JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY)
Vol. 2, No. 1, Maret 2022

Analisa Algoritma Kriptografi Klasik Caesar Cipher Viginere Cipher dan Hill Cipher – *Study Literature*

Noviyanti. P[1], Mira[2]
[1]Teknologi Informasi, Institut Shanti Bhuana
[2]Magister Sistem Informasi, Universitas Kristen Satya Wacana
[1]noviyanti@shantibhuana.ac.id, [2]miracle.yaa@gmail.com,

***Abstract*— The process of encryption and description of a message is a third party called cryptography. Cryptography is a technique for securely transferring information between two parties without intervention by external elements. The process of securing information can be done with several available cryptographic algorithms. Cryptographic algorithms consist of two eras, namely, classical algorithms and modern algorithms. Classical algorithms were generally used in the past using only substitution and permutation methods. While modern algorithms are algorithms that can be recognized, read and understood by computers that produce the numbers 0 and 1 or commonly called binary data. The purpose of the analysis is to determine the development of security and complexity of standard classical algorithms and classical algorithms with modifications.**

***Intisari*— Proses ekripsi dan deskripsi suatu pesan merupakan pihak ketiga yang disebut kriptografi. Kriptografi adalah teknik untuk mentransfer informasi secara aman antara dua pihak tanpa diintervensi oleh elemen eksternal. Proses pengaman informasi dapat dilakukan dengan beberapa algoritma kriptografi yang tersedia. Algoritma kriftografi terdiri dari dua era yaitu, algoritma klasik dan algoritma modern. Algoritma klasik pada umumnya digunakan pada jaman dulu dengan hanya menggunakan metode subtitusi dan permutasi. Sedangkan algoritma modern adalah algoritma yang dapat dikenali, dibaca dan dimengerti oleh komputer yang menghasilkan angka 0 dan 1 atau biasa disebut data biner. Tujuan analisis untuk mengetahui perkembangan keamanan dan kompleksitas algoritma klasik standar dan algoritma klasik dengan modifikasi.**

***Kata Kunci*— Classical Cryptography, Caesar Cipher, Vigenere Cipher, Hill Cipher**

I. PENDAHULUAN

Penyandian pesan merupakan upaya dalam mengamankan data atau informasi untuk menghindari terjadinya peretasan oleh pihak yang tidak bertanggungjawab. Sehingga pemilik pesan berupaya untuk melakukan penyandian terhadap pesan yang hendak dibagi kepada penerima pesan dengan terlebih dahulu melakukan enkrispi dan deskripi pesan. Proses ekripsi dan deskripsi suatu pesan merupakan pihak ketiga yang disebut kriptografi.

Kriptografi adalah teknik untuk mentransfer informasi atau pesan secara aman antara dua pihak yaitu pengirim dan penerima pesan atau informasi tanpa diintervensi oleh elemen eksternal[1]. Pengirim pesan harus dapat memastikan bahwa pesan yang dikirim benar-benar terjaga keamanan, tidak ada informasi yang diganti atau dikurangi, sehingga informasi sampai kepada penerima sesuai dengan keadaan semula dari pengirim informasi. Proses pengaman informasi dapat dilakukan dengan beberapa algoritma kriptografi yang tersedia. Algoritma kriftografi terdiri dari dua era yaitu, algoritma klasik dan algoritma modern. sedangkan kunci pada kriptografi terdiri dari kunci private dan kunci publik.

Algoritma klasik pada umumnya digunakan pada jaman dulu dengan hanya menggunakan metode subtitusi dan permutasi[2]. Sedangkan algoritma modern adalah algoritma yang dapat dikenali, dibaca dan dimengerti oleh komputer yang menghasilkan angka 0 dan 1 atau biasa disebut data biner. Sedangkan untuk kunci private merupakan kunci yang sama yang digunakan oleh pengirim dan penerima dalam melakukan enkripsi dan deskripi pesan. Sedangkan kunci modern merupakan kunci yang berbeda dalam melakukan enkripsi dan deskripsi pesan oleh pengirim pesan dan penerima pesan.

Berdasarkan uraian algoritma kriptogrfi klasik standar, dilakukan analisis berupa study literatur untuk mengetahui perkembangan keamanan dan kompleksitas algoritma klasik standar dan algoritma klasik dengan modifikasi. Adapun berikut ini beberapa penelitian terdahulu yang berkaitan dengan algoritma kriptografi klasik standar yang melakukan penyandian data pesan teks, file dan citra.

Pada penelitian terdahulu pertama oleh Kartika dan Yudi, yang melakukan pengamanan pesan dengan algoritma Caesar Cipher. Tujuan yang ingin dicapai penulis yaitu dapat meningkatkan keamanan pesan berbasis QRCode pada android. Proses enkripsi dengan melakukan pergeseran huruf ke kanan atau ke kiri dengan kunci yang diinginkan. Sedangkan proses deskripsi yang merupakan upaya untuk melakukan pemecahan sandi menggunakan proses sebaliknya dengan kunci yang sama kemudian dilakukan pengurangan terhadap plaintext dan key[3].

Penelitian terdahulu kedua oleh Susianto dan Mustika, yang melakukan perancangan sistem inventory menggunakan algoritma Caesar Cipher. Tujuan yang ingin dicapai penulis yaitu dapat melakukan pengamananan database inventory daftar obat, dengan melakukan enkrispi nama obat saat diinputkan kedatabase dengan key yang diinginkan. Sedangkan proses deskripsi merupakan kebalikan dari proses enkripsi. Kemudian merancang sebuah sistem aplikasi menggunakan bahasa PHP dan MYSQL untuk memudahkan proses enkripsi dan deskripsi pada database obat[4].

Penelitian terdahulu ketiga oleh Alasi dan Siahaan yang melakukan penyandian record pada database menggunakan algoritma Vigenere Cipher. Tujuan yang

diingin dicapai penulis yaitu dapat melakukan penyandian record aktivitas informasi pada database berdasarkan kunci yang diinputkan pengguna pada sebuah sistem aplikasi. Dengan proses analisa Vigenere Cipher menggunakan tabel 26 x 26 yang terdiri alfabet A sampai Z. Kemudian melakukan perancangan sistem dengan visual basic untuk dapat melakukan penyadian record informasi pada database PHPMyAdmin. Sehingga dihasilkan sebuah sistem aplikasi penyandian record informasi menggunakan visual basic[5].

Penelitian terdahulu keempat oleh Prasetyo dkk, yang melakukan perancanagan absensi online dengan algoritma Vigenere Cipher. Dengan tujuan dapan memudahkan absensi karyawan dan rekapitulasi kehadiran oleh admin. Proses absensi dengan menggunakan QRCode, yang dirancang menggunakan bahasa PHP, MySQL dan framework codeigniter. Sehingga dihasilkan sebuah sistem aplikasi absensi yang terdiri dari fitur pengguna, kehadiran, data karyawan, jadwal dan lokasi kerja[6].

Penelitian terdahulu kelima oleh Sholahudin dan Asmunin, yang melakukan implementasi enkripsi dan deskripsi citra berwarna menggunakan Hill Cipher. Dengan tujuan mengenkripsi deskripsi gambar untuk menghindari kejahatan dunia maya dengan memodifikasi padding gambar. Proses enkripsi dengan menambahkan padding pada piksel yang ganjil, sedangkan apabila genap, maka tidak perlu ditambahkan. Selanjutnya penulis merancang sistem menggunakan bahasa python sebagai upaya memudahkan proses enkripsi dan deskripsi citra. Sehingga dihasilkan sebuah sistem aplikasi yang dapat melakukan enkripsi deskripsi citra berwarna menggunakan python[7].

Penelitian terdahulu keenam oleh Siahaan dan Widodo, yang melakukan penyandian terhadap file teks dan citra menggunakan algoritma Hill Cipher. Dengan tujuan menjaga kerahasiaan terhadap pengiriman file teks dan citra berbasis android. Hasil sistem memberikan ciphertext dan cipherimage yang tidak dapat dipahami dengan kasat mata. Adapun proses enkripsi mengubah file teks atau citra menjadi kunci matriks, file teks akan di modulo dengan mod 26 sedangkan citra akan dimodulokan dengan mod 256. Selanjutnya matriks dirubah menjadi data array. Sehingga dihasilkan sebuah sistem android yang dapat melakukan proses enkripsi deskripsi file teks dan citra menggunakan algoritma Hill Cipher dengan memperhatikan batasan maks pixel citra yang diinputkan[8].

Berdasarkan keenam penelitian terdahulu, yang melakukan penyandian data, baik data pesan atau informasi, file teks dan citra dengan algoritma klasik yang terdiri dari algoritma Caesar Cipher, Vigenere Cipher dan Hill Cipher, bahwa secara keseluruhan struktur penulisan paper sudah baik, sehingga pembaca dapat memahami tujuan dan hasil yang dipaparkan dalam paper tersebut dengan membaca topik, abstrak dan kesimpulanya. Hal ini ditunjukan dengan keselarasan antara judul, abstark dan kesimpulan yang saling berkaitan, tujuan permasalahan yang terjawab pada hasil dan analisis. Selan itu dari segi teoritis juga dijelaskan, baik pengertian teori yang digunakan, metode yang sesuai dengan topik penelitian dan ruang lingkup penelitian yang jelas objeknya.

Namun dalam penelitian ini, yang membahas kriptografi dengan proses enkripsi dan deskripsi baik pesan teks, file dan citra, diperlukan membaca secara serius, teliti dan jeli pada proses enkripsi dan deskripsi yang dihasilkan agar dapat memahami secara mendalam proses enkripsi dan deskripsi yang dihasilkan. Berdasarkan penelitian terdahulu, yang melakukan beberapa penyandian data seperti pesan teks, file dan citra yang menggunakan satu algoritma tertentu bila dikaitkan dengan beberapa penelitian terdahulu yang membahas pengamanan data atau informasi baik pesan teks, file dan citra menggunakan satu algoritma dianggap memiliki keamanan yang rentan, serta berdasarkan beberapa penelitian terdahulu yang menyatakan tingkat keamanan algoritma kriptografi klasik lebih rentan dari algoritma kriptografi klasik [9], hal ini dikarenakan algoritma klasik sudah ada sejak lama, dengan teknologi yang terus berkambang membuat algoritma tersebut dapat dipecahkan oleh cryptanalysis, dengan menggunakan beberapa percobaan selain itu dapat menggunakan exhaustive key search[9]. Oleh karena itu, dilakukan study literatur terhadap perkembangan algoritma kriptografi klasik.

II. METODOLOGI PENELITIAN

Metode penelitian yang berkaitan dengan algoritma kriptografi klasik untuk melihat kembali teori, proses dan kontribusi yang dihasilkan. Oleh krena itu, dilakukan review terhadap beberpa penelitian terdahulu yang membahas algoritma kriptografi klasik. Review dilakukan sebagai upaya untuk melihat kesesuaian antara topik, permasalahan, teori yang menunjang, tujuan, hasil dan kontribusi yang dipaparkan. Serta memberikan tanggapan yang disertai dengan referensi yang menunjang sebagai dasar untuk memberikan tanggapan sebagai perbaikan paper dan peneliti selanjutnya. Kemudian memberikan saran berdasarkan kekurangan yang ditemukan yang didasari oleh referensi yang jelas dan sepadan. Selan itu, analisis ini juga sebagai upaya untuk dapat memahami algoritma kriptografi klasik untuk melihat pemforma dan kinerja dari algoritma klasik. Sehingga didapatkan kebaharuan dari proses algoritma berdasarkan kontribusi yang dihasilkan penelitian terdahulu.

III. HASIL DAN PEMBAHASAN

A. *Study Literatur*

Study literature merupakan proses mencari mendapatkan dan mengumpulkan referensi dari berbagai sumber dengan teori yang dapat mendukung proses penelitian, analisis dibeberapa penelitian terdahulu untuk dapat mengetahui informasi yang terkandung didalam paper. Proses *study literature* dengan mengumpulkan paper yang seseuai yang memiliki topik atau algoritma yang sama, dalam hal ini algoritma kriptografi klasik, yang digunakan sebagai dasar referensi perkembangan kriptogrfi klasik yang dimodifikasi.

Perkembangan teknologi yang semakin meningkat,

JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY)
Vol. 2, No. 1, Maret 2022

memberikan pengaruh terhadap beberapa algoritma lama, dalam hal ini algoritma kriptografi klasik. Beberapa penelitian mengagap algoritma kriptografi klasik dalam pengaman data atau informasi baik pesan teks maupun citra semakin rentan untuk dapat diretas oleh pihak yang tidak bertanggungjawab, oleh karena itu, penyandian data, file, dcitra maupun audio menggunakan algoritma klasik perlu dimodifikasi terlebih dahulu sebelum diimplementasikan, sebagai upaya dalam menjaga kualitas penyandian yang semakin kuat dan tidak mudah ditebak dan dipecahkan oleh *cryptanalysisi.* Adapun beberapa study literatur yang melakukan modifikasi terhadap algoritma kriptografi klasik terdapat pada tabel 1.

Tabel 1. Study Literatur

Penulis	Tahun	Algoritma	Metode	Tujuan	Kontribusi
Fatonah, Siti Yulandri, Anisa Ariyus, Dony	2019	Vigenere, Caesar, Vernam, & Hill Cipher	Algoritma Klasik	Modifikasi Algoritma	Dengan mengkombinasi 4 algoritma dalam mengaman pesan cukup kuat bila dibandingkan dengan 1 algoritma [10].
Alim, Zikrul Cancer, Yunie	2016	Vigenere Cipher	Algoritma Klasik & *brute force*.	Modifikasi Algoritma	Peningkatan pengamanan dengan Algoritma viginere cipher yang telah dimodifikasi lebih tahan terhadap penyerangan menggunakan metode *brute force*[11].
F. Lubis, H.Simbolon, T. Batubara, dkk	2017	Caesar Cipher	Algoritma Klasik	Mengkombinasi Algoritma	kombinasi dengan tiga langkah, caesar cipher, transposisi dan ASCII[2].
S. Anggarwal	2017	Caesar Cipher	Algoritma Klasik	Memodifikasi Algoritma Caesar Cipher	Keamanan yang disediakan dapat ditingkatkan dengan mengkombinasikan algoritma yang lainnya[12]
Agustini, Siti Rahmawati, Weny Mistarika Kurniawan, Muchamad	2019	Vegenere Cipher	Algoritma Klasik	Modifikasi Algoritma	Proses penyandian monoalphabetic cipher dan Vigenere cipher untuk meningkatkan kompleksitas [11]
Jamaludin, Romindo	2020	Viginere Cipher	Algoritma Klasik	Mengkombinasi Algoritma	Proses penyandian dengan dua penyandian, yaitu penyandian pesan dengan algoritma kriptografi Vigenere Cipher dan pengkodean kunci dengan algoritma kriptografi RSA[13]
Budiman, Saputra, Handrizal	2018	Viginere Cipher & Rabin-p	Algoritma Klasik & Algoritma Modern	Mengkombinasi Algoritma	sandi Vigenère digunakan untuk mengenkripsi file BMP dan algoritma Rabin-p digunakan untuk mengenkripsi kunci Vigenre[14]
Siahaan, Andysah Putera Utama	2016	Hill Cipher & Genetic Algorithm in	Algoritma Klasik	Mengkombinasi Algoritma	Algoritma genetika menyarankan pproses yang dioptimalkan untuk menentukan *key* yang dapat digunakan untuk enkripsi dan dekripsi pada Hill Cipher[15].
Andysah Putera Utama Siahaan	2016	Hill Cipher	Algoritma Klasik	Penerapan Three-Pass Protocol pada Hill Cipher	Pengirim teks dan penerima teks memiliki *key* yang berbeda, sehingga pihak lain tidak dapat mengetahuinya[16]
R. Megantara, F. Rafrastara, S. Mahendra,	2019	Hill Cipher	Algoritma Klasik	Kombinasi Hill Cipher pada RGB gambar	Menggabungkan *message security* dengan hill cipher dan LSB. Dapat meningkatan keamanan tanpa terlalu merusak gambar[17].
Rachmadsyah, Perdana, & Budiman	2020	Beaufort Cipher & Vigenere Cipher	Algoritma Klasik	Mengkombinasikan algoritma	Dapat menyamarkan pesan dengan menenkripsi dan deskripsi pesan yang berbasis android[18]
Frobenius, Arvin Claudy	2020	caesar, vigenere, hill	Algoritma Klasik	Modifikasi algoritma	Dapat menyisipkan teks dalam gambar tanpa mengalami perubahan

Hidayat S. H. S, Eko Rachmat		cipher dan playfair			ekstensi[19].
Victor Saputra Ginting Program	2020	Vigenere Cipher & Hill Cipher	Algoritma Klasik	Kombinasi algoritma	Pengiriman pesan dengan proses enkripsi deskripsi dari kombinasi algoritma Vigenere Cipher dan Hill Cipher dengan hasil tidak menimbulkan kecurigaan terhada *cryptanalysis*[20]
Megantara, Rama Aria Rafrastara, Fauzi Adi	2019	Hill Cipher & Transposisi Kolom	Algoritma Klasik	Kombinasi algoritma	Meghasilkan sistem dengan bahasa PHP Native untuk memudahkan proses enkripsi pengaman ganda[21].

B. Analisis Aloritma Kriptografi Klasik Caesar Cipher, Vigenere Cipher dan Hill Cipher

Algoritma kriptografi klasik ada sebelum era komputerisasi muncul yaitu era kriptografi modern dengan data yang terdiri dari angka 0 dan 1. Sedangkan algoritma kriptografi klasik merupakan algoritma yang terdiri dari dereten huruf a sampai z. Contoh algoritma kriptografi klasik yaitu: Caesar Cipher, Vigenere Cipher, dan Hill Cipher[22].

1. Caesar Cipher

Caesar Cipher adalah cipher substitusi yang menggunakan panjang *key* 1 karakter (karakter yang diambil dari alfabet) [23]. Adapun proses enkripsi dan deskripsi pada Caesar Cipher sebagai berikut :

Persamaan : C=E(K,P)=(P+K)mod26

Plainteks :SELECTION

Kunci : 7

Sehingga :

S = (18+7) mod 26 = 25 mod 26 = Z

E = (4+7) mod 26 = 11 mod 26 L

Dan seterusnya ...

Seingga, *ciphertext* dari *plaintext* SELECTION dengan kunci 7 menggunakan algoritma Caesar Cipher menghasilkan ZLSLJAPVU. Sedangkan proses deskripsi merupakan kebalikan dari proses enkripsi dengan melakukan pengurangan terhadap *plaintext* dengan kunci, dengan proses berikut ini:

Persamaan : C=E(K,P)=(P-K)mod26

Z = (25-7) mod 26 = 18 mod 26 = S

L = (11-7) mod 26 = 4 mod 26 = E

Dan seterusnya...

Sehingga *pliantext* dari *ciphertetxt* ZLSLJAPVU dengan kunci 7 menggunakan algoritma Caesar Cipher menghasilkan SELECTION.

2. Vigenere Cipher

Viginere Cipher merupakan salah satu metode enkripsi klasik yang digunakan untuk menyembunyikan pesan berupa teks dengan menggunakan teknik substitusi dimana tiap huruf pada *plaintext* diganti menjadi huruf lain berdasarkan kunci yang digunakan [24]. Adapun proses enkripsi dan deskripsi Vigenere Cipher dengan *plaintext* SELECTION, kunci NOTE adalah sebagai berikut :

Persamaan : $C_I = (P_I + K_I) \bmod 26$

S	E	L	E	C	T	I	O	N
N	O	T	E	N	O	T	E	N

(S+N) mod 26 = (18+13) mod 26 = 31 mod 26 = F

(E+O) mod 26 = (4+14) mod 26 = 18 mod 26 = S

Dan seterusnya...

Sehingga *ciphertext* dari *plaintext* SELECTION dengan kunci NOTE menggunakan algoritma Vigenere Cipher menghasilkan *ciphertext* FSEIPHBSA. Sedangan untuk proses deskripsi merupakan kebalikan dari proses enkripsi yang akan dilakukan pengurangan terhadap *plaintext* dengan kunci dengan proses sebagai berikut :

Persamaan : $C_I = (P_I - K_I) \bmod 26$

(F-N) = (5-13) mod 26 = - 8 mod 26 = (-8+26) = 18 mod 26 = S

(S-O) = (18-14) MOD 26 = 4 mod 26 = E

Dan seterusnya...

Sehingga *plaintext* dari *ciphertext* FSEIPHBSA dengan kunci Note menggunakan algoritma Vigenere Cipher menghasilkan plantext SELECTION.

3. Hill Cipher

Hill Cipher merupakan salah satu algoritma ktiprografi yang memanfaat aritmatika modulo dan matriks. Setiap karakter pada plaintext dan ciphertext dikonversikan kedalam angka [25]. Adapun proses enkripsi dan deskripsi pada Caesar Cipher sebagai berikut :

Persamaan : C = E(K,C) = K P mod 26

Plainteks : SELECTIONS

Kunci : $\begin{bmatrix} 4 & 7 \\ 6 & 2 \end{bmatrix}$

sehingga dengan menggunakan matriks 3x3 dengan tiap blok berisi 3 karakter yaitu

$\begin{bmatrix} S \\ E \end{bmatrix} = \begin{bmatrix} 18 \\ 4 \end{bmatrix}$ -> $\begin{bmatrix} L \\ E \end{bmatrix} = \begin{bmatrix} 11 \\ 4 \end{bmatrix}$ -> $\begin{bmatrix} C \\ T \end{bmatrix} = \begin{bmatrix} 2 \\ 19 \end{bmatrix}$ -> $\begin{bmatrix} I \\ O \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$ -> $\begin{bmatrix} N \\ S \end{bmatrix} =$

JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY)
Vol. 2, No. 1, Maret 2022

$\begin{bmatrix}13\\18\end{bmatrix}$Sehingga :

$\begin{bmatrix}4 & 7\\6 & 2\end{bmatrix}\begin{bmatrix}18\\4\end{bmatrix}=\begin{bmatrix}(4x18)+(7x4)\\(6x18)+(2x4)\end{bmatrix}=\begin{bmatrix}100\\116\end{bmatrix} mod\ 26 = \begin{bmatrix}22\\12\end{bmatrix}$

$\begin{bmatrix}4 & 7\\6 & 2\end{bmatrix}\begin{bmatrix}11\\4\end{bmatrix}=\begin{bmatrix}(4x11)+(7x4)\\(6x11)+(2x4)\end{bmatrix}=\begin{bmatrix}72\\74\end{bmatrix} mod\ 26 = \begin{bmatrix}20\\22\end{bmatrix}$

$\begin{bmatrix}4 & 7\\6 & 2\end{bmatrix}\begin{bmatrix}2\\9\end{bmatrix}=\begin{bmatrix}(4x2)+(7x9)\\(6x2)+(2x9)\end{bmatrix}=\begin{bmatrix}71\\30\end{bmatrix} mod\ 26 = \begin{bmatrix}19\\4\end{bmatrix}$

$\begin{bmatrix}4 & 7\\6 & 2\end{bmatrix}\begin{bmatrix}8\\14\end{bmatrix}=\begin{bmatrix}(4x8)+(7x14)\\(6x8)+(2x14)\end{bmatrix}=\begin{bmatrix}130\\76\end{bmatrix} mod\ 26 = \begin{bmatrix}0\\24\end{bmatrix}$

$\begin{bmatrix}4 & 7\\6 & 2\end{bmatrix}\begin{bmatrix}13\\18\end{bmatrix}=\begin{bmatrix}(4x13)+(7x18)\\(6x13)+(2x18)\end{bmatrix}=\begin{bmatrix}178\\114\end{bmatrix} mod\ 26 = \begin{bmatrix}22\\10\end{bmatrix}$

Sehingga menghasilkan

$\begin{bmatrix}22\\12\end{bmatrix}=\begin{bmatrix}W\\M\end{bmatrix}$ - > $\begin{bmatrix}20\\22\end{bmatrix}=\begin{bmatrix}U\\W\end{bmatrix}$ -> $\begin{bmatrix}19\\4\end{bmatrix}=\begin{bmatrix}T\\E\end{bmatrix}$->$\begin{bmatrix}0\\20\end{bmatrix}=\begin{bmatrix}A\\U\end{bmatrix}$->$\begin{bmatrix}22\\10\end{bmatrix}=\begin{bmatrix}W\\K\end{bmatrix}$

Sehingga *ciphertext* dari *plaintext* SELECTIONS dengan kunci $\begin{bmatrix}4 & 7\\6 & 2\end{bmatrix}$ menggunakan Hill Cipher menghasilkan *ciphertext* WMUWTEAUWK. Sedangkan proses deskripsi dilakukan dengan mencari nilai invers matriks *key* dengan proses sebagai berikut :

Persamaan : p = D(K,P) = $K^{-1}C$ mod 26

Ciphertext : WMUWTEAUWK

Kunci : $\begin{bmatrix}4 & 7\\6 & 2\end{bmatrix}$ dengan proses yang terdiri dari beberapa langkah yaitu:

Menghitung nilai determinan matriks kunci :

Det (k) = det$\begin{bmatrix}a & b\\c & d\end{bmatrix}=\begin{bmatrix}4 & 7\\6 & 2\end{bmatrix}$=((a*d)-(b*c))=((4*2)-(7*6))= 8-42=-31mod 26 = 5

Menghitung invers matriks kunci (k^{-1})

$k^{-1}=\frac{1}{\det(k)} mod\ 26 \begin{bmatrix}d & -b\\-c & a\end{bmatrix}$ = $k^{-1}=\frac{1}{5} mod\ 26 \begin{bmatrix}2 & -7\\-6 & 4\end{bmatrix}$= k^{-1} = 21 $\begin{bmatrix}2 & -7\\-6 & 4\end{bmatrix}$ = $\begin{bmatrix}42 & -147\\-126 & 84\end{bmatrix}$ mod26 sehingga dihasilkan $k^{-1} = \begin{bmatrix}16 & 17\\22 & 6\end{bmatrix}$

Ciphertext : WMUWTEAUWK

$\begin{bmatrix}22\\12\end{bmatrix}=\begin{bmatrix}W\\M\end{bmatrix}$ - > $\begin{bmatrix}20\\22\end{bmatrix}=\begin{bmatrix}U\\W\end{bmatrix}$ -> $\begin{bmatrix}19\\4\end{bmatrix}=\begin{bmatrix}T\\E\end{bmatrix}$->$\begin{bmatrix}0\\20\end{bmatrix}=\begin{bmatrix}A\\U\end{bmatrix}$ -> $\begin{bmatrix}22\\10\end{bmatrix}=\begin{bmatrix}W\\K\end{bmatrix}$ Kemudian, dilakukan perkalian matrix antara invers kunci dan ciphertext :

$\begin{bmatrix}16 & 17\\22 & 6\end{bmatrix}\begin{bmatrix}18\\4\end{bmatrix}=\begin{bmatrix}(16x18)+(17x4)\\(22x18)+(6x4)\end{bmatrix}=\begin{bmatrix}356\\420\end{bmatrix} mod\ 26 = \begin{bmatrix}18\\4\end{bmatrix}$

$\begin{bmatrix}16 & 17\\22 & 6\end{bmatrix}\begin{bmatrix}18\\4\end{bmatrix}=\begin{bmatrix}(16x18)+(17x4)\\(22x18)+(6x4)\end{bmatrix}=\begin{bmatrix}356\\420\end{bmatrix} mod\ 26 = \begin{bmatrix}18\\4\end{bmatrix}$

$\begin{bmatrix}16 & 17\\22 & 6\end{bmatrix}\begin{bmatrix}11\\4\end{bmatrix}=\begin{bmatrix}(4x11)+(7x4)\\(6x11)+(2x4)\end{bmatrix}=\begin{bmatrix}72\\74\end{bmatrix} mod\ 26 = \begin{bmatrix}20\\22\end{bmatrix}$

$\begin{bmatrix}16 & 17\\22 & 6\end{bmatrix}\begin{bmatrix}2\\9\end{bmatrix}=\begin{bmatrix}(4x2)+(7x9)\\(6x2)+(2x9)\end{bmatrix}=\begin{bmatrix}71\\30\end{bmatrix} mod\ 26 = \begin{bmatrix}19\\4\end{bmatrix}$

$\begin{bmatrix}16 & 17\\22 & 6\end{bmatrix}\begin{bmatrix}8\\14\end{bmatrix}=\begin{bmatrix}(4x8)+(7x14)\\(6x8)+(2x14)\end{bmatrix}=\begin{bmatrix}130\\76\end{bmatrix} mod\ 26 = \begin{bmatrix}0\\24\end{bmatrix}$

$\begin{bmatrix}16 & 17\\22 & 6\end{bmatrix}\begin{bmatrix}13\\18\end{bmatrix}=\begin{bmatrix}(4x13)+(7x18)\\(6x13)+(2x18)\end{bmatrix}=\begin{bmatrix}178\\114\end{bmatrix} mod\ 26 = \begin{bmatrix}22\\10\end{bmatrix}$ Sehingga menghasilkan

$\begin{bmatrix}22\\12\end{bmatrix}=\begin{bmatrix}W\\M\end{bmatrix}$ - > $\begin{bmatrix}20\\22\end{bmatrix}=\begin{bmatrix}U\\W\end{bmatrix}$ -> $\begin{bmatrix}19\\4\end{bmatrix}=\begin{bmatrix}T\\E\end{bmatrix}$->$\begin{bmatrix}0\\20\end{bmatrix}=\begin{bmatrix}A\\U\end{bmatrix}$->$\begin{bmatrix}22\\10\end{bmatrix}=\begin{bmatrix}W\\K\end{bmatrix}$

Sehingga *plaintext* daru *ciphertext* WMUWTEAUWK dengan kunci $\begin{bmatrix}16 & 17\\22 & 6\end{bmatrix}$ menggunakan algoritma Hill Cipher menghasilakn plaintext SELECTIONS.

C. Klasifikasi Trend Modifikasi Algoritma Kriptografi Klasik

Hasil paparan *study literature* yang terdiri 15 penelitian terdahulu yang melakukan modifikasi algoritma kriptografi klasik dengan rentang waktu 5 tahun kebelakang, dilakukan pengelompokan trend penelitian berdasarkan tahun penelitian. Adapun tahun penelitian yang digunakan sebagai *study literature* ialah, tahun 2016 sampai 2020 dengan klasifikasi sebagai berikut.

Tabel 2. Klasifikasi Trend Penelitian Berdasarkan Tahun

Tahun	Uraian Tren Penelitian
2016	Penelitian oleh Alim dkk, yang melakukan modifikasi untuk meningkatkan kompleksitas pengaman pesan dengan mengkombinasikan algoritma vigenere dan *brute for dengan* bantuan MATLAB sebagai tools untuk menguji algoritma yang dimodifikasi[11]. Kemudian Siahaan dkk melakukan modifikasi terhadap algoritma Hill Cipher dengan genetika Cipher untuk memudahkan dalam menentukan *key* enkripsi dan deskripsi [15]. Sedangkan Andysah dkk melakukan kombinasi terhadap algoritma Hill Cipher dengan Three-Pass Protocol kunci

	simetris untuk memberikan rasa aman saat melakukan pengiriman pesan sehingga penyadap tidak melakukan peretasan dikarenakan kunci pengirim dan penerimah berbeda [16].
2017	Penelitian oleh Lubis dkk yang melakukan modifikasi pada algoritma caesar cipher dengan transposition cipher yang memiliki proses enkripsi sebanyak 3 kali dengan melakukan modifikasi caesar cipher, transposition dan dienkripsi kembali dengan caesar kedua. Sedangkan proses deskripsi merupakan kebalikan dari proses enkripsi [2].
2018	Penelitian oleh Budiman dkk yang menggabungkan Vigenère cipher dan algoritma Rabin-p dalam skema kripto sistem hibrida untuk mengamankan file BMP dengan Vigenere Cipher [14].
2019	Penelitian oleh Frobenius dan Hidayat yang memodifikasi algoritma Caesar, Vigenere, Hill dan Playfair yang dapat menyisipkan teks pada gambar tanpa mengubah ektensi [19]. Penelitian oleh Agustini dkk yang melakukan pengabungan onoalphabetic cipher dan Vigenere cipher dengan menerapkan *key* enkripsi sebanyak dua *key* [11]. Penelitian oleh Megantara dkk yang melakukan kombinasi algoritma Hill Cipher dengan LSB Cipher dalam mengamankan RGB image dengan proses membuat sistem penentuan pilihan panjang karakter pesan yang terdiri dari 32, 64 dan 128 karakter, yang kemudian dienkripsikan kembali oleh Hill Cipher[17]. Penelitian oleh Megantara dkk yang melakukan peningkatan kompleksitas pengaman pesan dengan super enkrpsi yang dirancanag menggunakan PHP native dengan algoritma Hill Cipher dan Transposisi kolom untuk memudahkan proses enkripsi deskripsi [21].
2020	Penelitian oleh Jamaludin, Romindo, yang melakukan kombinasi algoritma dalam proses penyandian pesan dengan algoritma Vigenere cipher dan RSA. Sehingga dihasilkan tingkat keamanan yang lebih baik dengan 2 kali penyandian [13]. Sedangkan penelitian oleh Rachmadsyah dkk yang melakukan perancangan sistem untuk pengaman pesan menggunakan kombinasi beaufort cipher dan vigenere cipher yang berbasis *mobile application*. Sistem dirancang menggunakan java, dengan proses enkripsi menggunakan algoritma terlebih dahulu, kemudian dienkripsikan kembali melewati 2 (dua) putaran beaufort.[18]. penelitian selanjutnya oleh frobenius dan Hidayat yang melakukan modifikasi terhadap Caesar Cipher, Vigenere Cipher, Hill Cipher dan Playfair pada gambar sehingga akan menghasilakn *ciphertext* sementara. Sedangkan proses deskripsi dengan Least Significant Bit (LSB) untuk mengenkripsi pesan yang dimasukan dalam gambar dan mengembalikan kembali pada pesan original [19]. Penelitian selanjutnya oleh Victor Ginting yang melakukan perancangan pengamanan data dengan modifikasi terhadap algoritma Vigenere Cipher dan Hill Cipher. Proses enkripsi dengan memasukan *plaintext* berupa huruf, kemudian memodifikasi Hill Cipher dengan mod 26 dan matriks 2x2 dengan dimulai 3 digits awal nama Negara yang akan dirubah ke matrisk 2x1 dengan matriks mod 26 dibagi 10. Sedangkan proses deskripsi merupakan kebalikan dari proses enkripsi [20].

IV. KESIMPULAN DAN SARAN

Berdasarkan beberapa referensi diatas, yang terdiri dari algoritma caesar cipher, vignere cipher dan hill cipher sudah dapat melakukan penyandian data atau informasi pesan teks, file dan citra. Mengingat perubahan dan perkembangan pengetahuan semakin luas membuat proses enkripsi dan deskripsi dengan satu algoritma dapat dipecahkan oleh pihak yang tidak bertanggungjawab, karena beberapa algoritma dapat dipecahkan dengan algoritma lainnya. Oleh karena itu, diperlukan modifikasi atau kombinasi dengan beberapa algoritma untuk meningkatkan kompleksitas pengamana data, sehingga data menjadi bentuk yang semakin sulit dipahami oleh manusia, dan kemungkinana untuk dapat memecahkan kunci dengan melakukan banyak percobaan yang mmebutuh banyak waktu.

UCAPAN TERIMA KASIH

Terima kasih penulis sampaikankepada Tim Jurnal TI ISByang telah meluangkan waktu untuk membuat templateini dan juga kepada seluruh pihak yang turut andil memberikan dukungan dan masukan yang membangun.

REFERENSI

[1] A. Saraswat, C. Khatri, P. Thakral, and P. Biswas, “An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication,” *2nd Int. Conf. Intell. Comput. Commun.*

Converg., vol. 92, pp. 355–360, 2016, doi: 10.1016/j.procs.2016.07.390.

[2] F. I. Lubis, H. F. S. Simbolon, T. P. Batubara, and R. W. Sembiring, "Combination of caesar cipher modification with transposition cipher," *Adv. Sci. Technol. Eng. Syst.*, vol. 2, no. 5, pp. 22–25, 2017, doi: 10.25046/aj020504.

[3] L. Kartika and Y. Yudi, "Rancang Bangun Aplikasi Penyembunyian Pesan QRCode Dengan Menggunakan Metode Caesar Cipher Berbasis Android," *J. Mhs. Fak. Tek. …*, pp. 511–518, 2020, [Online]. Available: http://e-journal.potensi-utama.ac.id/ojs/index.php/FTIK/article/view/902.

[4] D. Susianto and D. Mustika, "Membangun Sistem Informasi Inventory menggunakan Algoritma Caesar Cipher sebagai Media Enkripsi (Studi Kasus: Klinik Ridho Husada)," *J. Cendikia*, vol. XVIII, no. Oktober, pp. 309–315, 2019.

[5] T. S. Alasi, A. T. Al, and A. Siahaan, "Algoritma Vigenere Cipher Untuk Penyandian Record Informasi Pada Database," *J. Inf. Komput. Log.*, vol. 1, no. 4, 2020, [Online]. Available: http://ojs.logika.ac.id/index.php/jikl.

[6] I. Technology and C. Science, "WEB-BASED ONLINE ATTENDANCE SYSTEM WITH QR CODE IN REAL," vol. 4, 2021.

[7] D. M. Sholahudin and Asmunin, "Implementasi Algoritma Hill Cipher untuk Proses Enkripsi dan Dekripsi Citra Berwarna dengan Modifikasi Padding," *J. Informatics Comput. Sci.*, vol. 01, no. 04, pp. 228–234, 2020.

[8] J. Freddy *et al.*, "Kriptografi Teks dan Citra dengan Menggunakan Algoritma Hill Cipher pada Perangkat Android," *J. Masy. Inform.*, vol. 8, no. 1, pp. 9–15, 2017.

[9] P. Studi and T. Informatika, "Modifikasi Ceasar Cipher menjadi Cipher Abjad-Majemuk dan Menambahkan Kunci berupa Barisan Bilangan."

[10] M. I. D. Ramdhani, "Perbandingan Kriptografi Klasik (Caesar Cipher) dan Kriptografi Modern (MD5)," no. May, 2016, [Online]. Available: https://www.researchgate.net/publication/303382769_Perbandingan_Kriptografi_Klasik_Caesar_Cipher_dan_Kriptografi_Modern_MD5.

[11] S. Agustini, W. M. Rahmawati, and M. Kurniawan, "Modified Vegenere Cipher to Enhance Data Security Using Monoalphabetic Cipher," *Int. J. Artif. Intell. Robot.*, vol. 1, no. 1, pp. 26–31, 2019, doi: 10.25139/ijair.v1i1.2029.

[12] S. Aggarwal, "A REVIEW ON ENHANCING CAESAR CIPHER," *Int. J. Res. Sci. Manag. A*, vol. 29, no. 8, pp. 1757–1760, 2017.

[13] R. Politeknik Ganesha Medan, "Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security," *Int. J. Inf. Syst. Technol. Akreditasi*, vol. 4, no. 1, pp. 471–481, 2020.

[14] H. Mohammad Andri Budiman, Muhammad Yogi Saputra, "A Hybrid Cryptosystem Using Vigenère Cipher and Rabin-p Algorithm in Securing BMP Files," *J. Comput. Appl. Informatics*, vol. 4, no. September 2016, pp. 2016–2017, 2018, [Online]. Available: https://www.data-science.ruhr/about_us/.

[15] A. P. U. Siahaan, "Genetic Algorithm in Hill Cipher Encryption," *Am. Int. J. Res. Sci. Technol. Eng. Math.*, vol. 15, no. 1, pp. 84–89, 2016.

[16] A. Putera, U. Siahaan, and A. H. Cipher, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," *Int. J. Sci. Res.*, vol. 5, no. 7, pp. 1149–1152, 2016, doi: 10.21275/v5i7.art2016437.

[17] R. A. Megantara, F. A. Rafrastara, and S. N. Mahendra, "A Combination of Hill CIPHER-LSB in RGB Image Encryption," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 4, no. 3, pp. 241–248, 2019, doi: 10.22219/kinetik.v4i3.785.

[18] A. Rachmadsyah, A. Perdana, and A. B. S. T, "Kombinasi Algoritma Beaufort Cipher Dan Vigenere Cipher Untuk Pengamanan Pesan Teks Berbasis Mobile Application," vol. 9, no. September, pp. 12–17, 2020.

[19] A. C. Frobenius and E. R. Hidayat S. H. S, "Steganografi LSB Dengan Modifikasi Kriptografi: Caesar, Vigenere, Hill Cipher dan Playfair Pada Image," *Melek IT Inf. Technol. J.*, vol. 6, no. 1, pp. 33–40, 2020, doi: 10.30742/melek-it.v6i1.301.

[20] V. S. Ginting, "Penerapan Algoritma Vigenere Cipher dan Hill Cipher Menggunakan Satuan Massa," *JurTI (Jurnal Teknol. Informasi)*, vol. 4, no. 2, pp. 241–246, 2020, [Online]. Available: http://www.jurnal.una.ac.id/index.php/jurti/article/view/1365.

[21] R. A. Megantara and F. A. Rafrastara, "Super Enkripsi Teks Kriptografi menggunakan Algoritma Hill Cipher dan Transposisi Kolom," *Pros. SENDI_U 2019*, pp. 85–92, 2019.

[22] Sumandri, "Studi Model Algoritma Kriptografi Klasik dan Modern," *Semin. Mat. dan Pendidik. Mat. UNY*, pp. 265–272, 2017.

[23] A. Antoni, S. Aryza, A. R. Lubis, B. Harahap, and M. Arfah, "A novelty methods of cryptography algorithms into layered cipher encryption and decryption," *Int. J. Eng. Technol.*, vol. 7, no. 14, pp. 289–292, 2018, doi: 10.14419/ijet.v7i2.8953.

[24] A. yudo Husodo, "Penerapan Metode Enkripsi Vigenere Cipher dalam Pengamanan Transaksi Mobile Banking," *Makal. If3058 Kriptografi*, pp. 1–10, 2010.

[25] A. Hidayat and T. Alawiyah, "Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang," *J. Mat. Integr.*, vol. 9, no. 1, p. 39, 2013, doi: 10.24198/jmi.v9i1.10196.