PENGGUNAAN ALGORITMA HILL CIPHER DALAM MENGAMANKAN PESAN DENGAN KUNCI SIDIK JARI

Hafif Komarullah[1*], Halimatus Sadiyah[2], Auliya Dwi Wulandari[3]
[1,2,3]*Tadris Matematika, Universitas Al Falah Assunniyyah, Jember, Indonesia*

**Penulis korespondensi: hafififa4@gmail.com*

ABSTRAK

Hill Cipher merupakan salah satu algoritma simetris yang mempunyai kunci enkripsi dan dekripsi sama. Perkembangan teknologi yang makin pesat mengakibatkan *Hill Cipher* dapat dipecahkan menggunakan perkalian matriks dan persamaan linear. Penelitian ini bertujuan untuk mendapatkan fungsi dari gambar sidik jari yang digunakan sebagai kunci enkripsi dan dekripsi pengamanan pesan menggunakan algoritma *Hill Cipher*. Sidik jari dipilih karena bersifat unik artinya tidak seorangpun memiliki sidik jari identik, bahkan pada bayi kembar sekalipun. Langkah-langkah penelitian yaitu pembentukan kunci *Hill Cipher*, proses enkripsi, dan proses dekripsi. Dalam paper ini, disimpulkan bahwa gambar sidik jari dapat digunakan sebagai kunci untuk melakukan enkripsi dan dekripsi pesan menggunakan algoritma *Hill Cipher*. Penggunaan gambar sebagai kunci algoritma *Hill Cipher* bukan merupakan sesuatu yang umum, sehingga hal ini akan menambah kesulitan kriptanalis dalam memecahkan ciphertext.

Kata kunci: kriptografi, *Hill Cipher*, sidik jari

1 PENDAHULUAN

Perkembangan teknologi komunikasi yang sangat pesat membuat masyarakat lebih mudah berinteraksi satu sama lain tanpa terbatas waktu dan lokasi (Saputri dkk., 2024). Masyarakat dapat bertukar informasi dengan mudah melalui berbagai media seperi *facebook*, *instagram*, *twitter*, *whatsapp*, *tiktok*, *youtube*, *telegram*, dan lain sebagainya. Kemudahan ini tentu juga memiliki dampak negatif seperti rentannya informasi yang dikirim diretas oleh pihak yang tidak bertanggung jawab atau disebut kriptanalis (Putri dkk., 2023). Hal tersebut menjadikan landasan bahwa dibutuhkan sebuah metode untuk melakukan pengamanan pesan yang biasanya dikenal sebagai kriptografi.

Kriptografi adalah disiplin ilmu yang memfokuskan pada teknik-teknik untuk melindungi informasi dan komunikasi dari akses yang tidak sah (Azhari dkk., 2024). Kriptografi memastikan bahwa data dan komunikasi tetap aman dengan memanfaatkan algoritma dan metode matematis, sehingga hanya pihak-pihak yang berwenang yang dapat mengakses dan membacanya (Rohmanu, 2017). Kriptografi memiliki beberapa tujuan diantaranya kerahasian, integritas data, autentifikasi, dan non repudiasi (Yusuf, 2020). Dalam kriptografi terdapat dua proses dasar yaitu proses enkripsi dan proses dekripsi. Proses enkripsi adalah proses mengubah pesan asli yang biasanya disebut *plaintext* menjadi pesan acak yang biasnya disebut *ciphertext*, sedangkan proses dekripsi adalah sebuah proses mengubah *ciphertext* menjadi *plaintext* (Muharram dkk., 2018). Dalam perkembangannya, kriptografi diklasifikasikan menjadi kriptografi klasik dan kriptografi modern. Kriptografi klasik merupakan sebuah algoritma yang bekerja dalam mode karakter dan pada umumnya menggunakan kunci simetris. Kriptografi modern merupakan sebuah algoritma

pengamanan pesan yang bekerja pada mode bit (Putra dkk., 2017). Salah satu contoh kriptografi klasik yang telah dikembangkan adalah *Hill Cipher*.

Hill Cipher merupakan salah satu algoritma simetris yang mempunyai kunci enkripsi dan dekripsi sama (Acharya dkk., 2009). Kunci *Hill Cipher* berbentuk matrik $n \times n$ yang merupakan matrik non singular (Endaryono dkk., 2021). *Ciphertext* pada Hill Cipher mempunyai jumlah karakter yang sama dengan *plaintext* sehingga tidak ada perubahan dalam jumlah memori yang digunakan. Proses enkripsi dan dekripsi pada algoritma *Hill* Cipher dapat dilihat pada persamaan (1) dan persamaan (2).

$$C_i = (K.P_i)\ mod\ 26 \quad (1)$$
$$P_i = (K^{-1}.C_i)\ mod\ 26 \quad (2)$$

Perkembangan teknologi yang makin pesat mengakibatkan *Hill Cipher* dapat dipecahkan menggunakan perkalian matriks dan persamaan linear (Wowor, 2013). Hal tersebut menunjukkan bahwa algoritma *Hill Cipher* memiliki tingkat keamanan yang lemah.

Beberapa peneliti lain telah memodifikasi kunci algoritma *Hill Cipher* untuk menyulitkan kriptanalis dalam melakukan peretasan pesan. Yunita dkk. (2019) memodifikasi algoritma *Hill Chiper* dan twofish menggunakan kode wilayah telepon. Makhomah dkk. (2021) mengkombinasikan operasi XOR dan *Hill* Cipher dalam melakukan pengamanan pesan. Siregar dkk. (2022) menggunakan kode ASCII dalam melakukan pengamanan teks menggunakan algoritma *Hill Cipher*. Diriyanti dkk. (2024) menggunakan algoritma *Hill Cipher* dengan kunci tandatangan pengirim pesan dalam pengamanan *message handling system* di Bandara Kualanamu. Nurfadila dkk. (2024) memodifikasi kunci algoritma *Hill Cipher* dengan menggunakan barisana Fibonaci. Berdasarkan beberapa penelitian diatas, maka dalam paper ini penulis mencoba memodifikasi kunci algoritma *Hill Cipher* dengan menggunakan gambar sidik jari pengirim pesan. Sidik jari dipilih karena bersifat unik artinya tidak seorangpun memiliki sidik jari identik, bahkan pada bayi kembar sekalipun.

2 METODE

Penelitian ini tergolong penelitian deskriptif kualitatif. Metode kualitatif dan deskriptif kualitatif ini merupakan metode penelitian dengan menggunakan studi literatur dalam mengumpulkan data atau informasi yang sesuai dengan topik pembahasan. Data yang digunakan pada penelitian ini merupakan data pada tabel ASCII *printable characters*. Langkah-langkah dalam penelitian ini adalah sebagai berikut.

1. Pembentukan kunci *Hill Cipher*

Kunci matriks yang digunakan dalam melakukan proses enkripsi dan dekripsi yang digunakan adalah matriks 2×2. Matriks kunci harus invertible yaitu memiliki invers. Jika kunci tidak memiliki invers maka membentuk kunci matriks lain, hal ini dilakukan agar *ciphertext* dapat didekripsi. Matriks diperoleh dengan cara membagi gambar sidik jari pengirim pesan menjadi empat bagian. Masing-masing bagian selanjutnya dikonversi ke dalam bentuk biner dan menjumlahkan nilai biner dari masing-masing bagian yang akan digunakan sebagai matriks kunci *Hill Cipher*.

2. Proses enkripsi

Dalam paper ini jenis karakter yang digunakan berdasarkan jumlah karakter dalam tabel ASCII, sehingga karakter yang dapat tercetak berada pada interval 32 sampai dengan 126. Dalam proses enkripsi *plaintext* dibagi menjadi beberapa blok, dengan tiap blok berisi 2 karakter. Jika

karakter berjumlah ganjil, maka pada blok terakhir ditambah karakter *dummy* yang dalam hal ini adalah karakter "x". Karakter setiap blok selanjutnya dikonversi ke dalam tabel ASCII. Rumus proses enkripsi dapat dilihat pada persamaan 3.

$$C_i = \left(K.(P_i - 32)\right) mod\ 95 + 32 \quad (3)$$

3. Proses dekripsi

Proses dekripsi sama dengan enkripsi. Kunci yang digunakan dalam proses dekripsi merupakan matriks invers dari matriks kunci. Rumus proses enkripsi dapat dilihat pada persamaan 4 berikut.

$$P_i = \left(K^{-1}.(C_i - 32)\right) mod\ 95 + 32 \quad (4)$$

3 HASIL DAN PEMBAHASAN

3.1 Hasil

Pada bagian ini akan dibahas tentang contoh penggunaan gambar sidik jari dalam mengamankan pesan menggunakan algoritma *Hill Cipher*. Hal tesebut akan dibahas secara lengkap sebagai berikut.

1. Pembentukan matriks kunci

Misalkan matriks kunci yang digunakan dalam proses enkripsi dan dekripsi adalah matriks $K = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Matriks ini dibentuk dari hasil konversi gambar sidik jari menjadi bilangan biner. Sebagai contoh Gambar 1 merupakan gambar sidik jari pengirim pesan.

Gambar 1. Sidik jari pengirim pesan

Langkah selanjutnya membagi Gambar 1 menjadi empat bagian. Masing-masing bagian kemudian dikonversi ke bentuk biner dan menjumlahkan bentuk biner tersebut. Bagian pertama digunakan untuk mengisi matriks kunci a_{11}, bagian kedua digunakan untuk mengisi matriks kunci a_{12}, bagian ketiga digunakan untuk mengisi matriks kunci a_{21}, dan bagian keempat digunakan untuk mengisi matriks kunci a_{22}. Gambar 2 merupakan hasil pembagian gambar menjadi empat bagian. Hasil biner dari masing-masing bagian pada Gambar 2 adalah sebagai berikut.

$$a_{11} = 1 + 1 + \cdots + 0 = 1.431$$
$$a_{12} = 1 + 1 + \cdots + 1 = 1.420$$
$$a_{21} = 1 + 1 + \cdots + 1 = 1.377$$
$$a_{22} = 0 + 1 + \cdots + 1 = 1.379$$

Berdasarkan proses diatas diperoleh matriks kunci $K = \begin{pmatrix} 1431 & 1420 \\ 1377 & 1379 \end{pmatrix}$.

(a) Elemen matriks a_{11}

(b) Elemen matriks a_{12}

(c) Elemen matriks a_{21}

(d) Elemen matriks a_{22}

Gambar 2. Hasil pemecahan gambar sidik jari menjadi empat bagian

2. Proses Enkripsi

Misalkan disediakan pesan asli atau *plaintext* "Matematika". Untuk melakukan proses enkripsi, *plaintext* dibagi menjadi beberapa blok dengan setiap blok berisi dua karakter dan selanjutnya setiap blok dikonversi terlebih dahulu ke dalam tabel ASCII. Hasil konversi *plaintext* sebagai berikut.

$\begin{pmatrix}\text{M}\\ \text{a}\end{pmatrix} \rightarrow \begin{pmatrix}77\\ 97\end{pmatrix}$
$\begin{pmatrix}\text{t}\\ \text{e}\end{pmatrix} \rightarrow \begin{pmatrix}116\\ 101\end{pmatrix}$
$\begin{pmatrix}\text{m}\\ \text{a}\end{pmatrix} \rightarrow \begin{pmatrix}109\\ 97\end{pmatrix}$
$\begin{pmatrix}\text{t}\\ \text{i}\end{pmatrix} \rightarrow \begin{pmatrix}116\\ 105\end{pmatrix}$
$\begin{pmatrix}\text{k}\\ \text{a}\end{pmatrix} \rightarrow \begin{pmatrix}107\\ 97\end{pmatrix}$

Plaintext yang sudah dikonversi selanjutnya dilakukan perhitungan sesuai dengan persamaan 3 dengan menggunakan matriks kunci $K = \begin{pmatrix}1431 & 1420\\ 1377 & 1379\end{pmatrix}$. Perhitungan proses enkripsi masing-masing blok sebagai berikut.

$$C_1 = \left(\begin{pmatrix}1431 & 1420\\ 1377 & 1379\end{pmatrix} \times \left(\begin{pmatrix}77\\ 97\end{pmatrix} - \begin{pmatrix}32\\ 32\end{pmatrix}\right)\right) mod\ 95\ + \begin{pmatrix}32\\ 32\end{pmatrix} = \begin{pmatrix}72\\ 107\end{pmatrix} = \begin{pmatrix}\text{H}\\ \text{k}\end{pmatrix}$$

$$C_2 = \left(\begin{pmatrix}1431 & 1420\\ 1377 & 1379\end{pmatrix} \times \left(\begin{pmatrix}116\\ 101\end{pmatrix} - \begin{pmatrix}32\\ 32\end{pmatrix}\right)\right) mod\ 95\ + \begin{pmatrix}32\\ 32\end{pmatrix} = \begin{pmatrix}96\\ 46\end{pmatrix} = \begin{pmatrix}`\\ .\end{pmatrix}$$

$$C_3 = \left(\begin{pmatrix}1431 & 1420\\ 1377 & 1379\end{pmatrix} \times \left(\begin{pmatrix}109\\ 97\end{pmatrix} - \begin{pmatrix}32\\ 32\end{pmatrix}\right)\right) mod\ 95\ + \begin{pmatrix}32\\ 32\end{pmatrix} = \begin{pmatrix}74\\ 91\end{pmatrix} = \begin{pmatrix}\text{J}\\ [\end{pmatrix}$$

$$C_4 = \left(\begin{pmatrix}1431 & 1420\\ 1377 & 1379\end{pmatrix} \times \left(\begin{pmatrix}116\\ 105\end{pmatrix} - \begin{pmatrix}32\\ 32\end{pmatrix}\right)\right) mod\ 95\ + \begin{pmatrix}32\\ 32\end{pmatrix} = \begin{pmatrix}76\\ 52\end{pmatrix} = \begin{pmatrix}\text{L}\\ 4\end{pmatrix}$$

$$C_5 = \left(\begin{pmatrix} 1431 & 1420 \\ 1377 & 1379 \end{pmatrix} \times \left(\begin{pmatrix} 107 \\ 97 \end{pmatrix} - \begin{pmatrix} 32 \\ 32 \end{pmatrix} \right) \right) mod\ 95 + \begin{pmatrix} 32 \\ 32 \end{pmatrix} = \begin{pmatrix} 62 \\ 92 \end{pmatrix} = \begin{pmatrix} > \\ \backslash \end{pmatrix}$$

Berdasarkan proses enkripsi dari masing-masing blok didapatkan *ciphertext* "Hk'.J[L4>/".

3. Proses Dekripsi

Untuk melakukan proses dekripsi, maka *ciphertext* harus dikonversi terlebih dahulu ke tabel ASCII. Kunci yang digunakan pada proses dekripsi merupakan matriks invers dari K. Perhitungan proses dekripsi adalah sebagai berikut.

$$P_1 = \left(\begin{pmatrix} 66 & 30 \\ 22 & 74 \end{pmatrix} \times \left(\begin{pmatrix} 72 \\ 107 \end{pmatrix} - \begin{pmatrix} 32 \\ 32 \end{pmatrix} \right) \right) mod\ 95 + 32 = \begin{pmatrix} 77 \\ 97 \end{pmatrix} = \begin{pmatrix} \mathrm{M} \\ \mathrm{a} \end{pmatrix}$$

$$P_2 = \left(\begin{pmatrix} 66 & 30 \\ 22 & 74 \end{pmatrix} \times \left(\begin{pmatrix} 96 \\ 46 \end{pmatrix} - \begin{pmatrix} 32 \\ 32 \end{pmatrix} \right) \right) mod\ 95 + 32 = \begin{pmatrix} 116 \\ 101 \end{pmatrix} = \begin{pmatrix} \mathrm{t} \\ \mathrm{e} \end{pmatrix}$$

$$P_3 = \left(\begin{pmatrix} 66 & 30 \\ 22 & 74 \end{pmatrix} \times \left(\begin{pmatrix} 74 \\ 91 \end{pmatrix} - \begin{pmatrix} 32 \\ 32 \end{pmatrix} \right) \right) mod\ 95 + 32 = \begin{pmatrix} 109 \\ 97 \end{pmatrix} = \begin{pmatrix} \mathrm{m} \\ \mathrm{a} \end{pmatrix}$$

$$P_4 = \left(\begin{pmatrix} 66 & 30 \\ 22 & 74 \end{pmatrix} \times \left(\begin{pmatrix} 76 \\ 52 \end{pmatrix} - \begin{pmatrix} 32 \\ 32 \end{pmatrix} \right) \right) mod\ 95 + 32 = \begin{pmatrix} 116 \\ 105 \end{pmatrix} = \begin{pmatrix} \mathrm{t} \\ \mathrm{i} \end{pmatrix}$$

$$P_5 = \left(\begin{pmatrix} 66 & 30 \\ 22 & 74 \end{pmatrix} \times \left(\begin{pmatrix} 62 \\ 92 \end{pmatrix} - \begin{pmatrix} 32 \\ 32 \end{pmatrix} \right) \right) mod\ 95 + 32 = \begin{pmatrix} 107 \\ 97 \end{pmatrix} = \begin{pmatrix} \mathrm{k} \\ \mathrm{a} \end{pmatrix}$$

Berdasarkan proses dekripsi di atas, diperoleh *plaintext* "Matematika".

Modifikasi kunci *Hill Cipher* ini memungkinkan karakter yang sama memiliki kode yang berbeda. Pada contoh diatas, karakter "a" pada blok ketiga dikodekan oleh karakter "[", sedangkan karakter "a" pada blok kelima dikodekan oleh karakter "\". Hal ini merupakan keunggulan algoritma *Hill Cipher* dibandingkan dengan algoritma yang lain, misalnya algoritma *Vignere Cipher*. Penggunaan gambar sebagai kunci algoritma *Hill Cipher* bukan merupakan sesuatu yang umum, sehingga hal ini akan menambah kesulitan kriptanalis dalam memecahkan *ciphertext.* Penggunaan sidik jari yang bersifat unik tentu menambah tingkat keamanan pesan pada penggunaan algoritma *Hill Cipher.*

3.2 Pembahasan

Dalam era digital yang sangat terbuka ini, perlindungan terhadap informasi menjadi kebutuhan yang tidak bisa dihindari. Kriptografi menjadi pilar utama dalam upaya pengamanan informasi, terlebih ketika komunikasi melalui media sosial dan aplikasi pesan instan semakin berkembang (Saputri dkk., 2024). Penelitian ini menunjukkan bagaimana modifikasi algoritma *Hill Cipher* dengan pemanfaatan gambar sidik jari dapat meningkatkan aspek keamanan dalam kriptografi klasik.

Hill Cipher merupakan algoritma kriptografi klasik yang menggunakan matriks sebagai kunci untuk proses enkripsi dan dekripsi. Dalam bentuk dasarnya, *Hill Cipher* menggunakan perkalian matriks pada blok-blok karakter dari *plaintext* dengan sebuah matriks kunci yang harus dapat diinverskan (Acharya dkk., 2009). Kelemahan algoritma ini adalah jika kriptanalis mengetahui struktur matriks dan teknik dasar dekripsi, maka pesan rahasia mudah untuk

dipecahkan. Oleh karena itu, diperlukan inovasi dalam pembuatan kunci agar algoritma *Hill Cipher* lebih sulit dipecahkan. Di sinilah pentingnya penggunaan elemen unik dan acak seperti sidik jari.

Sidik jari memiliki pola yang khas dan unik pada setiap individu, bahkan pada bayi kembar sekalipun. Dalam penelitian ini, gambar sidik jari dikonversi menjadi representasi digital biner yang kemudian digunakan untuk membentuk elemen-elemen dari matriks kunci *Hill Cipher*. Inovasi ini merupakan lompatan penting karena menggabungkan prinsip biometrik dalam penciptaan kunci kriptografi, sehingga meningkatkan kompleksitas dan keamanan sisteM.

Langkah pertama dalam pendekatan ini adalah pembentukan matriks kunci. Gambar sidik jari dibagi menjadi empat bagian, kemudian setiap bagian dikonversi ke dalam bentuk biner. Nilai biner dari setiap bagian dijumlahkan dan digunakan untuk mengisi elemen-elemen dari matriks kunci 2x2. Matriks kunci ini harus memenuhi syarat memiliki invers agar proses dekripsi dapat dilakukan. Dalam prakteknya, jika nilai determinan dari matriks tersebut tidak memiliki invers modulo ukuran karakter (dalam hal ini 95 karena ASCII *printable characters* berada pada rentang 32–126), maka matriks harus diubah atau diulang proses pembentukannya.

Proses enkripsi dilakukan dengan membagi *plaintext* menjadi blok-blok yang terdiri dari dua karakter. Jika jumlah karakter ganjil, maka karakter tambahan berupa karakter “x” ditambahkan di akhir. Setiap karakter dikonversi ke nilai numerik berdasarkan ASCII, kemudian diproses menggunakan rumus enkripsi matriks. Proses ini melibatkan perkalian matriks kunci dengan vektor karakter dan hasilnya dikonversi kembali ke karakter berdasarkan ASCII, menghasilkan *ciphertext*.

Pada studi kasus dalam artikel ini, *plaintext* "Matematika" setelah dienkripsi dengan menggunakan matriks kunci dari sidik jari menghasilkan *ciphertext* “Hk’.J[L4>/”. Menariknya, proses enkripsi ini menghasilkan representasi karakter yang tidak langsung dikenali oleh pembaca, yang merupakan tujuan utama dari kriptografi, yaitu mengaburkan pesan asli menjadi bentuk yang tidak bermakna tanpa kunci (Muharram dkk., 2018).

Proses dekripsi dilakukan dengan cara yang serupa, tetapi menggunakan invers dari matriks kunci. *Ciphertext* dipecah menjadi blok dua karakter, dikonversi ke ASCII, dan dikalikan dengan invers matriks kunci untuk mendapatkan kembali plaintext. Hasil dari proses ini menunjukkan bahwa *ciphertext* “Hk’.J[L4>/” berhasil didekripsi kembali menjadi “Matematika”, yang menunjukkan keberhasilan algoritma dalam menyembunyikan dan mengungkap kembali pesan asli secara akurat.

Salah satu kekuatan dari penggunaan sidik jari sebagai kunci adalah ketidakmungkinan duplikasi oleh pihak luar. Setiap individu memiliki sidik jari yang unik dan mustahil ditemukan kembarannya secara identik. Ini menambahkan lapisan keamanan tambahan dalam sistem, yang membuat peretasan menjadi sangat sulit, kecuali jika kriptanalis memiliki akses ke gambar sidik jari yang sama dan memahami bagaimana gambar tersebut dikonversi ke dalam matriks. Di sisi lain, hal ini juga menimbulkan tantangan baru dalam penyimpanan dan distribusi kunci, mengingat gambar biometrik harus diamankan dari penyalahgunaan.

Penelitian sebelumnya juga menyampaikan beberapa pendekatan dalam memodifikasi *Hill Cipher* untuk menambah keamanan, seperti menggabungkan algoritma dengan metode Twofish dan kode wilayah telepon (Yunita dkk., 2019), kode ASCII (Siregar dkk., 2022), tanda tangan digital dalam message handling system (Diriyanti dkk., 2024), hingga barisan Fibonacci (Nurfadila dkk., 2024). Namun, pendekatan yang digunakan dalam penelitian ini tergolong unik karena mengintegrasikan biometrik ke dalam sistem kriptografi klasik. Pendekatan ini tidak hanya

menambah kekuatan keamanan tetapi juga membuka kemungkinan pengembangan algoritma kriptografi hybrid yang lebih maju.

Dalam aspek implementasi praktis, metode ini memerlukan sistem pemrosesan citra untuk mengkonversi gambar sidik jari ke dalam bentuk biner, serta sistem validasi matriks agar dapat digunakan dalam proses dekripsi. Hal ini dapat dilakukan dengan menggunakan tools pemrograman seperti Python dengan pustaka NumPy, OpenCV, dan algoritma pendeteksian kontur atau fitur.

Namun, ada beberapa hal yang perlu diperhatikan terkait limitasi dari metode ini. Pertama, ukuran gambar sidik jari dan cara pemrosesannya sangat berpengaruh pada hasil konversi biner. Proses digitalisasi yang tidak standar dapat menyebabkan hasil berbeda dari satu perangkat ke perangkat lain. Kedua, apabila sistem ini diterapkan dalam skala besar, diperlukan metode enkripsi tambahan terhadap penyimpanan gambar sidik jari agar tidak mudah diakses oleh pihak ketiga. Ketiga, dari sisi efisiensi, metode ini tidak cocok untuk sistem real-time atau komunikasi cepat, karena melibatkan pemrosesan citra yang memerlukan waktu dan sumber daya lebih.

Selain itu, penulis menyoroti keunggulan lain dari *Hill Cipher*, yaitu bahwa karakter yang sama dapat dihasilkan dengan *ciphertext* yang berbeda tergantung pada posisi dan konteksnya. Ini menunjukkan resistensi terhadap frekuensi analisis yang umum digunakan dalam kriptanalisis klasik. Sebagai perbandingan, algoritma seperti Vigenère Cipher lebih rentan karena keterbatasan dalam ruang kunci dan ketergantungan pada pengulangan kunci.

Penggunaan pendekatan biometrik dalam kriptografi juga menjadi bagian dari tren global di bidang keamanan informasi. Hal ini sejalan dengan kebutuhan autentikasi yang lebih kuat dalam sistem keamanan seperti e-banking, e-voting, dan aplikasi militer. Dengan menggabungkan *Hill Cipher* dan biometrik, sistem keamanan menjadi lebih terpersonalisasi dan spesifik untuk tiap pengguna. Bahkan, jika pendekatan ini dikembangkan lebih lanjut, dapat digunakan sebagai metode pengamanan untuk arsip dokumen rahasia atau file digital dengan tingkat keamanan tinggi.

Dengan demikian, penelitian ini memberikan kontribusi penting dalam dunia kriptografi, terutama pada pengembangan dan penguatan algoritma klasik. Di tengah ketatnya kebutuhan akan pengamanan data digital, integrasi teknologi pengenalan biometrik dengan metode matematika klasik menjadi jalan tengah antara kepraktisan, keamanan, dan efisiensi. Meski begitu, pengembangan lebih lanjut masih diperlukan, terutama pada aspek validasi keamanan sistem terhadap serangan brute-force, side-channel, dan pemalsuan data biometrik.

4 KESIMPULAN

Berdasarkan hasil dan pembahasan dapat disimpulkan bahwa gambar sidik jari dapat digunakan sebagai kunci untuk melakukan enkripsi dan dekripsi pesan menggunakan algoritma *Hill Cipher*. Penggunaan gambar sebagai kunci algoritma *Hill Cipher* bukan merupakan sesuatu yang umum, sehingga hal ini akan menambah kesulitan kriptanalis dalam memecahkan *ciphertext*. Penggunaan sidik jari yang bersifat unik tentu menambah tingkat keamanan pesan pada penggunaan algoritma *Hill Cipher*. Peneliti menyarankan agar peneliti lain mengembangkan algoritma *Hill Cipher* dengan metode lain dengan tujuan menambah tingkat kesulitan pemecahan *ciphertext* oleh kriptanalis.

DAFTAR PUSTAKA

Acharya, B., Panigrahy, S. K., Patra, S. K., & Panda, G. (2009). Image encryption using advanced hill cipher algorithm. *International Journal of Recent Trends in Engineering*, *1*(1), 663-667.

Azhari, M. D., Hadiana, A. I., & Melina, M. (2024). Teknik Pengamanan Data Menggunakan Algoritma Advance Encryption Standard Dengan Common Event Format Untuk Meningkatkan Keamanan Log Jaringan. *INTECOMS: Journal of Information Technology and Computer Science*, *7*(4), 1167-1176. https://doi.org/10.31539/intecoms.v7i4.10849

Diriyanti, S., Pangaribuan, L. J., Sukra, R., & Achaddiah, B. N. (2024). Implementasi Kriptografi Algoritma Hillcipher Dengan Kunci Tandatangan Pengirim Pesan Terhadap Keamanan Message Handling System Di Bandara Kualanamu. *Innovative: Journal Of Social Science Research*, *4*(2), 5953-5965. https://doi.org/10.31004/innovative.v4i2.9695

Endaryono, E., Dwitiyanti, N., & Setiawan, H. S. (2021). Aplikasi Operasi Matriks pada Perancangan Simulasi Metode Hill Cipher Menggunakan Microsoft Excel. *STRING (Satuan Tulisan Riset dan Inovasi Teknologi)*, *6*(1), 41-49. http://dx.doi.org/10.30998/string.v6i1.8603

Makhomah, R., Santoso, K. A., & Kamsyakawuni, A. (2021, February). Pengkodean Teks menggunakan Kombinasi Hill Cipher dan Operasi XOR. In *PRISMA, Prosiding Seminar Nasional Matematika* (Vol. 4, pp. 548-552).

Muharram, F., Aziz, H., & Manga, A. R. (2018, September). Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES). In *Prosiding SAKTI (Seminar Ilmu Komputer dan Teknologi Informasi)* (Vol. 3, No. 2, pp. 112-115).

Nurfadila, R. A., Komarullah, H., & Saputri, M. D. (2024, March). Modifikasi Sandi Algoritma Hill Cipher Dengan Kunci Berentry Barisan Fibonaci. In *Prosiding Seminar Pendidikan Matematika dan Matematika* (Vol. 9).

Putra, M. E., Suroso, S., & Wasti, A. (2017). Perancangan Aplikasi Pengamanan Informasi Teks Dengan Menggunakan Algoritma Kriptografi Alpha-Qwerty Reverse. *Jurnal Elektro dan Telekomunikasi Terapan (e-Journal)*, *4*(1), 495-495.

Putri, C. P., Anggraini, W., Hasibuan, Y. M., & Nurbaiti, N. (2023). Strategi Pengamanan Cyber: Lingkup Kerjasama dalam Menghadapi Ancaman Cyber. *INSOLOGI: Jurnal Sains dan Teknologi*, *2*(6), 1124-1130. https://doi.org/10.55123/insologi.v2i6.2847

Rohmanu, A. (2017). Implementasi kriptografi dan steganografi dengan metode algoritma DES dan metode End Of File. *Jurnal Informatika SIMANTIK*, *2*(1), 1-11.

Saputri, M. D., Komarullah, H., & Nurfadila, R. A. (2024, March). Penggunaan Matriks Adjency Dalam Penyandian Pesan Menggunakan Algoritma Electronic Code Book. In *Prosiding Seminar Pendidikan Matematika dan Matematika* (Vol. 10).

Siregar, N., Faisal, I., & Handoko, D. (2022). Menerapkan Algoritma Hill Cipher dan Matriks 2x2 Dalam Mengamankan File Teks Menggunakan Kode ASCII. *Jurnal Ilmu Komputer dan Sistem Informasi*, *1*(2), 70-83. https://doi.org/10.70340/jirsi.v1i2.15

Wowor, A. D. (2013). Modifikasi Kriptografi Hill Cipher Menggunakan Convert Between Base. In *Seminar Nasional Sistem Informasi Indonesia (SESINDO)*. Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember.

Yunita, S., Hasan, P., & Ariyus, D. (2019). Modifikasi Algoritma Hill Chiper dan Twofish Menggunakan Kode Wilayah Telepon. *Sisfotenika*, *9*(2), 213-224. http://dx.doi.org/10.30700/jst.v9i2.489

Yusuf, K. (2020). Penerapan Algoritma Md5 Sebagai Pengaman Akun Pada Aplikasi Web Emusrenbang Kota Binjai. *JTIK (Jurnal Teknik Informatika Kaputama)*, *4*(1), 29-34.