Penggunaan Matriks Sirkulan dalam Modifikasi Metode Hill Cipher

Sisilia Sylvinani
Departemen Matematika FMIPA Universitas Padjadjaran, sisilia.sylviani@unpad.ac.id

Fahmi Candra Permana
Program Studi Pendidikan Multimedia, Universitas Pendidikan Indonesia

ABSTRAK, Metode Hill Cipher adalah salah satu teknik kriptografi klasik yang digunakan untuk mengenkripsi teks. Namun, metode ini memiliki beberapa kelemahan, seperti ketika ukuran matriks kunci tidak memenuhi syarat tertentu. Dalam artikel ini, dibahas modifikasi metode Hill Cipher dengan memanfaatkan matriks sirkulan untuk mengatasi kelemahan tersebut. Pada metode Hill Cipher, teks terbagi menjadi blok-blok yang memiliki ukuran yang sama dengan matriks kunci. Kemudian, matriks kunci digunakan untuk mengenkripsi setiap blok teks. Namun, jika ukuran matriks kunci tidak memenuhi syarat bahwa determinan matriks kunci harus relatif prima dengan ukuran alfabet, maka metode ini tidak dapat diterapkan. Matriks sirkulan adalah matriks khusus di mana elemen-elemennya diatur sedemikian rupa sehingga jika satu elemen digeser, elemen-elemen lainnya akan mengikuti pola tertentu. Dalam artikel ini ditunjukkan bahwa dengan menggunakan matriks sirkulan, dapat dihasilkan matriks kunci yang memenuhi syarat determinan untuk metode Hill Cipher.

***Kata Kunci**: Hill Cipher, kriptografi, matriks sirkulan*

1. PENDAHULUAN

Dalam dunia yang semakin terhubung dan tergantung pada teknologi digital, keamanan informasi menjadi isu yang sangat penting. Seiring dengan berkembang pesatnya dunia digital saat ini, kekhawatiran tentang tingkat keamanan dari data yang disimpan atau dikirim secara digital juga merupakan hal menjadi perhatian. Data sensitif dan rahasia harus dilindungi agar tidak jatuh ke tangan yang salah dan disalahgunakan. Oleh karena itu, teknik kriptografi hadir sebagai sarana untuk melindungi dan mengamankan data. Untuk menjawab tantangan tersebut, banyak metode yang ditawarkan, salah satunya adalah dengan menggunakan Kriptografi.

Secara umum, kriptografi merupakan ilmu atau seni mengirim dan menerima pesan yang dirahasiakan atau dikodekan (Baumslag et al., n.d.). Kriptografi telah ada selama berabad-abad, dan seiring dengan perkembangan teknologi, metode kriptografi juga mengalami evolusi. Salah satu teknik kriptografi klasik yang masih digunakan hingga saat ini adalah metode Hill Cipher. Metode ini pertama kali diperkenalkan oleh Lester S. Hill pada tahun 1929 dan menjadi populer karena kecepatan dan keamanannya. Pesan asli yang akan dirahasiakan atau disembunyikan disebut sebagai plainteks sedangkan pesan yang disembunyikan atau yang sudah berbentuk sandi disebut sebagai cipherteks. Adapun proses merubah suatu plainteks ke cipherteks disebut dengan proses enkripsi, sedangkan proses sebalikanya atau dengan kata lain merubah cipherteks ke plainteks disebut sebagai proses dekripsi.

Algoritma kriptografi terbagi ke dalam dua kategori yaitu simetris dan asimetris. Kategori yang pertama, Algoritma kriptografi simetris ialah algoritma yang memanfaatkan kunci yang identik untuk melakukan proses enkripsi dan dekripsi. Sedangkan algoritma kriptografi asimetris ialah algoritma yang memakai kunci yang berbeda untuk melakukan proses enkripsi dan dekripsi. Didalam artikel ini dibahas mengenai salah satu algoritma kriptografi simetris yaitu Hill cipher berbasis matriks sirkulan.

Hill cipher merupakan merupakan algoritma block cipher dimana plainteks dibagi menjadi blok-blok yang memiliki ukuran yang sama, alat pembuka atau kuncinya adalah matriks yang invertible dan berukuran $n \, x \, n$, dengan n merupakan ukuran blok (El et al., n.d.) . Namun, Hill cipher memiliki kekurangan yang cukup signifikan yaitu plainteks dan cipherteksnya sangat rentan untuk dapat diakses oleh orang lain. Dengan demikian informasi rahasia seperti kunci dan kodenya dapat diketahui dengan mudah. Oleh karena itu metode Hill Cipher sudah tidak digunakan lagi dalam proses pengiriman pesan rahasia. Namun demikian, secara pedagogic, Hill Cipher masih memiliki peranan yang penting dalam kriptologi, terutama

karena kombinasi keamanan dan fleksibilitasnya yang tergantung pada konsep aljabar linier.

Beberapa alasan mengapa Hill Cipher masih memegang peranan penting diantaranya adalah penggunaan matriks sebagai kunci enkripsi. Proses enkripsi melibatkan perkalian matriks dan operasi modulo, yang memanfaatkan sifat-sifat aljabar linier. Kemudian, keamanan Hill Cipher tergantung pada kesulitan memecahkan persamaan matriks, yang merupakan masalah yang rumit dan sulit dipecahkan jika ukuran matriks (kunci) cukup besar. Penelitian terkait Hill Cipher terus dilakukan dalam rangka meningkatkan kemanan dari hill cipher yang masih terus digunakan dikarenakan penggunaan matriks sebagai kunci memberikan keunikan dan fleksibilitas dalam desain kunci. Untuk itu, dalam artikel ini akan dibahas beberapa pengembangan dari metode tersebut.

Metode Hill Cipher menggunakan matriks kunci sebagai kunci enkripsi. Teks yang akan dienkripsi dibagi menjadi blok-blok yang memiliki ukuran yang sama dengan matriks kunci. Setiap blok teks diubah menjadi vektor kolom dan dikalikan dengan matriks kunci. Hasil perkalian tersebut menghasilkan teks terenkripsi. Meskipun metode Hill Cipher memiliki keunggulan, seperti kemampuan untuk mengenkripsi data dengan cepat walaupun metode ini juga memiliki beberapa kelemahan yang perlu diperhatikan. Salah satu kelemahan utamanya adalah pemilihan ukuran matriks kunci yang memenuhi syarat-syarat tertentu.

Salah satu syarat penting dalam metode Hill Cipher adalah determinan matriks kunci harus relatif prima dengan ukuran alfabet yang digunakan. Jika determinan matriks kunci tidak memenuhi syarat ini, matriks invers dari matriks kunci tidak akan ada, dan metode Hill Cipher tidak dapat diterapkan. Kelemahan ini menjadi kendala dalam penggunaan metode Hill Cipher, terutama ketika ingin mengenkripsi teks dengan ukuran yang tidak kompatibel dengan matriks kunci yang tersedia. Ini mengurangi fleksibilitas metode Hill Cipher dalam mengenkripsi berbagai jenis teks dengan ukuran yang beragam. Untuk mengatasi kelemahan ini, diusulkan modifikasi metode Hill Cipher dengan memanfaatkan konsep matriks sirkulan.

Matriks sirkulan adalah matriks persegi yang setiap baris atau kolomnya dapat dihasilkan dengan memutar baris atau kolom sebelumnya ke posisi berikutnya tanpa mengubah urutan elemennya, dan sifat ini memiliki aplikasi penting dalam perkalian matriks, invers matriks, pemrosesan sinyal, dan aljabar linier, memberikan kontribusi dalam pengolahan sinyal, analisis numerik, dan perancangan algoritma. Dengan menggunakan matriks sirkulan, dapat dibangun suatu matriks kunci yang memenuhi syarat determinan dengan lebih fleksibel.

2. METODOLOGI

Adapun metode penelitian yang digunakan adalah sebagai berikut:

1. Langkah pertama dalam penelitian ini adalah melakukan studi literatur yang mendalam tentang metode Hill Cipher, konsep matriks sirkulan, dan penelitian terkait lainnya. Studi literatur akan memberikan pemahaman yang kuat tentang dasar-dasar teori yang terkait dengan topik penelitian ini.
2. Selanjutnya, akan dianalisis secara rinci kelemahan metode Hill Cipher terkait dengan pemilihan ukuran matriks kunci. Akan ditinjau syarat-syarat yang harus dipenuhi oleh matriks kunci dan konsekuensinya jika syarat-syarat tersebut tidak terpenuhi.
3. Kajian Konsep Matriks Sirkulan yang ditinjau dari segi aljabar.
4. Berdasarkan pengetahuan yang diperoleh dari studi literatur dan analisis kelemahan metode Hill Cipher, dirancang modifikasi metode Hill Cipher dengan menggunakan matriks sirkulan.
5. Berdasarkan hasil dan analisis yang diperoleh, dilakukan diskusi terhadap hasil kajian ini.

Melalui pendekatan metodologi ini, diperoleh pemahaman yang komprehensif tentang penggunaan matriks sirkulan dalam modifikasi metode Hill Cipher. Metodologi ini memberi peluang untuk menganalisis keefektifan dan keamanan modifikasi ini, serta memberikan panduan untuk pengembangan lebih lanjut.

Di sisi lain, Pertanyaan-pertanyaan berikut menjadi fokus kajian yang disajikan dalam artikel ini adalah, yang pertama,a Bagaimana sifat-sifat matriks sirkulan? Kemudian Pertanyaan Penelitian yang kedua adalah Bagaimana implementasi matriks sirkulan dalam modifikasi metode hill-cipher? Pertanyaan Penelitian yang terakhir adalah Bagaimana Algoritma hasil modifikasi metode hill-cipher dengan menggunakan matriks sirkulan?

Untuk menjawab pertanyaan penelitian pertama dilakukan tinjauan pustaka yang relevan dengan definisi dan sifat-sifat dari matriks sirkulan. Untuk menjawab pertanyaan penelitian kedua dilakukan penelitian terkait dengan cara menggabungkan secara efektif suatu matriks sirkulan ke dalam metode hill cipher. Terakhir, untuk menyelidiki pertanyaan penelitian ketiga, dilakukan implementasi matriks sirkulan ke dalam metode hill cipher ke dalam algoritma

3. PEMBAHASAN

Hill cipher merupakan algoritma blok cipher polialfabet yang berbasis transformasi linier (Reddy et al., 2012). Teks cipher dituliskan sebagai $C = KP \bmod m$, di mana K adalah matriks kunci, P adalah plaintext, dan C adalah ciphertext, dan proses decoding dituliskan sebagai:

$$P = K^{-1}C \bmod m$$

Nilai dari m yang digunakan dalam Hill cipher adalah 26, namun nilainya dapat diubah sesuai dengan keperluan. Kunci dari Hill cipher adalah $GL\ (n, Z_m)$ yang merupakan sekumpulan matriks berukuran $n\ x\ n$ yang invertible terhadap Z_m . Peluang terambilnya matriks persegi yang invertible adalah satu, untuk nilai modula prima yang besar. Sementara nol untuk modula komposit dengan pembagi prima yang berbeda-beda. Jadi, kesalahan dalam mengambil determinan yang memiliki faktor dari modulus, dapat dikurangi dengan mengambil bilangan prima sebagai modulusnya. Sehingga, bilangan prima dapat membuat matriks kunci yang lebih banyak daripada bilangan komposit.

Kerahasiaan Hill cipher biasanya didasarkan pada kunci matriks K dengan Rank n. Tujuan utama dari Hill cipher adalah untuk mencegah diketahuinya plaintext. Adapun kekurangan-kekurangan dari metode Hill Cipher adalah sebagai berikut:

1. Hill Cipher sangat sensitif terhadap perubahan pada data teks asli yang akan dienkripsi. Jika ada perubahan sedikit pun pada teks asli, maka hasil enkripsi akan sangat berbeda. Hal ini membuat Hill Cipher tidak tahan terhadap kesalahan transmisi data, seperti kesalahan pengetikan atau kerusakan data saat transmisi.
2. Hill Cipher rentan terhadap serangan known plaintext, di mana penyerang memiliki pengetahuan tentang pasangan teks terenkripsi dan teks asli yang sesuai. Dalam Hill Cipher, jika penyerang memiliki cukup banyak pasangan plaintext-terenkripsi, mereka dapat menganalisis pola dan mencoba memecahkan matriks kunci. Dengan matriks kunci yang terungkap, teks terenkripsi dapat dengan mudah didekripsi.
3. Hill Cipher menggunakan matriks kunci sebagai komponen penting dalam proses enkripsi dan dekripsi. Ukuran matriks kunci bergantung pada ukuran blok teks yang dienkripsi. Namun, semakin besar ukuran matriks kunci, semakin kompleks operasi matematika yang terlibat dalam proses enkripsi dan dekripsi. Ini dapat mengakibatkan peningkatan overhead komputasi dan mempengaruhi efisiensi metode Hill Cipher, terutama saat mengenkripsi atau mendekripsi teks dengan ukuran yang besar.
4. Hill Cipher dirancang untuk mengenkripsi teks dalam alfabet tertentu, seperti alfabet Inggris dengan huruf kapital. Metode ini tidak secara langsung dapat diterapkan pada teks dengan karakter khusus, angka, atau alfabet lainnya. Jika digunakan untuk mengenkripsi teks dalam bahasa atau sistem lain yang memiliki aturan karakteristik yang berbeda, perlu dilakukan penyesuaian khusus dalam implementasinya.
5. Hill Cipher bekerja dengan membagi teks asli menjadi blok-blok n huruf, di mana n adalah ukuran matriks kunci. Kelemahan yang muncul adalah bahwa setiap blok hanya dipengaruhi oleh matriks kunci yang sama. Jika ada kesamaan pola atau korrelasi

yang terdeteksi di dalam blok-blok tersebut, penyerang dapat menggunakan informasi ini untuk menganalisis dan memecahkan matriks kunci.

Penting untuk mempertimbangkan kelemahan-kelemahan ini saat menggunakan metode Hill Cipher dan mengidentifikasi skenario di mana metode ini mungkin tidak memberikan keamanan yang optimal. Dalam beberapa kasus, alternatif lain seperti algoritma kriptografi modern dapat lebih direkomendasikan. Modifikasi metode Hill Cipher dengan menggunakan matriks sirkulan melibatkan perubahan pada langkah-langkah enkripsi dan dekripsi. Penggunaan matriks sirkulan dalam proses ini bertujuan untuk meningkatkan keamanan sistem dengan mengurangi kelemahan metode Hill Cipher terhadap serangan known plaintext.

Matriks sirkulan ialah matriks yang setiap barisnya dirotasikan satu entri ke kanan relatif terhadap vektor baris sebelumnya dengan entri diagonalnya yang sama. Matriks sirkulan dapat ditulis sebagai :

$$\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \cdots & c_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix}$$

dan dinotasikan dengan $circl(c_0, c_1, c_2, \dots, c_{n-1})$.

Sebuah matriks sirkulan $n\,x\,n$ disebut sirkulan utama jika gcd vektor barisnya adalah 1. Sebagai contohnya, matriks sirkulan $4\,x\,4$ dengan vektor baris (a, b, c, d) adalah sirkulan utama jika $gcd(a, b, c, d) = 1$. Misalkan G ialah sebuah matriks, Matriks koefisien G dinotasikan dengan G_c dan didefinisikan sebagai

$circ(circ(baris\ 1), circ(baris\ 2), .., circ(baris\ n)),$

dimana baris 1, baris 2,..., baris n adalah vektor baris dari matriks G dan $circ(baris\ i)$ adalah matriks sirkuler dari baris i. Sebagai contohnya jika G adalah matriks $2\,x\,2$ maka G_C adalah matriks $4\,x\,4$.

$$G = \begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \end{bmatrix}$$

$$G_c = \begin{bmatrix} g_1 & g_2 & g_3 & g_4 \\ g_2 & g_1 & g_4 & g_3 \\ g_3 & g_4 & g_1 & g_2 \\ g_4 & g_3 & g_2 & g_1 \end{bmatrix}$$

Modifikasi Hill Cipher dapat melibatkan representasi kunci kriptografi sebagai matriks sirkulan. Sifat-sifat khusus matriks sirkulan, seperti kemudahan dalam perkalian dan invers, dapat memengaruhi kekuatan dan keamanan kunci. Dalam proses enkripsi Hill Cipher, matriks kunci digunakan untuk mengalikan vektor teks terbuka.

Jika matriks kunci diubah menjadi matriks sirkulan, perkalian matriks dapat diimplementasikan dengan lebih efisien menggunakan algoritma seperti Transformasi Fourier Cepat (FFT). Sifat invers matriks sirkulan dapat digunakan dalam proses dekripsi Hill Cipher. Memanfaatkan kemudahan menghitung invers matriks sirkulan dapat meningkatkan efisiensi dalam proses dekripsi dan mengurangi kompleksitas algoritma. Teorema circulant, yang menyatakan bahwa setiap matriks sirkulan dapat diagonalisasi dalam basis dari vektor-eigen sirkulan, dapat memberikan wawasan yang berguna dalam analisis keamanan modifikasi Hill Cipher.

Implementasi matriks sirkulan dalam modifikasi metode Hill Cipher melibatkan penggunaan matriks kunci yang memiliki sifat-sifat khusus dari matriks sirkulan. Berikut adalah beberapa langkah yang dilakukan diantaranya yang pertama adalah penentuan Matriks Kunci Sirkulan. Matriks kunci Hill Cipher diubah agar memiliki struktur matriks sirkulan. Ini dapat dilakukan dengan menyusun matriks kunci sedemikian rupa sehingga setiap baris atau kolom dapat dihasilkan dengan rotasi sirkular dari baris atau kolom sebelumnya. Selanjutnya yang kedua adalah adanya Efisiensi Perkalian Matriks.

Keuntungan utama implementasi matriks sirkulan terletak pada efisiensi perkalian matriks. Dalam metode Hill Cipher yang dimodifikasi, perkalian matriks dapat dioptimalkan dengan memanfaatkan sifat-sifat aljabar linier matriks sirkulan. Kemudian, yang ketiga adalah Penggunaan Invers Matriks Sirkulan dalam Dekripsi. Jika matriks kunci diubah menjadi

matriks sirkulan, invers matriks sirkulan dapat digunakan dalam proses dekripsi. Hal ini dapat meningkatkan efisiensi dalam perhitungan invers matriks dan mengurangi kompleksitas algoritma dekripsi.

Teorema circulant dapat digunakan untuk menganalisis keamanan modifikasi Hill Cipher yang melibatkan matriks sirkulan. Konsep ini dapat memberikan wawasan mengenai struktur kunci dan keamanan kriptografi secara umum. Lebih lanjut lagi, implementasi matriks sirkulan dapat mempengaruhi cara kunci kriptografi dikombinasikan secara linear dalam metode Hill Cipher yang dimodifikasi. Pemilihan dan pengembangan kunci dapat dioptimalkan untuk meningkatkan keamanan. Untuk memberikan gambaran, berikut ini adalah contoh sederhana proses enkripsinya. Misalkan plainteks "halo dunia" dan matriks kunci sirkulan berikut:

| 2 | 3 | 1 |
| 1 | 2 | 3 |

Panjang plainteks adalah 10 karakter, sehingga matriks kunci juga harus memiliki ukuran 10x10.

| h | a | l | o | d | u | n | i | a |
| 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 | 1 |

Matriks plainteks dikalikan dengan matriks kunci secara element-wise.

h	a	l	o	d	u	n	i	a
2	3	1	2	3	1	2	3	1
14	23	26	29	32	35	38	41	44

Hasil perkalian merupakan cipherteks.

| 14 | 23 | 26 | 29 | 32 | 35 | 38 | 41 | 44 |

Adapun untuk proses dekripsi, digambarkan sebagai berikut. Misalkan cipherteks "142326293235384144" dan matriks kunci sirkulan yang sama dengan contoh sebelumnya.

| 1 | 4 | 2 | 3 | 2 | 6 | 2 | 9 | 3 | 2 |
| 3 | 5 | 3 | 8 | 4 | 1 | 4 | 4 |

Matriks cipherteks dikalikan dengan matriks invers kunci secara element-wise.

1	4	2	3	2	6	2	9	3	2
3	5	3	8	4	1	4	4
14	23	26	29	32	35	38	41	44

Hasil perkalian merupakan plainteks.

| h | a | l | o | d | u | n | i | a |

Algoritma

Bagian ini akan menjelaskan tentang modifikasi pada Hill cipher yang berbasis matriks sirkulan, dimana sebuah matriks sirkulan utama dikirimkan sebagai alat untuk memecahkan kode yang sifatnya rahasia dan sebuah matriks G non-singular dipilih sebagai sebuah kunci publik sehingga determinan dari matriks koefisien G_c adalah nol. Algoritmanya ialah sebagai berikut :

1. Pilih sebuah matriks G non-singuler dengan orde $n\,x\,n$ sebagai sebuah kunci publik sehingga determinan $G_c = 0$
2. Pilih sebuah matriks sirkulan utama A sebagai kunci rahasianya.
3. Hitung kunci $K = AGA^{-1}\ mod\ P$.
4. Enkripsi :
5. M_i adalah blok plaintext ke-i dengan ukuran n.
6. C_i adalah blok ciphertext ke i.
7. $C_i = KM_i + V_i^T\ mod\ P$, dimana V_i adalah baris ke$-i$ dari matriks sirkuler utama A.
8. Dekripsi :
9. Hitung $K^{-1} = AG^{-1}\ A^{-1}\ mod\ P$
10. $M_i = K^{-1}\ (C_i - V_i^T)\ mod\ P$

Disini V adalah baris pertama dari matriks sirkulan utama A. Untuk setiap blok enkripsi plaintext, digunakan sebuah vektor kolom V yang ditanspos kan menjadi bentuk vektor baris. ini akan meminimalisir teraksesnya ciphertext oleh pihak ketiga, selama modulanya angka prima. Ini mengurangi kapasitas kunci yang dibutuhkan dari n^2 elemen Z_p menjadi hanya n elemen, karena matriks sepenuhnya ditentukan oleh baris pertamanya. Ini juga mengurangi lamanya waktu yang dibutuhkan untuk menghitung perkalian matriks.

Keamanan dari kriptosistem yang dikemukakan ini dibuat berdasarkan pemikiran terhadap tingkat kesulitan dalam penyelesaian fungsi polinomial multi-variabel yaitu $K = AGA^{-1}\ mod\ P$. Ini akan sulit untuk diselesaikan jika modulanya ialah angka prima yang besar. Sederhanakan rumus tersebut menjadi $G_c\ X = Y\ mod\ P$ dimana elemen X adalah elemen-elemen dari matriks A dan A^{-1}, elemen Y adalah elemen matriks K. Sebagai contohnya : A adalah matriks sirkulan utama $2\,x\,2$, G adalah matriks non-singular $2\,x\,2$, dan kemudian rumus tersebut menjadi

$$\begin{bmatrix} g_1 & g_2 & g_3 & g_4 \\ g_2 & g_1 & g_4 & g_3 \\ g_3 & g_4 & g_1 & g_2 \\ g_4 & g_3 & g_2 & g_1 \end{bmatrix} \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} = \begin{bmatrix} k_{11} \\ k_{12} \\ k_{21} \\ k_{22} \end{bmatrix}$$

Kemudian, dilakukan implementasi algoritma tersebut dalam script program menggunakan Bahasa C++, adapaun hasil program tersebut digambarkan di bawah ini.

```
Program enkriptor dan dekriptor dengan Hll Cipher
Dengan Modifikasi sirkulan modulo 29 dan matriks kunci 2x2
====================================
Masukan matriks A[1][1] : 3
Masukan matriks A[1][2] : 4
Masukan matriks A[2][1] : 4
Masukan matriks A[2][2] : 3
Masukan matriks G[1][1] : 1
Masukan matriks G[1][2] : 2
Masukan matriks G[2][1] : 3
Masukan matriks G[2][2] : 4
PILIH! <1. Enkripsi/2. Dekripsi> : 1
Masukan banyaknya huruf : 4
Huruf ke-1 : m
Huruf ke-2 : a
Huruf ke-3 : t
Huruf ke-4 : h
2       24
10      3
xudx
```

Gambar 1. Contoh Output Program Modifikasi Hill Chiper dengan Matriks Sirkulan

Gambar 1 menguraikan hasil implementasi algoritma tersebut. Program tersebut mengimplementasikan bagaiaman melakukan proses enkripsi dan dekripsi dengan modifikasi Hill Cipher berbasis matriks sirkulan. Secara garis besar cara kerjanya adalah, terlebih dahulu tentukan matriks kunci yang akan digunakan. Kemudian pilih proses yang akan dilakukan Apakah enkripsi atau dekripsi. Setelah itu diminta untuk menginputkan pesan atau kode yang ingin diproses. Setelah itu hasilnya akan keluar. Program tersebut dapat menjadi alat bantu dalam proses pengiriman sandi menjadi lebih efektif dan edisien.

4. KESIMPULAN

Telah dilakukan kajian modifikasi metode Hill cipher yang memanfaatkan matriks sirkulan sebagai alat bantu di dalamnya. Algoritma ini menggunakan kunci rahasia dalam bentuk matriks sirkulan utama dan sebuah kunci publik dalam bentuk matriks, sehingga determinan dari matriks koefisiennya ialah nol. Algoritma yang dikemukakan ini mempunyai invers matriks dan perkalian sebagai satu-satunya operasi yang mana tidak membutuhkan operasi tambahan lainnya. Kriptosistem ini mencegah teraksesnya plaintext dan ciphertext oleh pihak ketiga. Ini juga mencegah teraksesnya ciphertext oleh pihak ketiga, selama modulanya ialah angka prima.

UCAPAN TERIMAKASIH

Penelitian ini didanai oleh Hibah Internal Unpad Riset Percepatan Lektor Kepala (RPLK) tahun 2023 dengan Nomor Kontrak 1549/UN6.3.1/PT.00/2023

5. DAFTAR PUSTAKA

[1] Baumslag, G., Fine, B. 1948-, Kreuzer, M., & Rosenberger, G. (n.d.). A Course in Mathematical Cryptography.

[2] Bakr, M. A., Mokhtar, M. A., & Takieldeen, A. E. S. (2018). Elliptic curve cryptography modified Hill Cipher dependent on circulant matrix. International Journal of Industrial Electronics and Electrical Engineering, 6(1), 24-29.

[3] El, M. A., Bakr, H., Mokhtar, M. A., El, A., & Takieldeen, S. (n.d.). Elliptic Curve Cryptography Modified Hill Cipher dependent on Circulant Matrix.

[4] ElHabshy, A. A. (2019). Augmented Hill Cipher. Int. J. Netw. Secur., 21(5), 812-818.

[5] Koukouvinos, C., & Simos, D. E. (2013). Encryption schemes based on Hadamard matrices with circulant cores. Journal of Applied Mathematics and Bioinformatics, 3(1), 17.

[6] Maxrizal, M. (2019). Hill Cipher Cryptosystem over Complex Numbers. Indonesian Journal of Mathematics Education, 2(1), 9-13.

[7] Rauhut, H., Romberg, J., & Tropp, J. A. (2012). Restricted isometries for partial random circulant matrices. Applied and Computational Harmonic Analysis, 32(2), 242-254.

[8] Reddy, K. A., Vishnuvardhan, B., Madhuviswanatham, & Krishna, A. V. N. (2012). A Modified Hill Cipher Based on Circulant Matrices. Procedia Technology, 4, 114–118.Ary, D., Jacobs, L.C. & Razavieh, A. 1976. Pengantar

Penelitian Pendidikan. Terjemahan oleh Arief Furchan. 1982. Surabaya: Usaha nasional

[9] Yu, F., Kumar, S., Gong, Y., & Chang, S. F. (2014, June). Circulant binary embedding. In International conference on machine learning (pp. 946-954). PMLR.ALIF, A., 2013. Komputasi cerdas untuk pemula. Malang: ABC Press.