Mandalika Mathematics and Education Journal
Volume 8 Nomor 2, Juni 2026
e-ISSN 2715-1190| |p-ISSN 2715-8292
DOI: http://dx.doi.org/10.29303/jm.v8i2.12682

Analisis Komparatif Algoritma Cipher Hill, Cipher Vigenère, dan Cipher Caesar pada Proses Enkripsi dan Dekripsi Data Teks

Yunita Septriana Anwar[1*], Rizki Azis Al Kautsar[1]

[1] *Pendidikan Matematika, FKIP, Universitas Muhammadiyah Mataram, Mataram*

yunitaseptriana@ummat.ac.id

Abstract
Classical cryptography is one of the information security methods that employs message transformation techniques to preserve data confidentiality. Several widely used classical cryptographic algorithms are the Caesar Cipher, Vigenère Cipher, and Hill Cipher, each of which has distinct encryption mechanisms and security levels. This study aims to analyze the characteristics, advantages, and limitations of these three algorithms and to compare their encryption and decryption processes. The results indicate that the Caesar Cipher is the simplest and easiest algorithm to implement; however, it provides a low level of security due to its vulnerability to frequency analysis attacks. The Vigenère Cipher offers a higher level of security through its polyalphabetic substitution mechanism, although it remains susceptible to cryptanalysis when the key pattern and length can be estimated. The Hill Cipher provides an even higher level of security by employing polygraphic substitution based on matrix operations, resulting in better diffusion and a larger key space. Nevertheless, its implementation is relatively more complex and requires the use of a key matrix that is invertible modulo a given integer.

Keywords: classical cryptography, Caesar Cipher, Vigenère Cipher, Hill Cipher, encryption, decryption.

Abstrak
Kriptografi klasik merupakan salah satu metode pengamanan informasi yang menggunakan teknik transformasi pesan untuk menjaga kerahasiaan data. Beberapa algoritma kriptografi klasik yang banyak digunakan adalah Cipher Caesar, Cipher Vigenère, dan Cipher Hill, yang masing-masing memiliki mekanisme enkripsi dan tingkat keamanan yang berbeda. Penelitian ini bertujuan untuk menganalisis karakteristik, kelebihan, dan keterbatasan ketiga algoritma tersebut serta melakukan komparasi terhadap proses enkripsi dan dekripsi pesan. Hasil analisis menunjukkan bahwa Caesar Cipher merupakan algoritma yang paling sederhana dan mudah diimplementasikan, tetapi memiliki tingkat keamanan yang rendah karena rentan terhadap serangan analisis frekuensi. Cipher Vigenère menawarkan tingkat keamanan yang lebih baik melalui mekanisme substitusi polialfabetik, meskipun masih rentan terhadap kriptoanalisis apabila pola dan panjang kunci dapat diperkirakan. Cipher Hill memberikan tingkat keamanan yang lebih tinggi karena menerapkan substitusi poligrafik berbasis operasi matriks yang menghasilkan difusi lebih baik dan ruang kunci yang lebih besar. Namun, implementasinya relatif lebih kompleks dan mensyaratkan penggunaan matriks kunci yang invertibel modulo tertentu.

Kata kunci: kriptografi klasik, Cipher Caesar, Cipher Vigenère, Cipher Hill Cipher, enkripsi, dekripsi.

1. PENDAHULUAN

Di era digital saat ini, keamanan data pribadi menjadi aspek krusial yang harus diperhatikan oleh setiap individu. Data pribadi mencakup informasi penting seperti nama, alamat, nomor identitas, nomor telepon, serta informasi keuangan, yang jika jatuh ke tangan yang salah dapat disalahgunakan untuk berbagai kejahatan siber.

Salah satu ancaman terbesar yang dihadapi masyarakat saat ini adalah pembobolan data pribadi, yang sering kali berujung pada penipuan keuangan, pencurian identitas, dan penyalahgunaan informasi untuk pinjaman online ilegal. Dalam banyak kasus, pelaku kejahatan menggunakan data yang bocor untuk mengakses rekening korban, melakukan transaksi tanpa izin, atau bahkan mendaftarkan pinjaman atas nama korban tanpa sepengetahuan mereka.

Salah satu solusi yang dapat diterapkan dalam pengamanan data pribadi adalah penggunaan kriptografi (Anwar et al., 2025). Kriptografi merupakan ilmu dan teknik yang digunakan untuk melindungi informasi dengan mengubahnya ke dalam bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang (Stinson & Paterson, 2018). Dalam kriptografi, pesan atau data asli (*plaintext*) dikonversi menjadi bentuk terenkripsi (*ciphertext*) menggunakan algoritma dan kunci tertentu, sehingga hanya pihak yang memiliki kunci dekripsi yang dapat mengembalikannya ke bentuk semula.

Tujuan utama kriptografi adalah untuk menjaga keamanan informasi dengan memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang. Salah satu aspek penting dalam kriptografi adalah kerahasiaan (*confidentiality*), yang memastikan bahwa pesan atau data hanya dapat dibaca oleh penerima yang sah. Selain itu, kriptografi juga berfungsi untuk menjaga integritas (*integrity*) data, sehingga informasi tidak dapat diubah atau dimanipulasi tanpa terdeteksi. Dengan tujuan utama ini, kriptografi menjadi teknologi yang sangat penting dalam melindungi informasi, baik dalam komunikasi online, transaksi perbankan, maupun sistem keamanan digital lainnya.

Kriptografi klasik terdiri atas berbagai algoritma, di antaranya Cipher Caesar, Cipher Vigenère, dan Cipher Hill, yang masing-masing memiliki mekanisme enkripsi, tingkat keamanan, serta karakteristik yang berbeda (Rosen, 2019). Masing-masing algoritma memiliki prinsip kerja, karakteristik, kelebihan, keterbatasan, serta tingkat ketahanan yang berbeda terhadap berbagai serangan kriptoanalisis. Cipher Caesar pertama kali ditemukan pada akhir tahun 1970-an dan berasal dari Julius Caesar dengan menerjemahkan huruf-huruf menjadi angka. Chiper Caesar merupakan salah satu metode enkripsi pesan yang paling sederhana dan tertua. Cipher Caesar menggunakan sandi yang didasarkan pada substitusi, di mana setiap huruf digantikan oleh huruf yang terletak tiga posisi setelahnya dalam alfabet, dengan tiga huruf terakhir digeser ke awal alfabet. Cipher Vigenère dinamai dari seorang diplomat dan kriptografer Prancis bernama *Blaise de Vigenère*. Cipher Vigenère dikembangkan untuk mengatasi kelemahan algoritma substitusi monoalfabetik pada Chiper Caesar yang rentan terhadap analisis frekuensi.

Sandi yang dienkripsi dengan Cipher Caesar atau Vigenère memiliki kelemahan apabila huruf-huruf tertentu muncul dengan frekuensi tinggi. Sebagai contoh, dalam bahasa Inggris, huruf 'E' merupakan huruf yang paling sering muncul, sedangkan dalam bahasa Indonesia, huruf 'A' sering muncul lebih dominan. Pola frekuensi ini tetap tampak dalam *ciphertext*, sehingga memungkinkan kriptanalisis berbasis frekuensi untuk menebak huruf-huruf yang sebenarnya dan mengungkap pesan asli. Cipher Hill

dikembangkan untuk menghindari kelemahan Cipher Caesar atau Vigenère yang mengganti setiap blok huruf *plaintext* dengan panjang tertentu menjadi blok huruf *ciphertext* dengan panjang yang sama. Sandi jenis ini disebut *sandi blok* (*block cipher*), dan dikembangkan oleh Lester Hill pada tahun 1929 (Stallings, 2017).

Dalam penelitian ini, Cipher Caesar, Cipher Vigenère, dan Cipher Hill dianalisis berdasarkan kelebihan dan keterbatasan masing-masing, serta dilakukan analisis komparatif terhadap ketiga algoritma tersebut dalam proses enkripsi dan dekripsi pesan.

2. PEMBAHASAN

2.1 CIPHER CAESAR

Untuk mengenkripsi sebuah pesan menggunakan Chiper Caesar, terlebih dahulu mengubahnya menjadi bentuk numerik, lalu mengelompokkan huruf-huruf dalam blok-blok berisi lima huruf. Kemudian dilakukan transformasi pada setiap angka. Pengelompokan huruf ke dalam blok-blok membantu mencegah keberhasilan kriptanalisis yang didasarkan pada pengenalan kata-kata tertentu. Misalkan P adalah nilai numerik dari suatu huruf dalam *plaintext*, yaitu pesan yang akan diubah ke dalam bentuk rahasia, dan C adalah nilai numerik dari huruf hasil enkripsi (*ciphertext*), sehingga

$$C \equiv P + 3 \ (mod\ 26), \ \ 0 \leq C \leq 25.$$

Untuk menerjemahkan sandi (*chipertext*) ke pesan asli (*plaintext*) digunakan hubungan:

$$P \equiv C - 3 \ (mod\ 26),$$

dengan $0 \leq P \leq 25$. Korespondensi antara *plaintext* dan *ciphertext* pada cipher Caesar sebagai berikut.

Plaintext (P)	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Chipertext (C)	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	D	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**

Plaintext (P)	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
	14	15	16	17	18	19	20	21	2	23	2	25
Chipertext (C)	17	18	19	20	21	22	23	24	2	0	1	2
	R	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**

Contoh 2.1. Untuk mengenskripsi pesan "ATTACK AT DAWN", terlebih dahulu dipecah menjadi kelompok lima huruf:

ATTAC KATDA WN,

kemudian huruf-huruf dirubah ke dalam bentuk numerik:

A	T	T	A	C	K	A	T	D	A	W	N
0	19	19	0	2	10	0	19	3	0	22	13

Selanjutnya, enkripsi dengan Cipher Caesar dengan transformasi $C \equiv P + 3 \ (mod\ 26)$:

0	19	19	0	2	10	0	19	3	0	22	13
3	22	22	3	5	13	3	22	6	3	25	16

Konversikan kembali ke huruf diperoleh:

3	22	22	3	5	13	3	22	6	3	25	16
D	W	W	D	F	N	D	W	G	D	Z	Q

Sehingga pesan terenkripsi menjadi: “DWWDF NDWGD ZQ”. Untuk mendekripsi pesan sandi “DWWDF NDWGD ZQ”, pertama huruf-huruf dirubah ke dalam bentuk numerik:

D	W	W	D	F	N	D	W	G	D	Z	Q
3	22	22	3	5	13	3	22	6	3	25	16

Selanjutnya, dilakukan transformasi $P \equiv C - 3 \ (mod\ 26)$ untuk mengubah pesan sandi menjadi pesan asli, dan diperoleh:

3	22	22	3	5	13	3	22	6	3	25	16
0	19	19	0	2	10	0	19	3	0	22	13

dan dirubah kembali angka-angka ini menjadi huruf-huruf untuk mendapatkan pesan aslinya:

0	19	19	0	2	10	0	19	3	0	22	13
A	T	T	A	C	K	A	T	D	A	W	N

Dengan menggabungkan huruf-huruf tersebut ke dalam kata-kata yang sesuai, ditemukan bahwa pesan tersebut berbunyi: “ATTACK AT DAWN”.

Transformasi pesan sandi dengan Cipher Caesar dapat diperumum dengan menggunakan hubungan:

$$C \equiv aP + b \ (mod\ 26)$$

dengan $0 \leq C \leq 25$ dan a, b bilangan-bilangan dengan $(a, 26) = 1$. Transformasi ini disebut transformasi afin (*affine transformations*). Untuk merubah pesan sandi (*ciphertext*) ke pesan asli (*plaintext*), digunakan hubungan:

$$P \equiv \bar{a}\ (C - b)\ (mod\ 26)$$

dengan $0 \leq P \leq 25$ dan $\bar{a}$ adalah invers a modulo 26.

Cipher Caesar sangat rentan terhadap analisis frekuensi karena menerapkan metode substitusi monoalfabetik. Akibatnya, distribusi frekuensi huruf pada ciphertext cenderung mempertahankan pola frekuensi pada plaintext. Sebagai contoh, huruf yang paling sering muncul pada plaintext umumnya tetap menjadi huruf yang paling sering muncul pada ciphertext. Selain itu, penggunaan nilai pergeseran yang tetap menyebabkan setiap huruf pada plaintext selalu dipetakan ke huruf ciphertext yang sama. Sifat deterministik ini memungkinkan pola-pola tertentu dalam pesan masih dapat dikenali, sehingga tingkat keamanan algoritma menjadi relatif rendah.

2.2. CIPHER VIGENÈRE

Untuk mengenkripsi pesan teks dengan cipher Vigenère, misalkan kunci dari cipher Vigenère terdiri dari $l_1 l_2 \cdots l_n$ dengan nilai numerik huruf yang bersesuaian k_1, k_2, ⋯, k_n. Sebuah blok yang terdiri dari huruf-huruf dengan nilai numerik p_1, p_2, ⋯, p_n diubah menjadi blok sandi berupa huruf-huruf dengan nilai numerik c_1, c_2, ⋯, c_n dengan:

$$c_i \equiv p_i + k_i \ (mod\ 26)$$

dimana $0 \leq c_i \leq 25$ dan $i = 1, 2, \cdots, n$. Untuk mendekripsi pesan sandi digunakan hubungan:

$$p_i \equiv c_i - k_i \ (mod\ 26)$$

dengan $0 \leq p_i \leq 25$ dan $i = 1, 2, \cdots, n$.

Contoh 2.2. Untuk mengenskripsi pesan "ATTACK AT DAWN" dengan Cipher Vigenère, misalkan dipilih kunci yang digunakan adalah "TEOBIL". Pertama, pesan teks dan kunci diberikan sebagai berikut:

$\boldsymbol{p_i}$	A	T	T	A	C	K	A	T	D	A	W	N
$\boldsymbol{k_i}$	T	E	O	B	I	L	T	E	O	B	I	L

Huruf-huruf dalam pesan dan kunci diterjemahkan dalam nilai numerik, kemudian nilai numerik sandi didapatkan dengan

$$c_i \equiv p_i + k_i \ (mod\ 26)$$

dengan $0 \leq c_i \leq 25$ dan $i = 1, 2, \cdots, 12$, dan dikonversikan kembali ke huruf diperoleh:

p_i	0	19	19	0	2	10	0	19	3	0	22	13
k_i	19	4	14	1	8	11	19	4	14	1	8	11
c_i	19	23	7	1	10	21	19	23	17	1	4	24
c_i	T	X	H	B	K	V	T	X	R	B	E	Y

Sehingga pesan terenkripsi menjadi: "TXHBK VTXRB EY".

Untuk mendekripsi pesan "TXHBK VTXRB EY" ke pesan asli, terlebih dahulu huruf-huruf pada pesan sandi dan kunci dirubah ke dalam bentuk numerik:

c_i	T	X	H	B	K	V	T	X	R	B	E	Y
c_i	19	23	7	1	10	21	19	23	17	1	4	24
k_i	T	E	O	B	I	L	T	E	O	B	I	L
k_i	19	4	14	1	8	11	19	4	14	1	8	11

Dengan menggunakan hubungan: $p_i \equiv c_i - k_i \ (mod\ 26)$ dengan $0 \leq p_i \leq 25$ dan $i = 1, 2, \cdots, 12$, diperoleh:

p_i	0	19	19	0	2	10	0	19	3	0	22	13
p_i	A	T	T	A	C	K	A	T	D	A	W	N

Dengan menggabungkan huruf-huruf tersebut ke dalam kata-kata yang sesuai, ditemukan bahwa pesan tersebut berbunyi: "ATTACK AT DAWN".

Jika panjang kunci pada Vigenère Cipher dapat diperkirakan, ciphertext dapat dipartisi menjadi beberapa kelompok yang masing-masing menyerupai Caesar Cipher sehingga analisis frekuensi masih dapat diterapkan. Selain itu, tingkat keamanan Vigenère Cipher sangat bergantung pada panjang dan kerahasiaan kunci yang digunakan. Penggunaan kunci yang pendek atau berupa kata-kata umum menyebabkan pola perulangan pada ciphertext lebih mudah dikenali, sehingga meningkatkan peluang keberhasilan serangan kriptoanalisis.

2.3. CIPHER HILL

Dalam cipher Hill, setiap blok yang terdiri atas n huruf *plaintext* digantikan oleh blok yang terdiri atas n huruf *ciphertext*. Apabila jumlah huruf pada pesan ganjil, maka akan ditambahkan huruf semu, misalnya 'X', di akhir pesan agar blok terakhir tetap terdiri atas n huruf. Selanjutnya, membentuk *ciphertext* menggunakan relasi berikut:

$$C \equiv AP \ (mod\ 26)$$

dengan A adalah matriks $n \times n$ sedemikian hingga $(\det A, 26) = 1$, $C = \begin{pmatrix} C_1 \\ \vdots \\ C_n \end{pmatrix}$, dan $P = \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix}$, serta $C_1 C_2 \cdots C_n$ merupakan *ciphertext* hasil enskripsi yang bersesuaian dengan *plaintext* $P_1 P_2 \cdots P_n$. Untuk mendekripsi pesan sandi digunakan hubungan:

$$P \equiv \bar{A}C \ (mod\ 26)$$

dengan $\bar{A}$ merupakan matriks invers A modulo 26.

Contoh 2.3. Untuk mengenkripsi pesan: "DO NOT OPEN THIS ENVELOPE" menggunakan Cipher Hill, langkah pertama adalah membagi pesan menjadi blok-blok, dalam hal ini dipilih masing-masing blok terdiri dari tiga huruf:

Blok 1	**Blok 2**	**Blok 3**	**Blok 4**	**Blok 5**	**Blok 6**	**Blok 7**
DON	OTO	PEN	THI	SEN	VEL	OPE

Selanjutnya, huruf-huruf dirubah ke dalam bentuk numerik:

3 14 13 14 19 14 15 4 13 19 7 8

18 4 13 21 4 11 14 15 4.

Diipilih matriks $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 2 \end{pmatrix}$ karena $\det A = 3$, sehingga $(\det A, 26) = 1$. Enkripsi pesan dengan hubungan:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv A \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} (mod\ 26).$$

Enkripsi Blok 1:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} 3 \\ 14 \\ 13 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 33 \\ 71 \\ 57 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 7 \\ 19 \\ 5 \end{pmatrix} (mod\ 26),$$

sehingga pesan pada Blok 1 terenkripsi menjadi: HTF.

Enkripsi Blok 2:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} 14 \\ 19 \\ 14 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 61 \\ 99 \\ 80 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 9 \\ 21 \\ 2 \end{pmatrix} (mod\ 26),$$

sehingga pesan pada Blok 2 terenkripsi menjadi: JVC.

Enkripsi Blok 3:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} 15 \\ 4 \\ 13 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 47 \\ 53 \\ 49 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 21 \\ 1 \\ 23 \end{pmatrix} (mod\ 26),$$

sehingga pesan pada Blok 3 terenkripsi menjadi: VBX.

Enkripsi Blok 4:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} 19 \\ 7 \\ 8 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 53 \\ 56 \\ 49 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 1 \\ 4 \\ 23 \end{pmatrix} (mod\ 26),$$

sehingga pesan pada Blok 4 terenkripsi menjadi: BEX.

Enkripsi Blok 5:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} 18 \\ 4 \\ 13 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 53 \\ 56 \\ 52 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix} (mod\ 26),$$

sehingga pesan pada Blok 5 terenkripsi menjadi: BEA.

Enkripsi Blok 6:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} 21 \\ 4 \\ 11 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 57 \\ 55 \\ 51 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 5 \\ 3 \\ 25 \end{pmatrix} (mod\ 26),$$

sehingga pesan pada Blok 6 terenkripsi menjadi: FDZ.

Enkripsi Blok 7:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} 14 \\ 15 \\ 4 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 47 \\ 67 \\ 52 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 21 \\ 15 \\ 0 \end{pmatrix} (mod\ 26),$$

sehingga pesan pada Blok 7 terenkripsi menjadi: VPA. Dengan demikian, pesan terenkripsi adalah "HTF JVC VBX BEX BEA FDZ VPA".

Untuk mendekripsi pesan "HTF JVC VBX BEX BEA FDZ VPA" digunakan hubungan:

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \equiv \overline{\begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 2 \end{pmatrix}} \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} (mod\ 26).$$

Karena $\overline{\begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 2 \end{pmatrix}} = \bar{3} \cdot adj(A)$ dan nilai $adj(A) = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 3 & -3 \\ -1 & -3 & 5 \end{pmatrix}$ dan $\bar{3} = 9$, sehingga

$$\overline{\begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 2 \end{pmatrix}} = 9 \cdot \begin{pmatrix} 2 & 0 & -1 \\ 0 & 3 & -3 \\ -1 & -3 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 18 & 0 & -9 \\ 0 & 27 & -27 \\ -9 & -27 & 45 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 18 & 0 & 17 \\ 0 & 1 & 25 \\ 17 & 25 & 19 \end{pmatrix} (mod\ 26).$$

Dekripsi HTF:

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \equiv \begin{pmatrix} 18 & 0 & 17 \\ 0 & 1 & 25 \\ 17 & 25 & 19 \end{pmatrix} \begin{pmatrix} 7 \\ 19 \\ 5 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 211 \\ 144 \\ 689 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 3 \\ 14 \\ 13 \end{pmatrix} (mod\ 26),$$

diperoleh pesan HTF terdekripsi menjadi: DON.

Dekripsi JVC:

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \equiv \begin{pmatrix} 18 & 0 & 17 \\ 0 & 1 & 25 \\ 17 & 25 & 19 \end{pmatrix} \begin{pmatrix} 9 \\ 21 \\ 2 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 196 \\ 71 \\ 716 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 14 \\ 19 \\ 14 \end{pmatrix} (mod\ 26),$$

diperoleh pesan JVC terdekripsi menjadi: OTO.

Dekripsi VBX:

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \equiv \begin{pmatrix} 18 & 0 & 17 \\ 0 & 1 & 25 \\ 17 & 25 & 19 \end{pmatrix} \begin{pmatrix} 21 \\ 1 \\ 23 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 769 \\ 576 \\ 819 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 15 \\ 4 \\ 13 \end{pmatrix} (mod\ 26),$$

diperoleh pesan VBX terdekripsi menjadi PEN.

Dekripsi BEX:

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \equiv \begin{pmatrix} 18 & 0 & 17 \\ 0 & 1 & 25 \\ 17 & 25 & 19 \end{pmatrix} \begin{pmatrix} 1 \\ 4 \\ 23 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 409 \\ 579 \\ 554 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 19 \\ 7 \\ 8 \end{pmatrix} (mod\ 26),$$

diperoleh pesan BEX terdekripsi menjadi THI.

Dekripsi BEA:

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \equiv \begin{pmatrix} 18 & 0 & 17 \\ 0 & 1 & 25 \\ 17 & 25 & 19 \end{pmatrix} \begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 18 \\ 4 \\ 117 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 18 \\ 4 \\ 13 \end{pmatrix} (mod\ 26),$$

diperoleh pesan BEA terdekripsi menjadi SEN.

Dekripsi FDZ:

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \equiv \begin{pmatrix} 18 & 0 & 17 \\ 0 & 1 & 25 \\ 17 & 25 & 19 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \\ 25 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 515 \\ 628 \\ 635 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 21 \\ 4 \\ 11 \end{pmatrix} (mod\ 26),$$

diperoleh pesan FDZ terdekripsi menjadi VEL.

Dekripsi VPA:

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \equiv \begin{pmatrix} 18 & 0 & 17 \\ 0 & 1 & 25 \\ 17 & 25 & 19 \end{pmatrix} \begin{pmatrix} 21 \\ 15 \\ 0 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 378 \\ 15 \\ 732 \end{pmatrix} (mod\ 26)$$

$$\equiv \begin{pmatrix} 14 \\ 15 \\ 4 \end{pmatrix} (mod\ 26),$$

diperoleh pesan VPA terdekripsi menjadi OPE. Dengan mengumpulkan semua pesan terdekripsi diperoleh:" "DON OTO PEN THI SEN VEL OPE". Selanjutnya, digabungkan huruf-huruf tersebut ke dalam kata-kata yang sesuai, ditemukan bahwa pesan tersebut berbunyi: "DO NOT OPEN THIS ENVELOPE".

Cipher Hill mengenkripsi beberapa karakter secara simultan dalam bentuk blok menggunakan operasi matriks, sedangkan Cipher Caesar dan Cipher Vigenère mengenkripsi karakter secara individual. Akibatnya, perubahan pada satu karakter plaintext dapat memengaruhi beberapa karakter pada ciphertext, sehingga pola statistik pada plaintext menjadi lebih tersamarkan dan algoritma ini lebih tahan terhadap analisis frekuensi. Selain itu, kunci pada Cipher Hill berupa matriks invertibel modulo (m), sehingga jumlah kemungkinan kuncinya jauh lebih besar dibandingkan Cipher Caesar yang hanya memiliki 25 kemungkinan pergeseran maupun Cipher Vigenère yang umumnya menggunakan kata kunci yang relatif pendek. Lebih lanjut, operasi perkalian matriks pada Cipher Hill menghasilkan tingkat difusi (*diffusion*) yang lebih baik, sehingga hubungan langsung antara plaintext dan ciphertext menjadi lebih kompleks dan sulit dikenali. Meskipun demikian, Cipher Hill masih memiliki beberapa keterbatasan. Matriks kunci yang digunakan harus bersifat invertibel pada modulo tertentu agar proses dekripsi dapat dilakukan dengan benar. Selain itu, implementasi Cipher Hill relatif lebih kompleks karena melibatkan operasi perkalian matriks dan pencarian invers modulo. Algoritma ini juga memerlukan penambahan karakter pengisi (*padding*) apabila panjang plaintext tidak merupakan kelipatan dari ukuran blok yang digunakan.

5. SIMPULAN

Cipher Caesar, Cipher Vigenère, dan Cipher Hill memiliki karakteristik, kelebihan, dan keterbatasan yang berbeda dalam proses enkripsi dan dekripsi pesan. Caesar Cipher merupakan algoritma yang paling sederhana dan mudah diimplementasikan, namun memiliki tingkat keamanan yang rendah karena rentan terhadap serangan analisis frekuensi. Cipher Vigenère menawarkan tingkat keamanan yang lebih baik melalui mekanisme substitusi polialfabetik, tetapi masih rentan terhadap kriptoanalisis apabila panjang dan pola kuncinya dapat diperkirakan. Sementara itu, Cipher Hill memberikan tingkat keamanan yang lebih tinggi karena menerapkan substitusi poligrafik berbasis operasi matriks, menghasilkan difusi yang lebih baik dan ruang kunci yang lebih besar. Meskipun demikian, implementasi Cipher Hill relatif lebih kompleks dan mensyaratkan penggunaan matriks kunci yang invertibel modulo tertentu. Oleh karena itu, pemilihan algoritma kriptografi klasik perlu disesuaikan dengan kebutuhan antara kemudahan implementasi, efisiensi komputasi, dan tingkat keamanan yang diinginkan.

6. REKOMENDASI

Studi lanjutan mengenai Cipher Caesar, Cipher Vigenère, dan Cipher Hill dapat diarahkan pada implementasi ketiga algoritma pada berbagai platform komputasi dan integrasinya dengan teknik kriptografi.

7. REFERENSI

Anwar, Y. S., Abdillah, A., & Sirajudin, S. (2025). Mengenal kriptografi sejak dini: membangun kesadaran keamanan data pribadi. *SELAPARANG: Jurnal Pengabdian Masyarakat Berkemajuan*, *9*(4), 2028–2033.

Rosen, K. H. (2019). *Discrete Mathematics and Its Applications* (8th ed.). McGraw-Hill Education.

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice (7th ed.)*. Pearson.

Stinson, D. R., & Paterson, M. B. (2018). *Cryptography: Theory and Practice* (4th ed.). CRC Press.