# PENGGUNAAN MATRIKS ORDO 7 × 4 DAN *HILL CIPHER* DALAM MODIFIKASI METODE *PLAYFAIR CIPHER*

**Sisilia Sylviani[1*], Fahmi Candra Permana[2]**

[1*] Departemen Matematika FMIPA Universitas Padjadjaran, Sumedang, Indonesia, sisilia.sylviani@unpad.ac.id

[2] Prodi Pendidikan Multimedia, Universitas Pendidikan Indonesia, Bandung, Indonesia

***Abstract***

*This article discusses the utilization of a 7×4 matrix and Hill Cipher in modifying the Playfair Cipher method. The modification involves transforming the 5x5 Playfair matrix into a 7×4 matrix by introducing symbols "*" and "#". The objective of this modification is to enhance the efficiency of the encryption and decryption processes while increasing security by establishing a one-to-one correspondence between plaintext and ciphertext. Following the encryption process using the Playfair method, Hill Cipher is employed to enhance the diversity of the generated ciphertext. The article covers the design of the modification, implementation, and performance analysis of the proposed method, along with presenting the results of security, efficiency, and resistance to cryptanalysis testing. The research findings indicate that the utilization of a 7×4 matrix and Hill Cipher in modifying the Playfair Cipher method significantly enhances the security and efficiency of the cryptographic process.*

**Keywords:** *Ciphertext* , Cryptography, hill *Cipher*, plaintext, *Playfair Cipher*, substitution *Cipher*, transposition *Cipher*.

**Abstrak**

Artikel ini membahas tentang penggunaan matriks ordo 7 × 4 dan Hill Cipher dalam modifikasi metode *Playfair* Cipher. Modifikasi dilakukan dengan mengubah matriks *Playfair* 5x5 menjadi matriks 7 $\backslash times$ 4 dengan memasukkan simbol "*" dan "#". Tujuan modifikasi ini adalah untuk meningkatkan efisiensi proses enkripsi dan dekripsi serta meningkatkan tingkat keamanan dengan menghasilkan korespondensi satu-ke-satu antara plaintext dan ciphertext. Setelah proses enkripsi dengan metode *Playfair* , dilanjutkan dengan Hill Cipher untuk meningkatkan keragaman ciphertext yang dihasilkan. Artikel ini membahas rancangan modifikasi, implementasi, dan analisis performa dari metode yang diusulkan, serta menyajikan hasil dari pengujian keamanan, efisiensi, dan ketahanan terhadap serangan kriptanalisis. Hasil penelitian menunjukkan bahwa penggunaan matriks ordo *7 \times 4* dan Hill Cipher dalam modifikasi metode *Playfair* Cipher mampu meningkatkan keamanan dan efisiensi proses kriptografi secara signifikan.

**Kata Kunci** : *Ciphertext , hill Cipher, Kriptografi, plaintext, Playfair Cipher, substitusi Cipher, transposisi Cipher.*

**Cara Menulis Sitasi:** Sylviani, S., Permana, F., C. (2023). Penggunaan Matrikz Ordo 7 × 4 dan Hill Cipher dalam Modifikasi Metode Playfair Cipher. *Jurnal Edukasi dan Sains Matematika (JES-MAT),10* (1), 41-54.

**PENDAHULUAN**

Keamanan informasi telah menjadi perhatian utama dalam era digital saat ini, ketika pertukaran data sensitif melalui jaringan komunikasi menjadi hal yang umum. Dalam konteks ini, kriptografi memainkan peran penting dalam menjaga kerahasiaan dan integritas data yang dikirimkan melalui internet atau sistem komunikasi lainnya (Mukhtar, 2018; Hasugian, 2017; Pabokory dkk., 2016). Salah satu teknik kriptografi klasik yang masih digunakan hingga saat ini adalah *Playfair Cipher*, yang telah terbukti efektif dalam mengenkripsi teks (Sinaga, 2021; Suriadi dkk., 2020; Suhelna 2020). Namun, semakin berkembangnya teknologi, keamanan dari metode kriptografi tersebut menjadi semakin rentan terhadap serangan kriptanalisis.

Untuk mengatasi kelemahan tersebut, penelitian ini mengusulkan sebuah modifikasi pada *Playfair Cipher* dengan mengintegrasikannya dengan Hill *Cipher*. Modifikasi ini dilakukan dengan mengubah matriks *Playfair* menjadi matriks ordo $7 \times 4$, yang tidak hanya meningkatkan efisiensi dalam proses enkripsi dan dekripsi, tetapi juga meningkatkan tingkat keamanan dengan menambahkan simbol "*" dan "#". Hal ini diharapkan dapat membuat teks *Ciphertext* lebih sulit terbaca dan mengurangi ambigu dalam proses enkripsi.

Urgensi dari penelitian ini terletak pada kebutuhan akan metode kriptografi yang lebih aman dan efisien dalam mengatasi tantangan keamanan yang semakin kompleks di era digital ini. Dengan menggabungkan modifikasi *Playfair Cipher* dengan Hill *Cipher*, diharapkan dapat menciptakan sebuah sistem kriptografi yang lebih tangguh dan dapat diandalkan dalam melindungi kerahasiaan informasi. Selain itu, penelitian ini juga memiliki implikasi praktis yang signifikan dalam berbagai aplikasi keamanan informasi, seperti pengamanan data sensitif, pertukaran pesan rahasia, dan komunikasi aman secara online. Dengan demikian, penelitian ini memiliki urgensi yang tinggi dalam konteks perlindungan data dan informasi sensitif di era digital saat ini. Kriptografi adalah kata Yunani yang berarti menulis rahasia. Sekarang istilah ini mengacu pada sains dan seni untuk mengubah pesan agar lebih aman dan kebal terhadap serangan. Untuk tujuan keamanan dan privasi, kita perlu mengenkripsi pesan di sisi pengirim dan mendekripsinya di sisi penerima. Jadi kriptografi adalah cara untuk membuat dan menggunakan teknik enkripsi dan dekripsi.

Terdapat dua jenis Kriptografi yaitu, *Symmetric Key Cryptography* dan *Asymmetric Key Cryptography* (Kabetta ; Arrija, dkk., 2016). Pada Kriptografi kunci simetris, satu kunci diberikan kepada pengirim dan penerima. Dalam melakukan proses enkripsi pesan, pengirim menggunakan algoritma kunci dan enkripsi. Di sisi lain, dalam melakukan proses dekripsi pesan, penerima menggunakan algoritma kunci dan dekripsi. Setiap pengguna pada jenis Kriptografi dengan *Asymmetric Key* diberi sepasang kunci, kunci publik dan kunci privat. Kunci publik diinformasikan kepada setiap anggota, sedangkan kunci privat

dirahasiakan pengguna. Pengirim pesan memakai kunci publik penerima untuk mengenkripsi pesan yang dikirim. Di sisi lain, penerima menggunakan kunci pribadinya untuk mendekripsi pesan yang diterima.

## LANDASAN/KAJIAN TEORI

### Metode *Playfair*

*Playfair* adalah teknik peng-enkripsian pesan berdasarkan kombinasi pasangan huruf, bukan hanya huruf tunggal seperti pada metode enkripsi klasik lainnya (Pristiwanto, 2019) Metode enkripsi *Playfair* pertama kali dikembangkan oleh seorang fisikawan Inggris bernama Sir Charles Wheatstone (1802 - 1875). Walaupun demikian, yang mempopuler-kan sandi tersebut bukanlah tokoh yang mempopulerkan sandi *Playfair* adalah Baron Lyon *Playfair* (1819 - 1898) menemukan metode *Playfair* pada tahun 1854 (Syahputra, A., 2018).

Pengggunaan pertama kali sandi *Playfair* adalah oleh pasukan Inggris untuk tujuan-tujuan taktis pada Perang Boer II dan Perang Dunia I (Mu'mi, N. F. A., 2017). Sandi ini juga digunakan dengan tujuan yang serupa oleh Australia dan Jerman dalam Perang Dunia II. Hal yang menjadi penyebab Sandi *Playfair* menjadi sandi yang paling sering dimanfaatkan, khususnya dalam tujuan taktis perang adalah karena kesederhanaannya serta tidak membutuhkan alat khusus untuk membaca atau menerjemahkannya.

Seiring berjalannya waktu dan banyaknya kemunculan berbagai alat enkripsi digital yang dibentuk untuk menerjemahkannya, sandi tersebut tidak lagi digunakan oleh pasukan militer. Hal itu disebabkan sandi tersebut dianggap keamanannya tidak lagi terjaga untuk menjaga kerahasiaan pesan, karena komputer yang dilengkapi dengan perangkat lunak tertentu dapat dengan mudah memecahkan sandi tersebut dalam hitungan detik.

*Playfair Cipher* adalah sebuah teknik substitusi digraf yang menggunakan matriks $5 \times 5$. Pada matriks ini, kata kunci ditulis pertama kali, dan sel-sel yang tersisa diisi dengan huruf-huruf alfabet lainnya, dengan pengecualian bahwa I dan J diwakilkan di sel yang sama. Pesan yang akan dienkripsi dibagi menjadi pasangan-pasangan digraf, dengan mengulangi huruf pada pasangan yang sama dan memisahkan pasangan digraf tersebut dengan huruf pengisi X jika diperlukan. Jika jumlah huruf dalam pesan adalah ganjil, maka huruf terakhir akan dilapisi dengan huruf pengisi (biasanya X) untuk melengkapi pasangan digraf.

Jika dibandingkan dengan metode enkripsi klasik lainnya, kode atau sandi *Playfair* memiliki banyak keunggulan, di antaranya adalah sebagai berikut (Umar, R., & Yudhana, A. (2020).:

- Kriptanalis yang menggunakan metode analisis frekuensi menghadapi kesulitan dalam mendekripsi sandi *Playfair* karena proses enkripsi dan dekripsi melibatkan kombinasi dua huruf.
- Tabel kunci hanya dipakai satu kali saja, hal tersebut dikarenakan ada ada kemungkinan bahwa tabel

tersebut telah dipecahkan oleh pihak yang tidak berkepentingan.

Namun demikian, sandi tersebut juga memiliki beberapa kelemahan dibandingkan dengan metode enkripsi klasik lainnya adalah sebagai berikut (Amin, 2016; Pradipta, 2016)

- Metode *Playfair* dapat dengan mudah didekripsi menggunakan teknik analisis frekuensi distribusi ganda. Hal ini dilakukan dengan menghitung frekuensi kemunculan pasangan dua huruf dalam sandi dan membandingkannya dengan frekuensi pasangan dua huruf dalam bahasa yang digunakan.
- Dalam proses penerjemahan sandi, *Playfair* dapat menghasilkan makna ganda yang membingungkan.
- Metode *Playfair* tidak ideal digunakan untuk mengirimkan pesan rahasia dengan panjang yang signifikan.

Peraturan pada *Playfair*

1. Huruf plaintext yang berpasangan dengan huruf yang sama dipisahkan dengan huruf pengisi, contoh X. Contoh BALLOON menjadi BA LX LO ON.
2. Dua huruf plaintext yang posisinya berada pada baris yang sama pada matriks akan digantikan oleh huruf sebelah kanannya, membentuk sebuah siklus. Pandang Contoh kasus berikut : AR→ RM

| | | | | |
|---|---|---|---|---|
| M | O | N | A | R |
| C | H | Y | B | D |
| E | F | G | I/J | K |
| L | P | Q | S | T |
| U | V | W | X | Z |

3. Ketika dua huruf plaintext memiliki posisi yang sama pada kolom yang bersesuaian dalam matriks, setiap huruf akan digantikan oleh huruf di bawahnya, membentuk sebuah siklus. Sebagai contoh, jika terdapat pasangan huruf "MU", maka "M" akan digantikan oleh "C", dan "U" akan digantikan oleh "M", sehingga membentuk pasangan "CM".
4. Jika huruf plaintext tidak berada pada baris atau kolom yang bersesuaian, maka penggantinya adalah huruf yang posisinya berada pada baris yang sama dan kolom yang sama dengan pasangan plaintextnya. Sebagai contoh:
   HS → BP,EA → IM/JM.

Untuk memperoleh gambaran yang lebih baik lagi, perhatikan contoh kasus berikut. Pilih *CIPHER* sebagai *keyword*nya, dengan huruf L dan M berada pada sel yang sama. Pada tahap ini akan dibentuk matriks $5 \times 5$ nya.

| | | | | |
|---|---|---|---|---|
| C | I | P | H | E |
| R | A | B | D | F |
| G | J | K | L/M | N |
| O | Q | S | T | U |
| V | W | X | Y | Z |

Selanjutnya akan dienkripsikan kalimat LOVE ALL PEOPLE.

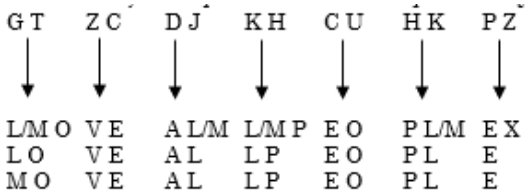
Pasangan huruf :

LO VE AL LP EO PL LX

*Ciphertext* :

GT ZC DJ KH CU HK PZ

Jika ciphertext dibalik, maka akan dicari plaintextnya, yang akan menghasilkan:




Terdapat dua penafsiran kata yang berbeda, sehingga bisa menjadi suatu hambatan/ kesalahan menerima pesan karena terdapat keambiguan. Pada kenyataannya *Playfair* chiper juga bisa dikerjakan dengan metode hill chiper. Hill *Cipher* adalah sebuah teknik kriptografi yang menerapkan operasi aritmatika modulo. Metode ini menggunakan sebuah matriks persegi sebagai kunci untuk melakukan proses enkripsi dan dekripsi.

**Dasar Teknik Hill *Cipher***

Teknik Kriptografi Hill *Cipher* pertama kali ditemukan oleh Lester S. Hill pada tahun 1929 (Pardede, dkk., 2017; Rasudin, dkk., 2022). Pada awalnya, teknik tersebut dikembangkan dengan tujuan untuk menciptakan suatu *Cipher* (kode) yang tidak dapat dengan mudah dipecahkan menggunakan teknik analisis frekuensi. Hill *Cipher* tidak mengganti-kan setiap huruf yang sama dalam plaintext dengan huruf lain yang sama dalam *Ciphertext* karena menggunakan operasi perkalian matriks dalam proses enkripsi dan dekripsi. Hill *Cipher*, sebagai teknik kriptografi, termasuk dalam kategori *polyalphabetic Cipher* dan dapat diklasifikasikan sebagai block *Cipher*. Penyebabnya adalah karena teks yang akan dienkripsi atau didekripsi akan dibagi menjadi blok-blok dengan ukuran yang tetap. Setiap huruf atau karakter yang terdapat dalam satu blok akan saling mempengaruhi satu sama lain dalam proses enkripsi dan dekripsi. Oleh karena itu, karakter yang memiliki nilai yang sama tidak akan dienkripsi menjadi karakter dengan nilai yang sama pula (Suriadi, dkk., 2013; Endaryono , dkk., 2021).

Hill *Cipher* merupakan salah satu algoritma kriptografi klasik yang sulit untuk didekripsi oleh kriptanalis hanya dengan menggunakan informasi *Ciphertext* saja. Akan tetapi, teknik ini dapat dengan mudah dipecahkan jika kriptanalis memiliki akses ke berkas *Ciphertext* dan potongan berkas plaintext. Teknik kriptanalisis ini disebut known-plaintext attack (Azhar, dkk., 2017; Rasudin, dkk., 2022).

Dasar dari metode Hill *Cipher* terletak pada penerapan aritmetika modulo pada matriks. Pada prakteknya, Teknik yang digunakan dalam Hill *Cipher* melibatkan operasi perkalian matriks dan inversi matriks. Kunci pada Hill *Cipher* terdiri dari sebuah matriks berukuran n x n, dengan n adalah ukuran blok matriks yang digunakan. Matriks K yang menjadi kunci memiliki sifat inversibel atau dapat diinverskan, atau dengan kata lain memiliki inverse $K^{-1}$ sehingga :

$$K.K^{-1} = I \qquad (1)$$

Alasan mengapa Dalam Hill *Cipher* kunci harus memiliki invers karena matriks invers $(K^{-1})$ digunakan sebagai kunci untuk melakukan proses dekripsi (Hasugian, 2013; Hidayat & Alawiyah, 2013; Laoli, 2018).

**Teknik Enkripsi pada Hill *Cipher***

Pada Hill Cipher, enkripsi dilakukan secara blok demi blok dalam

plaintext. Ukuran blok dalam Hill *Cipher* sama dengan ukuran matriks kunci. Plain text pertama-tama dikonversi menjadi angka, sebelum memecah teks menjadi serangkaian blok-blok. Konversi dilakukan dengan cara merepresentasikan huruf A sebagai angka 1, huruf B direpresentasikan sebagai angka 2, dan seterusnya hingga huruf Y direpresentasikan sebagai angka 25, serta huruf Z diberi nilai 26 atau (0 mod 26) (Andrea, dkk., 2013).

Tabel 1: Konversi Alfabet ke Angka dalam Hill *Cipher*

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

Dalam notasi matematika, proses enkripsi *Hill Cipher* dirumuskan sebagai berikut:

C = K . P mod 26 (2)

C = *Ciphertext*

K = Kunci

P = *Plaintext*

Apabila ada Plain text P yang didefinisikan sebagai P = STRIKE NOW,

*Plain text* tersebut melalui proses konversi terlebih dahulu sehingga berubah menjadi:

$$P = 19\ 20\ 18\ 9\ 11\ 5\ 14\ 15\ 23$$

Langkah selanjutnya adalah melakukan proses enkripsi pada *Plain text* tersebut dengan Hill *Cipher*, yang memanfaatkan kunci K yang berupa matriks berukuran 2×2.

$$K = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$$

Selanjutnya, plaintext dipecah menjadi blok-blok yang masing-masing memiliki panjang 2 karakter. Hal tersebut dilakukan dikarenakan matriks kunci K berordo 2x2. Perhatikan bahwa jumlah plain text tersebut berjumlah ganjil, sehingga karakter terakhir tidak mempunyai pasangan. Dengan demikian, untuk kasus seperti itu, hal yang perlu dilakukan adalah dengan menggandakan karakter terakhir. Kini, teks asli P telah berubah menjadi STRIKENOWW. Blok pertama dari plaintext P yang sudag berubah adalah :

$$P_{1,2} = \begin{bmatrix} 19 \\ 20 \end{bmatrix}$$

Selanjutnya, blok plaintext tersebut akan dienkripsi menggunakan kunci K sebagaimana digambarkan pada persamaan tersebut (2).

$$C_{1,2} = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 20 \end{bmatrix} = \begin{bmatrix} 215 \\ 98 \end{bmatrix}$$

Hasil tersebut belum dituliskan dalam bentuk moulo 26. Apabila hasil tersebut dituliskan dalam modulo 6, diperoleh

$$C_{1,2} = \begin{bmatrix} 215 \\ 98 \end{bmatrix} = \begin{bmatrix} 7 \\ 20 \end{bmatrix} (\text{mod } 26)$$

Seperti yang telah digambarkan pada tabel 1 di atas, dapat dilihat bahwa Huruf G dan huruf T berkorespondensi dengan angka 7 dan 20 pada Hill

*Cipher*. Dengan demikian S berubah menjadi G dan T tetap menjadi T. Setelah melalui proses enkripsi pada setiap blok pada teks asli P maka diperoleh *Ciphertext* C sebagai berikut:

$$P = STRIKENOW$$

$$C = 7\ 20\ 14\ 11\ 7\ 11\ 4\ 21\ 19\ 11$$

$$C = GTNKGKDUS\text{K}$$

Berdasarkan hasil tersebut dapat dilihat teknik *Ciphertext* yang dihasilkan oleh Hill *Cipher* tidak memiliki pola yang dapat dikaitkan dengan plaintext.

**Teknik Dekripsi pada Hill *Cipher***

Pada prinsipnya, proses dekripsi dalam Hill *Cipher* mirip dengan proses enkripsinya. Namun, penting untuk dicatat bahwa matriks kunci harus dapat diinvers terlebih dahulu. Secara matematika, langkah-langkah dekripsi dalam Hill *Cipher* dapat dijelaskan menggunakan persamaan berikut.

$$\begin{aligned} C &= K.P \\ K^{1}.C &= K^{1}.K.P \\ K^{1}.C &= I.P \\ P &= K^{1}.C \end{aligned}$$

Dengan memanfaatkan kunci

$$K = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$$

proses dekripsi dimulai dengan melakukan pencarian invers dari matriks K. Proses pencarian invers tersebut dapat dilakukan dengan menggunakan metode operasi baris elemen atau metode determinan. Dengan demikian diperoleh invers dari matriks K yaitu :

$$K^{-1} = \begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix} = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} (\text{mod } 26)$$

Kunci $K^{-1}$ dipakai dalam melakukan dekripsi dikarenakan

$$K.K^{-1} = \begin{bmatrix} 53 & 234 \\ 26 & 105 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (\text{mod } 26) = I$$

*Ciphertext* C = GTNKGKDUSK, akan didekripsi menggunakan kunci dekripsi $K^{-1}$ yang telah diperoleh di atas. Proses ini dilakukan secara blok per- blok seperti halnya yang dilakukan pada proses enkripsi. Langkah pertama, ubah huruf-huruf pada *Ciphertext* menjadi urutan numerik sebagai berikut.

$$C = 7\ 20\ 14\ 11\ 7\ 11\ 4\ 21\ 19\ 11$$

Langkah selanjutnya dilakukan dengan proses dekripsi sebagai berikut:

$$P_{1,2} = K^{-1}.C_{1,2}$$

$$P_{1,2} = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} . \begin{bmatrix} 7 \\ 20 \end{bmatrix} = \begin{bmatrix} 487 \\ 436 \end{bmatrix} = \begin{bmatrix} 19 \\ 20 \end{bmatrix} (\text{mod } 26)$$

Untuk blok kedua, adalah sebagai berikut:

$$P_{3,24} = K^{-1}.C_{3,4}$$

$$P_{3,4} = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} . \begin{bmatrix} 14 \\ 11 \end{bmatrix} = \begin{bmatrix} 278 \\ 321 \end{bmatrix} = \begin{bmatrix} 18 \\ 9 \end{bmatrix} (\text{mod } 26)$$

Sesudah setiap blok selesai didekripsi, maka diperoleh hasil plaintext sebagai berikut

$$P = 19\ 20\ 18\ 9\ 11\ 5\ 14\ 15\ 23$$

$$P = STRIKENOW$$

## METODE PENELITIAN

### Jenis Penelitian

Penelitian ini termasuk dalam kategori penelitian eksperimental. Melalui eksperimen, penelitian ini bertujuan untuk menguji efektivitas dan keamanan penggunaan matriks ordo $7 \times 4$ dan

Hill *Cipher* dalam modifikasi metode *Playfair Cipher*.

**Waktu dan Tempat Penelitian**

Penelitian ini dilaksanakan di departemen matematika FMIPA Unpad.

**Target/Subjek Penelitian**

Sasaran penelitian ini adalah meningkatkan keamanan dan efisiensi metode *Playfair Cipher* melalui penggunaan matriks ordo $7 \times 4$ dan Hill *Cipher*. Selain itu, penelitian ini juga ditujukan untuk menghasilkan modifikasi metode *Playfair Cipher* yang lebih robust terhadap serangan kriptanalisis.

**Prosedur**

1. Mengumpulkan data awal terkait dengan metode *Playfair Cipher* yang akan menjadi dasar perbandingan dengan hasil modifikasi.
2. Menerapkan modifikasi metode *Playfair Cipher* dengan menggunakan matriks ordo $7 \times 4$ dan Hill *Cipher*.

**Data, Intrumen, dan Teknik Pengumpulan Data**

Instrumen pengumpulan data mencakup software simulasi kriptografi, dokumen-dokumen terkait metode *Playfair Cipher*, matriks ordo $7 \times 4$, dan Hill *Cipher*. Teknik pengumpulan data melibatkan eksperimen dan simulasi menggunakan perangkat luna k khusus kriptografi.

**Teknik Analisis Data**

Analisis data dilakukan dengan membandingkan hasil modifikasi dengan metode *Playfair Cipher* asli. Teknik analisis melibatkan evaluasi keamanan, efisiensi, dan ketahanan terhadap serangan. Selain itu, data juga akan dianalisis menggunakan metode statistik untuk mengukur signifikansi perbedaan antara kedua metode. Secara khusus, dalam analisis statistik, kami akan mengevaluasi perbedaan dalam distribusi frekuensi simbol-simbol pada teks *Ciphertext* antara metode modifikasi dan metode *Playfair Cipher* asli. Hal ini bertujuan untuk mengetahui apakah terdapat perbedaan signifikan dalam distribusi simbol-simbol antara kedua metode tersebut. Analisis ini penting untuk menunjukkan efektivitas modifikasi yang diusulkan dalam meningkatkan kerahasiaan dan keamanan data, serta untuk memastikan bahwa perubahan yang dilakukan tidak mengorbankan efisiensi atau ketahanan terhadap serangan kriptanalisis. Dengan menggunakan metode statistik, kami dapat secara objektif mengukur dan mengevaluasi dampak dari modifikasi yang diusulkan terhadap kinerja keseluruhan dari sistem kriptografi yang dikembangkan.

## HASIL PENELITIAN DAN PEMBAHASAN

Matriks $7 \times 4$ diperluas dengan penambahan simbol "*" untuk menggantikan huruf yang berulang dan simbol "#" untuk mengisi kekosongan pada huruf/pasangan terakhir. Dengan demikian, untuk contoh yang sama seperti di atas, dengan menggunakan metode ini, hasilnya adalah:

| | | | |
|---|---|---|---|
| C | I | P | H |
| E | R | A | B |
| D | F | G | J |
| K | L | M | N |
| O | Q | S | T |
| U | V | W | X |
| Y | Z | * | # |

Plaintext:

LO VE AL LP EO PL E#

*Ciphertext* :

KQ UR RM MI DU IM BY

Jika dibalik, dari *Ciphertext* akan dicari plaintextnya maka akan menjadi :

| KQ | UR | RM | MI | DU | IM | BY |
|---|---|---|---|---|---|---|
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| LO | VE | AL | LP | EO | PL | E# |
| LO | VE | AL | LP | EO | PL | E |

Tidak terdapat keambiguan atau 2 penafsiran, sehingga metode ini baik untuk digunakan. Bagaimana jika matriks yang digunakan ialah matriks berordo 4x7?

Kita bentuk matriks dari contoh sebelumnya dengan ordo 4x7.

| | | | | | | |
|---|---|---|---|---|---|---|
| C | I | P | H | E | R | A |
| B | D | F | G | J | K | L |
| M | N | O | Q | S | T | U |
| V | W | X | Y | Z | * | # |

Selanjutnya akan dienkripsi LOVE ALL PEOPLE

| LO | VE | AL | LP | EO | PL | E# |
|---|---|---|---|---|---|---|
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| FU | ZC | LU | FA | PS | AF | AZ |

Sehingga diperoleh *Ciphertext* nya FUZCLUFAPSAFAZ. Tahap selanjutnya adalah melakukan analisis perbedaan antara *Ciphertext* dengan matriks $7 \times 4$ dan matriks $4 \times 7$.

| Matriks | *Ciphertext* | Simpangan baku* |
|---|---|---|
| $7 \times 4$ | KQURRMMIDUIMBY | 6.596702 |
| $4 \times 7$ | FUZCLUFAPSAFAZ | 9.488281 |

* nilai simpangan baku ini didapatkan dengan mengkonversi huruf-huruf dalam *Ciphertext* ke dalam bilangan bulat modulo 28 dan dicari simpangan bakunya dari huruf-huruf yang ada dalam *Ciphertext* tersebut.

Dari data di atas dapat disimpulkan bahwa variasi dari *Ciphertext* matriks $4 \times 7$ lebih besar dari matriks $7 \times 4$, sehingga modifikasi *Playfair Cipher* dengan matriks $4 \times 7$ lebih baik dalam kasus ini dibandingkan dengan matriks $7 \times 4$.

Kesimpulan di atas tidak dapat dinyatakan sebagai kesimpulan yang bersifat universal atau umum untuk semua situasi. Terdapat kemungkinan bahwa kasus sebaliknya juga dapat terjadi, di mana matriks $7 \times 4$ lebih efektif daripada matriks $4 \times 7$ dalam metode *Playfair* , bahkan ada situasi di mana keduanya memiliki kinerja yang setara. Oleh karena itu, kesimpulan yang dapat kita tarik adalah bahwa tidak mungkin menentukan secara pasti mana yang lebih baik antara matriks $7 \times 4$ dan $4 \times 7$ dalam konteks metode *Playfair* Cipher. Faktor-faktor tertentu, seperti kata kunci yang digunakan dan teks asli yang akan dienkripsi, dapat memengaruhi kinerja dari masing-masing matriks. Oleh karena itu, dalam penelitian ini, kami akan melanjutkan pembahasan dengan menggunakan matriks *Playfair* $7 \times 4$.

## MODIFIKASI DENGAN HILL *CIPHER*

Setelah dilakukan modifikasi *Playfair* menggunakan matriks $7 \times 4$, akan dilakukan penambahan metode Hill *Cipher* untuk mempersulit proses enkripsi dan dekripsi. Untuk kasus ini kami akan menggunakan Hill-2-*Cipher* untuk proses enkripsi dan dekripsinya. Cara enkripsinya ialah:

1. *Ciphertext* yang dihasilkan dari cara modifikasi *Playfair Cipher*

dilakukan proses penekripsian Hill-2-*Cipher* dengan mengelompokkannya ke dalam pasangan huruf dan mengkonversikan huruf-huruf tersebut ke dalam bilangan bulat mod 28.

2. Pilih matriks enkripsi. Matriks enkripsi ini didapat dari keyword awal yang hendak dibuat. Sehingga keyword tidak bisa sembarangan untuk dapat mencapai proses ini. Ketentuannya ialah, di dalam keyword haruslah terdapat 4 huruf yang bersesuaian dengan bilangan bulat mod 28 yang invertible.
3. Lakukan proses pengalian antara matriks enkripsi dan vektor pasangan huruf untuk mendapatkan *Ciphertext* baru.

Sebagai gambaran, perhatikan kasus berikut. Gunakan keyword: *CIPHER* dan *Ciphertext* (1) nya:

KQURRMMIDUIMBY

Pada tahap ini akan dilakukan pengelompokan *Ciphertext* (1) ke dalam pasangan huruf

KQ UR RM MI DU IM BY

Selanjutnya, akan dikonversikan pasangan huruf di atas ke dalam bilangan bulat mod 26

11 17 21 18 18 13 13 9 4 21 9 13 2 25

Kemudian akan dituliskan vektor untuk pasangan huruf

$$c_1 = \begin{pmatrix}11\\17\end{pmatrix}, c_2 = \begin{pmatrix}21\\18\end{pmatrix}, c_3 = \begin{pmatrix}18\\13\end{pmatrix},$$
$$c_4 = \begin{pmatrix}13\\9\end{pmatrix}, c_5 = \begin{pmatrix}4\\21\end{pmatrix}, c_6 = \begin{pmatrix}9\\13\end{pmatrix}, c_7 = \begin{pmatrix}2\\25\end{pmatrix}$$

Pilih matriks enkripsi dari keyword *CIPHER*. Akan dikonversi keyword ke dalam bilangan bulat mod 28

3 9 16 8 5 18

Dari bilangan bulat di atas akan dipilih 4 huruf berurutan yang dapat digunakan untuk proses enkripsi. Pilih 4 angka dengan angka pertama dan keempatnya ialah bilangan yang memiliki invers mod 28. Dari keyword di atas dipilihlah IPHE. Sehingga matriks enkripsinya ialah

$$A = \begin{bmatrix}9 & 16\\8 & 5\end{bmatrix}$$

Selanjutanya, akan dicari *Ciphertext* baru dengan mengalikan matriks $A$ dengan vektor $c$.

$$c_1' = \begin{pmatrix}9 & 16\\8 & 5\end{pmatrix}\begin{pmatrix}11\\17\end{pmatrix} = \begin{pmatrix}371\\173\end{pmatrix} = \begin{pmatrix}7\\5\end{pmatrix} mod\ 28$$
$$c_2' = \begin{pmatrix}9 & 16\\8 & 5\end{pmatrix}\begin{pmatrix}21\\13\end{pmatrix} = \begin{pmatrix}477\\258\end{pmatrix} = \begin{pmatrix}1\\6\end{pmatrix} mod\ 28$$
$$c_3' = \begin{pmatrix}9 & 16\\8 & 5\end{pmatrix}\begin{pmatrix}18\\13\end{pmatrix} = \begin{pmatrix}370\\209\end{pmatrix} = \begin{pmatrix}6\\13\end{pmatrix} mod\ 28$$
$$c_4' = \begin{pmatrix}9 & 16\\8 & 5\end{pmatrix}\begin{pmatrix}13\\9\end{pmatrix} = \begin{pmatrix}261\\149\end{pmatrix} = \begin{pmatrix}9\\9\end{pmatrix} mod\ 28$$
$$c_5' = \begin{pmatrix}9 & 16\\8 & 5\end{pmatrix}\begin{pmatrix}4\\21\end{pmatrix} = \begin{pmatrix}372\\137\end{pmatrix} = \begin{pmatrix}8\\25\end{pmatrix} mod\ 28$$
$$c_6' = \begin{pmatrix}9 & 16\\8 & 5\end{pmatrix}\begin{pmatrix}9\\13\end{pmatrix} = \begin{pmatrix}289\\137\end{pmatrix} = \begin{pmatrix}9\\25\end{pmatrix} mod\ 28$$
$$c_7' = \begin{pmatrix}9 & 16\\8 & 5\end{pmatrix}\begin{pmatrix}2\\25\end{pmatrix} = \begin{pmatrix}418\\141\end{pmatrix} = \begin{pmatrix}26\\1\end{pmatrix} mod\ 28$$

Kemudian akan dikonversi bilangan-bilangan di atas ke dalam huruf.

7 5 1 6 6 13 9 9 8 25 9 25 26 1

G E A F F M I I H Y I Y Z A

Dengan demikian diperoleh *Ciphertext* barunya ialah

GEAFFMIIHYIYZA.

Bandingkan *Ciphertext* sebelumnya dan *Ciphertext* yang baru

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sebelum | K | Q | U | R | R | M | M | I | D | U | I | M | B | Y |
| Sesudah | G | E | A | F | F | M | I | I | H | Y | I | Y | Z | A |

Terdapat perbedaan yang cukup signifikan sehingga modifikasi dengan menambahkan metode Hill-2-*Cipher* akan mempersulit proses dekripsi dan tentu sulit untuk bagi hacker untuk menebaknya.

Selanjutnya akan dilakukan proses dekripsi dari contoh di atas dengan cara:

1. *Ciphertext* dikelompokkan ke dalam pasangan huruf dan konversikan huruf-huruf tersebut ke dalam bilangan bulat mod 28.
2. Pilih matriks dekripsi. Matriks dekripsi ini didapat dari hasil invers matriks mod 28 atas keyword yang diberikan. Tidak sembarangan keyword digunakan. Pilihlah 4 huruf dari keyword yang bersesuaian dengan bilangan bulat mod 28 yang invertible.
3. Lakukan proses pengalian antara matriks dekripsi dan vektor pasangan huruf untuk mendapatkan *Ciphertext* (1) yang selanjutnya dilakukan proses dekripsi dengan metode modifikasi *Playfair Cipher* dengan matriks $7 \times 4$.

Perhatikan kembali contoh kasus berikut. Misalkan

*Ciphertext* : GEAFFMIIHYIYZA

Keyword : *CIPHER*

Tahap selanjutnya adalah pengelompokkan *Ciphertext* ke dalam pasangan huruf

GE AF FM II HY IY ZA

Kemudian, akan dikonversikan pasangan huruf ke dalam bilangan bulat mod 28

7 5 1 6 6 13 9 9 8 25 9 25 26 1

Selanjutnya, akan dituliskan vektor untuk pasangan bilangan di atas

$$c_1' = \begin{pmatrix} 7 \\ 5 \end{pmatrix}, c_2' = \begin{pmatrix} 1 \\ 6 \end{pmatrix}, c_3' = \begin{pmatrix} 6 \\ 13 \end{pmatrix},$$

$$c_4' = \begin{pmatrix} 9 \\ 9 \end{pmatrix}, c_5' = \begin{pmatrix} 8 \\ 25 \end{pmatrix}, c_6' = \begin{pmatrix} 9 \\ 25 \end{pmatrix}, c_7' = \begin{pmatrix} 26 \\ 1 \end{pmatrix}$$

Pilih matriks dekripsi Dari keyword *CIPHER* akan dikonversikan ke dalam bilangan bulat mod 28

3 9 16 8 5 18

Kemudian akan dipilih 4 bilangan yang angka pertama dan keempatnya memiliki invers mod 28

9 16 8 5

Dengan demikian diperoleh matriks enkripsinya

$$A = \begin{bmatrix} 9 & 16 \\ 8 & 5 \end{bmatrix}$$

Kemudian akan dicari matriks dekripsinya dengan menginverskan matriks $A$

$$\left(\begin{array}{cc|cc} 9 & 16 & 1 & 0 \\ 8 & 5 & 0 & 1 \end{array}\right) 25b_1 \sim \left(\begin{array}{cc|cc} 1 & 8 & 25 & 0 \\ 8 & 5 & 0 & 1 \end{array}\right) mod\ 28$$

$$20b_1 + b_2 \sim \left(\begin{array}{cc|cc} 1 & 8 & 25 & 0 \\ 0 & 25 & 24 & 1 \end{array}\right) mod\ 28$$

$$9b_2 \sim \left(\begin{array}{cc|cc} 1 & 8 & 25 & 0 \\ 0 & 1 & 20 & 9 \end{array}\right) mod\ 28$$

$$20b_2 + b_1 \sim \left(\begin{array}{cc|cc} 1 & 0 & 5 & 12 \\ 0 & 1 & 20 & 9 \end{array}\right) mod\ 28$$

Dengan demikian, diperoleh matriks dekripsinya ialah

$$A^{-1} = \begin{bmatrix} 5 & 12 \\ 20 & 9 \end{bmatrix}$$

Kemudian akan dicari $c_1, c_2, \dots, c_7$ dengan $c_1 = A^{-1} \cdot c_1', c_2 = A^{-1} \cdot c_2', \dots, c_7 = A^{-1} \cdot c_7'$

$$c_1 = \begin{pmatrix} 5 & 12 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 5 \end{pmatrix} = \begin{pmatrix} 95 \\ 185 \end{pmatrix} = \begin{pmatrix} 11 \\ 17 \end{pmatrix} mod\ 28$$

$$c_2 = \begin{pmatrix} 5 & 12 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 6 \end{pmatrix} = \begin{pmatrix} 77 \\ 74 \end{pmatrix} = \begin{pmatrix} 21 \\ 18 \end{pmatrix} mod\ 28$$

$$c_3 = \begin{pmatrix} 5 & 12 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 13 \end{pmatrix} = \begin{pmatrix} 186 \\ 237 \end{pmatrix} = \begin{pmatrix} 18 \\ 13 \end{pmatrix} mod\ 28$$

$$c_4 = \begin{pmatrix} 5 & 12 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 9 \\ 9 \end{pmatrix} = \begin{pmatrix} 153 \\ 261 \end{pmatrix} = \begin{pmatrix} 13 \\ 9 \end{pmatrix} mod\ 28$$

$$c_5 = \begin{pmatrix} 5 & 12 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 8 \\ 25 \end{pmatrix} = \begin{pmatrix} 340 \\ 385 \end{pmatrix} = \begin{pmatrix} 4 \\ 21 \end{pmatrix} mod\ 28$$

$$c_6 = \begin{pmatrix} 5 & 12 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 9 \\ 25 \end{pmatrix} = \begin{pmatrix} 345 \\ 405 \end{pmatrix} = \begin{pmatrix} 9 \\ 13 \end{pmatrix} mod\ 28$$

$$c_7 = \begin{pmatrix} 5 & 12 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 26 \\ 1 \end{pmatrix} = \begin{pmatrix} 142 \\ 529 \end{pmatrix} = \begin{pmatrix} 2 \\ 25 \end{pmatrix} mod\ 28$$

Pada tahap ini akan dikonversi $c_1, c_2, .., c_7$ menjadi *Ciphertext* (1)

11 17 21 18 18 13 13 9 4 21 9 13 2 25

dengan,

K Q U R R M M I D U I M B Y

Kemudian akan dicari plaintext dari *Ciphertext* (1) di atas dengan menggunakan metode modifikasi *Playfair Cipher* dengan matriks $7 \times 4$

Dengan keyword *CIPHER*, akan dibentuk matriks $7 \times 4$ nya

| | | | |
|---|---|---|---|
| C | I | P | H |
| E | R | A | B |
| D | F | G | J |
| K | L | M | N |
| O | Q | S | T |
| U | V | W | X |
| Y | Z | * | # |

Terakhir, akan didekripsikan huruf

KQ UR RM MI DU IM BY

Dengan menggunakan metode *Playfair* diperoleh

LO VE AL LP EO PL E#

Dengan demikian didapat *plaintext*nya ialah LOVE ALL PEOPLE

## ANALISIS KRIPTOGRAFI

Dalam kriptografi, kebingungan dan difusi memainkan peranan penting dalam pengembangan sebuah *Cipher*. Kebingungan mengacu pada membuat hubungan sekompleks mungkin antara kunci dan *Ciphertext* dan dapat diselesaikan dengan transposisi. Di sisi lain difusi mengacu pada membuat hubungan sekompleks mungkin antara plaintext dan *Ciphertext* . Kebingungan dan difusi yang kuat membuatnya sulit bagi attacker untuk menemukan kunci atau plaintext jika attacker mempunyai banyak pasangan plaintext dan *Ciphertext* .

Seperti *Playfair Cipher*, algoritma yang disajikan dalam makalah ini juda dapat dengan mudahnya dipecahkan jika seseorang memiliki pasangan *Ciphertext* dan plaintext yang cukup.

## SIMPULAN DAN SARAN

Modifikasi *Playfair Cipher* dilakukan dengan mengubah matriks 5x5 menjadi matriks $7 \times 4$ dengan menambahkan simbol “*” dan “#” sehingga menimbulkan korespondensi satu-satu antara plaintext dan *Ciphertext* yang bertujuan untuk mempermudah proses enkripsi dan dekripsi serta tidak menimbulkan keambiguan dalam menafsirkan pesan. Metode ini juga dapat digunakan untuk bahasa apapun dengan mengganti matriksnya menjadi matriks yang proporsional dengan huruf pada bahasa tersebut. Penambahan metode Hill *Cipher* dalam proses kriptografi membuat *Ciphertext* lebih sulit untuk dipecahkan dan bilangan modulo 28 digunakan dalam prosesnya menyesuaikan dengan matriks *Playfair* ordo $7 \times 4$.

## DAFTAR PUSTAKA

Mukhtar, H. (2018). Kriptografi untuk Keamanan Data. Deepublish

Hasugian, B. S. (2017). Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah. Warta Dharmawangsa, (53).

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer, 10(1), 20-31.

Sinaga, I. P. (2021). Implementasi Kriptografi Hybrid Algoritma Elgamal Dan Double Playfair Cipher Dalam Pengamanan File Jpeg Berbasis Dekstop. Journal of Informatics, Electrical and Electronics Engineering, 1(2), 67-74.

Suriadi, R., Satra, R., & Fattah, F. (2020). Peningkatan Keamanan Data dengan Menggunakan Equation pada Metode Playfair Cipher. Buletin Sistem Informasi dan Teknologi Islam (BUSITI), 1(4), 266-269.

Suhelna, Y. (2020). Perancangan Aplikasi Penyandian Pesan Teks dengan Menggunakan Algoritma Digraph Cipher. JUKI: Jurnal Komputer dan Informatika, 2(1), 25-34.

Pristiwanto, M. (2019). Perancangan Aplikasi Enkrisi Dan Deskripsi Teks Menggunakan Algoritma Playfair Cipher Berbasi Web (Doctoral Dissertation, Universitas Labuhanbatu).

Syahputra, A. (2018). Analisa Implementasi Pengamanan Fileaudio Menggunakan Algoritma Playfair. Pelita Informatika: Informasi dan Informatika, 7(2), 130-137.

Mu'mi, N. F. A. (2017). Steganografi Citra Menggunakan Kriptografi Hybrid Playfair Cipher Dan Caesar Cipher (Doctoral dissertation, FMIPA).

Pardede, A. M. H., Manurung, H., & Filina, D. (2017). Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Keamanan Data Pada File Dokumen. JTIK (Jurnal Teknik Informatika Kaputama), 1(1), 26-33.

Rasudin, R., Zulfan, Z., & Rizki, P. (2022). Analisis Perbandingan Keamanan Kriptografi Klasik Pada Algoritma Secure Hill Cipher Berbasis Kode ASCII Dan Monoalphabetic. Jurnal Teknologi Terapan and Sains 4.0, 3(1), 729-742.

Hasugian, A. H. (2013). Implementasi Algoritma Hill Cipher Dalam Penyandian Data. Pelita Informatika Budi Darma, 4(2), 115-122.

Endaryono, E., Dwitiyanti, N., & Setiawan, H. S. (2021). Aplikasi Operasi Matriks pada Perancangan Simulasi Metode Hill Cipher Menggunakan Microsoft Excel. STRING (Satuan Tulisan Riset dan Inovasi Teknologi), 6(1), 41-49.

Azhar, W. Y., Supriyadi, S., & Yanitasari, Y. (2017). Kriptanalisis Hill Cipher Terhadap Known Plaintext Attack Menggunakan Metode Determinan Matriks Berbasis Android. Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer, 8(2), 579-592.

Rasudin, R., Zulfan, Z., & Rizki, P. (2022). Analisis Perbandingan Keamanan Kriptografi Klasik Pada Algoritma Secure Hill Cipher Berbasis Kode Ascii Dan Monoalphabetic. Jurnal Teknologi Terapan and Sains 4.0, 3(1), 729-742.

Hasugian, A. H. (2013). Implementasi Algoritma Hill Cipher Dalam Penyandian Data. Pelita Informatika Budi Darma, 4(2), 115-122.

Hidayat, A., & Alawiyah, T. (2013). Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang. Jurnal Matematika Integratif ISSN, 1412, 6184.

Laoli, D. (2018). Penerapan Algoritma Hill Cipher Dan Least Significant Bit (LSB) Untuk Pengamanan Pesan Pada Citra Digital. Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI), 1(2), 30-40.

Andrea, K., Wardana, A., Wanandi, B. S., & Ikhwan, A. (2023). Penerapan Kriptografi Caesar Cipher Pada Fitur Aplikasi Chatting Whatsapp. Jurnal Penelitian Dan Pengkajian Ilmiah Eksakta, 2(1), 6-11.

Kabetta, H. (2017). Analisis Kompleksitas Waktu Algoritma Kriptografi Elgamal Dan Data Encryption Standard. *Teknikom: Teknologi Informasi, Ilmu Komputer dan Manajemen*, *1*(1), 13-18.

Arrijal, I. M. A., Efendi, R., & Susilo, B. (2016). Penerapan Algoritma

Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks. *Pseudocode*, *3*(1), 69-82

Amin, M. M. (2016). Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks. *Pseudocode*, *3*(2), 129-136.

Pradipta, G. A. (2016). Penerapan Kombinasi Metode Enkripsi Vigenere Chiper Dan Transposisi Pada Aplikasai Client Server Chatting. *Jurnal Sistem dan Informatika (JSI)*, *10*(2), 119-127.

Umar, R., & Yudhana, A. (2020). Implementation of Playfair Cipher and Least Significant Bit Algorithms in Digital Imagery. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *4*(3), 454-461.