Jurnal Ilmiah Matematika dan Pendidikan Matematika (JMP)
Vol. 14 No. 1, Juni 2022, hal. 45-58
ISSN (Cetak) : 2085-1456; ISSN (*Online*) : 2550-0422

KOMPUTASI ENKRIPSI DAN DEKRIPSI MENGGUNAKAN ALGORITMA *HILL CIPHER*

Rara Wardhani

Jurusan Matematika, Universitas Jenderal Soedirman
rarawardhani4@gmail.com

Siti Rahmah Nurshiami*

Jurusan Matematika, Universitas Jenderal Soedirman
siti.nurshiami@unsoed.ac.id

Niken Larasati

Jurusan Matematika, Universitas Jenderal Soedirman
nikenlaras15@gmail.com

ABSTRACT. *The Hill Cipher algorithm is one of the symmetric cryptographic algorithms that can be used to encrypt and decrypt. The Hill Cipher algorithm is one of the best cryptographic algorithms because it uses modulo and matrix operations. This study discusses encryption and decryption programs using the Hill Cipher Algorithm with the Java programming language. The resulting program is capable of encrypting and decrypting with key* 2×2, 3×3, *and* 4×4.

Keywords*: Hill Cipher, cryptography, encryption, decryption.*

ABSTRAK. Algoritma *Hill Cipher* merupakan salah satu algoritma kriptografi simetris yang dapat digunakan untuk mengenkripsi dan mendekripsi. Algoritma *Hill Cipher* merupakan salah satu dari algoritma kriptografi yang cukup baik karena menggunakan modulo dan operasi matriks. Penelitian ini membahas program enkripsi dan dekripsi menggunakan *Algoritma Hill Cipher* dengan bahasa pemrograman *Java*. Program yang dihasilkan mampu mengenkripsi dan mendekripsi dengan ordo kunci 2×2, 3×3, dan 4×4.

Kata kunci: *Hill Cipher*, kriptografi, enkripsi, dekripsi.

1. PENDAHULUAN

Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Keamanan pesan diperoleh dengan menyandikan pesan tersebut menjadi pesan yang tidak memiliki makna. Pesan yang dirahasiakan dinamakan plainteks, sedangkan pesan hasil penyandian disebut cipherteks. Proses menyandikan plainteks menjadi cipherteks disebut enkripsi, dan proses membalikkan cipherteks menjadi plainteks disebut dekripsi [1]. Berdasarkan penggunaan kunci, algoritma kriptografi dibedakan menjadi dua jenis yaitu simetris dan asimetris. Algoritma

*Penulis Korespondensi
Info Artikel : dikirim 13 Apr. 2022; direvisi 16 Jun. 2022; diterima 29 Jun. 2022.

simetris adalah algoritma yang menggunakan kunci enkripsi yang sama dengan kunci deskripsinya. Pengirim dan penerima pesan harus menyepakati kunci yang akan dipakai dalam proses komunikasi. Algoritma asimetris yang disebut juga sebagai algoritma kunci publik menggunakan dua kunci yaitu kunci publik dan kunci rahasia. Kunci publik digunakan untuk mengenkripsi pesan sedangkan kunci rahasia digunakan untuk mendekripsi pesan [2]. Salah satu yang termasuk dalam algoritma kriptografi simetris adalah *Hill Cipher*. Algoritma *Hill Cipher* merupakan salah satu dari algoritma kriptografi yang cukup baik karena menggunakan operasi matriks dan modulo. Proses dari algoritma *Hill Cipher* dalam setiap karakter plainteks maupun cipherteks dikonversikan ke dalam bentuk angka atau desimal. Proses enkripsi dilakukan dengan mengalikan matriks kunci dengan matriks plainteks, sedangkan proses dekripsi mengalikan invers matriks kunci dengan cipherteksnya. Karena itulah, *Hill Cipher* hanya dapat menggunakan matriks persegi [3]. Penggunaan matriks berordo $n \times n$ dengan $n > 3$ sebagai kunci untuk enkripsi dan dekripsi diperlukan ketelitian dan waktu yang lebih lama. Oleh karena itu, salah satu cara untuk menanggulanginya adalah dengan membuat alat bantu berupa program komputer untuk enkripsi dan dekripsi menggunakan algoritma *Hill Cipher* agar lebih efisien.

Penelitian sebelumnya yang mengkaji tentang algoritma *Hill Cipher* diantaranya; [4] menggunakan matriks 2×2 sebagai kunci untuk enkripsi dan dekripsi, modulo 26, serta bahasa pemrograman *Visual Basic* 6.0 dalam pembuatan program komputer. Selanjutnya, [5] menggunakan matriks 2×2 yang memiliki determinan 1 dan -1 sebagai kunci untuk enkripsi dan dekripsi pada pengenalan dan pengamanan plat nomor kendaraan, [6] menggunakan matriks 3×3 dan modulo 29 sebagai kunci untuk enkripsi dan dekripsi, [2] menggunakan matriks 2×2, modulo 95, dan bahasa pemrograman Delphi untuk proses enkripsi dan dekripsi, [7] menggunakan matriks 3×3 dan modulo 95 untuk mengkombinasikan *Hill Cipher* dengan operasi *XOR*. Penelitian ini membahas enkripsi dan dekripsi menggunakan matriks $n \times n$ dengan $2 \leq n \leq 4$, determinan matriks tidak nol, dan modulo 256. Hal ini dikarenakan terdapat 256 karakter ASCII (*American Standard Code for Information Interchange*) yang

dapat dikonversi, serta bahasa pemrograman *Java* dalam pembuatan program komputer.

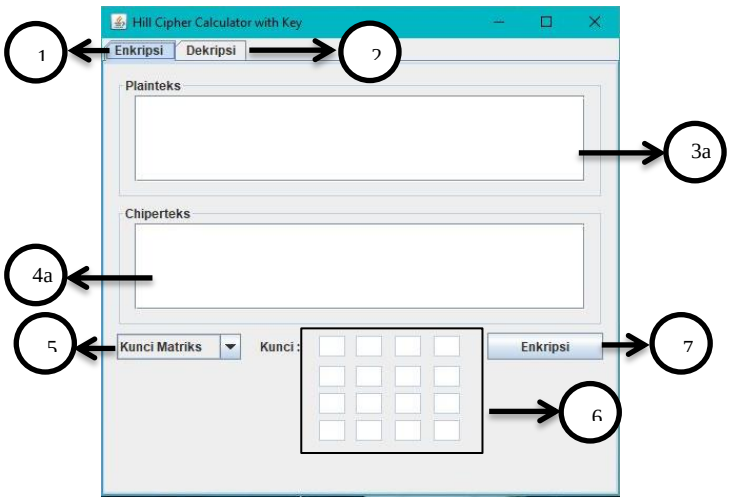
2. METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah studi literatur mengenai algoritma kriptografi *Hill Cipher*, serta pemrograman untuk pembuatan aplikasinya. Langkah pertama yang dilakukan adalah menganalisa tahapan-tahapan dalam pengenkripsian dan pendekripsian menggunakan *Hill Cipher*. Kemudian merancang program komputer berdasarkan hasil analisa dan mengembangkan program komputer melalui proses pengkodean ke dalam Bahasa pemrograman *Java*. Langkah terakhir, melakukan uji coba program komputer untuk memastikan program sudah berjalan sesuai analisa.

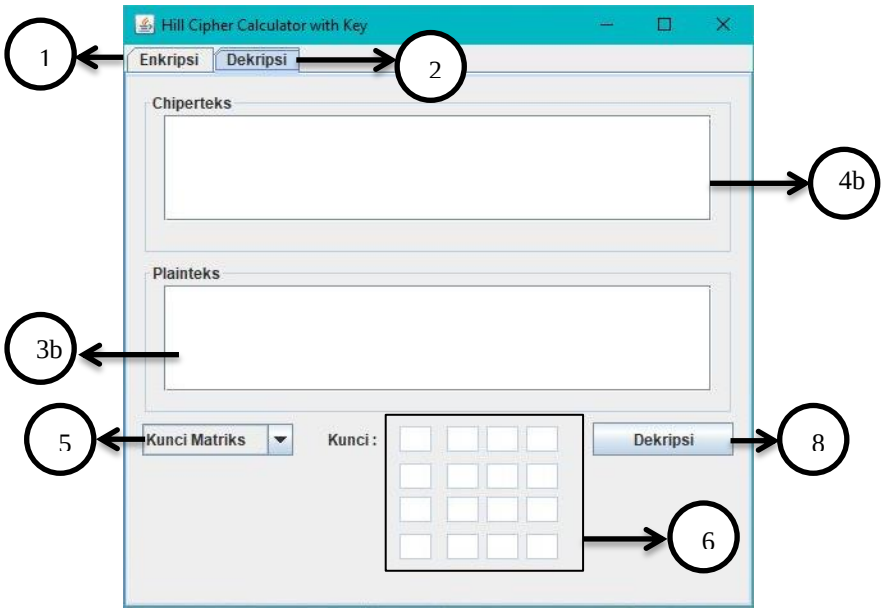
3. HASIL DAN PEMBAHASAN

3.1. Implementasi

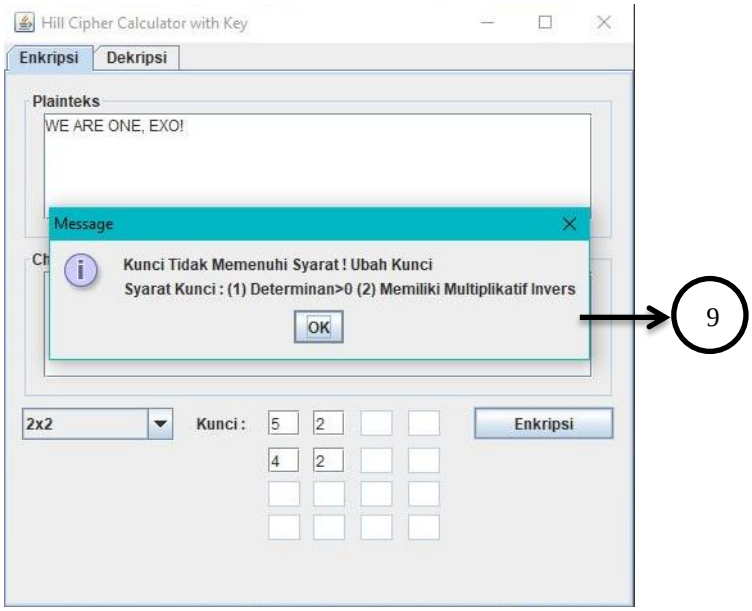
Algoritma atau langkah-langkah enkripsi dan dekripsi menggunakan algoritma *Hill Cipher* dapat diimplementasikan ke dalam pemrograman *Java* sehingga dihasilkan suatu program yang memudahkan baik dalam enkripsi dan dekripsi menggunakan algoritma *Hill Cipher*. Berikut adalah beberapa *interface* program enkripsi dan dekripsi menggunakan algoritma *Hill Cipher*.



Gambar 1. *Interface* Program Halaman Enkripsi



Gambar 2. *Interface* Program Halaman Dekripsi



Gambar 3. *Interface* Program Jika Kunci Tidak Memenuhi Syarat

Berikut adalah penjelasan fungsi dari masing-masing komponen pada *Interface*

1 : *Panel Enkripsi* adalah halaman untuk proses enkripsi.

2 : *Panel Dekripsi* adalah halaman untuk proses dekripsi.

3a : *Text Field Plainteks* pada *Panel Enkripsi* untuk memasukkan pesan yang akan dienkripsi.

3b : *Text Field Plainteks* pada *Panel Dekripsi* untuk menampilkan hasil pesan yang

telah didekripsi.

4a : *Text Field Cipherteks* pada *Panel Enkripsi* untuk menampilkan hasil pesan yang telah dienkripsi.

4b : *Text Field Cipherteks* pada *Panel Dekripsi* untuk memasukkan pesan yang akan didekripsi.

5 : *Combo Box Kunci Matriks* untuk memilih ordo kunci.

6 : *Text Field Kunci* untuk memasukkan entri-entri kunci.

7 : *Button Enkripsi* untuk mengenkripsi plainteks yang telah dimasukkan.

8 : *Button Dekripsi* untuk mendekrispi cipherteks yang telah dimasukkan.

9 : Peringatan apabila kunci yang dimasukkan tidak memenuhi syarat.

3.2 Hasil Pengujian

Kunci untuk enkripsi dan dekripsi pada algoritma *Hill Cipher* adalah matriks berordo $n \times n$ yang memiliki determinan matriks tak nol. Jika kunci enkripsi adalah matriks K_e, maka matriks K_e memiliki *inverse* ${K_e}^{-1}$ sedemikian sehingga

$$K_e \cdot {K_e}^{-1} = {K_e}^{-1} \cdot K_e = I.$$

Jika plainteks dilambangkan dengan P dan cipherteks dilambangkan dengan C serta kunci enkripsi adalah K_e, maka secara matematis proses enkripsi pada algoritma *Hill Cipher* ditulis sebagai berikut:

$$C = K_e \cdot P.$$

Secara matematis, proses dekripsi pada algoritma *Hill Cipher* dapat diturunkan dari persamaan enkripsi sehingga diperoleh persamaan sebagai berikut:

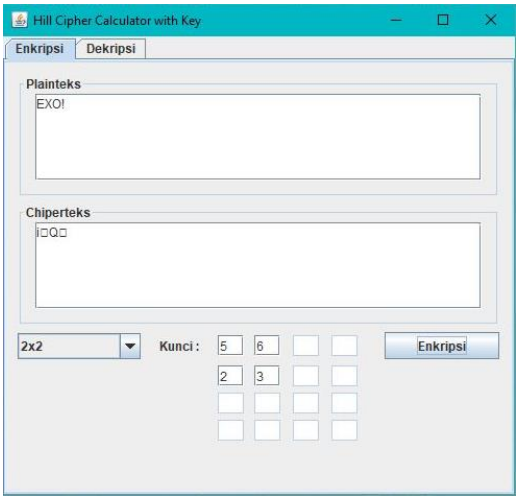
$$P = {K_e}^{-1} \cdot C = K_d \cdot C$$

dengan K_d adalah kunci untuk dekripsi.

Contoh 1. Berikut ini adalah contoh proses enkripsi pada algoritma *Hill Cipher* menggunakan matriks berordo 2×2 sebagai kunci. Misalkan diberikan plainteks sebagai berikut: EXO!dengan kunci

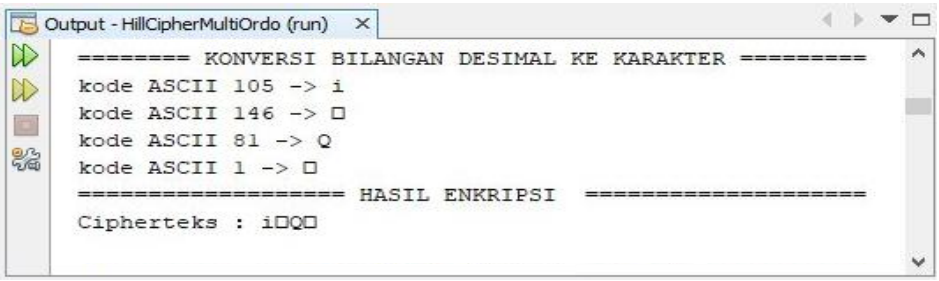
$$K_e = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}.$$

Karakter tersebut akan dienkripsi menggunakan program "*algoritma Hill Cipher Calculator with Key*".



Gambar 4. Tampilan Program Proses Enkripsi dengan Ordo Kunci 2 × 2

Berdasarkan Gambar 5 hasil enkripsi menggunakan program adalah i'QSOH. Hasil tersebut bersesuaian dengan hasil pada perhitungan secara manual.

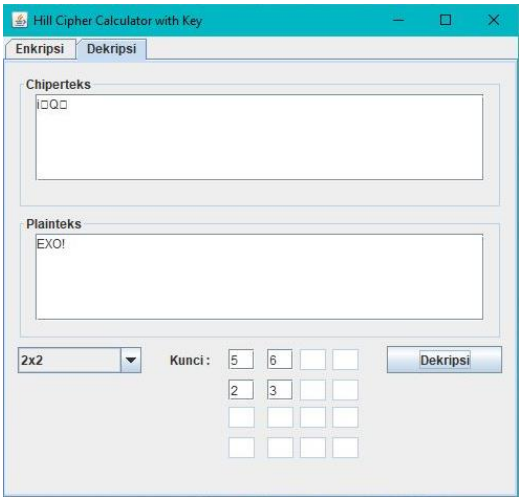


Gambar 5. Hasil Enkripsi Menggunakan Program dengan Ordo Kunci 2 × 2

Berikut ini adalah contoh proses dekripsi pada *Algoritma Hill Cipher* menggunakan matriks berordo 2 × 2 sebagai kunci. Misalkan diberikan chiperteks sebagai berikut: i'QSOH dengan kunci

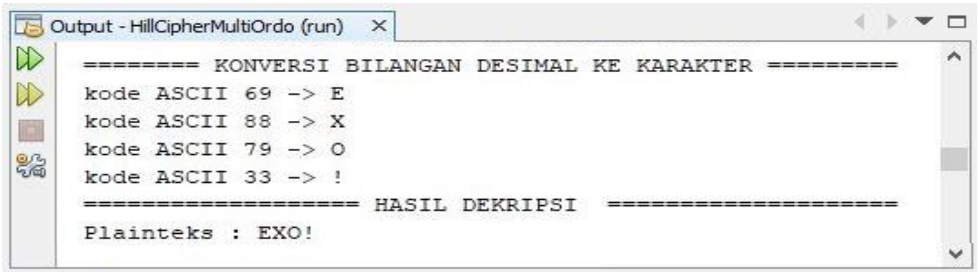
$$K_e = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}.$$

Karakter tersebut akan didekripsi menggunakan program "algoritma *Hill Cipher Calculator with Key*".



Gambar 6. Tampilan Program Proses Dekripsi dengan Ordo Kunci 2×2

Berdasarkan Gambar 7 hasil dekripsi menggunakan program adalah EXO!. Hasil tersebut bersesuaian dengan hasil pada perhitungan secara manual.

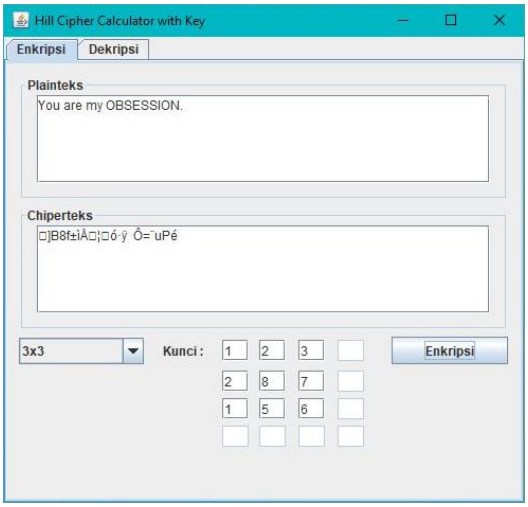


Gambar 7. Hasil Dekripsi Menggunakan Program dengan Ordo Kunci 2×2

Contoh 2. Berikut ini adalah contoh proses enkripsi pada algoritma *Hill Cipher* menggunakan matriks berordo 3×3 sebagai kunci. Misalkan diberikan plainteks sebagai berikut: You are my OBSESSION. dengan kunci

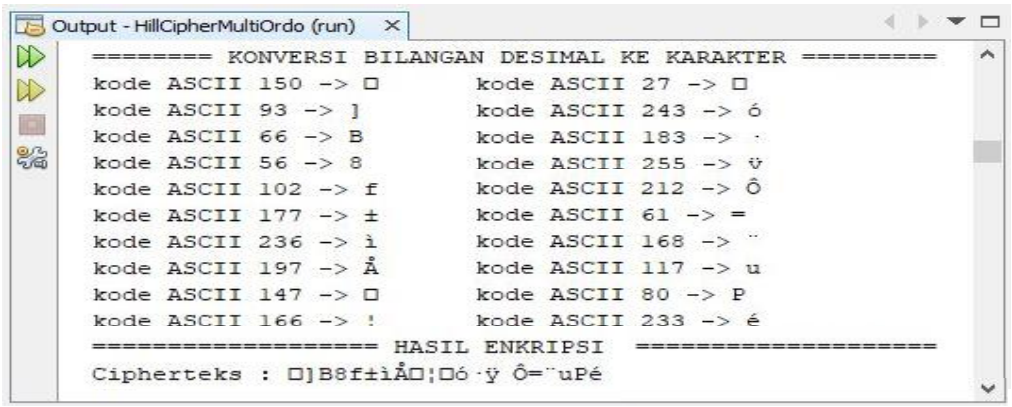
$$K_e = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix}.$$

Karakter tersebut akan dienkripsi menggunakan program "*Algoritma Hill Cipher Calculator with Key*".



Gambar 8. Tampilan Program Proses Enkripsi dengan Ordo Kunci 3 × 3

Berdasarkan Gambar 9 hasil enkripsi menggunakan program adalah •]B8f±ìÅ“¦ESCó·ÿDELÔ=¨uPé, sehingga hasil tersebut bersesuaian dengan hasil pada perhitungan secara manual.



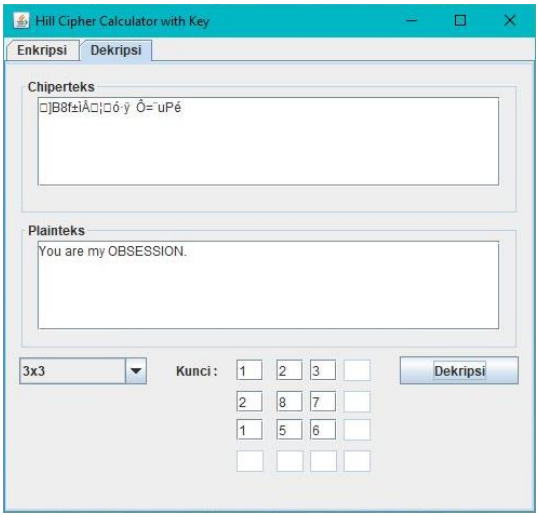
Gambar 9. Hasil Enkripsi Menggunakan Program dengan Ordo Kunci 3 × 3

Berikut ini adalah contoh proses dekripsi pada *Algoritma Hill Cipher* menggunakan matriks berordo 3 × 3 sebagai kunci.

Misal diberikan chiperteks sebagai berikut:•]B8f±ìÅ“¦ESCó·ÿDELÔ=¨uPé dengan kunci

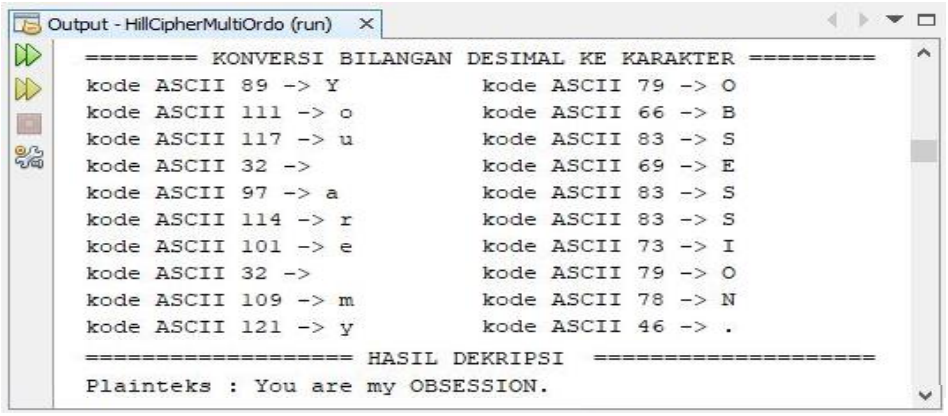
$$K_e = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix}.$$

Karakter tersebut akan didekripsi menggunakan program "*Algoritma Hill Cipher Calculator with Key*".



Gambar 10. Tampilan Program Proses Dekripsi dengan Ordo Kunci 3 × 3

Berdasarkan Gambar 11 hasil dekripsi menggunakan program adalah You are my OBSESSION., sehingga hasil tersebut bersesuaian dengan hasil pada perhitungan secara manual.

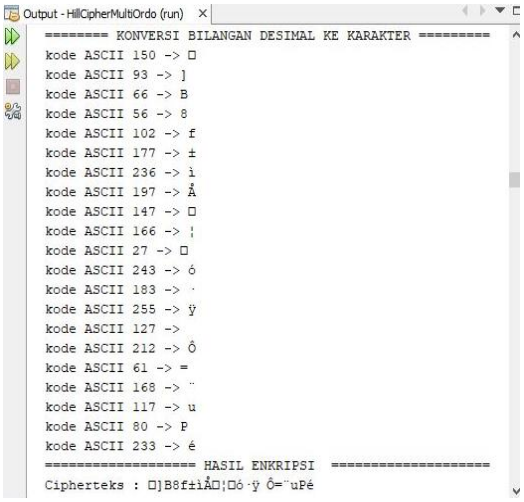


Gambar 11. Hasil Dekripsi Menggunakan Program dengan Ordo Kunci 3 × 3

Contoh 3. Berikut ini adalah contoh proses enkripsi pada *Algoritma Hill Cipher* menggunakan matriks berordo 4 × 4 sebagai kunci. Misalkan diberikan plainteks sebagai berikut: Tell me what you waiting for dengan kunci

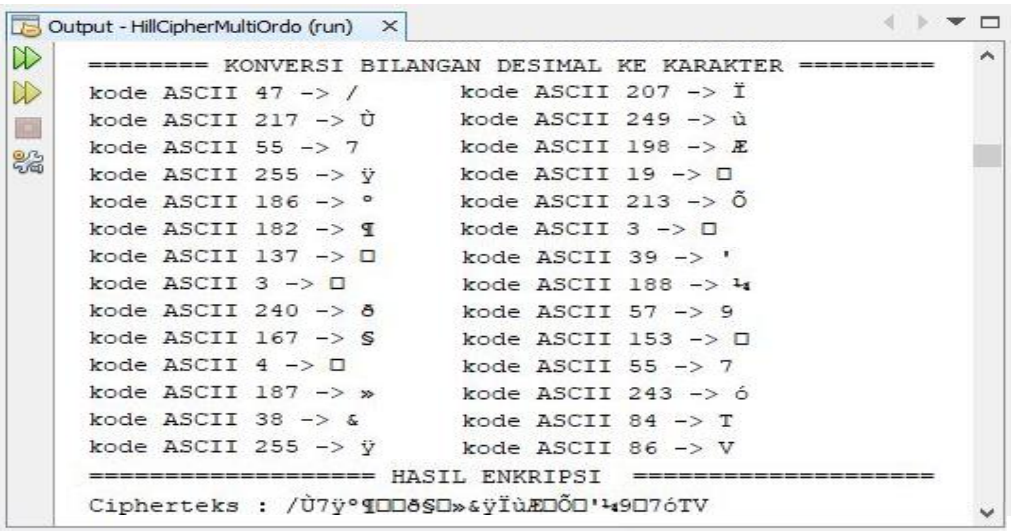
$$K_e = \begin{bmatrix} 7 & 11 & 15 & 10 \\ 6 & 13 & 9 & 7 \\ 6 & 19 & 10 & 6 \\ 5 & 7 & 8 & 10 \end{bmatrix}.$$

Karakter tersebut akan dienkripsi menggunakan program "*Algoritma Hill Cipher Calculator with Key*".



Gambar 12. Tampilan Program Proses Enkripsi dengan Ordo Kunci 4 × 4

Berdasarkan Gambar 13 hasil enkripsi menggunakan program adalah /Ù7ÿº¶‰ETXð§EOT»&ÿÏùÆDC3ÕETX'¼9™7óTV, sehingga hasil tersebut bersesuaian dengan hasil pada perhitungan secara manual.

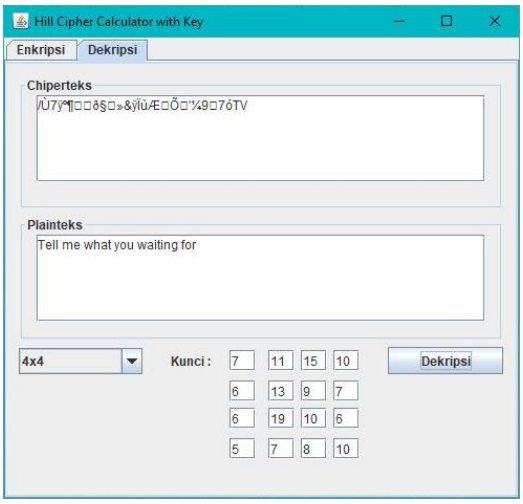


Gambar 13. Hasil Enkripsi Menggunakan Program dengan Ordo Kunci 4 × 4

Berikut ini adalah contoh proses dekripsi pada *Algoritma Hill Cipher* menggunakan matriks berordo 4 × 4 sebagai kunci. Misalkan diberikan chiperteks sebagai berikut: /Ù7ÿº¶‰ETXð§EOT»&ÿÏùÆDC3ÕETX‘¼9™7óTV dengan kunci

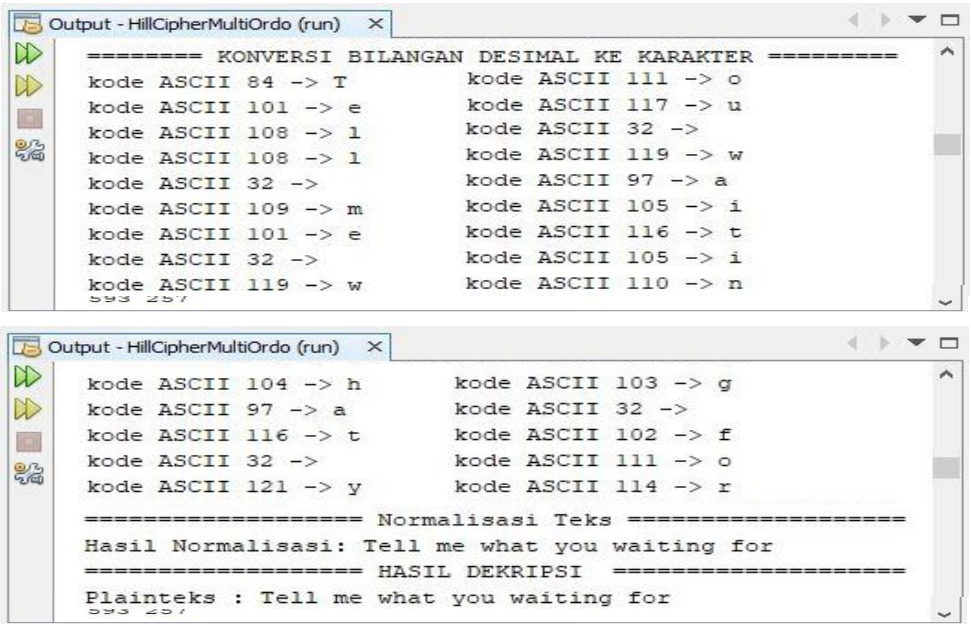
$$K_e = \begin{bmatrix} 7 & 11 & 15 & 10 \\ 6 & 13 & 9 & 7 \\ 6 & 19 & 10 & 6 \\ 5 & 7 & 8 & 10 \end{bmatrix}.$$

Karakter tersebut akan didekripsi menggunakan program "*Algoritma Hill Cipher Calculator with Key*".



Gambar 14. Tampilan Program Proses Dekripsi dengan Ordo Kunci 4 × 4

Berdasarkan Gambar 15 hasil dekripsi menggunakan program adalah Tell me what you waiting for, sehingga hasil tersebut bersesuaian dengan hasil pada perhitungan secara manual.



Gambar 15. Hasil Dekripsi Menggunakan Program dengan Ordo Kunci 4×4

4. KESIMPULAN DAN SARAN

Berdasarkan hasil dan pembahasan mengenai komputasi enkripsi dan dekripsi menggunakan *Algoritma Hill Cipher*, program dengan bahasa pemrograman *Java* yang telah dibuat dapat mengenkripsi dan mendekripsi dengan baik untuk matriks kunci 2×2, 3×3, maupun 4×4.

Penelitian selanjutnya dapat dilakukan dengan mengkaji lebih lanjut pemrograman *Java* untuk enkripsi dan dekripsi menggunakan *Algoritma Hill Cipher* dengan kunci berupa matriks berordo $n \times n$ dengan $n > 4$ serta mengaplikannya dalam bentuk aplikasi berbasis android maupun web.

DAFTAR PUSTAKA

[1] Munir, R., *Matematika Diskrit*, Edisi ke-3, Informatika, Bandung, 2010.

[2] Puspita, N. P. dan Bahtiar, N., *Kriptografi Hill Chiper dengan Menggunakan Operasi Matriks*, Seminar Nasional Ilmu Komputer UNDIP, 2010.

[3] Hidayat, A. dan Alawiyah, T., *Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang*, Jurnal

Matematika Integratif, **9**(1) (2012), 39–51., 2013, https://doi.org/10.24198/jmi.v9.n1.10196.39-52

[4] Hasugian, A. H., *Implementasi Algoritma Hill Cipher dalam Penyandian Data*, Pelita Informatika Budi Darma, **4**(2) (2013), 115–122.

[5] Gumelar, M. G., Fibriani, I., Setiabudi, D., dan Supeno, B., *Analisis Sistem Pengenalan dan Keamanan Kriptografi Hill Cipher pada Plat Nomor Kendaraan Menggunakan Metode Template Matching*, Prosiding Seminar Nasional ReTII ke-11, 2016.

[6] Serdano, A., Zarlis, M., Sawaluddin, Hartama, D., *Pengamanan Pesan Menggunakan Algoritma Hill Cipher dalam Keamanan Komputer*, Jurnal Mahajana Informasi, **4**(2) (2019), 5-9.

[7] Makhomah, R., Santoso, K. A., dan Kamsyakawuni, A., *Pengkodean Teks Menggunakan Kombinasi Hill Cipher dan Operasi XOR*, **4** (2021), PRISMA : Prosiding Seminar Nasional Matematika.