Volume 4 No 2 Desember (2021)

e-ISSN: **2615-3270**

p-ISSN: **2615-3599**

Eigen Mathematics Journal

Homepage jurnal: http://eigen.unram.ac.id

# Hill Cipher Algorithm with Generalized Fibonacci Matrix in Message Encoding

***Husni Fitroti*** [a], ***Mamika Ujianita Romdhini*** [b], ***Ni Wayan Switrayni*** [c*]

[a]Universitas Mataram, Jl. Majapahit No. 62, Mataram, 83125, Indonesia,. Email: husnifitroti17@gmail.com
[b]Universitas Mataram, Jl. Majapahit No. 62, Mataram, 83125, Indonesia,. Email: mamika_ur@yahoo.com
[c*]Universitas Mataram, Jl. Majapahit No. 62, Mataram, 83125, Indonesia,. Email: niwayan.switrayni@unram.ac.id

## ABSTRACT

*Hill Cipher* algorithm is a technique of message encoding by implementing a matrix of order $n \times n$ as a key matrix. The key matrix is a matrix that has a multiplicative inverse. The security of message is measured by the number of processes in encoding. The more processes in encoding the longer time it takes. Consequently, the massage will be more secure. The purpose of this research is to modify the *Hill Cipher* algorithm by using generalized Fibonacci matrix $Q_p^n$ whose degree-$p$ and rank-$n$. This research showed that for any non-negative integer $p$ and positive integer $n$, matrix $Q_p^n$ can be used as a key matrix in *Hill Cipher* algorithm. The modification of the *Hill Cipher* algorithm has been done by modifying the former key by making the degree ($p$) and rank ($n$) of $Q_p^n$ as the key used in the encryption and decryption process of data (message).

**Keywords:** *Hill Cipher*, Generalized Fibonacci Matrix; Encryption; Decryption.

## ABSTRAK

Algoritma *Hill Cipher* merupakan suatu teknik enkoding pesan dengan menggunakan suatu matriks berorde $n \times n$ sebagai suatu matriks kunci. Matriks kunci merupakan suatu matriks yang memiliki invers. Keamanan pesan diukur berdasarkan banyaknya proses dalam enkoding. Semakin banyak proses dalam enkoding semakin panjang waktu yang dibutuhkan. Akibatnya, pesan akan lebih aman. Tujuan penelitian ini adalah memodifikasi algoritma *Hill Cipher* dengan menggunakan matriks Fibonacci diperumum $Q_p^n$ berderajat $p$ dan rank $n$. Penelitian ini menunjukkan bahwa untuk setiap bilangan bulat tak-negatif $p$ dan bilangan bulat positif $n$, matriks $Q_p^n$ dapat digunakan sebagai matriks kunci dalam algoritma *Hill Cipher*. Modifikasi algoritma *Hill Cipher* telah dilakukan dengan cara mengganti kunci yang lama dengan kunci yang berasal dari derajat dan rank dari matriks $Q_p^n$ dalam proses enkripsi dan dekripsi pesan.

**Kata kunci:** *Hill Cipher*, Matriks Fibonacci Diperumum, Enkripsi, Dekripsi.

Diserahkan: 14-06-2021; Diterima: 24-12-2021; Doi: https://doi.org/10.29303/emj.v4i2.107

* Corresponding author.
Alamat e-mail: *niwayan.switrayni@unram.ac.id*

## 1. PENDAHULUAN

Menurut Eko Satria (2009) dalam Hasugian (2013) keamanan algoritma kriptografi sering diukur dari banyaknya kerja yang dibutuhkan untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan. Apabila semakin banyak proses yang diperlukan berarti juga semakin lama waktu yang dibutuhkan, maka semakin kuat algoritma tersebut dan semakin aman digunakan untuk penyandian pesan.

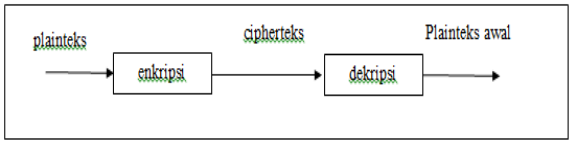
Dalam penelitian ini, penyandian pesan dilakukan dengan menggunakan algoritma kriptografi *Hill Cipher*. Algoritma kriptografi tersebut dipilih karena sederhana dan mudah dalam pengaplikasiannya serta merupakan algoritma klasik yang masih sangat kuat dari segi keamanannya karena menggunakan metode perkalian matriks sehingga pencarian kunci menjadi tidak mudah (Tuasikal, 2020). Berdasarkan Penelitiannya (Tuasikal, 2020) penggunaan matriks kunci minimal berordo $3 \times 3$ sebagai kunci pada kriptografi *Hill Cipher* masih sangat aman digunakan sehingga diharapkan terhindar dari serangan *Known-plaintext attacki* dan *Chosen-plaintext attack* pada metode *Hill Cipher*.

Untuk memperbanyak proses yang digunakan dalam penyandian pesan diperlukan modifikasi algoritma kriptografi *Hill Cipher* ini yaitu dengan menerapkan matriks generalisasi dari bilangan Fibonacci. Dalam penggunaanya, proses penyandiaan pesan dilakukan dengan tidak menjadikan matriks $n \times n$ sebagai matriks kunci. Namun yang dijadikan kunci adalah derajat $(p)$ dan pangkat $(n)$ matriks untuk menentukan bilangan dari generalisasi bilangan Fibonacci dalam matriks generalisasi bilangan Fibonacci. Sehingga dari derajat dan pangkat matriks generalisasi bilangan Fibonacci yang diketahui dapat ditentukan matriks tertentu yaitu matriks $(p+1) \times (p+1)$. Adapun dalam proses enkripsi dan dekripsinya mengunakan aritmatika modulo dalam modulo 256 yang merupakan jumlah karakter yang terdapat pada kode *ASCII.*

## 2. TINJAUAN PUSTAKA

### 2.1 Algoritma Kriptografi *Hill Cipher*

Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Keamanan pesan diperoleh dengan menyandikannya menjadi pesan yang tidak mempunyai makna. Pesan yang dirahasiakan dinamakan **plainteks** *(plainteks, artinya teks jelas yang dapat dimengerti)*, sedangkan pesan hasil penyandian disebut **cipherteks** (*cipherteks, artinya teks tersandi)*. Pesan yang telah disandikan dapat dikembalikan lagi ke pesan aslinya hanya oleh orang yang berhak (orang yang berhak adalah orang mengetahui metode penyandian atau memiliki kunci penyandian). Proses menyandikan plainteks menjadi cipherteks disebut **enkripsi** *(encryption)* dan proses membalikkan cipherteks menjadi plainteksnya disebut **dekripsi** *(decryption).* Proses tersebut diperlihatkan dalam diagram pada gambar berikut (Munir, 2012: 203):




**Gambar 2.6.2 Proses Penyandian Pesan**

Salah satu teknik Kriptografi klasik yang masih sangat aman digunakan adalah Teknik kriptografi *Hill Cipher*. Algoritma kriptografi ini diciptakan dengan maksud untuk menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. *Hill Cipher* ini tidak mengganti setiap abjad yang sama pada plainteks dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar *enkripsi* dan *dekripsi*nya. Oleh karena itu *Hill Cipher* termasuk dalam salah satu kriptosistem *polyalphabetic* ( Supiyanto, 2015).

### Algoritma Enkripsi *Hill Cipher*

Tahapan-tahapan algoritma Enkripsi Hill Cipher sebagai berikut (Rojali, 2011):

1. Korespondensikan abjad dengan numerik.
2. Buat matriks kunci berukuran $m \times m$.

$$K_{m\times m} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}$$

3. Matriks $K$ merupakan matriks yang *invertible* yaitu memiliki *multiplicative inverse* $K^{-1}$ sehingga $KK^{-1} = I$

4. Plaintext $P = p_1, p_2, \dots, p_n$, diblok dengan ukuran sama dengan baris atau kolom matriks $K$, sehingga

$$P_{q\times m} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} & \cdots & p_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ p_{q1} & p_{q2} & \dots & p_{qm} \end{bmatrix}$$

5. Matriks $P$ ditranspos menjadi

$$P^T{}_{m\times q} = \begin{bmatrix} p_{11} & p_{21} & \cdots & p_{q1} \\ p_{12} & p_{22} & \cdots & p_{q2} \\ \cdots & \cdots & \cdots & \cdots \\ p_{1m} & p_{2m} & \dots & p_{qm} \end{bmatrix}$$

6. Kalikan matriks K dengan matriks $P$ transpos dalam modulo 26

$$C^T = K_{m\times m} P^T{}_{m\times q}$$

$$C^T = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix} \begin{bmatrix} p_{11} & p_{21} & \cdots & p_{qm} \\ p_{12} & p_{22} & \cdots & p_{q2} \\ \cdots & \cdots & \cdots & \cdots \\ p_{1m} & p_{2m} & \dots & p_{qm} \end{bmatrix}$$

$$= \begin{bmatrix} c_{11} & c_{21} & \cdots & c_{m1} \\ c_{12} & c_{22} & \cdots & c_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ c_{1q} & c_{2q} & \dots & c_{mq} \end{bmatrix}$$

7. Kemudian ditransposkan

$$C = (C^T)^T = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1q} \\ c_{21} & c_{22} & \cdots & c_{2q} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \dots & c_{mq} \end{bmatrix}$$

8. Ubahlah hasil langkah ke-7 kedalam abjad menggunakan korespondensi abjad dengan numerik pada langkah 1 sehingga diperoleh cipherteks.

## Algoritma Dekripsi Hill Cipher

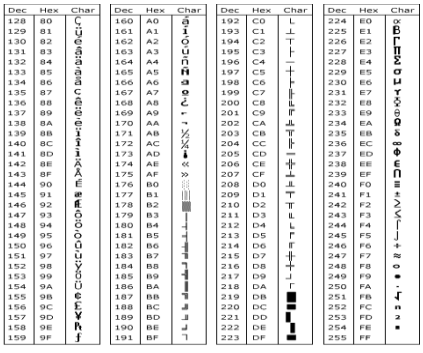
1. Korespondenkan abjad dengan numerik.
2. Ubah cipherteks kedalam numerik.
3. Kunci yang digunakan untuk mendekripsikan cipherteks ke plainteks adalah invers dari matriks kunci $K_{m\times m}$.
4. Menghitung invers matriks $K$ yaitu $K^{-1}$.
5. Kalikan invers matriks kunci dengan cipherteks transpos dalam modulo 26. Diperoleh plainteks transpos
   $P^T = K^{-1}C^T$
6. Dari langkah ke-5 diperoleh $P = (P^T)^T$
7. Korespondensikan abjad dengan matriks hasil langkah 6 diperoleh plainteks.

## Kode *ASCII*

Kode *ASCII (American Standard Code for Information Interchange)* merupakan sebuah kode yang digunakan untuk merepresentasikan karakter-karakter kedalam numerik. Adapun Kode *ASCII* ini merepresentasikan sebanyak 256 karakter dengan bilangan desimal dari 0 sampai 255. Berikut ini merupakan tabel yang memuat daftar karakter pada kode *ASCII* (Parekh, 2006, 77).

**Tabel 2.6.1** Daftar Kode *ASCII*

| Dec | Char | | Dec | Char | Dec | Char | Dec | Char |
|---|---|---|---|---|---|---|---|---|
| 0 | NUL | (null) | 32 | Space | 64 | @ | 96 | ` |
| 1 | SOH | (start of heading) | 33 | ! | 65 | A | 97 | a |
| 2 | STX | (start of text) | 34 | " | 66 | B | 98 | b |
| 3 | ETX | (end of text) | 35 | # | 67 | C | 99 | c |
| 4 | EOT | (end of transmission) | 36 | $ | 68 | D | 100 | d |
| 5 | ENQ | (enquery) | 37 | % | 69 | E | 101 | e |
| 6 | ACK | (acknowledge) | 38 | & | 70 | F | 102 | f |
| 7 | BEL | (bell) | 39 | | 71 | G | 103 | g |
| 8 | BS | (backspace) | 40 | ( | 72 | H | 104 | h |
| 9 | TAB | (horizontal tab) | 41 | ) | 73 | I | 105 | i |
| 10 | LF | (NL line feed, new line) | 42 | * | 74 | J | 106 | j |
| 11 | VT | (vertical tab) | 43 | + | 75 | K | 107 | k |
| 12 | FF | (NP formfeed, new page) | 44 | , | 76 | L | 108 | l |
| 13 | CR | (carriage return) | 45 | - | 77 | M | 109 | m |
| 14 | SOH | (shift out) | 46 | . | 78 | N | 110 | n |
| 15 | SI | (shift in) | 47 | / | 79 | O | 111 | o |
| 16 | DLE | (data link escape) | 48 | 0 | 80 | P | 112 | p |
| 17 | DC1 | (device control 1) | 49 | 1 | 81 | Q | 113 | q |
| 18 | DC2 | (device control 2) | 50 | 2 | 82 | R | 114 | r |
| 19 | DC3 | (device control 3) | 51 | 3 | 83 | S | 115 | s |
| 20 | DC4 | (device control 4) | 52 | 4 | 84 | T | 116 | t |
| 21 | NAK | (negative acknowledge) | 53 | 5 | 85 | U | 117 | u |
| 22 | SYN | (synchronous idle) | 54 | 6 | 86 | V | 118 | v |
| 23 | ETB | (end of trans. Block) | 55 | 7 | 87 | W | 119 | w |
| 24 | CAN | (cancel) | 56 | 8 | 88 | X | 120 | x |
| 25 | EM | (end of medium) | 57 | 9 | 89 | Y | 121 | y |
| 26 | SUB | (subbstitute) | 58 | : | 90 | Z | 122 | z |
| 27 | ESC | (escape) | 59 | ; | 91 | [ | 123 | { |
| 28 | FS | (file separator) | 60 | < | 92 | \ | 124 | \| |
| 29 | GS | (group separator) | 61 | = | 93 | ] | 125 | } |
| 30 | RS | (record separator) | 62 | > | 94 | ^ | 126 | ~ |
| 31 | US | (unit separator) | 63 | ? | 95 | _ | 127 | DEL |



## 2.2 Aritmatika Modular

**Definisi 2.2.1 (Munir, 2012: 191)**
*Misalkan $a$ adalah bilangan bulat dan $x$ suatu bilangan bulat $> 0$, operasi $a$ **mod** $x$ (dibaca $a$ modulo $x$) memberikan sisa jika $a$ dibagi dengan $x$. Dengan kata lain, $a$ **mod** $m = r$ sedemikian sehingga $a = xq + r$, dengan $0 \leq r < x$.*

**Definisi 2.2.2 (Subarinah, 2004: 22)**
*Jika $m$ suatu bilangan bulat positif $a$ kongruen $b$ modulo $x$ jika dan hanya jika $x$ membagi $(a - b)$, ditulis $a \equiv b \ (mod\ x)$.*

**Definisi 2.3.3 (Subarinah, 2004: 23)**
*Jika $a \equiv r \ (mod\ x)$ dengan $0 \leq r < x$ maka $r$ disebut residu terkecil dari $a \bmod x$.*

Untuk kekongruenan ini, $\{0, 1, 2, \dots, (x-1)\}$ disebut himpunan residu terkecil modulo $m$. Adapun himpunan residu terkecil ini dapat dengan menuliskannya sebagai

$$\mathbb{Z}_x = \{0, 1, 2, \dots, (x-1)\}$$

Menurut Anton (2005: 310) jika $a$ adalah sebuah bilangan bulat *taknegatif*, maka residu dari modulo $x$-nya secara sederhana adalah sisa yang dihasilkan ketika $a$ dibagi $x$. Sehingga jika dimisalkan $r \in \mathbb{Z}_x$ maka

$$r = sisa\ dari\ \left(\frac{a}{x}\right)$$

**Definisi 2.2.3 (Anton, 2005: 311)**
*Jika $a$ adalah sebuah bilangan dalam $\mathbb{Z}_x$, maka sebuah bilangan $a^{-1}$ di dalam $\mathbb{Z}_x$ disebut sebuah **Resiprok** atau **invers perkalian** dari $a$ modulo $x$ jika $aa^{-1} = a^{-1}a = 1 \ (mod\ x)$.*

**Teorema 2.2.1 (Anton, 2005: 312)**
*Sebuah matriks bujur sangkar $A$ dengan entri-entri di dalam $\mathbb{Z}_x$ dapat dibalik jika dan hanya jika residu dari $det(A)$ mempunyai sebuah modulo $x$ resiprok.*

## 2.3 Generalisasi Bilangan Fibonacci

**Definisi 2.3.1 Generalisasi bilangan Fibonacci (Purnamayanti, 2012: 40)**
*Generalisasi bilangan Fibonacci yang kemudian disebut dengan bilangan Fibonacci berderajat p didefinisikan sebagai:*

$$F_p(n) = F_p(n-1) + F_p(n-p-1),$$

$$untuk\ n > p+1,$$

*Dengan kondisi*

$$F_p(1) = F_p(2) = \cdots = F_p(p+1) = 1.$$

**Definisi 2.3.2 Generalisasi matriks Fibonacci (Purnamayanti, 2012: 41)**

*Generalisasi matriks dari generalisasi bilangan Fibonacci berderajat-p $(p = 0,1,2,3,\dots)$ didefinisikan sebagai matriks $Q_p$ berorde $(p+1) \times (p+1)$ sebagai:*

$$Q_p = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \dots & \ddots & \dots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

*Dan matriks $Q_p$ pangkat n didefinisikan sebagai $Q_p^n = \left(q_{ij}\right)$ dimana*

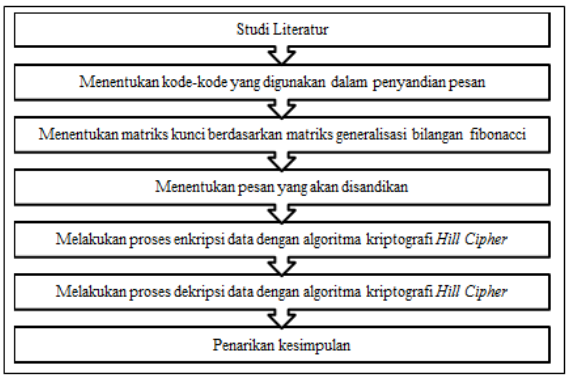
$q_{ij} = F_p(n+j-i-p)$ *untuk* $j \geq 2$ *dan* $q_{i,1} = F_p(n+2-i)$,

$$Q_p^n = \begin{pmatrix} F_p(n+1) & F_p(n-p+1) & \dots & F_p(n-1) & F_p(n) \\ F_p(n) & F_p(n-p) & \dots & F_p(n-2) & F_p(n-1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ F_p(n-p+2) & F_p(n-2p+2) & \cdots & F_p(n-p) & F_p(n-p+1) \\ F_p(n-p+1) & F_p(n-2p+1) & \cdots & F_p(n-p-1) & F_p(n-p) \end{pmatrix}$$

## 3. METODE PENELITIAN

Jenis penelitian ini berdasarkan pada metode penelitian yang bersifat studi literatur yaitu berupa mengumpulkan, mempelajari dan memahami referensi-referensi yang berkaitan dengan aljabar matriks, aritmatika modulo, bilangan Fibonacci beserta generalisasinya dan kriptografi. Selanjutnya beberapa teori tersebut dapat diaplikasikan pada kriptografi khususnya pada kriptografi *Hill Cipher*.

Adapun langkah-langkah pada penelitian ini digambarkan dalam diagram alir berikut:




**Gambar 3.1** ***Diagram alir penelitian***

## 4. HASIL DAN PEMBAHASAN

### 4.1 Penentuan Kode dan *modulus* $x$

Karakter-karakter dari kode *ASCII* ini terdiri atas 256 karakter sehingga berdasarkan jumlah karakter yang terdapat pada kode *ASCII* ini dapat dijadikan untuk menentukan *modulus* $x$ dimana bilangan $x$ dijadikan sebagai pembagi bilangan. Adapun bilangan $m$ menyatakan jumlah karakter yang digunakan dalam proses penyandian pesan. Dalam algoritma kriptografi *Hill Cipher* biasa digunakan nilai $x = 26$ yang merupakan jumlah alphabet yang dijadikan karakter-karakter yang digunakan pada algoritma ini. Akan tetapi, pada penelitian ini nilai $x$ yang digunakan adalah $x = 256$ berdasarkan jumlah karakter pada kode *ASCII*.

### 4.2 Penentuan matriks kunci

Dalam Algoritma Kriptografi *Hill Cipher*, terdapat dua ketentuan yang harus dipenuhi sebuah matriks untuk dapat dijadikan sebagai matriks kunci, yaitu:

1. Matriks kunci harus berupa matriks berukuran $m \times m$ atau disebut sebagai matriks bujur sangkar orde-$m$.

Matriks generalisasi bilangan Fibonacci ${Q_p}^n$ yang merupakan matriks berukuran $(p+1) \times (p+1)$ sehingga satu syarat matriks kunci dari algoritma kriptografi *Hill Cipher* telah terpenuhi oleh matriks generalisasi bilangan Fibonacci.

2. Matriks kunci harus memiliki invers perkalian

Ada syarat lain yang harus dipenuhi Matriks generalisasi bilangan Fibonacci sehingga dapat dijadikan sebagai matriks kunci dalam algoritma kriptografi *Hill Cipher* yaitu matriks kunci tersebut haruslah memiliki invers perkalian. Eksistensi invers ini dijelaskan pada teorema berikut.

**Teorema 2.2.1.**

*Untuk setiap bilangan bulat $p \geq 0$, matriks $Q_p^n$ dengan entri-entri dalam $\mathbb{Z}_x$ dapat dibalik.*

**Bukti:**

Untuk $p = 0$ jelas $Q_p^n = (1)^n = (1)$ adalah matriks yang dapat dibalik. Sekarang misalkan $p$ bilangan bulat dengan $p > 0$. Untuk menunjukkan $Q_p^n$ dapat dibalik cukup ditunjukkan bahwa $\det(Q_p^n)$ memiliki invers perkalian modulo $x$. Diberikan matriks

$$Q_p = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \ldots & \ddots & \ldots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}$$

Maka

$$(Q_p)^n = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \ldots & \ddots & \ldots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}^n$$

Akan ditentukan terlebih dahulu $\det(Q_p)$

Dalam menentukan nilai $\det(Q_p)$ dapat dilakukan dengan membentuk matriks $Q_p$ menjadi matriks segitiga melalui operasi baris elementer. Perhatikan bahwa

$$Q_p = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \ldots & \ddots & \ldots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}$$

Langkah-langkah membentuk matriks segitiga:

i. Pertukarkan dua baris yaitu baris ke-1 dipertukarkan dengan baris ke-2 diperoleh

$$(Q_p)_{12} = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \ldots & \ddots & \ldots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}$$

Sehingga $\det(Q_p) = -1 \det\left((Q_p)_{12}\right)$

ii. Dari matriks $(Q_p)_{12}$, Pertukarkan dua baris yaitu baris ke-2 dipertukarkan dengan baris ke-3 diperoleh

$$\left((Q_p)_{12}\right)_{23} = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 1 \\ \vdots & \ldots & \ddots & \ldots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}$$

Sehingga $\det(Q_p) = -1\left(-1 \det\left((Q_p)_{12}\right)_{23}\right)$.

iii. Seterusnya, dilakukan pertukaran baris sebanyak $p$ kali. Sehingga diperoleh

$$\left(\left((Q_p)_{12}\right)_{\ldots}\right)_{(i-1)i} = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & 1 & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}$$

Dengan $i = 2, \ldots, p+1$ dengan $p = 1, 2, 3, \ldots$
Diperoleh nilai

$$\det(Q_p) = \underbrace{(-1) \times (-1) \times \ldots \times (-1)}_{sebanyak\ p\ kali}\left(\det\left(\left((Q_p)_{12}\right)_{\ldots}\right)_{(i-1)i}\right)$$

$$\det(Q_p) = (-1)^p\left(\det\left(\left((Q_p)_{12}\right)_{\ldots}\right)_{(i-1)i}\right)$$

Karena matriks $\left(\left((Q_p)_{12}\right)_{\ldots}\right)_{(i-1)i}$ merupakan sebuah matriks segitiga bawah sehingga

$$det\left(\left((Q_p)_{12}\right)_{\ldots}\right)_{(i-1)i} = det\begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & 1 & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix} = 1$$

Maka nilai determinan dari matriks $Q_p$ adalah

$$\det(Q_p) = (-1)^p\left(\det\left(\left((Q_p)_{12}\right)_{\ldots}\right)_{(i-1)i}\right)$$
$$\det(Q_p) = (-1)^p(1)$$
$$\det(Q_p) = (-1)^p$$

Sehingga terdapat dua kemungkinan, yaitu:

1. Jika derajat dari matriks generalisasi bilangan fibonacci $(p)$ ganjil maka
   $\det(Q_p) = (-1)^p = -1$
2. Jika derajat dari matriks generalisasi bilangan fibonacci $(p)$ genap maka
   $\det(Q_p) = (-1)^p = 1$

Selanjutnya, karena $\det(Q_p^n) = \left(\det(Q_p)\right)^n$, maka $\det(Q_p^n) = 1$ atau $\det(Q_p^n) = -1$. Diperoleh bahwa $\det(Q_p^n)$ selalu punya invers dalam $\mathbb{Z}_x$ yaitu $(1)^{-1} = 1$ dan $(-1)^{-1} = x - 1$. Jadi, $Q_p^n$ dapat dibalik.

■

Berdasarkan paparan di atas, matriks generalisasi bilangan Fibonacci $Q_p^n$ merupakan matriks bujursangkar dan selalu memiliki invers perkalian terhadap $modulo\ x$. Akibatnya, untuk semua matriks generalisasi bilangan Fibonacci dengan derajat-$p$ dan pangkat-$n$ memenuhi syarat matriks kunci dalam algoritma kriptografi *Hill Cipher*.

## 4.3 Penerapan dalam Teknik Penyandian Pesan

Pada bagian ini akan diberikan contoh kasus yakni sebuah pesan yang dilakukan enkripsi dan dekripsi. Kasus ini diberikan untuk menerapkan bagaimana Algoritma Kriptografi *Hill Cipher* dalam melakukan proses penyandian pesan dengan memanfaatkan Matriks Generalisasi Bilangan Fibonacci sebagai matriks kunci.

### Proses enkripsi pesan

Diberikan sebuah kalimat:
**"Bilangan Fibonacci"**
Enkripsikan kalimat tersebut dengan kunci $p = 2$ dan $n = 4$ dari Matriks Generalisasi Bilangan Fibonacci.
**Penyelesaian:**

Untuk meneyelesaikan kasus tersebut, dengan beberapa langkah yang telah dijelaskan pada bagian sebelumnya, yaitu:

1. Menentukan matriks kunci

Diketahui:
$p = 2$ dan $n = 4$
Sehingga diperoleh matriks generalisasi bilangan Fibonacci berderajat-2 dan pangkat-4.

$$Q_2^4 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} F_2(5) & F_2(3) & F_2(4) \\ F_2(4) & F_2(2) & F_2(3) \\ F_2(3) & F_2(1) & F_2(2) \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Jadi matriks kunci yang diperoleh adalah

$$Q_2{}^4 = \begin{pmatrix} 3 & 1 & 2 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

2. Korespondensikan setiap karakter pada pesan dengan numerik berdasarkan pada kode *ASCII*.

| “ | B | i | l | a | n | g | a | n | SP | F |
|---|---|---|---|---|---|---|---|---|---|---|
| 34 | 66 | 105 | 108 | 97 | 110 | 103 | 97 | 110 | 32 | 70 |
| i | b | o | n | a | c | c | i | “ | | |
| 105 | 98 | 111 | 110 | 97 | 99 | 99 | 105 | 22 | 255 | |

3. Disusun bilangan-bilangan hasil konversi karakter tersebut kedalam sebuah matriks *plaintext* $P_{7\times3}$ berarti

$$P_{7\times3} = \begin{pmatrix} 34 & 66 & 105 \\ 108 & 97 & 110 \\ 103 & 97 & 110 \\ 32 & 70 & 105 \\ 98 & 111 & 110 \\ 97 & 99 & 99 \\ 105 & 22 & 255 \end{pmatrix}$$

4. Dari matriks $P_{7\times3}$ dibentuk sebuah matriks transpose $P^T{}_{3\times7}$ menjadi

$$P^T{}_{3\times7} = \begin{pmatrix} 34 & 108 & 103 & 32 & 98 & 97 & 105 \\ 66 & 97 & 97 & 70 & 111 & 99 & 22 \\ 105 & 110 & 110 & 105 & 110 & 99 & 255 \end{pmatrix}$$

5. Selanjutnya dilakukan operasi perkalian matriks kunci dengan matriks *plaintext* transpose

$$R \equiv \begin{pmatrix} 3 & 1 & 2 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 34 & 108 & 103 & 32 & 98 & 97 & 105 \\ 66 & 97 & 97 & 70 & 111 & 99 & 22 \\ 105 & 110 & 110 & 105 & 110 & 99 & 255 \end{pmatrix} mod\ 256$$

$$R \equiv \begin{pmatrix} 378 & 641 & 626 & 376 & 625 & 588 & 847 \\ 239 & 423 & 413 & 239 & 417 & 392 & 487 \\ 205 & 315 & 310 & 207 & 319 & 295 & 387 \end{pmatrix} mod\ 256$$

$$R \equiv \begin{pmatrix} 122 & 129 & 114 & 120 & 113 & 76 & 79 \\ 239 & 167 & 157 & 239 & 161 & 136 & 231 \\ 205 & 59 & 54 & 207 & 63 & 38 & 126 \end{pmatrix} mod\ 256$$

6. Dapat ditentukan matriks *ciphertext* yang merupakan transpose matriks $R$ yang diperoleh pada langkah 5 namakan matriks $C$. Diperoleh

$$C = \begin{pmatrix} 122 & 239 & 205 \\ 129 & 167 & 59 \\ 114 & 157 & 54 \\ 120 & 239 & 207 \\ 113 & 161 & 63 \\ 76 & 136 & 38 \\ 79 & 231 & 126 \end{pmatrix}$$

7. Terakhir dengan mengkonversikan bilangan-bilangan dari matriks *ciphertext* kedalam karakter-karater yang disesuaikan pada kode *ASCII*.

| 122 | 239 | 205 | 129 | 167 | 59 | 114 | 157 | 54 | 120 | 239 |
|---|---|---|---|---|---|---|---|---|---|---|
| z | ´ | = | ü | ° | ; | r | Ø | 6 | x | ´ |
| 207 | 113 | 161 | 63 | 76 | 136 | 38 | 79 | 231 | 126 | |
| ¤ | q | í | ? | L | ê | & | O | þ | ~ | |

Setelah langkah-langkah enkripsi pesan tersebut dilakukan diperoleh sebuah pesan enkripsi (pesan tersandi) menjadi

**z´=ü°;rØ6x´¤qí?Lê&Oþ~**

## Proses dekripsi pesan

Pesan tersandi:

**z´=ü°;rØ6x´¤qí?Lê&Oþ~**

Pecahkan kalimat tersebut dengan kunci $p = 2$ dan $n = 4$ dari Matriks Generalisasi Bilangan Fibonacci sehingga pesan dapat dimengerti!

**Penyelesaian:**

1. Menentukan matriks kunci

   Karena merupakan kunci simetris maka matriks kunci merupakan invers matriks dari matriks generalisasi bilangan Fibonacci dimana
   Diketahui:
   $p = 2$ dan $n = 4$
   Sehingga diperoleh matriks generalisasi bilangan Fibonacci berderajat-2 dan pangkat-4

$$Q_2{}^4 = \begin{pmatrix} 3 & 1 & 2 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

   Selanjutnya dapat ditentukan invers matriks dari matriks tersebut terhadap modulo 256. Invers matriks dapat ditentukan dengan

$$(Q_2^4)^{-1} = \det(Q_2^4)^{-1}\, Adj(Q_2^4)$$

Dan didapatkan matriks kunci untuk proses dekripsinya adalah

$$(Q_2{}^4)^{-1} = \begin{pmatrix} 0 & 1 & 255 \\ 255 & 1 & 1 \\ 1 & 254 & 1 \end{pmatrix}$$

2. Korespondensikan setiap karakter pesan yang diketahui dengan numerik berdasarkan pada kode *ASCII*.

| z | ´ | = | ü | ° | ; | r | Ø | 6 | x | ´ |
|---|---|---|---|---|---|---|---|---|---|---|
| 122 | 239 | 205 | 129 | 167 | 59 | 114 | 157 | 54 | 120 | 239 |
| ¤ | q | í | ? | L | ê | & | O | þ | ~ | |
| 207 | 113 | 161 | 63 | 76 | 136 | 38 | 79 | 231 | 126 | |

3. Disusun bilangan-bilangan hasil konversi karakter tersebut kedalam sebuah matriks *ciphertext* $C_{7\times3}$ berarti

$$C = \begin{pmatrix} 122 & 239 & 205 \\ 129 & 167 & 59 \\ 114 & 157 & 54 \\ 120 & 239 & 207 \\ 113 & 161 & 63 \\ 76 & 136 & 38 \\ 79 & 231 & 126 \end{pmatrix}$$

4. Dari matriks $C_{7\times3}$ dibentuk sebuah matriks transpose ${C^T}_{3\times7}$ menjadi

$$(C_{3\times7})^T \equiv \begin{pmatrix} 122 & 129 & 114 & 120 & 113 & 76 & 79 \\ 239 & 167 & 157 & 239 & 161 & 136 & 231 \\ 205 & 59 & 54 & 207 & 63 & 38 & 126 \end{pmatrix}$$

5. Selanjutnya dilakukan operasi perkalian matriks kunci dengan matriks *plaintext* transpose

$$S \equiv (Q_2{}^4)^{-1} \times (C_{3\times7})^T \; mod\; 256$$

$$S \equiv \begin{pmatrix} 0 & 1 & 255 \\ 255 & 1 & 1 \\ 1 & 254 & 1 \end{pmatrix} \times \begin{pmatrix} 122 & 129 & 114 & 120 & 113 & 76 & 79 \\ 239 & 167 & 157 & 239 & 161 & 136 & 231 \\ 205 & 59 & 54 & 207 & 63 & 38 & 126 \end{pmatrix} mod\ 256$$

$$S \equiv \begin{pmatrix} 52514 & 15212 & 13927 & 53024 & 16226 & 10081 & 32361 \\ 31554 & 33121 & 29281 & 31046 & 29039 & 19555 & 20520 \\ 61033 & 42606 & 40046 & 61033 & 41070 & 34659 & 58879 \end{pmatrix} mod\ 256$$

$$S \equiv \begin{pmatrix} 34 & 108 & 103 & 32 & 98 & 97 & 105 \\ 66 & 97 & 97 & 70 & 111 & 99 & 22 \\ 105 & 110 & 110 & 105 & 110 & 99 & 255 \end{pmatrix} mod\ 256$$

.

6. Selanjutnya dapat ditentukan matriks *plaintext* yang merupakan transpose matriks $S$ yang diperoleh pada langkah 5.

$$P_{7\times3} = \begin{pmatrix} 34 & 66 & 105 \\ 108 & 97 & 110 \\ 103 & 97 & 110 \\ 32 & 70 & 105 \\ 98 & 111 & 110 \\ 97 & 99 & 99 \\ 105 & 22 & 255 \end{pmatrix}$$

7. Konversikan bilangan-bilangan dari matriks plain*text* kedalam karakter-karater yang disesuaikan pada kode *ASCII*.

| 34 | 66 | 105 | 108 | 97 | 110 | 103 | 97 | 110 | 32 | 70 |
|---|---|---|---|---|---|---|---|---|---|---|
| " | B | i | l | a | n | g | a | n | SP | F |
| 105 | 98 | 111 | 110 | 97 | 99 | 99 | 105 | 22 | 255 | |
| i | b | o | n | a | c | c | i | " | | |

Jadi pesan tersandi tersebut sudah terpecahkan menjadi sebuah pesan yang dapat dimengerti yaitu:

**"Bilangan Fibonacci"**

## 5. KESIMPULAN

Berdasarkan hasil dan pembahasan dari penelitian ini dapat disimpulkan bahwa modifikasi algoritma kriptografi *Hill Cipher* dengan matriks Generalisasi Bilangan Fibonacci dilakukan dengan memodifikasi kunci dari algoritma kriptografi *Hill Cipher* yakni dengan menjadikan derajat $p$ dan pangkat $n$ dari matriks generalisasi bilangan fibonacci $(Q_p^n)$ sebagai matriks kunci yang digunakan dalam melakukan proses enkripsi dan dekripsi. Hal ini dapat dilakukan karena setiap matriks generalisasi bilangan fibonacci $(Q_p^n)$ memenuhi syarat matriks kunci dalam algoritma kriptografi *Hill Cipher*. Adapun penggunaan kunci dengan mengambil minimal $p = 2$ diharapkan dapat melindungi informasi dari serangan seperti *Known-Plaintext attack* dan *Chosen-plaintext Attack.*

## DAFTAR PUSTAKA


Anton, H. & Rorres, C. (2004). *Aljabar Linear Elementer versi Aplikasi Edisi Delapan jilid Satu*. Jakarta: Erlangga.

Gere, J. M., William, Jr. W. (1987). *Aljabar Matriks untuk Para Insinyur Edisi kedua.* Jakarta: Erlangga.

Hasugian, A. H. (2013). Imlementasi Algoritma Hil Cipher dalam Penyandian Data. *Pelita Informatika Budi Darma, Volume: IV, Nomor: 2, Agustus 2013.*

Leon, S. J. (2001). *Aljabar Linear dan Aplikasinya Edisi 5*. Jakarta: Erlangga.

Munir, R. (2012) *Matematika Diskrit*. Bandung: INFORMATIKA.

Parekh, R. (2006). *Principle of Multimedia*. New Delhi: Tata McGraw-Hill Publishing Company Limited.

Purnamayanti. (2012). Formula Binet dan Jumlah n suku pertama pada Generelisasi Bilangan Fibonacci dengan Metode Matriks. *Jurnal Matematika Murni dan Terapan Vol. 6 no. 1 Juni 2012: 38-46*.

Rosen, K. H. (1986). *Elementary Number Theory and Its Applications*, Canada: Addison-Wesley Publishing Company.

Supiyanto. (2015). Implementasi Hill Cipher pada Citra menggunakan Koefisien Binomial Sebagai Matriks Kunci. *Seminar Nasional Informatika 2015 UPN "Veteran" Yogyakarta, 14 November 2015 ISSN: 1979-2328*.

Tuasikal, A. R., Indra, D., & Fattah, F. (2020). Kriptanalalisis pada Metode Hill Cipher. *Buletin Sistem Informasi dan Teknologi Islam Vol 1, No. 1, Februari 2020, pp. 1-5.*