**Jurnal Sains dan Teknologi**
Volume 12 Number 2, Tahun 2023, pp. 502-515
P-ISSN: 2303-3142 E-ISSN: 2548-8570
Open Access: https://doi.org/10.23887/jstundiksha.v12i2.52801

# Aplikasi Matriks untuk Meningkatkan Keamanan Proses Kriptografi *Caesar*, *Vernam*, dan *Hill Cipher*

**Sisilia Sylviani[1*], Alit Kartiwa[2], Fahmi Candra Permana[3], A. N. Hadi[4], M. P. Kadir[5], R. Wilopo[6]**

[1,2,4,5,6] Departemen Matematika FMIPA, Universitas Padjadjaran, Bandung, Indonesia
[3] Prodi Pendidikan Multimedia, Universitas Pendidikan Indonesia, Bandung, Indonesia

**ARTICLE INFO**

**Article history:**
Received October 05, 2022
Revised October 11, 2022
Accepted may 20, 2023
Available online July 25, 2023

**Kata Kunci:**
Kriptografi, *Caesar Cipher*, *Vernam Cipher*, *Hill Cipher*

***Keywords:***
*Cryptography, Caesar Cipher, Vernam Cipher, Hill Cipher*



**ABSTRAK**

Dalam era smart society 5.0 ini, kemajuan teknologi informasi dan komunikasi berkembang sangat pesat. Seiring dengan hal tersebut, resiko terjadinya gangguan informasi, seperti penyalahgunaan informasi oleh pihak yang tidak berwenang, juga meningkat. Dalam artikel ini dibahas kombinasi metode Hill Cipher, Vernam Cipher, dan Caesar Cipher sebagai salah satu upaya untuk meningkatkan kemanan dalam penyampaian pesan rahasia. Metode Hill Cipher, Vernam Cipher, dan Caesar Cipher tersebut memiliki kelebihan dan kelemahannya masing-masing. Untuk itu dilakukan modifikasi dengan mengkombinasikan ketiga metode tersebut secara bersamaan, dengan tujuan untuk menimalisasi kelemahan dan meningkatkan keamanan dalam penyampaian pesan. Penelitian yang dilakukan ini termasuk ke dalam jenis penelitian kualitatif, dengan menggunakan instrumen eksperimen atau percobaan. Adapun desain penelitiannya adalah dengan melakukan Kombinasi proses kriptografi dengan ketiga metode tersebut yang di dalamnya melibatkan matriks. Hasil yang diperoleh adalah tingkat kerahasiaan pesan yang dikirim lebih tinggi dan kelemahan dari masing-masing metode dapat diminimalisir dibandingkan dengan penggunaan ketiga metode tersebut secara berdiri sendiri.

***ABSTRACT***

*In this era of smart society 5.0, advances in information and communication technology are growing very rapidly. Along with this, the risk of information tampering, such as misuse of information by unauthorized parties, also increases. This article discusses the combination of Hill Cipher, Vernam Cipher, and Caesar Cipher methods in an effort to increase security in delivering secret messages. The Hill Cipher, Vernam Cipher, and Caesar Cipher methods have their respective advantages and disadvantages. For this reason, modifications were made by combining the three methods simultaneously, with the aim of minimizing weaknesses and increasing security in delivering messages. This research is included in the type of qualitative research, using experimental or experimental instruments. The research design is to combine the cryptographic process with the three methods which involve a matrix. The results obtained are the level of confidentiality of messages sent is higher and the weaknesses of each method can be minimized compared to using the three methods independently.*

## 1. PENDAHULUAN

Saat ini, teknologi telah menjadi hal yang selalu ditemui bahkan dalam hampir setiap aspek kehidupan, khususnya dalam bidang komunikasi. Teknologi komunikasi berkembang sangat pesat, bahkan dalam setiap tahun selalu saja ada hal yang baru terkait teknologi dalam melakukan komunikasi. Seiring dengan begitu pesatnya perkembangan teknologi komunikasi dan informasi digital, di sisi lain terdapat kondisi bahwa karena orang mengirimkan dan memperoleh informasi dengan lebih mudah, masalah keamanan informasi menjadi sangat penting selama proses komunikasi tersebut. Salah satu hal yang dapat dilakukan adalah proses kriptografi. Kriptografi telah dikenal dan dipakai cukup lama sejak kurang lebih tahun 1900 sebelum masehi pada prasasti-prasasti kuburan. Kriptografi sendiri berasal dari kata "Crypto" yang berarti rahasia dan "graphy" yang berarti tulisan. Jadi, dapat dikatakan kriptografi adalah tulisan yang tersembunyi (Anwar, Nugroho, & Ahmadi, 2015; Astuti, 2015; Lubis, 2017). Di jaman Romawi kuno, Julius Caesar telah menggunakan teknik kriptografi yang dijuluki Caesar cipher untuk mengirim pesan secara rahasia, meskipun teknik yang digunakannya sangat tidak memadai untuk ukuran kini. Sewaktu perang dunia kedua, pihak sekutu berhasil memecahkan kode mesin kriptografi Jerman, Enigma; keberhasilan yang sangat membantu pihak sekutu dalam memenangkan perang. Sejarah kriptografi penuh dengan intrik dan

*Corresponding author.
E-mail addresses: sisilia.sylviani@unpad.ac.id (Sisilia Sylviani)

banyak orang melihat kriptografi sebagai sesuatu yang penuh dengan misteri (Rahim & Steganografi, 2016).

Enkripsi merupakan proses penyandian pesan atau informasi sedemikian rupa sehingga hanya pihak yang berwenang yang dapat mengaksesnya dan pihak yang tidak berwenang tidak dapat mengaksesnya (Es-Sabry, Akkad, N. el, Merras, Saaidi, & Satori, 2018). Enkripsi itu sendiri tidak mencegah terjadinya interferensi, namun dapat mencegah pesan dapat dibaca oleh selain yang berwenang. Dalam skema enkripsi, informasi atau pesan yang dimaksud, disebut sebagai plaintext. Pesan atau plaintext tersebut dienkripsi dengan menggunakan algoritma enkripsi, yang disebut dengan cipher. Hasil enkrpsi tersebut menghasilkan teks sandi yang hanya dapat dibaca jika didekripsi (proses merubah pesan yang telah dienkripsi menjadi pesan aslinya).

Terdapat beberapa metode yang dapat digunakan dalam kriptografi, beberapa diantaranya: Caesar cipher, monoalphabetic cipher, homophonic substitution cipher, polygram substitution cipher, polyalphabetic substitution cipher (Apdilah & Swanda, 2018; Mesran & Nasution, 2020; Novianto & Setiawan, 2019; Rauf, 2020; Simargolang, 2017). Namun dalam penelitian ini, metode yang digunakan adalah kombinasi dari Caesar Cipher, Vernam Cipher, dan Hill Cipher. Metode Caesar Cipher sendiri lebih dikenal sebagai metode pergeseran cipher yang merupakan salah satu proses enkripsi yang paling sederhana dan paling mudah untuk dilakukan. Dengan proses yang sederhana dan mudah untuk dilakukan ini malah menyebabkan metode Caesar Cipher mempunyai tingkat keamanan yang sangat rendah (Dewi, 2020; Gunawan, Sumarno, Tambunan, Irawan, Qurniawan, & Hartama, 2019; Hammad et al., 2022; Jain, Dedhia, & Patil, 2015; Maihankali & Eze, 2021). Metode Vernam Cipher telah memegang peran penting dalam kriptografi dengan sistem keamanannya yang telah sempurna, walaupun demikian masih ada sedikit kelemahan (Caniago, 2019; Irnanda, 2019). Metode ini memungsikan boolean ekslusif (Ex-OR dan Ex-Nor). Sedangkan metode Hill Cipher adalah cipher simetris klasik berdasarkan transformasi matriks. Walapun memiliki kelemahan seperti dua metode yang disebutkan sebelumnya (Deolika, 2020; Elhabshy, 2019; Zamara, 2019), Metode ini memiliki beberapa keuntungan termasuk ketahanan terhadap analisis frekuensi dan implicity karena metode ini menggunakan perkalian matriks dan inversi untuk enkripsi dan dekripsi. Dengan tingkat keamanan yang beranekaragam mulai dari keamanan yang paling rendah sampai dengan sistem keamanan yang sempurna, maka penulis melakukan proses kombinasi dari ketiga metode ini agar dapat terciptanya metode kriptografi dengan tingkat keamanan yang jauh lebih baik dibandingkan hanya menggunakan satu jenis metode saja.

Caesar Cipher adalah salah satu teknik enkripsi yang paling sederhana dan paling terkenal, metode ini merupakan salah satu contoh teknik substitusi (Mesran & Nasution, 2020; Nasution, 2019; Putri, Rosihan, & Lutfi, 2019). Dalam plaintext Caesar Cipher diganti dengan huruf lainnya. Misalnya dengan pergeseran (yang selanjutnya disebut dengan key) 3 langkah, A akan digantikan oleh D, B akan menjadi E, dan seterusnya. Dalam penulisan paper ini metode Caesar Cipher yang digunakan dengan mengubah plaintextnya ke dalam bentuk bilangan biner agar terdapat kesinambungan antar metode ini dengan metode Vernam Cipher. Dalam penggunaannya akan terdapat dua macam proses yaitu proses enkripsi dan proses dekripsi. Untuk proses enkripsi sendiri langkah-langkahnya ialah sebagai berikut. Langkah pertama adalah Akan diubah plaintext ke dalam bentuk bilangan biner. Kemudian, langkah kedua Akan dilakukan pergeseran sebanyak key langkah ke arah kanan. Terakhir, lakukan konversi dari hasil pergeseran tersebut ke dalam bentuk karakter atau huruf. Sementara untuk proses dekripsinya memiliki beberapa langkah juga. Langkah pertama yaitu mengubah ciphertext ke dalam bentuk bilangan biner. Langkah kedua adalah dilakukan pergeseran sebanyak key ke arah kiri. Langkah terakhir adalah dengan melakukan konversi dari hasil pergeseran tersebut ke dalam bentuk karakter atau huruf.

Metode Vernam Cipher merupakan sistem kerahasiaan yang sempurna di mana metode ini adalah stream cipher simetris di mana plaintext dikombinasikan dengan key stream (pseudorandom) yang sama panjang untuk menghasilkan ciphertext yang memungsikan boolean ekslusif (Ex-OR dan Ex-Nor) (Pawar & Hatkar, 2016; Ryabko, 2015; Siahaan & Siahaan, 2018). Langkah-langkah dari proses enkripsi sendiri ialah sebagai berikut. Langkah pertama adalang mengubah plaintext dan key ke dalam bentuk bilangan biner. Kemudian lakukan proses enkripsi dengan menggunakan logika Boolean ekslusif (Ex-OR dan Ex-Nor) pada plaintext dan key. Langkah yang terakhir adalah Lakukan konversi ke dalam bentuk karakter atau huruf. Sementara untuk proses dekripsinya yaitu, langkah pertama mengubah ciphertext dan key ke dalam bentuk bilangan biner. Kemudian gunakan boolean ekslusif (Ex-OR dan Ex-Nor) pada key dan ciphertext-nya. Hal yang terakhir dilakukan konversi ke dalam bentuk karakter atau huruf.

Metode Hill Cipher adalah cipher simetris klasik yang memecah plaintext menjadi blok-blok ukuran m dan kemudian mengalikan setiap blok oleh sebuah kunci matriks m x m untuk menghasilkan ciphertext (Dawahdeh, Yaakob, & Razif bin Othman, 2018; Elhabshy, 2019; Kriptografi et al., 2016; Merlin Tan et al., 2020; Paragas, Sison, & Medina, 2019; Sundarayya & Prasad, 2019). Sama halnya dengan metode yang lain, metode Hill Cipher juga memiliki dua macam proses, yaitu proses enkripsi dan proses dekripsi. Proses enkripsinya sendiri memiliki langkah-langkah sebagai berikut. Pertama, tentukan terlebih dahulu matriks

enkripsi A yang memiliki ordo $m \times m$. Langkah kedua yang dilakukan adalah melakukan pengelompokkan plaintext sebanyak m karakter dan konversikan menjadi bilangan bulat. Langkah ketiga adalah membentuk kelompok bilangan bulat tersebut menjadi bentuk vector $p_1, p_2, \ldots$. Langkah terakhir, dilakukan pencari vector $c_1, c_2, \ldots$ dengan cara mengalikan matriks A dengan vector $p$, atau dapat dituliskan $c_k = A.p_k$. Setelah itu, konversikan bilangan pada vector $c_1, c_2, \ldots$menjadi karakter sehingga diperoleh ciphertext nya. Adapun untuk proses dekripsinya sendiri memiliki langkah-langkah sebagai berikut. Pertama, tentukan invers dari matriks enkripsi A. Langkah kedua kelompokkan ciphertext sebanyak $m$ karakter konversikan menjadi bilangan bulat. Langkah selanjutnya, bentuk kelompok bilangan bulat tersebut menjadi bentuk vector $c_1, c_2, \ldots$ Kemudian cari vector $p_1, p_2, \ldots$ dengan cara mengalikan matriks A-1 dengan vector c., atau dituliskan $p_k = A - 1.c_k$. langkah terkhir adalah konversikan bilangan pada vector $p_1, p_2, \ldots$ menjadi karakter sehingga diperoleh plaintextnya.

Beberapa penelitian sebelumnnya menunjukkan bahwa *metode Hill Cipher dan Stream Cipher* dapat meningkatkan keamanan database lebih baik (Deolika, 2020; Merlin Tan et al., 2020). Penelitian lainnya menunjukkan bahwa menggabungkan dua algoritma kriptografi dapat lebih meningkatkan keamanan dari citra dibandingkan dengan hanya satu algoritma (Nasuton, Haryanto, & Saleh, 2020). Ketiga metode tersebut sebenarnya dapat digunakan berdiri sendiri. Dengan kata lain, masing-masing metode tersebut dapat digunakan untuk proses enkripsi dan dekripsi. Namun demikian, masing-masing metode tersebut memiliki kelemahannya masing-masing, sehingga memiliki celah pesan yang disampaikan dapat dibaca oleh pihak yang tidak berwenang. Dalam peneltian ini dilakukan upaya dalam memperbaiki setiap kelemahan yang terdapat dalam setiap metode tersebut. Khususnya, dalam penelitian ini dilakukan kombinasi dari ketiga metode tersebut, tujuannya untuk memperoleh metode yang lebih baik dan lebih tinggi tingkat kemanannya dalam menyampaikan pesan rahasia.

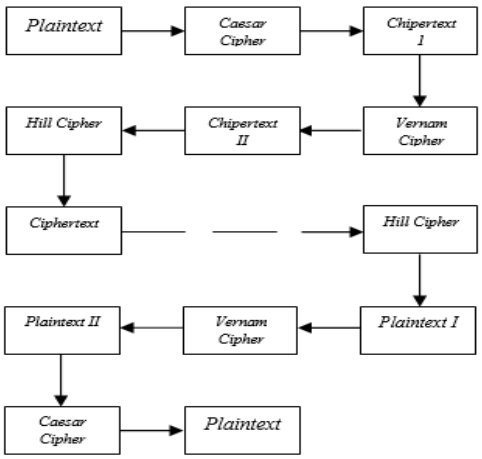
## 2. METODE

Penelitian yang dilakukan ini temasuk kedalam jenis penelitian kualitatif. Oleh karena itu, dalam penelitian ini tidak digunakan pengambilan data dan sampel. Adapun yang dilakukan adalah melakukan modifikasi dari metode yang telah ada kemudian mengimplementasikannya ke dalam contoh kasus sederhana terlebih dahulu untuk memperoleh gambaran yang jelas terkait hal yang dilakukan. Namun, pengambilan contoh kasus sederhana tersebut tidak membatasi penggunaan kombinasi metode yang dihasilkan. Dengan kata lain, hasil penelitian ini dapat diimplementasikan untuk sembaang kasus,namun untuk pesan yang banyak, diperlukan bantuan software. Dalam proses kriptografi telah banyak dikenal banyak cara dengan kekurangan dan kelebihannya masing-masing. Untuk itu pengembangan yang dilakukan dalam penelitian ini adalah dengan menggabungkan tiga jenis proses kriptografi yang pupuler. Adapun dan desain rinci penelitian ini digambarkan pada Gambar 1 hingga Gambar 3 (Agung et al., 2020).

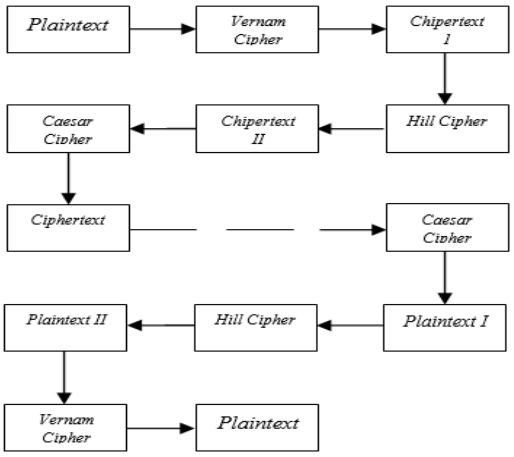
Subjek penelitian yang terlibat dalam penelitian ini adalah Hill Cipher, Vernam Cipher, dan Caesar Cipher. Penelitian dilakukan dengan mengkombinasikan ketiga metode enkripsi deskripi tersebut, sehingga terbentuk 3 buah metode baru dalam proses enkripsi dan dekripsi. Pengujian dilakukan dengan mengambil sampel satu kalimat atau plaintext untuk diubah kedalam bentuk kode. Pengambilan sampel tersebut dimaksudkan untuk mempermudah dalam menggambarkan cara kerja kombinasi metoda tersebut. Namun bukan berarti metode tersebut terbatas hanya dapat digunakan untuk plaintext ukuran kecil. Kombinasi dari metode-metode tersebut dapat digunakan untuk plaintext ukuran besar, namun tentu saja untuk plaintext dengan ukurab besar diperlukan bantukan software dalam melakukan komputasinya.

Data-data yang digunakan dalam penelitian ini, baik data literatur ataupun data yang terkait dengan objek peneltian diperoleh secara online. Pencarian literature dilakukan dengan menjelajah website-website penyedia literatur terkait, dari mulai buku, maupun artikel-artikel dalam jurnal bereputasi. Instrument pengujian yang digunakan dalam penelitian ini adalah dengan menggunakan software Maple.

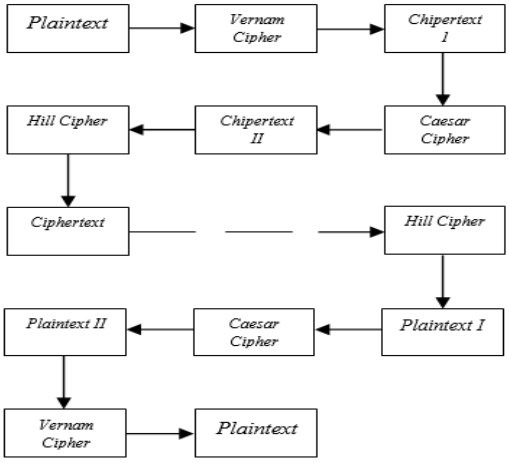
Analisis yang dilakukan dalam penelitian ini dilakukan terhadap metode Caesar Cipher, Vernam Cipher, dan Hill Cipher dengan mengombinasikan ketiga metode tersebut dalam proses enkripsi maupun proses dekripsi guna meningkatkan keamanan data. Untuk proses kombinasi yang pertama yaitu Caesar Cipher – Vernam Cipher – Hill Cipher, proses kombinasi yang kedua yaitu Vernam Cipher – Hill Cipher – Caesar Cipher, dan proses kombinasi yan ketiga yaitu dengan melakukan enkripsi dan dekripsi.




**Gambar 1.** Kombinasi *Caesar-Vernam-Hill*




**Gambar 2.** Kombinasi *Vernam-Hill-Caesar*




**Gambar 3.** Kombinasi *Vernam-Caesar-Hill*

## 3. HASIL DAN PEMBAHASAN

### Hasil

Proses kriptografi dengan kombinasi metode Caesar Cipher, Vernam Cipher, dan Hill Cipher dengan terlebih dahulu membuat pesan yang akan dienkripsikan dan menentukan key (n) yang akan digunakan dalam proses enkripsi. Adapun tahapan dari proses enkripsi yang akan dilakukan ialah sebagai berikut. Langkah pertama dilakukan dengan mengubah plaintext ke dalam bentuk bilangan biner, selanjutnya adalah dengan melakukan pergeseran sebanyak n langkah ke arah kanan. Kemudian, dilakukan proses enkripsi dari hasil Caesar Cipher ke bentuk Vernam Cipher, dengan cara mengubah plaintext dan key ke dalam bentuk bilangan biner. Kemudian dilakukan proses enkripsi dengan menggunakan logika Ex-OR dan ubah ke bentuk desimal. Langkah selanjutnya adalah dengan melakukan proses enkripsi dari hasil Vernam Cipher ke bentuk Hill Cipher. Kemudian, tentukan matriks enkripsi A yang memiliki ordo $nxn$. Matriks tersebut dapat dibuat dari key dengan cara :

$$A = \begin{bmatrix} key & key+1 \\ key-1 & key-2 \end{bmatrix}$$

Selanjutnya kelompokan bilangan bulat hasil cipher sebelumnya sebanyak dua bilangan dan dibentuk menjadi vector. Kemudian dicari vector $c_1, c_2, \dots, c_n$ dengan cara mengalikan matriks A dengan vector p dan hasil perkaliannya diubah ke modulo 255.

$$c_k = Ap_k$$

Selanjutnya dilakukan konversi bilangan pada vector $c_1, c_2, \dots$ menjadi karakter sehingga didapat ciphertext akhir :

[Shift Out]t·\Ö[Unit Separator][Synchronous Idle][File Separator](dÔ[File Separator]H·[Device Control 4]›,7V;Uú[Device Control 2]Ù

Untuk proses dekripsi dari kombinasi Caesar Cipher, Vernam Cipher, dan Hill Cipher dilakukan dengan langkah-langkah sebagai berikut. Langkah pertama, Tentukan invers dari matriks enkripsi A. Langkah kedua adalah dengan mengelompokkan ciphertext sebanyak n karakter konversikan menjadi bilangan bulat. Langkah ketiga dilakukan dengan membentuk kelompok bilangan bulat tersebut menjadi vektor $c_1, c_2, \dots, c_k$. Langkah keempat dilakukan dengan mencari vektor $p_1, p_2, \dots, p_n$ dengan cara mengalikan matriks $A^{-1}$ dengan vektor c, atau dapat dituliskan dengan $p_k = A^{-1}c_k$. Langkah kelima dilakukan dengan mengenkripsikan hasil dari Hill Cipher ke bentuk Vernam Cipher. Langkah kelima adalah dengan mengubah ciphertext dan key ke dalam bentuk bilangan biner. Langkah keenam dilakukan proses enkripsi dengan menggunakan logika Ex-Or. Langkah ketujuh, Hasil enkripsi Vernam Cipher lalu dienkripsikan ke bentuk Caesar Cipher. Langkah kedelapan dilakukan perubahan chipertext ke dalam bentuk bilangan biner. Langkah kesembilan dilakukan pergeseran sebanyak n ke arah kiri. Langkah terakhir adalah konversi dari hasil pergeseran tersebut ke dalam bentuk karakter atau huruf. Kemudian dikelompokkan bilangan bulat hasil cipher sebelumnya sebanyak tiga bilangan dan dibentuk menjadi vector. Selanjutnya, Akan dicari vector $c_1, c_2, \dots, c_n$ dengan cara mengalikan matriks A dengan vector p dan hasil perkaliannya diubah ke modulo 255.

$$A = \begin{bmatrix} key & key-1 & key-2 \\ key+1 & key+2 & key+3 \\ key+2 & key+3 & key+4 \end{bmatrix}$$

Selanjutnya dilakukan dikonversi hasil modulo dari modulo di atas ke dalam bilangan biner. Langkah selanjutnya adalah melakukan pergeseran sebanyak n langkah kearah kanan. Kemudian dilakukan dikonversi hasil bilangan biner tersebut ke dalam huruf atau karakter. Sehingga diperoleh ciphertext dari plaintext tersebut adalah ®¹[DEL]¢›[øæ½Í²WÉY^Üä%ƒE†ä[LINE FEED]. Untuk proses dekripsi dari kombinasi Vernam Cipher, Hill Cipher, dan Caesar Cipher yaitu, pertama dilakukan perubahan ciphertext dan key ke dalam bentuk bilangan biner. Kemudian dilakukan pergeseran ke arah kiri sebanyak n langkah. Hasil enkripsi Caesar Cipher lalu dienkripsikan ke bentuk Hill Cipher. Kemudian, dilakukan penentuan invers dari matriks enkripsi A. Selanjutnya dibentuk kelompok bilangan bulat tersebut menjadi bentuk vector $c_1, c_2, \dots, c_k$. Kemudian dicari vektor $p_1, p_2, \dots, p_n$ dengan cara mengalikan matriks $A^{-1}$ dengan vektor $c$, atau dapat ditulis $p_k = A^{-1}c_k$. Selanjutnya, dienkripsikan hasil dari Hill Cipher ke bentuk Vernam Cipher. Langkah selanjutnya adalah melakukan perubahan ciphertext dan key ke dalam bentuk bilangan biner. Kemudian dilakukan proses enkripsi dengan menggunakan logika Ex-Or. Terakhir, hasil enkripsi Vernam Cipher lalu dikonversi ke dalam bilangan bulat

**Pembahasan**

Caesar cipher merupakan suatu mono sandi alfabet yang sering digunakan untuk proses enkripsi dan dekripsi. Cipher ini adalah jenis sandi substitusi di mana setiap huruf dalam plaintext diganti dengan huruf. Enkripsinya direpresentasikan dengan menggunakan aritmatika modulo dua puluh enam. Cipher ini juga memiliki banyak kelebihan salah satunya adalah mudah digunakan. Namun demikian, dengan kemudahan tersebut masih memberi celah untuk Caesar cipher ditembus oleh pihak yang tidak berwenang. Vernam cipher merupakan salah satu teknik dalam kriptografi yang sulit untuk ditembus. Vernam juga dikenal dengan satu-satunya kriptosistem yang tidak dapat ditembus (Agung, Heryana, & Solehudin, 2020; Deolika, 2020). Namun kesulitannya adalah pembuatan kunci dari algoritma ini bergantung pada waktu sistem saat ini. Oleh karena itu kunci yang berbeda dihasilkan untuk meningkatkan keamanan. Hill Cipher secara garis besar merupakan cipher blok yang memiliki beberapa keunggulan seperti menyamarkan frekuensi huruf plaintext, kesederhanaannya karena menggunakan perkalian matriks dan inversi untuk penyandian dan menguraikan, kecepatannya yang tinggi (Hammad et al., 2022; Rauf, 2020). Di sisi lain, Hill cipher masih memiliki kelemahan, salah satunya adalah mudahnya sandi tersebut untuk dapat dipecahkan. Ketiga jenis cipher tersebut, secara berdiri sendiri, masih memiliki celah-celah untuk dapat ditembus oleh pihak yang tidak berwenang. Dengan demikian, untuk meminimalisir hal tersebut, salah satu caranya adalah melakukan modifikasi. Dalam hal ini yang dilakukan adalah dengan menggabungkan ketiga jenis cihper tersebut untuk meminimalisir kemungkinan untuk dapat ditembus namun tetap lebih sederhana dan mudah untuk digunakan.

Telah dilakukan proses kriptografi dengan menggunakan kombinasi dari metode Caesar Cipher, Vernam Cipher, dan Hill Cipher untuk contoh pesan yang akan dienkripsikan adalah

*Kelompok1HadiBowoRinaldi* dan dipilih key (n) 3. Adapun uraiannya adalah sebagai berikut. . Langkah pertama dilakukan dengan mengubah plaintext ke dalam bentuk bilangan biner.

K : 01001011
e : 01100101
l : 01101100
o : 01101111
m: 01101101
p : 01110000
o : 01101111
k : 01101011
1 : 00110001
H : 01001000
a : 01100001
d : 01100100
i : 0 1101001
B : 01000010
o : 01101111
w: 01110111
o : 01101111
R : 01010010
i : 01101001
n : 01101110
a : 01100001
l : 01101100
d : 01100100
i : 01101001

Langkah selanjutnya adalah dengan melakukan pergeseran sebanyak n langkah kearah kanan

K : 01101001
e : 10101100
l : 10001101
o : 11101101
m: 10101101
p : 00001110
o : 11101101
k : 01101101
1 : 00100110
H : 00001001
a : 00101100
d : 10001100
i : 00101101
B : 01001000
o : 11101101
w: 11101110
o : 11101101
R : 01001010
i : 00101101
n : 11001101
a : 00101100
l : 10001101
d : 10001100
i : 00101101

Selanjutnya, dilakukan proses enkripsi dari hasil Caesar Cipher ke bentuk Vernam Cipher, dengan cara mengubah plaintext dan key ke dalam bentuk bilangan biner

K : 01101001

e : 10101100
l : 10001101
o : 11101101
m: 10101101
p : 00001110
o : 11101101
k : 01101101
1 : 00100110
H : 00001001
a : 00101100
d : 10001100
i : 00101101
B : 01001000
o : 11101101
w: 11101110
o : 11101101
R : 01001010
i : 00101101
n : 11001101
a : 00101100
l : 10001101
d : 10001100
i : 00101101
3 : 00110011

Kemudian dilakukan proses enkripsi dengan menggunakan logika Ex-OR dan ubah ke bentuk desimal.

K : 01011010 : 90
e : 10011111 : 191
l : 10111110 : 190
o : 11011110 : 222
m: 11101101 : 237
p : 00110011 : 67
o : 11011110 : 222
k : 01011110 : 94
1 : 00010101 : 21
H : 00111010 : 58
a : 00011111 : 31
d : 10111111 : 221
i : 00011110 : 30
B : 01111011 : 123
o : 11011110 : 222
w: 11011101 : 221
o : 11011110 : 222
R : 01001010 : 121
i : 00011110 : 30
n : 11111110 : 254
a : 00011111 : 31
l : 10111110 : 190
d : 10111111 : 221
i : 00011110 : 30

langkah selanjutnya adalah dengan melakukan proses enkripsi dari hasil Vernam Cipher ke bentuk Hill Cipher. Kemudian, tentukan matriks enkripsi A yang memiliki ordo $nxn$. Matriks tersebut dapat dibuat dari key dengan cara :

$$A = \begin{bmatrix} key & key+1 \\ key-1 & key-2 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix}$$

Selanjutnya kelompokan bilangan bulat hasil cipher sebelumnya sebanyak dua bilangan dan dibentuk menjadi vector.

$$p_1 = \begin{bmatrix} 90 \\ 191 \end{bmatrix}, p_2 = \begin{bmatrix} 190 \\ 222 \end{bmatrix}, p_3 = \begin{bmatrix} 237 \\ 67 \end{bmatrix}, p_4 = \begin{bmatrix} 222 \\ 94 \end{bmatrix}, p_5 = \begin{bmatrix} 21 \\ 58 \end{bmatrix}, p_6 = \begin{bmatrix} 31 \\ 221 \end{bmatrix}, p_7 = \begin{bmatrix} 30 \\ 123 \end{bmatrix}, p_8 = \begin{bmatrix} 222 \\ 221 \end{bmatrix},$$
$$p_9 = \begin{bmatrix} 222 \\ 121 \end{bmatrix}, p_{10} = \begin{bmatrix} 30 \\ 254 \end{bmatrix}, p_{11} = \begin{bmatrix} 30 \\ 190 \end{bmatrix}, p_{12} = \begin{bmatrix} 221 \\ 30 \end{bmatrix}$$

Kemudian dicari vector $c_1, c_2, \dots, c_n$ dengan cara mengalikan matriks A dengan vector p dan hasil perkaliannya diubah ke modulo 255.

$$c_k = Ap_k$$
$$c_1 = Ap_1 = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 90 \\ 191 \end{bmatrix} = \begin{bmatrix} 14 \\ 116 \end{bmatrix}$$
$$c_2 = Ap_2 = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 190 \\ 222 \end{bmatrix} = \begin{bmatrix} 183 \\ 92 \end{bmatrix}$$
$$c_3 = Ap_3 = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 237 \\ 67 \end{bmatrix} = \begin{bmatrix} 214 \\ 31 \end{bmatrix}$$
$$c_4 = Ap_4 = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 222 \\ 94 \end{bmatrix} = \begin{bmatrix} 22 \\ 28 \end{bmatrix}$$
$$c_5 = Ap_5 = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 21 \\ 58 \end{bmatrix} = \begin{bmatrix} 40 \\ 100 \end{bmatrix}$$

$$c_k = Ap_k$$
$$c_1 = Ap_1 = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 90 \\ 191 \end{bmatrix} = \begin{bmatrix} 14 \\ 116 \end{bmatrix}$$
$$c_2 = Ap_2 = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 190 \\ 222 \end{bmatrix} = \begin{bmatrix} 183 \\ 92 \end{bmatrix}$$
$$c_3 = Ap_3 = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 237 \\ 67 \end{bmatrix} = \begin{bmatrix} 214 \\ 31 \end{bmatrix}$$
$$c_4 = Ap_4 = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 222 \\ 94 \end{bmatrix} = \begin{bmatrix} 22 \\ 28 \end{bmatrix}$$
$$c_5 = Ap_5 = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 21 \\ 58 \end{bmatrix} = \begin{bmatrix} 40 \\ 100 \end{bmatrix}$$

Selanjutnya dilakuakn konversi bilangan pada vector $c_1, c_2, \dots$ menjadi karakter sehingga didapat ciphertext akhir :

| |
|---|
| [Shift Out]t·\Ö[Unit Separator][Synchronous Idle][File Separator](dÔ[File Separator]H·[Device Control 4]›,7V;Uú[Device Control 2]Ù |

Untuk proses dekripsi dari kombinasi Caesar Cipher, Vernam Cipher, dan Hill Cipher dilakukan dengan langkah-langkah sebagai berikut. Langkah pertama, Tentukan invers dari matriks enkripsi A. Langkah kedua adalah dengan mengelompokkan ciphertext sebanyak n karakter konversikan menjadi bilangan bulat. Langkah ketiga dilakukan dengan membentuk kelompok bilangan bulat tersebut menjadi vektor $c_1, c_2, \dots, c_k$. Langkah keempat dilakukan dengan mencari vektor $p_1, p_2, \dots, p_n$ dengan cara mengalikan matriks $A^{-1}$ dengan vektor c, atau dapat dituliskan dengan $p_k = A^{-1}c_k$. Langkah kelima dilakukan dengan mengenkripsikan hasil dari Hill Cipher ke bentuk Vernam Cipher. Langkah kelima adalah dengan mengubah ciphertext dan key ke dalam bentuk bilangan biner. Langkah keenam dilakukan proses enkripsi dengan menggunakan logika Ex-Or. Langkah ketujuh, Hasil enkripsi Vernam Cipher lalu dienkripsikan ke bentuk Caesar Cipher. Langkah kedelapan dilakukan perubahan chipertext ke dalam bentuk bilangan biner. Langkah kesembilan dilakukan pergeseran sebanyak n ke arah kiri. Langkah terakhir adalah konversi dari hasil pergeseran tersebut ke dalam bentuk karakter atau huruf.

Proses kriptografi dengan kombinasi metode Vernam Cipher, Hill Cipher, dan Caesar Cipher dengan terlebih dahulu membuat pesan yang akan dienkripsikan dan menentukan key (n) yang akan digunakan dalam proses enkripsi. Contoh pesan yang akan dienkripsikan adalah Kelompok1HadiBowoRinaldi dengan key (n) 3. Adapun tahapan dari proses enkripsi yang akan dilakukan ialah sebagai berikut. Pertama dilakukan pengubahan plaintext dan key ke dalam bentuk bilangan biner.

K : 01001011
e : 01100101
l : 01101100
o : 01101111
m: 01101101

p : 01110000
o : 01101111
k : 01101011
1 : 00110001
H : 01001000
a : 01100001
d : 01100100
i : 01101001
B : 01000010
o : 01101111
w : 01110111
o : 01101111
R : 01010010
i : 01101001
n : 01101110
a : 01100001
l : 01101100
d : 01100100
i : 01101001
3 : 00110011

Kemudian lakukan proses enkripsi dengan menggunakan logika Ex-OR

K : 01111000
e : 01010110
l : 01011111
o : 01011100
m : 01011110
p : 01000011
o : 01011100
k : 01011000
1 : 00000010
H : 01111011
a : 01010010
d : 01010111
i : 01011010
B : 01110001
o : 01011100
w : 01000100
o : 01011100
R : 01100001
i : 01011010
n : 01011101
a : 01010010
l : 01011111
d : 01010111
i : 01011010

Selanjutnya dilakukan konversi dari hasil enkripsi Vernam Cipher ke dalam bilangan decimal

K : 01111000 : 120
e : 01010110 : 86
l : 01011111 : 95
o : 01011100 : 92
m : 01011110 : 94
p : 01000011 : 67
o : 01011100 : 92
k : 01011000 : 88
1 : 00000010 : 2

H : 01111011 : 123
a : 01010010 : 82
d : 01010111 : 87
i : 01011010 : 90
B : 01110001 : 113
o : 01011100 : 92
w : 01000100 : 68
o : 01011100 : 92
R : 01100001 : 97
i : 01011010 : 90
n : 01011101 : 93
a : 01010010 : 82
l : 01011111 : 95
d : 01010111 : 87
i : 01011010 : 90

Kemudian dikelompokkan bilangan bulat hasil cipher sebelumnya sebanyak tiga bilangan dan dibentuk menjadi vector

$$p_1 = \begin{bmatrix}120\\86\\95\end{bmatrix}, p_2 = \begin{bmatrix}92\\94\\67\end{bmatrix}, p_3 = \begin{bmatrix}92\\88\\2\end{bmatrix}, p_4 = \begin{bmatrix}123\\82\\87\end{bmatrix}, p_5 = \begin{bmatrix}90\\113\\92\end{bmatrix}, p_6 = \begin{bmatrix}68\\92\\97\end{bmatrix}, p_7 = \begin{bmatrix}90\\93\\82\end{bmatrix}, \quad p_8 = \begin{bmatrix}95\\87\\90\end{bmatrix}$$

Akan dicari vector $c_1, c_2, \dots, c_n$ dengan cara mengalikan matriks A dengan vector p dan hasil perkaliannya diubah ke modulo 255.

$$A = \begin{bmatrix} key & key-1 & key-2 \\ key+1 & key+2 & key+3 \\ key+2 & key+3 & key+4 \end{bmatrix}$$

$$A = \begin{bmatrix}3&2&1\\4&5&6\\5&6&7\end{bmatrix}$$

$$c_1 = Ap_1 = \begin{bmatrix}3&2&1\\4&5&6\\5&6&7\end{bmatrix}\begin{bmatrix}120\\86\\95\end{bmatrix} = \begin{bmatrix}117\\205\\251\end{bmatrix}$$

$$c_2 = Ap_2 = \begin{bmatrix}3&2&1\\4&5&6\\5&6&7\end{bmatrix}\begin{bmatrix}92\\94\\67\end{bmatrix} = \begin{bmatrix}21\\220\\218\end{bmatrix}$$

$$c_3 = Ap_3 = \begin{bmatrix}3&2&1\\4&5&6\\5&6&7\end{bmatrix}\begin{bmatrix}92\\88\\2\end{bmatrix} = \begin{bmatrix}199\\55\\237\end{bmatrix}$$

$$c_4 = Ap_4 = \begin{bmatrix}3&2&1\\4&5&6\\5&6&7\end{bmatrix}\begin{bmatrix}123\\82\\87\end{bmatrix} = \begin{bmatrix}110\\149\\186\end{bmatrix}$$

$$c_5 = Ap_5 = \begin{bmatrix}3&2&1\\4&5&6\\5&6&7\end{bmatrix}\begin{bmatrix}90\\113\\92\end{bmatrix} = \begin{bmatrix}78\\202\\242\end{bmatrix}$$

$$c_6 = Ap_6 = \begin{bmatrix}3&2&1\\4&5&6\\5&6&7\end{bmatrix}\begin{bmatrix}68\\92\\97\end{bmatrix} = \begin{bmatrix}230\\39\\41\end{bmatrix}$$

$$c_7 = Ap_7 = \begin{bmatrix}3&2&1\\4&5&6\\5&6&7\end{bmatrix}\begin{bmatrix}90\\93\\82\end{bmatrix} = \begin{bmatrix}28\\42\\52\end{bmatrix}$$

$$c_8 = Ap_8 = \begin{bmatrix}3&2&1\\4&5&6\\5&6&7\end{bmatrix}\begin{bmatrix}95\\87\\90\end{bmatrix} = \begin{bmatrix}39\\80\\97\end{bmatrix}$$

Selanjutnya dilakukan dikonversi hasil modulo dari modulo di atas ke dalam bilangan biner.

117 : 01110101
205 : 11001101
251 : 11111011

21 : 00010101
220 : 11011100
218 : 11011010
199 : 11000111
55 : 00110111
237 : 11101101
110 : 01101110
149 : 10010101
186 : 10111010
78 : 01001110
202 : 11001010
242 : 11110010
230 : 11100110
39 : 00100111
41 : 00101001
28 : 00011100
42 : 00101010
52 : 00110100
39 : 00100111
80 : 01010000
97 : 01100001

Langkah selanjutnya adalah melakukan pergeseran sebanyak n langkah kearah kanan.

117 : 10101110
205 : 10111001
251 : 01111111
21 : 10100010
220 : 10011011
218 : 01011011
199 : 11111000
55 : 11100110
237 : 10111101
110 : 11001101
149 : 10110010
186 : 01010111
78 : 11001001
202 : 01011001
242 : 01011110
230 : 11011100
39 : 11100100
41 : 00100101
28 : 10000011
42 : 01000101
52 : 10000110
39 : 11100100
80 : 00001010
97 : 00101100

Kemudian dilakukan dikonversi hasil bilangan biner tersebut ke dalam huruf atau karakter.

117 : ®
205 : ¹
251 : [DEL]
21 : ¢
220 : ›
218 : [
199 : ø
55 : æ

237 : ½
110 : Í
149 : ²
186 : W
78 : É
202 : Y
242 : ^
230 : Ü
39 : ä
41 : %
28 : ƒ
42 : E
52 : †
39 : ä
80 : [LINE FEED]
97 : ,

Sehingga diperoleh ciphertext dari plaintext tersebut adalah ®[1][DEL]¢›[øæ½Í²WÉY^Üä%ƒE†ä[LINE FEED]. Untuk proses dekripsi dari kombinasi Vernam Cipher, Hill Cipher, dan Caesar Cipher yaitu, pertama dilakukan perubahan ciphertext dan key ke dalam bentuk bilangan biner. Kemudian dilakukan pergeseran ke arah kiri sebanyak n langkah. Hasil enkripsi Caesar Cipher lalu dienkripsikan ke bentuk Hill Cipher. Kemudian, dilakukan penentuan invers dari matriks enkripsi A. Selanjutnya dibentuk kelompok bilangan bulat tersebut menjadi bentuk vector $c_1, c_2, \dots, c_k$. Kemudian dicari vektor $p_1, p_2, \dots, p_n$ dengan cara mengalikan matriks $A^{-1}$ dengan vektor $c$, atau dapat ditulis $p_k = A^{-1}c_k$. Selanjutnya, dienkripsikan hasil dari Hill Cipher ke bentuk Vernam Cipher. Langkah selanjutnya adalah melakukan perubahan ciphertext dan key ke dalam bentuk bilangan biner. Kemudian dilakukan proses enkripsi dengan menggunakan logika Ex-Or. Terakhir, hasil enkripsi Vernam Cipher lalu dikonversi ke dalam bilangan bulat

Proses tersebut di atas merupakan pengembangan dari metode yang telah ada, dalam hal ini, metode Caesar Cipher, Vernam Cipher, dan Hill Cipher yang dalam penggunaannya dilakukan secara terpisah. Namun demikian, permasalahan yang ada adalah masing-masing metode tersebut masih memiliki kekurangan dalam penggunaannya. Oleh karena itu, pengembangan dilakukan dengan melakukan penggabungan ketiga metode tersebut dengan urutan langkah pertama digunakan metode Caesar Cipher, langkah kedua menggunakan Vernam Cipher, dan langkah terakhir menggunakann Hill Cipher. Tujuannya adalah meminimalisir kekurangan yang ditimbulkan dari penggunaan ketiga metode tersebut secara tersendiri. Dalam langkah enkripsi dengan menggunakan metode Caesar Cipher terdiri dari empat langkah perubahan plaintext ke dalam bentuk biner. Berdasarkan hasil tersebut, dilakukan perubahan ke dalam bentuk matriks yang berukuran 2x2. Setelah itu diperoleh pula 12 vektor dari pengelompokkan bilangan bulat hasil cipher sebelumnya. Selanjutnya vektor-vektor tersebut dikalikan dengan matriks berukuran 2x2 untuk memperoleh vektor baru yang akhirnya dirubah kedalam karakter, yang menjadi ciphertext. Telah dilakukan pula proses dengan menggunakan kombinasi dari ketiga metode tersebut. Berdasarkan hasil penelitian yang telah dilakukan tersebut, kombinasi dari ketiga metode Caesar Cipher, Vernam Cipher, dan Hill Cipher , menghasilkan tingkat keamanan yang jauh lebih baik dibandingkan dengan penggunaan metode tersebut dengan berdiri sendiri. Kemudahan dalam penggunaan sandi diperoleh dari langkah pertama dengan Caesar Cipher yang memiliki keunggulan mudah untuk digunakan. Selanjutnya kekurangan dari Caesar Cipher yang mudah untuk ditembus, dapat diminimalisir dengan cukup signifikan dengan adanya penggunaan Vernam Cipher yang terkenal dengan istilah salah satu metode kriptografi yang sulit untuk ditembus. Namun demikian, kekurangan dari Vernam Cipher dengan rumitnya pembuatan kunci dapat diminimalisir dengan penggunaan Hill Cipher yang dalam penggunaannya memanfaatkan matriks. Dengan demikian penggunan kombinasi ketiga metode tersebut disarankan untuk digunakan dibandingkan dengan penggunaannya secara bediri sendiri (Agung et al., 2020; Dewi, 2020). Beberapa penelitian sebelumnnya menunjukkan bahwa *metode Hill Cipher dan Stream Cipher* dapat meningkatkan keamanan database lebih baik (Deolika, 2020; Merlin Tan et al., 2020). Penelitian lainnya menunjukkan bahwa menggabungkan dua algoritma kriptografi dapat lebih meningkatkan keamanan dari citra dibandingkan dengan hanya satu algoritma (Nasuton, Haryanto, & Saleh, 2020).

Namun demikian, terdapat sedikit keterbatsan dalam penelitian ini. Proses yang dilakukan cukup panjang dan memerlukan kehati-hatian dalam setiap prosesnya. Hal tersebut dikarenakan apabila terdapat kesalahan dalam satu langkah saja, maka akan berdampak dengan terganggunya pesan yang akan disampaikan. Bahkan dapat mengakibatkan tidak tersampaikannya pesan. Oleh karena itu, walaupun

penelitian ini dapat dilakukan secara manual, namun hal tersebut tidak dilakukan (disarankan). Proses komputasi pada penelitian ini dilakukan dengan menggunakan bantuan C++ dan Maple.

## 4. SIMPULAN

Metode Caesar Cipher, Vernam Cipher, dan Hill Cipher Metode cipher dapat memberikan tingkat kemanan data yang berbeda-beda. Telah diuraikan pula pengembangan ketiga metode tersebut yang di dalamnya melibatkan matriks. Adapun pengembangan yang dilakukan adalah dengan melakukan kombinasi atau penggabungan dari ketiga metode tersebut. Berdasarkan hasil penelitian yang telah diuraikan di atas, proses kombinasi dari berbagai ketiga metode cipher tersebut dapat menghasilkan tingkat keamanan data yang jauh lebih baik daripada hanya dengan menggunakan satu metode cipher saja. Kombinasi Cipher dari metode Caesar cipher, Vernam cipher dan Hill cipher, dapat dikombinasikan menjadi suatu metode dalam proses kriptografi dengan tingkat keamanan yang cukup kuat. Namun demikian, dalam proses komputasinya memerlukan kehati-hatian untuk mencegah terjadinya gangguan pada saat pengiriman pesan.

## 5. UCAPAN TERIMAKASIH

Penelitian ini didanai oleh Hibah Riset Unpad dengan Nomor Kontrak “1549/UN6.3.1/PT.00/2023 Tanggal 27 Maret 2023.

## 6. DAFTAR PUSTAKA

Agung, A., Heryana, N., & Solehudin, A. (2020). Combination of Hill Cipher Algorithm and Caesar Cipher Algorithm for Exam Data Security. *Buana Information Technology and Computer Sciences (BIT and CS)*, *1*(2), 42–45. https://doi.org/10.36805/BIT-CS.V1I2.1072.

Anwar, S., Nugroho, I., & Ahmadi, A. (2015). Implementasi Kriptografi Dengan Enkripsi Shift Vigenere Chiper Serta Checksum Menggunakan CRC32 Pada Data Text. *JSiI (Jurnal Sistem Informasi)*, *2*. https://doi.org/10.30656/JSII.V2I0.69.

Apdilah, D., & Swanda, H. (2018). Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP. *(JurTI) Jurnal Teknologi Informasi*, *2*(1), 45–52. https://doi.org/10.36294/JURTI.V2I1.407.

Astuti, P. (2015). Kajian Dan Penerapan Penggabungan Steganograpi Dan Kryptograpi Pada Gambar Dan Teks. *Faktor Exacta*, *5*(4), 296–303. https://doi.org/0.30998/FAKTOREXACTA.V5I4.210.

Caniago, T. (2019). Peningkatan Keamanan Pesan Text Menggunakan Metode XOR Dengan Algoritma Vernam. *Kumpulan Karya Ilmiah Mahasiswa Fakultas Sains Dan Tekhnologi*, *1*(1), 385–385. Retrieved from https://journal.pancabudi.ac.id/index.php/fastek/article/view/2164.

Dawahdeh, Z. E., Yaakob, S. N., & Razif bin Othman, R. (2018). A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. *Journal of King Saud University - Computer and Information Sciences*, *30*(3), 349–355. https://doi.org/10.1016/J.JKSUCI.2017.06.004.

Deolika, A. (2020). Modifikasi Metode Hill Cipher dan Vernam Cipher Mengunakan Kode Administrasi dan Pajak. *(JurTI) Jurnal Teknologi Informasi,* *4*(2), 224–227. https://doi.org/10.36294/JURTI.V4I2.1345.

Dewi, Y. P. (2020). Pengembangan Teknik Steganografi Dengan Kriptografi Modifikasi dari Caesar Cipher dan SHA-256 Untuk Merahasiakan Pesan. *Journal of Computer Science and Visual Communication Design*, *5*(1), 10–21.

Elhabshy, A. A. (2019). Augmented Hill Cipher. *International Journal of Network Security*, *21*(5), 812. https://doi.org/10.6633/IJNS.201909.

Es-Sabry, M., Akkad, N. el, Merras, M., Saaidi, A., & Satori, K. (2018). A novel text encryption algorithm based on the two-square cipher and caesar cipher. *Communications in Computer and Information Science*, (78–88). https://doi.org/10.1007/978-3-319-96292-4_7/COVER.

Gunawan, I., Sumarno, Tambunan, H. S., Irawan, E., Qurniawan, H., & Hartama, D. (2019). Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages. *Journal of Physics: Conference Series*, *1255*(1). https://doi.org/10.1088/1742-6596/1255/1/012077.

Hammad, R., Latif, K. A., Amrullah, A. Z., Hairani, Subki, A., Irfan, P., Zulfikri, M., … Marzuki, K. (2022). Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message. *Journal of Physics: Conference Series*, *2279*(1). https://doi.org/10.1088/1742-6596/2279/1/012006.

Irnanda, Y. (2019). Enkripsi dan Dekripsi Dengan Menggunakan Metode Kriptografi Vernam Cipher(XOR).

*Kumpulan Karya Ilmiah Mahasiswa Fakultas Sains Dan Tekhnologi*, *1*(1), 47. Retrieved from https://journal.pancabudi.ac.id/index.php/fastek/article/view/1397.

Jain, A., Dedhia, R., & Patil, A. (2015). Enhancing the security of caesar cipher substitution method using a randomized approach for more secure communication. *International Journal of Computer Applications*, *129*(13), 6–11. https://doi.org/10.5120/ijca2015907062.

Kriptografi, M., Cipher, H., Matriks, K., Panjang, P., Fungsi, M., Dan, X. Hikmah, A. B. (2016). Modifikasi Kriptografi Hill Cipher Kunci Matriks Persegi Panjang Menggunakan Fungsi Xor Dan Fungsi Xnor. *IJCIT (Indonesian Journal on Computer and Information Technology)*, *1*(1). https://doi.org/10.31294/IJCIT.V1I1.423.

Lubis, A. H. (2017). Enkripsi Data Dengan Algoritma Kriptrografi Noekeon. *Cess (Journal of Computer Engineering, System and Science)*, *2*(1), 22–26. https://doi.org/10.24114/CESS.V2I1.4966.

Maihankali, M., & Eze, E. C. (2021). Symmetric Cryptography for Confidential Communications: Implemented by Enhancing the Caesar Cipher. *International Journal of Computing and Engineering, 2*(1). Retrieved from https://carijournals.org/journals/index.php/IJCE/article/view/605.

Merlin Tan, C. S., Arada, G. P., Abad, A. C., al, Julianita Siregar, S., Zarlis, M., Situmorang -, Z., … Kelana Simpony, B. (2020). Generation of Rectangular Matrix Key for Hill Cipher Algorithm Using Playfair Cipher. ,. *Journal of Physics: Conference Series*, *1641*(1). https://doi.org/10.1088/1742-6596/1641/1/012094.

Mesran, M., & Nasution, S. D. (2020). Peningkatan Keamanan Kriptografi Caesar Cipher dengan Menerapkan Algoritma Kompresi Stout Codes. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(6), 1209 – 1215. https://doi.org/10.29207/RESTI.V4I6.2730.

Nasution, A. B. (2019). Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher Dan Transposisi Cipher. *(Jurti) Jurnal Teknologi Informasi*, *3*(1), 1–6. https://doi.org/10.36294/Jurti.V3i1.680.

Nasuton, M. A., Haryanto, E. V., & Saleh, A. (2020). Penerapan Metode Hill Cipher Dan Stream Cipher Dalam Mengamankan Database MySQL. *Jurna l Mahasiswa Fakultas Teknik Dan Ilmu KOmputer*, *1*(1). Retrieved from https://www.e-journal.potensi-utama.ac.id/ojs/index.php/FTIK/article/view/904/0.

Novianto, D., & Setiawan, Y. (2019). Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Informatika Global*, *9*(2). https://doi.org/10.36982/JIIG.V9I2.561.

Paragas, J. R., Sison, A. M., & Medina, R. P. (2019). Hill cipher modification: A simplified approach. 2019 IEEE 11th International Conference on Communication Software and Networks,. *ICCSN*, 821–825. https://doi.org/10.1109/ICCSN.2019.8905360.

Pawar, B. K., & Hatkar, S. S. (2016). Symmetric Key Algorithm Using Vernam Cipher:VSA. *Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016*. https://doi.org/10.1109/INVENTIVE.2016.7830196.

Putri, Y. D., Rosihan, R., & Lutfi, S. (2019). Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance. *Jurnal Informatika Dan Komputer*, *2*(2), 87–94. https://doi.org/10.33387/Jiko.V2i2.1319.

Rahim, R., & Steganografi, A. (2016). Penyisipan Pesan Dengan Algoritma Pixel Value Differencing Dengan Algoritma Caesar Cipher Pada Proses Steganografi. ,. *Jurnal Times*, *5*(1), 6–11. Retrieved from https://ejournal.stmik-time.ac.id/Index.Php/Jurnaltimes/Article/View/239.

Rauf, B. W. (2020). Kombinasi Steganografi Bit Matching dan Kriptografi Playfair Cipher, Hill Cipher dan Blowfish. *(JurTI) Jurnal Teknologi Informasi*, *4*(2), 228–233. https://doi.org/10.36294/JURTI.V4I2.1346.

Ryabko, B. Y. (2015). The Vernam cipher is robust to small deviations from randomness. *Problems of Information Transmission*, *51*(1), 82–86. https://doi.org/10.1134/S0032946015010093.

Siahaan, M. D. L., & Siahaan, A. P. U. (2018). Application of Hill Cipher Algorithm in Securing Text Messages. *International Journal For Innovative Research in Multidiscliplinary Field*, *4*(10), 55–59. https://doi.org/10.31227/OSF.IO/N2KDB.

Simargolang, M. Y. (2017). Implementasi Kriptografi Rsa Dengan Php. *Jurnal Teknologi Informasi*, *1*(1), 1. https://doi.org/10.36294/JURTI.V1I1.1.

Sundarayya, P., & Prasad, G. V. (2019). A public key cryptosystem using Affine Hill Cipher under modulation of prime number. *Journal of Information and Optimization Sciences*, *40*(4), 919–930. https://doi.org/10.1080/02522667.2018.1470751.

Zamara, S. (2019). Penerapan Algoritma Vegenere Cipher Dan Vernam Cipher Dalam Penggamanan File Text. *Jurnal Riset Komputer (JURIKOM)*, *6*(3).