

# Penyandian Super Enkripsi Menggunakan Columnar Transposition dan Modifikasi Hill Cipher dengan Invers Kiri Matriks Persegi Panjang

Fika Wahyuni<sup>1</sup>, Muhammad Khudzaifah<sup>2\*</sup>, Muhammad Nafie Jauhari<sup>3</sup>

<sup>1,2,3</sup>Program Studi Matematika, Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia

Email: fikawahyuni7@gmail.com, khudzaifah@uin-malang.ac.id\*, nafie.jauhari@uin-malang.ac.id

## ABSTRAK

Perkembangan zaman dan teknologi saat ini berkembang begitu cepat sehingga saat ini banyak komputer terhubung ke internet untuk penyampaian data dari satu pihak ke pihak yang lain. Karenanya, diperlukan suatu keamanan pada proses penyampaian pesan. Salah satu solusi yang dapat dilakukan untuk melindungi pesan dengan melakukan penyandian atau kriptografi. Super enkripsi merupakan suatu metode kriptografi yang mengkombinasikan dua algoritma kriptografi atau lebih yang merupakan algoritma metode substitusi dan transposisi. Pada penelitian ini, digunakan algoritma *columnar transposition* sebagai metode transposisi dan modifikasi algoritma *Hill cipher* dengan invers kiri matriks persegi panjang sebagai metode substitusi. Penyandian dilakukan menggunakan *columnar transposition* terlebih dahulu kemudian *ciphertextnya* disandikan kembali menggunakan modifikasi *Hill cipher*. Penyandian pesan menggunakan metode super enkripsi dengan algoritma *columnar transposition* dan modifikasi algoritma Hill cipher dengan invers kiri matriks persegi panjang menghasilkan pesan akhir yang tidak mengubah pesan awal sehingga dapat diimplementasikan pada pesan dengan baik. Hasil penyandian dengan *columnar transposition* dan modifikasi *Hill cipher* dengan invers kiri matriks persegi panjang ini dapat melipat gandakan keamanan suatu pesan, sehingga penelitian ini diharapkan dapat menjadi solusi bagi pihak yang menggunakan teknologi informasi dan komunikasi untuk dapat melakukan pengiriman pesan dengan aman.

**Kata kunci:** Enkripsi; Dekripsi; Super Enkripsi; *Columnar Transposition*; *Hill Cipher*

---

## ABSTRACT

The development of the times and technology is currently developing so fast that currently many computers are connected to the internet for transmitting data from one party to another. Therefore, a security is needed in the message delivery process. One solution that can be done to protect messages is to perform encryption or cryptography. Super encryption is a cryptographic method that combines two or more cryptographic algorithms which are substitution and transposition method algorithms. In this study, the columnar transposition algorithm is used as a transposition method and a modification of the hill cipher algorithm with the left inverse of the rectangular matrix as the substitution method. The encoding is done using columnar transposition first, then the ciphertext is re-encoded using a modified hill cipher. Encryption of messages using the super encryption method with columnar transposition algorithm and modification of the hill cipher algorithm with the left inverse of a rectangular matrix produces a final message that does not change the initial message so that it can be implemented in the message properly. The results of encoding with columnar transposition and modified hill cipher with the left inverse of this rectangular matrix can double the security of a message, so this research is expected to be a solution for those who use information and communication technology to be able to send messages safely.

**Keywords:** Encryption; Decryption; Super Encryption; *Columnar Transposition*; *Hill Cipher*

---

## PENDAHULUAN

Perkembangan teknologi begitu pesat dan cepat termasuk dalam perkembangan teknologi komunikasi dan informasi hingga saat ini teknologi informasi telah menjadi bagian yang sangat penting di berbagai aspek kehidupan manusia [1]. Perkembangan teknologi juga mempermudah keterbukaan terhadap akses data dan informasi [2]. Seiring dengan kemajuan pada teknologi informasi, banyak data dan informasi yang terhubung dalam satu jaringan komputer dengan jaringan yang lainnya. Hal tersebut tentu saja menimbulkan risiko yang besar apabila informasi yang disampaikan bersifat berharga dan sensitif apabila di akses oleh orang lain yang tidak bertanggung jawab. Sehingga sangat diperlukan keamanan terhadap kerahasiaan dalam sebuah pertukaran informasi. Salah satu yang dapat digunakan untuk mempertahankan kerahasiaan suatu informasi atau pesan adalah dengan melakukan penyandian pada pesan atau kriptografi [3].

Kriptografi adalah teknik pengamanan informasi di mana informasi diubah dengan kunci tertentu melalui enkripsi sehingga menjadi informasi yang baru yang tidak dapat dimengerti oleh orang yang tidak berhak menerimanya [4]. Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus, sedangkan dekripsi adalah proses mengembalikan suatu informasi dengan cara tertentu dan sesuai dengan algoritma enkripsi yang dipakai [5]. Dasar matematis yang mendasari kriptografi pada proses enkripsi adalah relasi antara dua himpunan yaitu antara himpunan *plaintext* dan himpunan *ciphertext* [6]. Misalkan  $P$  menyatakan *plaintext* dan  $C$  menyatakan *ciphertext*, maka fungsi enkripsi  $E$  memetakan  $P$  ke  $C$ ,

$$E(P) = C$$

Sedangkan fungsi dekripsi  $D$  memetakan  $C$  ke  $P$

$$D(C) = P$$

Karena proses enkripsi dilanjutkan dengan dekripsi yaitu mengembalikan pesan rahasia ke pesan asal, maka persamaan berikut haruslah benar

$$D(E(P)) = P$$

Pada penelitian sebelumnya telah dibahas modifikasi algoritma kriptografi. Penelitian Kaur [7] memodifikasi algoritma Hill cipher dengan matriks persegi panjang pada kunci yang digunakannya guna meningkatkan keamanan komunikasi menjadi lebih baik. Hill cipher merupakan teknik kriptografi yang menerapkan aritmatika modulo [8]. Modulo di definisikan dengan misalkan  $a$  adalah bilangan bulat dan  $m$  adalah bilangan bulat lebih dari 0. Operasi  $a \bmod m$  ( $a$  modulo  $m$ ) memberikan sisa jika  $r$  dibagi dengan  $m$  dengan kata lain,  $a \bmod m = r$  sedemikian sehingga  $a = mq + r$ , dengan  $0 \leq r < m$  [9]. Kunci yang digunakan pada Hill cipher tradisional merupakan matriks yang berordo  $n \times n$  [10]. Adapun proses enkripsi Hill cipher secara matematis dapat ditulis sebagai berikut [8]:

$$\begin{bmatrix} c1 \\ c2 \\ \vdots \\ cn \end{bmatrix} = A \begin{bmatrix} p1 \\ p2 \\ \vdots \\ pn \end{bmatrix} \bmod a$$

Pada penelitiannya, Ravinder Kaur menggunakan matriks persegi panjang pada proses enkripsinya, sedangkan invers kiri dari matriks persegi panjang tersebut digunakan untuk proses dekripsi. Karena matriks yang digunakan pada kunci enkripsi maka untuk mendekripsi *ciphertext* dapat menggunakan invers matriks tergeneralisasi dengan invers kiri. Invers matriks diperumum (Generalized Inverse of Matrix) adalah

perumuman pengertian invers matriks. Invers dari matriks  $A_{m \times n}$  dapat diselesaikan dengan invers matriks tergeneralisasi [11]. Ciphertext yang dihasilkan dari modifikasi Hill cipher dengan invers kiri matriks persegi panjang ini lebih panjang dari plaintext sehingga dapat menambah keamanan suatu pesan. Namun pada penelitian ini algoritma yang digunakan hanya modifikasi dari algoritma Hill cipher sehingga penyandian pesan hanya dilakukan satu kali. Kemudian Reswan dkk [12] melakukan penelitian dengan super enkripsi pada implementasi kompilasi algoritma kriptografi transposisi columnar dan RSA untuk mengamankan pesan rahasia. Transposisi columnar merupakan cipher yang termasuk dalam teknik transposisi, Enkripsi yang digunakan dalam teknik transposisi adalah permutasi [13]. Proses enkripsi pada penelitian tersebut dilakukan menggunakan transposisi columnar terlebih dahulu kemudian di enkripsi kembali menggunakan algoritma RSA. Transposisi columnar digunakan untuk menambah kerumitan penyandian suatu pesan, sehingga dapat mengamankan pesan lebih kuat.

solusi yang dapat dilakukan untuk mengamankan pesan agar lebih kuat adalah dengan mengombinasikan dua algoritma kriptografi yang dinamakan dengan metode super enkripsi. Super enkripsi merupakan metode kriptografi yang mengombinasikan teknik substitusi dan transposisi [14]. Teknik substitusi pada kriptografi yaitu teknik dengan cara penggantian pada setiap karakter teks biasa (plaintext) dengan karakter lain, sedangkan teknik transposisi yaitu teknik yang menggunakan permutasi karakter [15]. Karena pada super enkripsi mengombinasikan beberapa algoritma maka super enkripsi ini sulit untuk dipecahkan, sehingga keamanan pada suatu pesan atau informasi dapat terjaga. Pada penelitian ini akan dilakukan penyandian pesan menggunakan super enkripsi di mana teknik substitusi yang digunakan pada penyandian ini ialah modifikasi algoritma Hill cipher dengan invers matriks persegi, sedangkan teknik transposisinya menggunakan transposisi columnar.

## **METODE**

Pada Penelitian terdapat beberapa langkah penelitian. yang pertama, melakukan proses penyandian menggunakan columnar transposition. Kemudian yang kedua melakukan proses penyandian modifikasi Hill cipher dengan invers kiri matriks persegi panjang. Dan yang terakhir adalah melakukan proses penyandian super enkripsi, proses enkripsi dilakukan menggunakan columnar transposition terlebih dahulu kemudian hasil enkripsi dari columnar transposition di enkripsi kembali menggunakan modifikasi Hill cipher dengan invers kiri matriks persegi panjang. Sedangkan proses dekripsinya adalah sebaliknya.

## **HASIL DAN PEMBAHASAN**

### **1. Proses Penyandian Super Enkripsi Menggunakan Columnar Transposition dan Modifikasi Hill Cipher dengan Invers Kiri Matriks Persegi Pajang**

Berikut ini merupakan proses dari penyandian super enkripsi menggunakan columnar transposition dan modifikasi Hill cipher dengan invers kiri matriks persegi panjang.

#### **a. Teknik Penyandian Columnar Transposition**

Algoritma *columnar transposition* merupakan algoritma simetri yaitu menggunakan kunci yang sama pada proses enkripsi dan dekripsinya. Pada metode super

enkripsi ini, algoritma *columnar transposition* digunakan untuk menambah kerumitan penyandian pesan.

Berikut ini merupakan algoritma dari proses enkripsi dan dekripsi menggunakan *columnar transposition*:

1. Menentukan kunci *columnar transposition*
2. Menuliskan *plaintext* dalam sebuah tabel dari baris pertama dan seterusnya dengan banyaknya kolom sesuai panjang kunci
3. Mengurutkan kolom sesuai urutan angka
4. Mendapatkan pesan teks yang telah disandikan (*ciphertext*)

Sedangkan proses dekripsi pesan menggunakan *columnar transposition* adalah dengan tahapan berikut ini:

1. Menentukan kunci *columnar transposition* yang digunakan pada proses enkripsinya
2. Menuliskan *ciphertext* dalam sebuah tabel dari kolom pertama dan seterusnya dengan banyaknya baris sesuai dengan panjang *ciphertext* dibagi dengan panjang kuncinya
3. Mengurutkan kolom sesuai urutan kunci
4. Mendapatkan teks asli (*plaintext*)

### **b. Teknik Penyandian Modifikasi Hill Cipher dengan Invers Kiri Matriks Persegi Panjang**

Modifikasi algoritma *Hill cipher* dengan invers kiri yaitu dengan memodifikasi kunci yang digunakan pada proses penyandiannya. Dalam algoritma *Hill cipher* tradisional, kunci yang digunakan adalah matriks persegi  $n \times n$ . Sedangkan kunci yang digunakan pada modifikasi *Hill cipher* ini adalah matriks persegi panjang  $m \times n$  di  $\mathbb{Z}_{53}$ .

Pada pembahasan ini, penulis mengambil data-data yang berupa huruf dikonversikan terlebih dahulu ke dalam angka pada suatu himpunan  $\mathbb{Z}_{53}$ , sehingga perhitungannya dengan modulo 53. Setiap *plaintext* yang disandikan menggunakan metode ini dapat dikembalikan dengan baik ke *plaintext*nya, maka akan dibuktikan bahwa *ciphertext* dapat kembali ke *plaintext*.

Misalkan  $x_1, x_2, \dots, x_n$  merupakan huruf *plaintext* dan  $y_1, y_2, \dots, y_n$  adalah *ciphertext*. Misalkan ambil sembarang suatu huruf *plaintext*  $x_1, x_2 \in \mathbb{Z}_{53}$ . Kemudian ambil suatu kunci matriks persegi panjang  $3 \times 2$  maka terdapat

$$A = \begin{bmatrix} a & b \\ c & d \\ e & f \end{bmatrix} \in M_{3 \times 2}(\mathbb{Z}_{53})$$

Implementasi terhadap rumus penyandian Hill cipher yaitu

$$C = KP \text{ mod } n.$$

Sehingga,

$$C = \begin{bmatrix} a & b \\ c & d \\ e & f \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \text{ mod } 53$$

$$C = \begin{bmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \\ ex_1 + fx_2 \end{bmatrix} \text{ atau } \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \\ ex_1 + fx_2 \end{bmatrix}$$

Sehingga didapatkan persamaan

$$ax_1 + bx_2 \equiv y_1 \text{ modulo } 53 \quad (1)$$

$$cx_1 + dx_2 \equiv y_2 \text{ modulo } 53 \quad (2)$$

$$ex_1 + fx_2 \equiv y_3 \text{ modulo } 53 \quad (3)$$

Misalkan  $a, b, c, d, e, f, x_1, x_2, y_1, y_2, y_3$  dan suatu  $n$  merupakan bilangan bulat elemen  $\mathbb{Z}_{53}$  dengan  $n = 53$ , sedemikian sehingga  $(\Delta, n) = 1$  dengan  $\Delta = ad - bc, \Delta = af - be, \Delta = cf - de$ .

a) Kongruensi (1) dan (2)

Dengan menggunakan sistem kongruensi, kalikan kongruensi pertama dengan  $d$  dan yang kedua dengan  $b$  maka diperoleh

$$\begin{aligned} adx_1 + bdx_2 &\equiv dy_1 \text{ modulo } 53 \\ bdx_1 + bdx_2 &\equiv by_2 \text{ modulo } 53 \\ \hline (ad - bc)x_1 &\equiv dy_1 - by_2 \text{ (mod } 53) \\ \Delta = ad - bc, &\text{ maka} \end{aligned}$$

$$\Delta x_1 \equiv dy_1 - by_2 \text{ (mod } 53)$$

Kemudian kalikan kedua ruas dengan  $\bar{\Delta}$  yang merupakan invers dari  $\Delta$ , sehingga diperoleh

$$x_1 \equiv \bar{\Delta}(dy_1 - by_2) \text{ (mod } 53).$$

Dengan cara yang sama, kalikan kongruensi (1) dengan  $c$  dan kongruensi (2) dengan  $a$  maka diperoleh

$$\begin{aligned} acx_1 + adx_2 &\equiv ay_2 \text{ (mod } 53) \\ acx_1 + bcx_2 &\equiv cy_1 \text{ (mod } 53) \\ \hline (ad - bc)x_2 &\equiv ay_2 - cy_1 \text{ (mod } 53) \\ \Delta x_2 &\equiv ay_2 - cy_1 \text{ (mod } 53) \end{aligned}$$

Kemudian kalikan kedua ruas dengan  $\bar{\Delta}$  yang merupakan invers dari  $\Delta$ , sehingga diperoleh

$$x_2 \equiv \bar{\Delta}(ay_2 - cy_1) \text{ (mod } 53).$$

Untuk mengecek bahwa  $x_1, x_2$  adalah penyelesaian, maka

$$\begin{aligned} ax_1 + bx_2 &\equiv a\bar{\Delta}(dy_1 - by_2) \text{ (mod } 53) + b\bar{\Delta}(ay_2 - cy_1) \text{ (mod } 53) \\ &\equiv \bar{\Delta}(ady_1 - aby_2) \text{ (mod } 53) + \bar{\Delta}(aby_2 - bcy_1) \text{ (mod } 53) \\ &\equiv \bar{\Delta}(ady_1 - aby_2 + aby_2 - bcy_1) \text{ (mod } 53) \\ &\equiv \bar{\Delta}(ad - bc)y_1 \text{ (mod } 53) \\ &\equiv \bar{\Delta}\Delta y_1 \text{ (mod } 53) \\ &\equiv y_1 \text{ (mod } 53) \end{aligned}$$

Selanjutnya

$$\begin{aligned} cx_1 + dx_2 &\equiv c\bar{\Delta}(dy_1 - by_2) \text{ (mod } 53) + d\bar{\Delta}(ay_2 - cy_1) \text{ (mod } 53) \\ &\equiv \bar{\Delta}(cdy_1 - bcy_2) \text{ (mod } 53) + \bar{\Delta}(ady_2 - cdy_1) \text{ (mod } 53) \\ &\equiv \bar{\Delta}(cdy_1 - bcy_2 + ady_2 - cdy_1) \text{ (mod } 53) \\ &\equiv \bar{\Delta}(ad - bc)y_2 \text{ (mod } 53) \\ &\equiv \bar{\Delta}\Delta y_2 \text{ (mod } 53) \\ &\equiv y_2 \text{ (mod } 53) \end{aligned}$$

b) Kongruensi (1) dan (3)

Dengan menggunakan sistem kongruensi, kalikan kongruensi (1) dengan  $f$  dan kongruensi (3) dengan  $b$  maka diperoleh

$$afx_1 + bfx_2 \equiv fy_1 \text{ modulo } 53$$

$$\begin{aligned} bex_1 + bfx_2 &\equiv by_3 \text{ modulo } 53 \\ \hline (af - be)x_1 &\equiv fy_1 - by_3 \pmod{53} \\ \Delta = af - be, &\text{ maka} \end{aligned}$$

$$\Delta x_1 \equiv fy_1 - by_3 \pmod{53}$$

Kemudian kalikan kedua ruas dengan  $\bar{\Delta}$  yang merupakan invers dari  $\Delta$ , sehingga diperoleh

$$x_1 \equiv \bar{\Delta}(fy_1 - by_3) \pmod{53}.$$

Dengan cara yang sama, kalikan kongruensi (1) dengan  $e$  dan kongruensi (3) dengan  $a$  maka diperoleh

$$\begin{aligned} aex_1 + afx_2 &\equiv ay_3 \pmod{53} \\ aex_1 + bex_2 &\equiv ey_1 \pmod{53} \\ \hline (af - be)x_2 &\equiv ay_3 - ey_1 \pmod{53} \\ \Delta x_2 &\equiv ay_3 - ey_1 \pmod{53} \end{aligned}$$

Kemudian kalikan kedua ruas dengan  $\bar{\Delta}$  yang merupakan invers dari  $\Delta$ , sehingga diperoleh

$$x_2 \equiv \bar{\Delta}(ay_3 - ey_1) \pmod{53}.$$

Untuk mengecek bahwa  $x_1, x_2$  adalah penyelesaian, maka

$$\begin{aligned} ax_1 + bx_2 &\equiv a\bar{\Delta}(fy_1 - by_3) \pmod{53} + b\bar{\Delta}(ay_3 - ey_1) \pmod{53} \\ &\equiv \bar{\Delta}(afy_1 - aby_3) \pmod{53} + \bar{\Delta}(aby_3 - bey_1) \pmod{53} \\ &\equiv \bar{\Delta}(afy_1 - aby_3 + aby_3 - bey_1) \pmod{53} \\ &\equiv \bar{\Delta}(af - be)y_1 \pmod{53} \\ &\equiv \bar{\Delta}\Delta y_1 \pmod{53} \\ &\equiv y_1 \pmod{53} \end{aligned}$$

Selanjutnya

$$\begin{aligned} ex_1 + fx_2 &\equiv e\bar{\Delta}(fy_1 - by_3) \pmod{53} + f\bar{\Delta}(ay_3 - ey_1) \pmod{53} \\ &\equiv \bar{\Delta}(efy_1 - bey_3) \pmod{53} + \bar{\Delta}(afy_3 - efy_1) \pmod{53} \\ &\equiv \bar{\Delta}(efy_1 - bey_3 + afy_3 - efy_1) \pmod{53} \\ &\equiv \bar{\Delta}(af - be)y_3 \pmod{53} \\ &\equiv \bar{\Delta}\Delta y_3 \pmod{53} \\ &\equiv y_3 \pmod{53} \end{aligned}$$

c) Kongruensi (2) dan (3)

Dengan menggunakan sistem kongruensi, kalikan kongruensi (2) dengan  $f$  dan kongruensi (3) dengan  $d$  maka diperoleh

$$\begin{aligned} cf x_1 + df x_2 &\equiv fy_2 \text{ modulo } 53 \\ dex_1 + df x_2 &\equiv dy_3 \text{ modulo } 53 \\ \hline (cf - de)x_1 &\equiv fy_2 - dy_3 \pmod{53} \\ \Delta = cf - de, &\text{ maka} \end{aligned}$$

$$\Delta x_1 \equiv fy_2 - dy_3 \pmod{53}$$

Kemudian kalikan kedua ruas dengan  $\bar{\Delta}$  yang merupakan invers dari  $\Delta$ , sehingga diperoleh

$$x_1 \equiv \bar{\Delta}(fy_2 - dy_3) \pmod{53}.$$

Dengan cara yang sama, kalikan kongruensi (2) dengan  $e$  dan kongruensi (3) dengan  $c$  maka diperoleh

$$\begin{aligned} cex_1 + cf x_2 &\equiv cy_3 \pmod{53} \\ cex_1 + dex_2 &\equiv ey_2 \pmod{53} \\ \hline (cf - de)x_2 &\equiv cy_3 - ey_2 \pmod{53} \end{aligned}$$

$$\Delta x_2 \equiv cy_3 - ey_2 \pmod{53}$$

Kemudian kalikan kedua ruas dengan  $\bar{\Delta}$  yang merupakan invers dari  $\Delta$ , sehingga diperoleh

$$x_2 \equiv \bar{\Delta}(cy_3 - ey_2) \pmod{53}.$$

Untuk mengecek bahwa  $x_1, x_2$  adalah penyelesaian, maka

$$\begin{aligned} cx_1 + dx_2 &\equiv c\bar{\Delta}(fy_2 - dy_3) \pmod{53} + d\bar{\Delta}(cy_3 - ey_2) \pmod{53} \\ &\equiv \bar{\Delta}(cfy_2 - cdy_3) \pmod{53} + \bar{\Delta}(cdy_3 - dey_2) \pmod{53} \\ &\equiv \bar{\Delta}(cfy_2 - cdy_3 + cdy_3 - dey_2) \pmod{53} \\ &\equiv \bar{\Delta}(cf - de)y_2 \pmod{53} \\ &\equiv \bar{\Delta}\Delta y_2 \pmod{53} \\ &\equiv y_2 \pmod{53} \end{aligned}$$

Selanjutnya

$$\begin{aligned} ex_1 + fx_2 &\equiv e\bar{\Delta}(fy_2 - dy_3) \pmod{53} + f\bar{\Delta}(cy_3 - ey_2) \pmod{53} \\ &\equiv \bar{\Delta}(efy_2 - dey_3) \pmod{53} + \bar{\Delta}(cfy_3 - efy_2) \pmod{53} \\ &\equiv \bar{\Delta}(efy_2 - dey_3 + cfy_3 - efy_2) \pmod{53} \\ &\equiv \bar{\Delta}(cf - de)y_3 \pmod{53} \\ &\equiv \bar{\Delta}\Delta y_3 \pmod{53} \\ &\equiv y_3 \pmod{53} \end{aligned}$$

Maka terbukti bahwa  $x_1$  dan  $x_2$  yang merupakan *plaintext* kemudian dioperasikan sehingga menghasilkan  $y_1, y_2, y_3$  yang merupakan hasil *ciphertextnya*, dapat dikembalikan ke huruf *plaintext* menggunakan inversnya. Karena  $n$  pada  $\mathbb{Z}_{53}$  merupakan prima maka menurut teorema  $\mathbb{Z}_{53}$  merupakan *field*, sehingga teori-teori yang telah dibahas dapat berlaku.

Pada modifikasi algoritma Hill cipher dengan matriks persegi panjang ini dengan  $n = 53$  sehingga  $\mathbb{Z}_{53} \in \mathbb{Z}_p$ , dengan  $n \leq m$  maka  $P = (\mathbb{Z}_{53})^n$  dan  $C = (\mathbb{Z}_{53})^m$  di mana  $K = \{k \in K_{m \times n}(\mathbb{Z}_{53}) | \text{rank}(K) = n\}$ . Sehingga untuk suatu  $k \in K$  dan  $x = (x_1, x_2, \dots, x_n) \in P, y = (y_1, y_2, \dots, y_n) \in C$  maka didapatkan

$$E_k(x) = Kx$$

dan

$$D_k(y) = K^{-1}y$$

Dengan  $K^{-1} = (A^T A)^{-1} A^T$

Proses penyandian pada modifikasi algoritma *Hill cipher* dengan invers kiri dibutuhkan konversi alfabet ke dalam angka, maka digunakan tabel konversi berikut ini untuk proses enkripsi dan dekripsi.

**Tabel 1.** Konversi Modifikasi Hill cipher

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

M = 12	N = 13	O = 14	P = 15	Q = 16	R = 17
S = 18	T = 19	U = 20	V = 21	W = 22	X = 23
Y = 24	Z = 25	a = 26	b = 27	c = 28	d = 29
e = 30	f = 31	g = 32	h = 33	i = 34	j = 35
k = 36	l = 37	m = 38	n = 39	o = 40	p = 41
q = 42	r = 43	s = 44	t = 45	u = 46	v = 47
w = 48	x = 49	y = 50	z = 51	Spasi = 52	

**c. Teknik Penyandian Super Enkripsi Menggunakan Columnar Transposition dan Modifikasi Hill Cipher dengan Invers Kiri Matriks Persegi Panjang**

penggabungan dua fungsi bijektif bersifat bijektif maka penggabungan dua algoritma antara *columnar transposition* dan modifikasi *Hill cipher* dapat dilakukan. Berikut ini proses enkripsi dan dekripsi pada super enkripsi *columnar transposition* dan modifikasi *Hill cipher* dengan invers kiri matriks persegi.

a) Enkripsi

Adapun algoritma dari enkripsi pada metode super enkripsi pada suatu pesan adalah sebagai berikut:

1. Menentukan kunci *columnar transposition*
2. Menuliskan *plaintext* dalam sebuah tabel dari baris pertama dan seterusnya dengan banyaknya kolom sesuai panjang kunci
3. Mengurutkan kolom sesuai urutan angka
4. Mendapatkan pesan teks yang telah disandikan (*ciphertext*)
5. Menentukan matriks kunci yang memiliki invers untuk enkripsi pada modifikasi *Hill cipher*
6. Membagi *plaintext*  $p = x_1x_2x_3 \dots x_i$  menjadi matriks berorde  $n \times 1$  dengan modulo 53 yang telah disebutkan dalam tabel sebelumnya sehingga

$$P = P_1P_2P_3 \dots P_i$$

di mana

$$P_1 = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \text{ mod } 53, P_2 = \begin{bmatrix} x_{n+1} \\ x_{n+2} \\ \vdots \\ x_{2n} \end{bmatrix} \text{ mod } 53 \dots P_i = \begin{bmatrix} x_{(i-1)n+1} \\ x_{(i-1)n+2} \\ \vdots \\ x_{in} \end{bmatrix} \text{ mod } 53$$

7. Enkripsi kedua kunci  $K_e$ , panjang matriks dari orde  $m \times n (m > n)$  akan diaplikasikan pada setiap  $P_i$  untuk mendapat kolom matrik  $C_i$  dari peningkatan orde m

$$C_i = (K_e P_i) \text{ mod } 53 = (A P_i) \text{ mod } 53$$

$$C = C_1 C_2 \dots C_i$$

8. Mengonversi matriks  $C$  kedalam huruf sehingga didapatkan *ciphertext* nya

$$C = y_1 y_2 \dots$$

Berikut ini contoh penerapan enkripsi dengan algoritma super enkripsi *columnar transposition* dan modifikasi *Hill cipher* dengan invers kiri matriks persegi panjang dengan pesan yang berisi "Jurusan Matematika":

1. Misalkan kunci pada *columnar transposition* adalah "Melati". Sehingga panjang kunci adalah 6 dengan urut "5 2 4 1 6 3"
2. Menyusun *plaintext* dalam tabel secara mendatar dengan kolom tabel sebanyak 6, karena panjang kunci 6



**Tabel 2.** Enkripsi Super Enkripsi Terurut Kunci

5	2	4	1	6	3
J	u	r	u	s	a
n		M	a	t	e
m	a	t	i	k	a

3. Mengurutkan tabel berdasarkan pada urutan baris pertama diikuti seluruh kolomnya dimulai dari urut satu

**Tabel 3.** Enkripsi Super Enkripsi Terurut Angka

1	2	3	4	5	6
u	u	a	r	J	s
a		e	M	n	t
i	a	a	t	m	k

4. Sehingga didapatkan *ciphertext* pertama yaitu “uuiu aearMtJnmstk” yang merupakan *plaintext* untuk enkripsi pada modifikasi *Hill cipher*
5. Menentukan matriks kunci untuk enkripsi pada modifikasi *Hill cipher*, misalkan matriks kunci yang digunakan adalah

$$K_e = A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix}$$

6. Menyusun *plaintext* “uuiu aearMtJnmstk” dalam matriks  $n \times 1$  dengan modulo 53 pada tabel 3.6 sehingga

$$P = P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 = \begin{bmatrix} u \\ a \end{bmatrix} \begin{bmatrix} i \\ u \end{bmatrix} \begin{bmatrix} a \\ a \end{bmatrix} \begin{bmatrix} e \\ r \end{bmatrix} \begin{bmatrix} M \\ t \end{bmatrix} \begin{bmatrix} J \\ n \end{bmatrix} \begin{bmatrix} m \\ s \end{bmatrix} \begin{bmatrix} t \\ k \end{bmatrix}$$

Di mana

$$\begin{aligned} P_1 &= \begin{bmatrix} u \\ a \end{bmatrix} = \begin{bmatrix} 46 \\ 26 \end{bmatrix} & P_6 &= \begin{bmatrix} M \\ t \end{bmatrix} = \begin{bmatrix} 12 \\ 45 \end{bmatrix} \\ P_2 &= \begin{bmatrix} i \\ u \end{bmatrix} = \begin{bmatrix} 34 \\ 46 \end{bmatrix} & P_7 &= \begin{bmatrix} J \\ n \end{bmatrix} = \begin{bmatrix} 9 \\ 39 \end{bmatrix} \\ P_3 &= \begin{bmatrix} a \\ a \end{bmatrix} = \begin{bmatrix} 52 \\ 26 \end{bmatrix} & P_8 &= \begin{bmatrix} m \\ s \end{bmatrix} = \begin{bmatrix} 38 \\ 44 \end{bmatrix} \\ P_4 &= \begin{bmatrix} e \\ r \end{bmatrix} = \begin{bmatrix} 26 \\ 30 \end{bmatrix} & P_9 &= \begin{bmatrix} t \\ k \end{bmatrix} = \begin{bmatrix} 45 \\ 36 \end{bmatrix} \\ P_5 &= \begin{bmatrix} a \\ r \end{bmatrix} = \begin{bmatrix} 26 \\ 43 \end{bmatrix} \end{aligned}$$

7. Menerapkan matriks kunci  $K_e$  pada setiap  $P_i$  untuk mendapatkan *ciphertext*  $C = C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8 C_9$ , di mana  $C_i = (K_e P_i) \bmod 53$  sehingga:

$$\begin{aligned} C_1 &= \begin{pmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 46 \\ 26 \end{bmatrix} \end{pmatrix} \bmod 53 = \begin{bmatrix} 92 \\ 78 \\ 184 \end{bmatrix} \bmod 53 = \begin{bmatrix} 39 \\ 25 \\ 25 \end{bmatrix} \\ C_2 &= \begin{pmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 34 \\ 46 \end{bmatrix} \end{pmatrix} \bmod 53 = \begin{bmatrix} 68 \\ 138 \\ 136 \end{bmatrix} \bmod 53 = \begin{bmatrix} 15 \\ 32 \\ 30 \end{bmatrix} \\ C_3 &= \begin{pmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 52 \\ 26 \end{bmatrix} \end{pmatrix} \bmod 53 = \begin{bmatrix} 104 \\ 78 \\ 208 \end{bmatrix} \bmod 53 = \begin{bmatrix} 51 \\ 25 \\ 49 \end{bmatrix} \\ C_4 &= \begin{pmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 26 \\ 30 \end{bmatrix} \end{pmatrix} \bmod 53 = \begin{bmatrix} 52 \\ 90 \\ 104 \end{bmatrix} \bmod 53 = \begin{bmatrix} 52 \\ 37 \\ 51 \end{bmatrix} \end{aligned}$$

$$\begin{aligned}
 C_5 &= \begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{pmatrix} \begin{bmatrix} 26 \\ 43 \end{bmatrix} \pmod{53} = \begin{bmatrix} 52 \\ 129 \\ 104 \end{bmatrix} \pmod{53} = \begin{bmatrix} 52 \\ 23 \\ 51 \end{bmatrix} \\
 C_6 &= \begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{pmatrix} \begin{bmatrix} 12 \\ 45 \end{bmatrix} \pmod{53} = \begin{bmatrix} 24 \\ 135 \\ 48 \end{bmatrix} \pmod{53} = \begin{bmatrix} 24 \\ 29 \\ 48 \end{bmatrix} \\
 C_7 &= \begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{pmatrix} \begin{bmatrix} 9 \\ 39 \end{bmatrix} \pmod{53} = \begin{bmatrix} 18 \\ 117 \\ 36 \end{bmatrix} \pmod{53} = \begin{bmatrix} 18 \\ 11 \\ 36 \end{bmatrix} \\
 C_8 &= \begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{pmatrix} \begin{bmatrix} 38 \\ 44 \end{bmatrix} \pmod{53} = \begin{bmatrix} 76 \\ 132 \\ 152 \end{bmatrix} \pmod{53} = \begin{bmatrix} 23 \\ 26 \\ 46 \end{bmatrix} \\
 C_9 &= \begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{pmatrix} \begin{bmatrix} 45 \\ 36 \end{bmatrix} \pmod{53} = \begin{bmatrix} 90 \\ 108 \\ 180 \end{bmatrix} \pmod{53} = \begin{bmatrix} 37 \\ 2 \\ 21 \end{bmatrix}
 \end{aligned}$$

8. Mengonversi matriks  $C$  kedalam huruf sehingga didapatkan *ciphertext* nya

$$\begin{aligned}
 C &= y_1 y_2 \dots \\
 C &= \begin{bmatrix} 39 & 15 & 51 & 52 & 52 & 24 & 18 & 23 & 37 \\ 25 & 32 & 25 & 37 & 23 & 29 & 11 & 26 & 2 \\ 25 & 30 & 49 & 51 & 51 & 48 & 36 & 46 & 21 \end{bmatrix} \\
 &= \begin{bmatrix} n & P & z & l & X & Y & S & X & l \\ Z & g & Z & l & X & d & L & a & B \\ Z & e & x & z & z & w & k & u & V \end{bmatrix}
 \end{aligned}$$

Sehingga *ciphertext* nya adalah “ **nZZPgezZx lz XzYdwSLkXaulBV**”

b) Dekripsi

Kemudian dari proses enkripsi sebelumnya, pesan bersandi akan didekripsi dengan algoritma super enkripsi *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang dengan pesan atau *ciphertext* yang didapat dari proses enkripsi sebelumnya yaitu

**“ nZZPgezZx lz XzYdwSLkXaulBV”.**

Adapun algoritma dari proses dekripsi menggunakan metode tersebut adalah sebagai berikut:

1. Menentukan kunci *columnar transposition* yang digunakan pada proses enkripsinya
2. Menuliskan *ciphertext* dalam sebuah tabel dari kolom pertama dan seterusnya dengan banyaknya baris sesuai dengan panjang *ciphertext* dibagi dengan panjang kuncinya
3. Mengurutkan kolom sesuai urutan kunci
4. Mendapatkan teks asli (*plaintext*)
5. Menentukan invers kiri dari matriks kunci yang digunakan pada enkripsi
6. Ekspresikan cipher teks ke dalam matriks kolom berorde  $m$  dan mengkonversi setiap karakter dalam matriks sebagai kode nomor menggunakan tabel 1. konversi Modifikasi Hill Cipher

$$C = C_1 C_2 \dots C_i$$

7. Dekripsi dengan kunci  $K_d = B$ , lebar matriks berorde  $n \times m$  ( $n < m$ ) yang mana invers kiri  $A$  diaplikasikan pada setiap  $C_i$  dengan mod 53 untuk mendapatkan pesan dekripsi pertama  $P$

$$P = P_1 P_2 \dots P_i$$

8. Mengonversi Matriks  $P$  ke dalam huruf sehingga didapatkan kembali teks aslinya (*plaintext*).

sehingga dari proses enkripsi sebelumnya maka dekripsinya adalah sebagai berikut:

1. Menentukan invers dari matriks kunci, di mana matriks kuncinya adalah

$$K_e = A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix}$$

Maka akan dicari invers dari kunci matriks dengan  $K^{-1} = (A^T A)^{-1} A^T$

$$K^{-1} = \left( \begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ 4 & 0 \end{bmatrix} \right)^{-1} \begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \end{bmatrix} \pmod{53}$$

$$K^{-1} = \left( \begin{bmatrix} 20 & 0 \\ 0 & 9 \end{bmatrix} \right)^{-1} \begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \end{bmatrix} \pmod{53}$$

$$K^{-1} = \frac{1}{180} \begin{bmatrix} 20 & 0 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \end{bmatrix} \pmod{53}$$

$$K^{-1} = 48 \begin{bmatrix} 9 & 0 \\ 0 & 20 \end{bmatrix} \begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \end{bmatrix} \pmod{53}$$

$$K^{-1} = \begin{bmatrix} 432 & 0 \\ 0 & 960 \end{bmatrix} \begin{bmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \end{bmatrix} \pmod{53}$$

$$K^{-1} = \begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \pmod{53}$$

2. Mengekspresikan *ciphertext* " **nZZPgezZx lz XzYdwSLkXaulBV**" ke dalam matriks kolom berorde m sehingga

$$C = \begin{bmatrix} n \\ Z \\ Z \end{bmatrix} \begin{bmatrix} P \\ g \\ e \end{bmatrix} \begin{bmatrix} z \\ Z \\ x \end{bmatrix} \begin{bmatrix} l \\ l \\ z \end{bmatrix} \begin{bmatrix} X \\ X \\ z \end{bmatrix} \begin{bmatrix} Y \\ d \\ w \end{bmatrix} \begin{bmatrix} S \\ L \\ k \end{bmatrix} \begin{bmatrix} X \\ a \\ u \end{bmatrix} \begin{bmatrix} l \\ B \\ V \end{bmatrix}$$

$$= \begin{bmatrix} 39 \\ 25 \\ 25 \end{bmatrix} \begin{bmatrix} 15 \\ 32 \\ 30 \end{bmatrix} \begin{bmatrix} 51 \\ 25 \\ 49 \end{bmatrix} \begin{bmatrix} 52 \\ 37 \\ 51 \end{bmatrix} \begin{bmatrix} 52 \\ 23 \\ 51 \end{bmatrix} \begin{bmatrix} 24 \\ 29 \\ 48 \end{bmatrix} \begin{bmatrix} 18 \\ 11 \\ 36 \end{bmatrix} \begin{bmatrix} 23 \\ 26 \\ 46 \end{bmatrix} \begin{bmatrix} 37 \\ 2 \\ 21 \end{bmatrix}$$

$$= C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8 C_9$$

3. Mendekripsi dengan kunci dekripsi  $K_d = B$  pada setiap  $C_i$  dengan mod 53 untuk mendapat P di mana  $P_1 = (K_d C_i) \pmod{53}$  sehingga

$$P_1 = \left( \begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 39 \\ 25 \\ 25 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 1424 \\ 450 \end{bmatrix} \pmod{53} = \begin{bmatrix} 46 \\ 26 \end{bmatrix}$$

$$P_2 = \left( \begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 15 \\ 32 \\ 30 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 1200 \\ 576 \end{bmatrix} \pmod{53} = \begin{bmatrix} 34 \\ 46 \end{bmatrix}$$

$$P_3 = \left( \begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 51 \\ 25 \\ 49 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 2384 \\ 450 \end{bmatrix} \pmod{53} = \begin{bmatrix} 52 \\ 26 \end{bmatrix}$$

$$P_4 = \left( \begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 52 \\ 37 \\ 51 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 2464 \\ 666 \end{bmatrix} \pmod{53} = \begin{bmatrix} 26 \\ 30 \end{bmatrix}$$

$$P_5 = \left( \begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 52 \\ 23 \\ 51 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 2464 \\ 414 \end{bmatrix} \pmod{53} = \begin{bmatrix} 26 \\ 43 \end{bmatrix}$$

$$P_6 = \left( \begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 24 \\ 29 \\ 48 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 1920 \\ 522 \end{bmatrix} \pmod{53} = \begin{bmatrix} 12 \\ 45 \end{bmatrix}$$

$$P_7 = \left( \begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 18 \\ 11 \\ 36 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 1440 \\ 198 \end{bmatrix} \pmod{53} = \begin{bmatrix} 9 \\ 39 \end{bmatrix}$$

$$P_8 = \left( \begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 23 \\ 26 \\ 46 \end{bmatrix} \right) \pmod{53} = \begin{bmatrix} 1840 \\ 468 \end{bmatrix} \pmod{53} = \begin{bmatrix} 38 \\ 44 \end{bmatrix}$$

$$P_9 = \left( \begin{bmatrix} 16 & 0 & 32 \\ 0 & 18 & 0 \end{bmatrix} \begin{bmatrix} 37 \\ 2 \\ 21 \end{bmatrix} \right) \text{mod } 53 = \begin{bmatrix} 1264 \\ 36 \end{bmatrix} \text{mod } 53 = \begin{bmatrix} 45 \\ 36 \end{bmatrix}$$

4. Mengonversi Matriks P ke dalam huruf sehingga didapatkan kembali teks aslinya (*plaintext*)

$$P = \begin{bmatrix} 46 & 34 & 52 & 26 & 26 & 12 & 9 & 38 & 45 \\ 26 & 46 & 26 & 30 & 43 & 45 & 39 & 44 & 36 \end{bmatrix}$$

$$= \begin{bmatrix} u & i & a & a & M & J & m & t \\ a & u & a & e & r & t & n & s & k \end{bmatrix}$$

Sehingga didapatkan hasil dekripsi dari modifikasi *Hill cipher* yaitu “**uaiu aaearMtjnmstk**”

5. Hasil dekripsi dari modifikasi *Hill cipher* didekripsi kembali menggunakan *columnar transposition* dengan kunci “Melati” sehingga panjang kunci 6 dengan urut “5 2 4 1 6 3”
6. Memetakan ciphertext ke dalam tabel, panjang *ciphertext* yaitu 18 sehingga  $\frac{18}{6} = 3$  maka banyaknya baris pada tabel adalah 3 sedangkan banyak kolomnya 6 karena panjang kunci yaitu

**Tabel 4.** Dekripsi Super Enkripsi Terurut Angka

1	2	3	4	5	6
u	u	a	r	J	s
a		e	M	n	t
i	a	a	t	m	k

7. Mengurutkan sesuai urutan kunci yaitu “5 2 4 1 6 3”

**Tabel 5.** Dekripsi Super Enkripsi Terurut Kunci

5	2	4	1	6	3
J	u	r	u	s	a
n		M	a	t	e
m	a	t	i	k	a

8. Sehingga didapatkan hasil dekripsi sesuai *plaintextnya* yaitu “**Jurusan Matematika**”.

## KESIMPULAN

Berdasarkan pembahasan di atas, dapat disimpulkan bahwa penyandian super enkripsi menggunakan *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang menghasilkan pesan akhir yang tidak mengubah, menambah maupun mengurangi pesan awal, sehingga dapat diimplementasikan pada pesan dengan baik. Penyandian super enkripsi yang mengombinasikan *columnar transposition* dan modifikasi *hill cipher* dengan invers kiri matriks persegi panjang didapatkan keamanan ganda. Keamanan pertama terletak pada keamanan menggunakan *columnar transposition* kemudian yang kedua ialah pada *hill cipher* yang telah dimodifikasi menggunakan invers kiri matriks persegi panjang.

## DAFTAR PUSTAKA

- [1] A. Y. Efrandi, "Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher," *Media Infotama*, vol. 10, pp. 120-128, 2014.
- [2] I. Z. Muhammad, "Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA)," pp. 19-26, 2019.
- [3] J. P. Lisda, "Kriptografi Hybrida Algoritma Hill Cipher dan Rivest Shamir Adleman (RSA)," *Teknologi Informasi dan Komunikasi*, vol. 7, pp. 11-26, 2018.
- [4] A. P. Nurdin, "Analisa dan Implementasi Kriptografi pada Pesan Rahasia Menggunakan Algoritma Cipher Transposition," *Elektronik Sistem Informasi dan Komputer*, vol. 3, pp. 1-10, 2017.
- [5] M. Rinaldi, Diktat Kuliah IF 2153 Matematika Diskrit, Bandung: Departemen Teknik Informatika, 2006.
- [6] M. Rinaldi, Kriptografi, Bandung: Penerbit Informatika, 2019.
- [7] K. Ravinder, "Rectangular Matrix with Left Inverse For Variation in Hill Cipher: Communication Safe Guard," vol. 21, pp. 1234-1240, 2019.
- [8] B. Forouzan, *Cryptography and Network Security*, McGraw-Hill, 2008.
- [9] M. Rinaldi, *Matematika Diskrit*, Bandung: Penerbit Informatika, 2002.
- [10] E. Setyaningsih, "Konsep Super Enkripsi untuk Penyandian Citra Warna Menggunakan Kombinasi Hill Cipher dan Playfair Cipher," vol. 6, pp. 38-48, 2010.
- [11] Y. H, T. K and T. Y, *Projection Matrices, Generalized Inverse Matrices, and Singular Value Decomposition*, New York: Springer, 2011.
- [12] Y. d. Reswan, "Implementasi Kompilasi Algoritma Kriptografi Transposisi Columnar dan RSA untuk Pengamanan Pesan Rahasia," vol. 4, pp. 194-202, 2018.
- [13] S. Daurat, "Teknik Super Enkripsi Menggunakan Transposisi Koom Berbasis Vigenere Cipher Pada Citra Digital," vol. 14, pp. 57-64, 2018.
- [14] D. Ariyus, *Kriptografi Keamanan Data dan Komunikasi*, Yogyakarta: Graha Ilmu, 2006.
- [15] D. Ariyus, *Pengantar Ilmu Kriptografi*, Yogyakarta: C.V Andi Offset, 2008.