudian konversi ke desimal dalam bentuk matriks :
$C1=\begin{vmatrix}173\\128\\186\end{vmatrix}, C2 = \begin{vmatrix}225\\188\\0\end{vmatrix}, C3 = \begin{vmatrix}225\\175\\222\end{vmatrix}$
Berdasarkan persamaan 2, rumus plaintext diperoleh :
$P=K^{-1} C \bmod 256$

K^{-1} merupakan invers matriks kunci :
$K^{-1} = \begin{vmatrix}3 & -3 & 1\\-2 & 3 & -1\\1 & -2 & 1\end{vmatrix}$

Untuk kelompok 1 :
$P1 = K^{-1} C1 \bmod 256$

$= \begin{vmatrix}3 & -3 & 1\\-2 & 3 & -1\\1 & -2 & 1\end{vmatrix} \begin{vmatrix}173\\128\\186\end{vmatrix} \text{ mod } 256 = \begin{vmatrix}321\\-148\\103\end{vmatrix} \text{ mod } 256 = \begin{vmatrix}65\\108\\103\end{vmatrix}$
Selanjutnya hasil dekripsi dikonversi ke karakter :
65=A, 108=l, 103=g
P1=Alg
Untuk kelompok 2:
$P2= K^{-1} C2 \bmod 256$

$= \begin{vmatrix}3 & -3 & 1\\-2 & 3 & -1\\1 & -2 & 1\end{vmatrix} x \begin{vmatrix}225\\188\\0\end{vmatrix} \text{ mod } 256 = \begin{vmatrix}111\\114\\-151\end{vmatrix} \text{ mod } 256 = \begin{vmatrix}111\\114\\105\end{vmatrix}$

Selanjutnya hasil dekripsi dikonversi ke karakter :
111=0,114=r, 105=i
P2 = ori
Untuk kelompok 3:
$P3= K^{-1} C3 \bmod 256$

$= \begin{vmatrix}3 & -3 & 1\\-2 & 3 & -1\\1 & -2 & 1\end{vmatrix} x \begin{vmatrix}225\\175\\222\end{vmatrix} \text{ mod } 256 = \begin{vmatrix}372\\-147\\97\end{vmatrix} \text{ mod } 256 = \begin{vmatrix}116\\109\\97\end{vmatrix}$

Selanjutnya hasil dekripsi dikonversi ke karakter
116=t, 109=m, 97=a
Selanjutnya gabungkan hasil P1,P2, dan P3:
P=Algoritma

3.1.3 Contoh Proses Enkripsi Hill Cipher Tiga Kunci

Diketahui data plaintext = Algoritma, akan dilakukan proses enkripsi dengan tiga kunci. Dibutuhkan tiga kunci untuk rotasi proses enkripsi tiap blok. Disini dipilih tiga kunci matriks yang nilai determinannya tidak sama dengan nol :

$$K1 = \begin{vmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 1 & 3 & 3 \end{vmatrix}, K2 = \begin{vmatrix} 1 & 2 & 3 \\ 1 & 3 & 4 \\ 1 & 2 & 2 \end{vmatrix}, K3 = \begin{vmatrix} 1 & 8 & 6 \\ 0 & 1 & 7 \\ 0 & 0 & 1 \end{vmatrix}$$

Kelompokkan data plaintext ke dalam kelipatan 3 : P1=Alg, P2=ori,P3=tma. Selanjutnya konversi masing-masing kelompok data plaintext ke desimal dalam bentuk matriks :

$$P1 = \begin{vmatrix} 65 \\ 108 \\ 103 \end{vmatrix}, P2 = \begin{vmatrix} 111 \\ 114 \\ 105 \end{vmatrix}, P3 = \begin{vmatrix} 116 \\ 109 \\ 97 \end{vmatrix}$$

Berdasarkan persamaan 1, rumus plaintext diperoleh :
C = $K \; x \; P$ mod 256
Untuk Kelompok 1 :
C1 = K1 x P1

$$= \begin{vmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 1 & 3 & 3 \end{vmatrix} \text{ x } \begin{vmatrix} 65 \\ 108 \\ 103 \end{vmatrix} \text{ mod } 256 = \begin{vmatrix} 173 \\ 384 \\ 698 \end{vmatrix} \text{ mod } 256 = \begin{vmatrix} 173 \\ 128 \\ 186 \end{vmatrix}$$

Selanjutnya hasil enkripsi dikonversi ke karakter :
173=- , 128=€, 186=º

Untuk kelompok 2 :
C2 = K2 x P1

$$= \begin{vmatrix} 1 & 2 & 3 \\ 1 & 3 & 4 \\ 1 & 2 & 2 \end{vmatrix} \text{ x } \begin{vmatrix} 111 \\ 114 \\ 105 \end{vmatrix} \text{ mod } 256 = \begin{vmatrix} 654 \\ 873 \\ 549 \end{vmatrix} \text{ mod } 256 = \begin{vmatrix} 142 \\ 105 \\ 37 \end{vmatrix}$$

Selanjutnya hasil enkripsi dikonversi ke karakter :
42=Ž , 105=i, 37=%

Untuk kelompok 3 :
C3 = K x P3

$$= \begin{vmatrix} 1 & 8 & 6 \\ 0 & 1 & 7 \\ 0 & 0 & 1 \end{vmatrix} \text{ x } \begin{vmatrix} 116 \\ 109 \\ 97 \end{vmatrix} \text{ mod } 256 = \begin{vmatrix} 1570 \\ 788 \\ 97 \end{vmatrix} \text{ mod } 256 = \begin{vmatrix} 34 \\ 20 \\ 97 \end{vmatrix}$$

Selanjutnya hasil enkripsi dikonversi ke karakter :
34 = '', 20 = DC4, 97=a
Selanjutnya gabungkan hasil enkripsi kelompok 1,kelompok 2, dan kelompok 3 :
C = -€ º Ži% " DC4 a

3.1.4 Contoh Proses Dekripsi Hill Cipher Tiga Kunci

Diketahui ciphertext = -€ º Ži% " DC4 a, kelompokkan data ciphertext ke dalam kelipatan tiga :
C1==-€ º, C2= Ži%, C3= " DC4 a kemudianmasing-masik blok dikonversi ke desimal dalam bentuk matriks :

$$C1 = \begin{vmatrix} 173 \\ 128 \\ 186 \end{vmatrix}, C2 = \begin{vmatrix} 142 \\ 105 \\ 37 \end{vmatrix}, C3 = \begin{vmatrix} 34 \\ 20 \\ 97 \end{vmatrix}$$

Berdasarkan persamaan 2, rumus plaintext diperoleh :
P=K^{-1} C mod 256

$K1^{-1}, K2^{-1}, K3^{-1},$ merupakan invers matriks kunci K1, K2, dan K3.

$$K^{-1} = \begin{vmatrix} 3 & -3 & 1 \\ -2 & 3 & -1 \\ 1 & -2 & 1 \end{vmatrix}, K2^{-1} = \begin{vmatrix} 2 & -2 & 1 \\ -2 & 1 & 1 \\ 1 & 0 & -1 \end{vmatrix}, K3^{-1} = \begin{vmatrix} 1 & -8 & 50 \\ 0 & 1 & -7 \\ 0 & 0 & 1 \end{vmatrix}$$

Untuk kelompok 1 :
P1 = K^{-1} C1 mod 256

$$= \begin{vmatrix} 3 & -3 & 1 \\ -2 & 3 & -1 \\ 1 & -2 & 1 \end{vmatrix} \begin{vmatrix} 173 \\ 128 \\ 186 \end{vmatrix} \text{ mod } 256 \quad = \begin{vmatrix} 321 \\ -148 \\ 103 \end{vmatrix} \text{ mod } 256 \quad = \quad \begin{vmatrix} 65 \\ 108 \\ 103 \end{vmatrix}$$

Selanjutnya hasil proses dekripsi dikonversi ke karakter :
65=A, 108=l, 103=g
P1=Alg

Untuk kelompok 2 :
P2= $K2^{-1}$ C2 mod 256

$$= \begin{vmatrix} 2 & -2 & 1 \\ -2 & 1 & 1 \\ 1 & 0 & -1 \end{vmatrix} x \begin{vmatrix} 142 \\ 105 \\ 37 \end{vmatrix} \text{ mod } 256 \quad = \begin{vmatrix} 111 \\ -142 \\ 105 \end{vmatrix} \text{ mod } 256 = \begin{vmatrix} 111 \\ 114 \\ 105 \end{vmatrix}$$

Selanjutnya hasil dekripsi dikonversi ke karakter :
111=0,114=r, 105=i
P2 = ori
Untuk kelompok 3 :
P3= K^{-1} C3 mod 256

$$= \begin{vmatrix} 1 & -8 & 50 \\ 0 & 1 & -7 \\ 0 & 0 & 1 \end{vmatrix} x \begin{vmatrix} 225 \\ 175 \\ 222 \end{vmatrix} \text{ mod } 256 \quad = \begin{vmatrix} 372 \\ -147 \\ 97 \end{vmatrix} \text{ mod } 256 \quad = \begin{vmatrix} 116 \\ 109 \\ 97 \end{vmatrix}$$

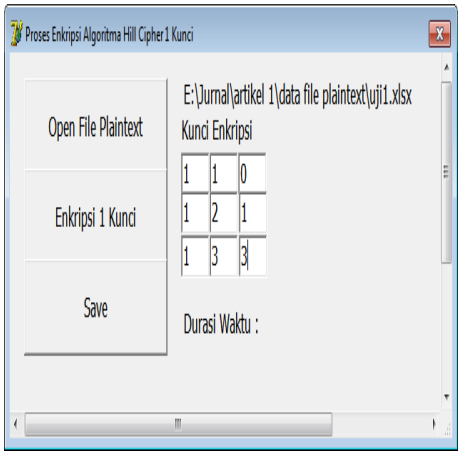
Selanjutnya hasil dekripsi dikonversi ke karakter
116=t, 109=m, 97=a
Selanjutnya gabungkan hasil P1,P2, dan P3:
P=Algoritma

3.2 Implementasi Sistem

Pembuatan kode program menggunakan Embarcadero, kode program terdiri dari dua proses yaitu proses enkripsi dan dekripsi. Untuk pengujian sistem menggunakan file dokumen
uji1(excel size:106 KB), uji2(ppt size:224 KB), uji3(pdf size:245 KB),uji4(ppt size:901 KB), uji5(excel size:992 KB), Uji6 (word size:1,17 MB) ,uji7(pdf size:2,37 MB),uji8(word size:4,22 MB),

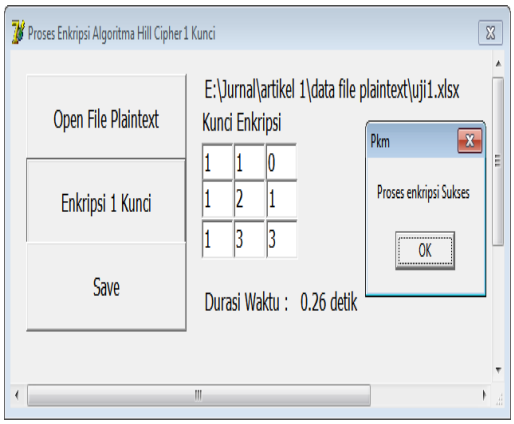
3.2.1 Implementasi Proses Enkripsi 1 Kunci

Untuk menjalankan proses enkripsi,input file yang akan dienkripsi kemudian input kunci enkripsi di kotak yang sudah disediakan.Proses enkripsi dapat dilihat pada gambar 4.1 :



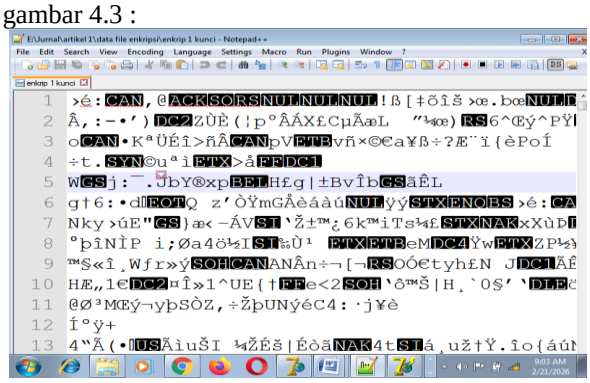
Gambar 3.1 Proses Enkripsi 1 Kunci

Untuk melihat hasil proses enkripsi klik tombol enkripsi 1 kunci, hasilnya dapat dilihat pada gambar 3.2 :



Gambar 3.2 Hasil Proses Enkripsi 1 Kunci

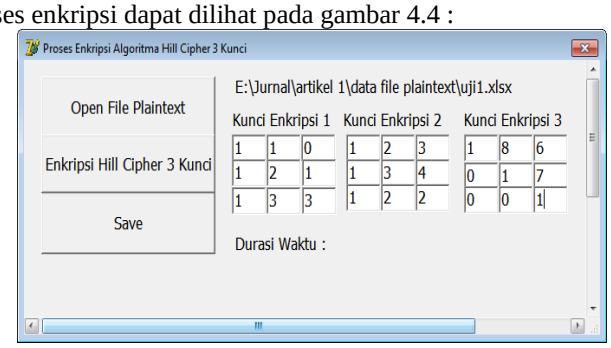
Selanjutnya klik tombol save untuk menyimpan hasil proses enkripsi ke dalam file ciphertext. Isi dari file ciphertext dapat dilihat pada gambar 4.3 :



Gambar 3.3 isi dokumen file ciphertext 1 kunci

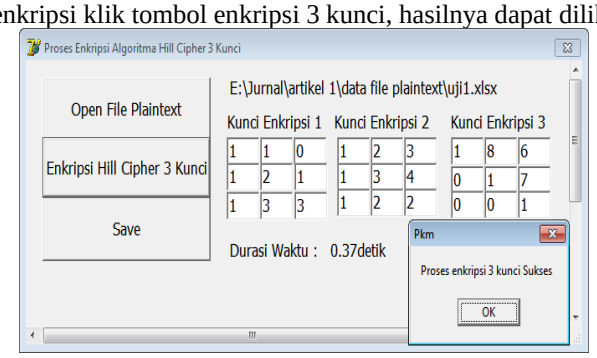
3.2.2 Implementasi Proses Enkripsi 3 Kunci

Untuk menjalankan proses enkripsi 3 kunci ,input file yang akan dienkripsi kemudian input kunci enkripsi di kotak yang sudah disediakan.Proses enkripsi dapat dilihat pada gambar 4.4 :



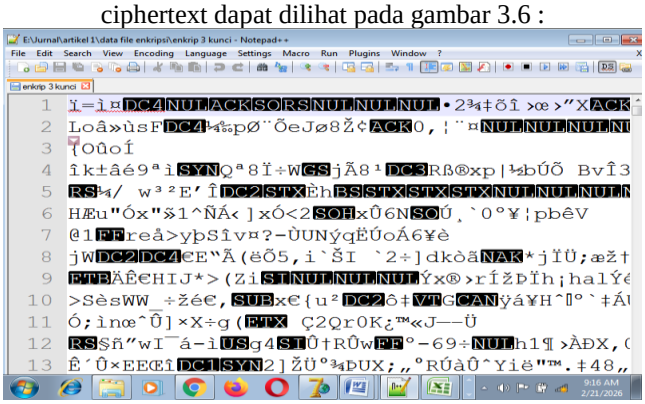
Gambar 3.4 Proses Enkripsi 3 kunci

Untuk melihat hasil proses enkripsi klik tombol enkripsi 3 kunci, hasilnya dapat dilihat pada gambar 3.5



Gambar 3.5 Hasil Proses Enkripsi 3 kunci

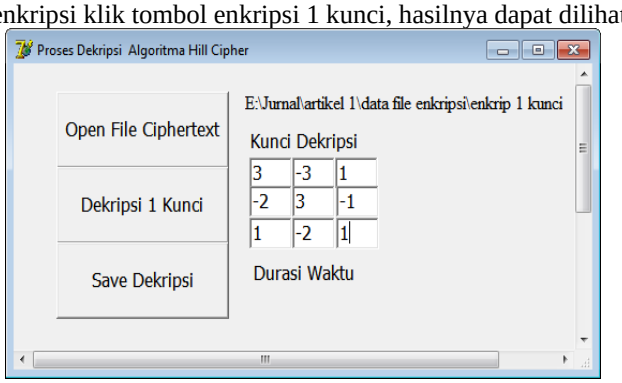
Selanjutnya klik tombol save untuk menyimpan hasil proses enkripsi ke dalam file ciphertext. Isi dari file ciphertext dapat dilihat pada gambar 3.6 :



Gambar 3.6 isi dokumen file ciphertext 3 kunci

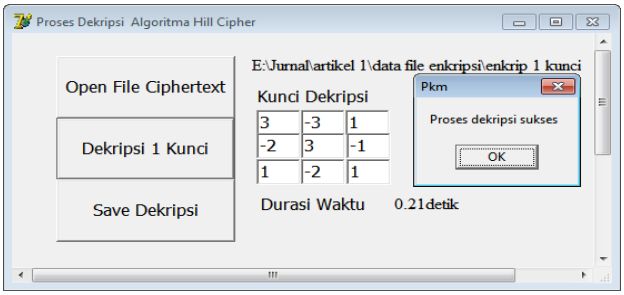
3.3.3 Implementasi Proses Dekripsi 1 Kunci

Untuk melihat hasil proses enkripsi klik tombol enkripsi 1 kunci, hasilnya dapat dilihat pada gambar 3.7



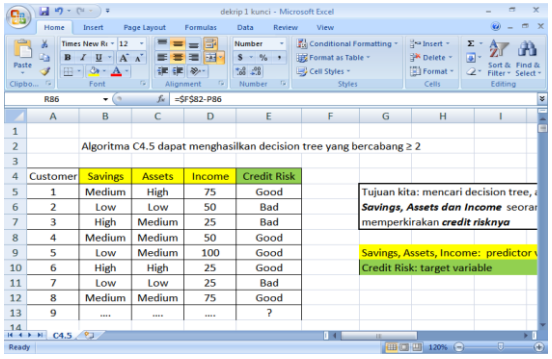
Gambar 3.7 Proses Dekripsi 1 Kunci

Untuk melihat hasil proses enkripsi klik tombol enkripsi 1 kunci, hasilnya dapat dilihat pada gambar 3.8



Gambar 3.8 Hasil Proses Dekripsi 1 Kunci

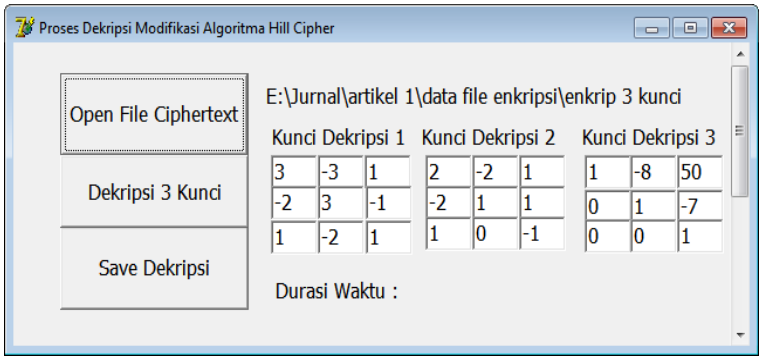
Selanjutnya klik tombol save untuk menyimpan hasil proses enkripsi ke dalam file ciphertext. Isi dari file ciphertext dapat dilihat pada gambar 4.3 :



Gambar 3.9 Isi Dokumen File Dekripsi 1 Kunci

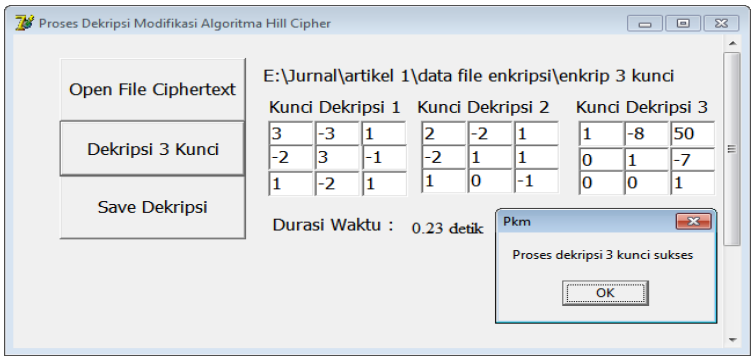
3.3.4 Implementasi Proses Dekripsi 3 Kunci

Untuk melihat hasil proses dekripsi klik tombol dekripsi 3 kunci, hasilnya dapat dilihat pada gambar 3.10:



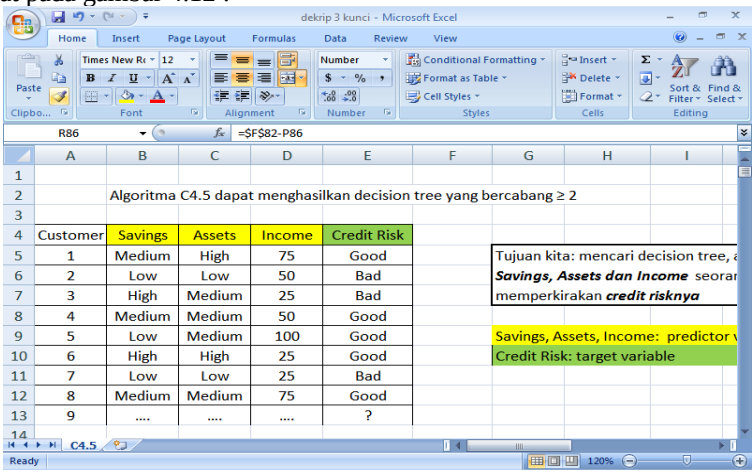
Gambar 3.10 Proses Dekripsi 3 Kunci

Untuk melihat hasil proses enkripsi klik tombol enkripsi 1 kunci, hasilnya dapat dilihat pada gambar 3.11:



Gambar 3.11 Hasil Proses Dekripsi 3 Kunci

Selanjutnya klik tombol save untuk menyimpan hasil proses enkripsi ke dalam file ciphertext. Isi dari file ciphertext dapat dilihat pada gambar 4.12 :



Gambar 4.12 Isi Dokumen File Dekripsi 3 Kunci

Tabel 3.1 Perbandingan Proses Enkripsi 1 Kunci Dengan 3 Kunci

No	Nama File Dokumen	Jenis Dokumen	Size File	Jenis Dokumen	Durasi Watu Proses Enkripsi	
					1 Kunci	3 Kunci
1	File uji 1	MS Excel	106 KB	MS Excel	0,26 detik	0,37 detik
2	File uji 2	Power Point	222 KB	Power Point	0,36 detik	0,49 detik
3	File uji 3	PDF	245 KB	PDF	0,38 detik	0,53 deik

4	File uji 4	Power Point	901 KB	Power Point	1,68 detik	1,72 detik
5	File uji 5	MS Excel	992 KB	MS Excel	1,83 detik	3,07 detik
6	File uji 6	MS Word	1,17 MB	MS Word	1,10 detik	1,35 detik
7	File uji 7	PDF	2,37 MB	PDF	4,84 detik	9,22 detik
8	File uji 8	MS Word	4,22 MB	MS Word	7,41 detik	8,01 detik

Tabel 3.2 Perbandingan Proses Dekripsi 1 Kunci Dengan 3 Kunci

No	Nama File Dokumen	Jenis Dokumen	Size File	Jenis Dokumen	Durasi Watu Proses Enkripsi	
					1 Kunci	3 Kunci
1	File uji 1	MS Excel	106 KB	MS Excel	0,21 detik	0,21 detik
2	File uji 2	Power Point	222 KB	Power Point	0,30 detik	0,33 detik
3	File uji 3	PDF	245 KB	PDF	0,32 detik	0,36 deik
4	File uji 4	Power Point	901 KB	Power Point	0,90 detik	1,22 detik
5	File uji 5	MS Excel	992 KB	MS Excel	0,94 detik	1,33 detik
6	File uji 6	MS Word	1,17 MB	MS Word	1,13 detik	2,10 detik
7	File uji 7	PDF	2,37 MB	PDF	2,15 detik	2,27 detik
8	File uji 8	MS Word	4,22 MB	MS Word	3,65 detik	3,9 detik

3.3 Pengujian Sistem

Pengujian sistem menggunakan black box testing. Black box testing adalah pengujian sistem tanpa mengetahui struktur kode dari perangkat lunak.Pengujian ini dilakukan di akhir pembuatan perangkat lunak untuk mengetahui apakah sistem sudah dapat berfungsi dengan baik.

Tabel 3.2 Pengujian Sistem

Jenis Uji	Skenario	Hasil Yang Diharapkan
Uji validitas kunci dekripsi	Input kunci dekripsi yang salah	Hasil proses dekripsi salah
Uji kesesuaian file MS Excel	Enkripsi file MS Excel,lalu dekripsi kembali	File dapat dibuka kembali sesuai dengan data plaintext(data aslinya)
Uji kesesuaian file MS Word	Enkripsi file MS Word,lalu dekripsi kembali	File dapat dibuka kembali sesuai dengan data plaintext(data aslinya)
Uji kesesuaian file powerpPoint	Enkripsi file Power point ,lalu dekripsi kembali	File dapat dibuka kembali sesuai dengan data plaintext(data aslinya)
Uji kesesuaian file PDF	Enkripsi file PDF ,lalu dekripsi kembali	File dapat dibuka kembali sesuai dengan data plaintext(data aslinya)

4. KESIMPULAN

Berdasarkan hasil rancang bangun dan pengujian yang telah dilakukan pada sistem keamanan data file menggunakan modifikasi algoritma Hill Cipher dengan rotasi tiga kunci, maka dapat ditarik yaitu: a). Peningkatan Keamanan**:** Modifikasi dengan rotasi kunci (*K*1,*K*2,*K*3) berhasil memecah pola *ciphertext* yang monoton. Hal ini membuat data lebih tahan terhadap *Known Plaintext Attack* karena penyerang tidak dapat menggunakan satu kunci yang sama untuk seluruh blok file. b) Validitas Data**:** Penggunaan Modulo 256 memungkinkan algoritma ini diterapkan pada seluruh jenis file (dokumen, gambar, dan executable) dengan tingkat keberhasilan dekripsi 100% (nilai *hash* identik). c) Efisiensi Performa**:** Meskipun sistem melakukan pergantian kunci pada setiap blok, proses komputasi tetap berjalan efisien dengan selisih waktu eksekusi yang sangat kecil dibandingkan Hill Cipher standar., d) Kelayakan Matriks: Penggunaan matriks 3×3 memberikan keseimbangan yang baik antara kompleksitas matematis dan kecepatan proses enkripsi.

DAFTAR PUSTAKA

[1] Azizhil, Hakim, dkk. Penerapan Super Enkripsi Hill Cipher dan RSA Untuk Pengamanan Data File Audio MP3. (2025). Jurnal Sistem Informasi Kaputama (JSIK), Vol. 9 No. 9.2
[2] Adetya, M. M. , dkk. (2023). Perancangan Sistem Keamanan Website Dengan Metode Hill Cipher. Jurnal Sains dan Teknologi (JSIT), Vol. 3 No. 1 http://jurnal.minartis.com/index php/jsit.
[3] Ankit, K. , et al.(2025). Enhancing The Security Of Hill Cipher Algorithm. IJCET, 16(2), 361-370, DOI: https://doi.org/10.34218/IJCET_16_02_025.
[4] Annisa, N. A. , et al. (2023). Application Of Extended Euclid Algorithm On Hill Cipher Criptography Modulo 95. Jurnal Ilmiah Multi Sciences, Vol. 15 No. 2, pp. 119-124, https://doi.org/10.30599/jti.v15i2.2850.
[5] Bayu, Firmanto dkk.(2021). Perbandingan Hasil Performa Optimasi Transposisi Hil Cipher Dan Vigenere Cipher Pada Citra Digital. SMARTICS, Vol. 7 No. 2, DOI : https://doi.org/10.21067/smartics.v7i2.5931
[6] Celine, A. H. , Dony, A. (2020). Kombinasi dan Modifikasi Vigenere Cipher dan Hill Cipher Menggunakan Metode Hybrid Kode Pos, Trigonometri dan Konversi Suhu Sebagai Pengamanan Pesan. Jurnal Ilmiah Komputer, Vol. 15 No. 2. DOI: http://dx.doi.org/10.30872/jim.v15i2.3746.
[7] Dani, E. M. , et al. (2023). Enhacing Image Encryption With the Kronecker xor Product the Hill Cipher and th Sigmoid Logistic Map. Applied Sainces https://doi.org/10.3390/app13064034.
[8] Fauzul, A. , Tommy. (2025). Implementation of the Hill Cipher Algorithm with a Random Generator in Key Validation for File Security. Journal of Technology and Computer (JOTECHCOM), Vol. 2 No.3, pp. 146-156.
[9] Giki, K. , Kiswara, A.S. , Ahmad, K. (2021). Modifikasi Huffman Dengan Hill Cipher Pada Pengkodean Teks. Prisma, Vol. 4, pp. 534-539, https://journal.unnes.ac.id/sju/index.php/prisma
[10] Heri, S. , Nia, S. R. , Suharji. (2024). Combinet Performance of Hill Cipher and Rivest Code 6 (RC6). International Journal of Information System & Technology, Vol. 7 No. 6
[11] Humaira, I. A. , Evi, N. , Yudhi. (2021). Invers Matriks Dengan Menggunakan Metode Faddeev Dan Algoritma Leverrier-Faddeev. Buletin Ilmiah Mat Stat DanTerapannya (Bimaster), Vol. 10 No. 4. https://jurnal.untan.ac.id/index.php/jbmstr.
[12] Ikhsan, N. A., dkk. (2024). Implementasi Algoritma Hill Cipher Untuk Pengamanan Invoice. Sain dan Teknologi (SAINTEK), Vol. 3 No. 1
[13] Indah, Saputri. , et al. (2022). Pengamanan Pesan Menggunakan Metode Hill Cipher Dalam Keamanan Informasi. Bulletin Of Information Technology(BIT), Vol. 3 No. 4, pp. 341-349, DOI 10.47065/ bit.v3i1. 415
[14] Muhaimi, R. S. , Heri, S. , Aidil, H. L. (2024). Kombinasi Algoritma Beaufort Cipher dan Hill Cipher Dalam Mengamankan File Dokumen Berbasis Mobile. Journal of Islamic Science and Technology (JISTECH), Vol. 9 No. 2, pp. 146-156. DOI: http://dx.doi.org/10.30829/jistech.v9i2.22633
[15] Muthiah As, S. , Aggry, S. , Zulkipli . (2024). Bangkit Indonesia, Vol. 3 No. 2. DOI : 10.52771/bangkitindonesia.v13i2.323
[16] Muhamad, Nurtanzis, dkk. Pengamanan Data Berbasis Hill Cipher dengan Operasi Modulo Pada Karakter Ascii. (2024). Jurnal Techno.com, Vol. 23 No. 4, pp. 786-795,
[17] Nurharianna, S. , Ilham, F. , Divi, H. (2022). Menerapkan Algoritma Hill Cipher Dan Matriks 2x2 Dalam Mengamankan File Teks Menggunakan Kode Ascii. Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI), Vol. 1 No. 2, https://jurnal.unity-academy.sch.id/index.php/jirsi/index.
[18] Radila, Pratiwi, dkk. Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher. (2022). Bulletin Of Information Technology (BIT), Vol. 3 No. 4, DOI 10.47065/ bit.v3i1. 420
[19] Rahmad, A. , Hermawati, Muhammad, M. M. Pewngembangan Metode Hill Cipher Untuk Enkripsi dan Dekripsi Pada Resep Obat Guna Meningkatkan Keamanan Data. (2024). Jurnal Sistem Informasi (SISTEMASI), Vol. 13 No. 5. http://sistemasi.ftik.unisi.ac.id
[20] Roman, G. , Haryansyah, Adimulya, D. W. (2023). Implementasi Algoritma Hill Cipher dengan Matriks Kunci 2x2 Dalam Mengamankan Data Teks. Jurnal Generation , Vol. 7 No. 3
[21] Ronaldo, M. S., dkk. Implementasi Algoritma Hill Cipher Untuk Keamanan Rekam Medis di Puskesmas Pematang Raya. (2023). Jurnal Penelitian Ilmu dan Teknologi Komputer (JUPITER), Vol. 15 No. 2. DOI: https://doi.org/10.5281/zenodo.10068238
[22] Samsul, A. , dkk. (20230. Algorithm for Digital Image Encryption Using Multiple Hill Cipher a Unimodular Matrix and a Logistic Map. International Journal of Intelligent Systems and Applications In Engineering, 11(6s), pp. 311-324.
[23] Susi , D. , dkk. (2024). Implementasi Kriptografi Algoritma Hill Cipher dengan Kunci Tandatangan Pengirim Pesan Terhadap Keamanan Message Handling System Di Bandara Kualanamu. Journal of Social Science Research, Vol. 4 No. 2, pp. 5953-5965. https://j-innovative.org/index.php/Innovative.
[24] Sri, W. , Abdul, H. H. , Suharji. (2025). Implementasi Algoritma Hill Cipher dan Discrete Cosine Transform Dalam Keamanan Pesan E-Mail. Journal of Science and Social Research, VII(2), pp. 2036-2041
[25] Veradella, Y. M. (2025). Hill Cipher-Based Visual Cryptography for Copyright Protection of Images Using Flexible Matrix Keys. JSCE (Journal of System and Computer Engineering), Vol.6 No. 1, pp. 101-116. DOI : https://doi.org/10.61628/jsce.v6i1.1634.