Jurnal Matematika, Komputasi dan Statistika
Volume 4 Nomor 3, pp. 790 - 800, September - Desember 2024
ISSN: 2503 – 2984

KRIPTOGRAFI *HILL CIPHER* MENGGUNAKAN MATRIKS FIBBONACCI

Chaeril Anwar Beddolo[1)]
[1)]Program Studi Matematika, Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Halu Oleo, Kendari, Indonesia
Email: chaerilanwarbeddolo.3745@gmail.com

Arman[1,a)], dan **Herdi Budiman**[1,b)]
[1)]Program Studi Matematika, Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Halu Oleo, Kendari, Indonesia
Email: [a)] arman.mtmk@uho.ac.id, dan [b)]herdi_budiman@yahoo.com

ABSTRAK

Era digital telah membuat informasi online menjadi bagian integral dari kehidupan sehari-hari, tetapi masalah keamanan data telah meningkat. Teknik Kriptografi *Hill Cipher* dan Fibonacci dapat digunakan untuk enkripsi dan dekripsi data. Penelitian ini menjelaskan penerapan dan kekuatan dari Matriks Fibonacci sebagai kunci dalam enkripsi dan dekripsi pesan dalam Kriptografi *Hill Cipher*. Penelitian ini membahas tentang algoritma Kriptografi *Hill Cipher*, pembentukan Matriks Fibonacci, kelayakan matriks Fibonacci, menentukan algoritma enkripsi dan dekripsi, menilai kualitas cipherteks dari hasil enkripsi, dan melakukan pemrograman dalam enkripsi dan dekripsi Kriptografi *Hill Cipher*. Implementasi matriks Fibonacci dapat digunakan dalam proses enkripsi dan dekripsi algoritma *Hill Cipher*. Enkripsi melibatkan konversi plainteks ke ASCII, memodulasi hasil perkalian plaintext dengan kunci, dan konversi karakter sesuai tabel ASCII. Dekripsi melibatkan konversi ciphertext ke ASCII, memodulasi hasil perkalian ciphertext dengan kunci yang telah diinvers, dan konversi ke tabel ASCII. Menggunakan Fibonacci sebagai kunci dalam algoritma *Hill Cipher* dapat meningkatkan kompleksitas sistem kriptografi. Menggabungkan konsep Fibonacci dan *Hill Cipher* dapat menghasilkan penggunaan kunci yang lebih dinamis dan efisien, menghasilkan enkripsi yang lebih baik dan metode kriptografi yang lebih kuat.

Kata Kunci: Keamanan siber, Kriptografi, Hill Cipher, Fibonacci, Matriks**.**

ABSTRACT

In the digital age, online information has become a fundamental component of daily life. However, this has led to an escalation in concerns surrounding data security. Techniques such as Hill Cipher and Fibonacci Cryptography can be employed for the encryption and decryption of data. This study elucidates the utilization and efficacy of the Fibonacci Matrix as a key for encrypting and decrypting messages within the framework of Hill Cipher Cryptography. The research encompasses an examination of the Hill Cipher Cryptography algorithm, the construction of the Fibonacci Matrix, the viability of the Fibonacci matrix, the determination of encryption and decryption algorithms, the evaluation of the ciphertext quality derived from the encryption process, and the programming involved in the encryption and decryption of Hill Cipher Cryptography. The Fibonacci matrix can be implemented in the encryption and decryption procedures of the Hill Cipher algorithm. The encryption process entails the conversion of plaintext to ASCII, modulation of the product of plaintext and key multiplication, and character conversion in accordance with the ASCII table. Conversely, decryption involves the conversion of ciphertext to ASCII, modulation of the product of ciphertext and inverse key multiplication, and conversion to the ASCII table. The incorporation of Fibonacci as a key in the Hill Cipher algorithm can augment the complexity of the cryptographic system. The amalgamation of Fibonacci and Hill Cipher concepts can lead to a more dynamic and efficient utilization of keys, thereby enhancing encryption and fortifying cryptographic methods.

Keywords: *Cybersecurity, Cryptography, Hill Cipher, Fibonacci, Matrix****.***

1. Pendahuluan

Keamanan siber melindungi komunikasi, integritas, dan kerahasiaan, komunikasi, serta kehidupan, integrasi, aset yang berwujud dan tidak terwujud, serta data yang disimpan dalam sistem informasi elektronik oleh lembaga, organisasi, dan individu. Serangan yang dapat mengancam data dan informasi berupa interupsi, penyadapan informasi, pencurian identitas, pelanggaran hak privat, penyisipan virus, dan penyisipan data maupun informasi. Jumlah ancaman semakin meningkat setiap hari dengan jumlah dan kompleksitas yang tinggi. Tidak hanya jumlah penyerang berpotensial yang

semakin meningkat, namun jaringan semakin meluas dan alat yang tersedia lebih canggih, efektif dan efisien. Oleh karena itu, keamanan data dan informasi diperlukan. Meyamarkan data menjadi tidak bermakna adalah salah satu cara untuk mengamankan data tersebut. Sehingga perlu teknik pendekatan data yang dimana salah satunya Kriptografi [6].

Dalam bahasa Yunani kriptografi (*cryptography*) berasal dari kata "*kriptos*" dan "*graphien*", yang berarti "*secret*" (rahasia) dan "*writing*" (tulisan). Sehingga dapat dikatakan bahwa Kriptografi adalah *"secret writing"* (tulisan rahasia). Dalam bidang kriptografi terdapat dua proses utama yang relevan. Pertama, terdapat proses enkripsi dan dekripsi. Untuk menjalankan kedua proses ini, diperlukan mekanisme serta kunci yang ditentukan umumnya dikenal sebagai *"cipher"* [7].

Salah satu penerapan dari aritmatika modulo pada kriptografi adalah *Hill Cipher*, yaitu teknik yang menggunakan sebuah matriks persegi sebagai kunci yang digunakan dalam proses enkripsi serta dekripsi. Teknik *Hill Cipher* ini diciptakan oleh ilmuan matematika yang berasal dari Amerika bernama Lester Hill pada tahun 1929 [23].

Cipher (kode) yang dihasilkan tidak bisa dipecahkan menggunakan metode analisis frekuensi. Ini disebabkan oleh penggunaan operasi perkalian matriks dalam proses enkripsi dan dekripsi *Hill Cipher*. *Hill Cipher* termasuk dalam kategori kriptografi simetris yang memiliki tingkat kesulitan yang tinggi untuk dipecahkan [20].

Pada dasarnya matriks kunci yang dipergunakan dalam Algoritma *Hill Cipher* memiliki peran utama dalam proses enkripsi dan dekripsi, dimana kunci ini memiliki syarat yang harus dipenuhi yaitu matriks kuncinya harus memiliki sifat *invertible* atau memiliki invers. Dengan menggunakan matriks yang memiliki sifat *invertible* maka dapat mendekripsikan pesan yang terenskripsi. Oleh karena itu dalam penelitian ini digunakan matriks kunci yang entri-entrinya berasal dari matriks Fibonacci dengan menggunakan *American Standard Code for Information Interchange* (ASCII) sebagai dasar penginputan data serta menghitung tingkat keacakan dan korelasi dari pesan yang di enkripsi.

Pada bagian dua membahas mengenai kriptografi *Hill Cipher*, kode *ASCII*, *flowchart*, matriks, aritmatika modulo, relasi rekurensi, matriks fibonacci, entropy, dan analisi korelasi pearson. Pada bagian tiga dijelaskan mengenai metode penelitian yang akan dilakukan pada penelitian ini. Pada bagian empat menjelaskan hasil penelitian dan pembahasan dari penelitian yang dilakukan. Pada bagian lima membahas kesimpulan dan saran.

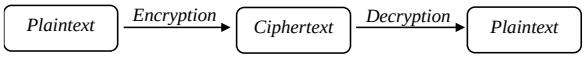
2. Tinjauan Pustaka

2.1 Kriptografi *Hill Chipher*

2.1.1 Pengertian Kriptografi

Kriptografi juga diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan keamanan informasi, seperti kerahasian data, keabsahan data integritas data dan autentikasi data. Keamanan pesan dalam kriptografi diperoleh dengan mengubah pesan yang dimengerti (*plaintext)* menjadi pesan yang tidak memiliki makna atau pesan yang tersandi (*ciphertext*). Proses mengubah *plaintext* menjadi *ciphertext* disebut *encryption* (enkripsi), sementara proses membalikkan *ciphertext* menjadi *plaintext* disebut *decryption* (dekripsi). Ilustrasi proses ini dapat dilihat pada diagram di Gambar 2.1 berikut [15].

Gambar 2.1 Proses Penyandian Pesan



2.1.2 Sejarah Kriptografi

Dalam sejarahnya, kriptografi sudah digunakan pada tahun 4000 SM yang digunakan oleh bangsa Mesir dalam bentuk *hieroglyphcs* untuk menyembunyikan tulisan – tulisan mereka yang bersifat rahasia. Kemudian *hieroglyphs* mengalami evolusi menjadi *hieratic* yaitu berupa *stylized script* yang memiliki cara penggunaan yang lebih mudah. Sekitar 400 SM, kriptografi mulai di implementasi dalam dunia kemiliteran yang dilakukan oleh bangsa Spartan yang menulis pesan rahasia dalam sepotong *papyrus* atau perkamen dibungkus dengan batang kayu yang disebut *Scytale System* yang merupakan teknik transposisi *cipher* yang tertua. Pada tahun 50 SM, kriptografi berkembang dengan *cipher* atau kuncinya menggunakan teknik substitusi matematika dalam penyandian pesan yang ditemukan oleh Julius Caesar yang merupakan kaisar kerajaan Roma [7].

2.1.3 Prinsip Kriptografi

Fungsi enkripsi dan fungsi dekripsi telah menjadi prinsip dasar dalam ilmu Kriptografi. Enkripsi adalah proses mengubah *plaintext* menjadi *ciphertext*. Dalam matematika misalnya *ciphertext* dilambangkan dengan C dan *plaintext* dilambangkan dengan P maka fungsi enkripsi E memetakan P ke C.

$$E(P) = C \qquad (2.1)$$

Sementara dekripsi merupakan kebalikan dari enkripsi yaitu proses mengembalikan pesan yang telah dienkripsi dari *ciphertext* menjadi *plaintext* sehingga pesan dapat dimengerti. Proses kebalikannya ini dapat ditulis menjadi fungsi dekripsi D memetakan C ke P.

$$D(C) = P \qquad (2.2)$$

Dengan kata lain, dekripsi D merupakan fungsi invers dari E atau $D = E^{-1}$ [15].

2.1.4 Tujuan Kriptografi

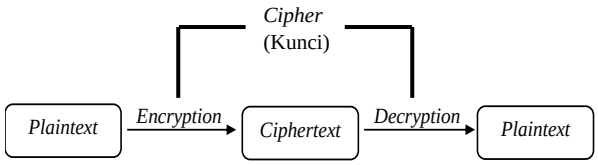
Terdapat 4 (empat) hal yang menjadi tujuan kriptografi dalam aspek keamanan informasi yaitu sebagai berikut.

1. Kerahasiaan (*confidentiality)*

2. Integritas data.
3. Otentikasi
4. Nirpenyangkalan (*non-repudiatio)* [15].

2.1.5 *Hill Cipher*

Hill Cipher merupakan salah satu kriptografi simetris dengan model logaritma seperti Gambar 2.2 berikut [7].



Gambar 2.2 Proses Kriptografi Simetris

Algoritma kriptografi ini dirancang dengan tujuan menghasilkan *cipher* (kode). *Hill Cipher* tidak melakukan penggantian langsung pada setiap huruf yang sama pada plainteks dengan huruf lain yang sama pada ciphertext, melainkan menggunakan operasi perkalian matriks dalam proses enkripsi dan dekripsi. Oleh karena itu, *Hill Cipher* masuk dalam kategori kriptosistem polialfabetik [25]. Matriks yang digunakan pada *Hill Cipher* adalah matriks yang *invertible*. Matriks *invertible* adalah matriks berukuran $n \times n$ dan memiliki determinan $\neq 0$ sehingga memiliki invers. Jika matriks tidak *invertible* maka matriks dapat digunakan dalam proses enkripsi, namun akan gagal ketika proses dekripsi [23].

2.2 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. Dalam penelitian ini hanya menggunakan nilai desimal karakter yang biasa digunakan. karakter huruf maupun angka yang bisa diliat dalam Tabel 2.1 berikut.

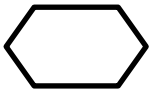
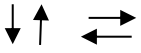
Tabel 2.1 Tabel Kode ASCII

Decimal Value	*Character*	*Decimal Value*	*Character*	*Decimal Value*	*Character*
32	*space*	64	@	96	‘
33	!	65	A	97	a
34	“	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	`	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

2.3 *Flowchart*

Diagram alir program adalah diagram yang menggambarkan alur logika dari data yang akan diolah dalam suatu program dari awal hingga akhir. Diagram alir terdiri dari simbol-simbol yang mewakili fungsi-fungsi langkah program dan garis alir (*flowlines*) yang menunnjukan urutan dari simbol yang akan dijalankan [8].

Tabel 2.2 Simbol-Simbol *Flowchart*

Simbol	Fungsi
	Simbol terminal untuk menyatakan awal atau akhir suatu program.
	Simbol proses, untuk menggambarkan proses pengolahan data
	Simbol persiapan (*preparation*), untuk memberikan nilai awal pada suatu variabel atau pencacah
	Simbol keputusan, menyatakan suatu pilihan berdasarkan suatu kondisi tertentu
	Simbol *input/output*, untuk menunjukkan operasi masukan atau keluaran
	Simbol proses terdefinisi (*predefined process symbol*), untuk proses yang detilnya dijelaskan terpisah, misal dalam bentuk subroutine
	Simbol *display*, menyatakan penggunaan output seperti monitor, printer, dan lain lain.
	Simbol arah aliran, untuk menunjukkan arah aliran proses

2.4 Matriks

Definisi 2.1. [2] Suatu matriks adalah jajaran empat persegi panjang dari bilangan-bilangan. Bilangan-

bilangan dalam jajaran tersebut disebut entri dari matriks.

Definisi 2.2 [2] Jika A adalah matriks $m \times r$ dan B adalah matriks $r \times n$, maka hasil kali AB adalah matriks $m \times n$ yang entri-entrinya ditentukan sebagai berikut.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m1} & \cdots & b_{mr} \end{bmatrix}, B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{r1} & b_{r2} & \cdots & b_{rn} \end{bmatrix}$$

Maka perkalian matriks $A\ B$ adalah sebagai berikut:

Dengan $C_{ij} = \sum_{k=1}^{n} a_{ik}\, b_{kj}$, untuk $i = 1, 2, \ldots, m$ dan $j = 1, 2, \ldots, p$. Sehingga $AB = C$ adalah sebagai berikut.

$$A\ B = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m1} & \cdots & b_{mr} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{r1} & b_{r2} & \cdots & b_{rn} \end{bmatrix}$$

$$C = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix}$$

Perkalian dilakukan antara baris-baris dari matirks A dan kolom-kolom dari matriks B yang menghasilkan matriks C. Elemen c_{11} berasal dari jumlah perkalian antara baris pertama matriks A dengan kolom pertama matriks B, yaitu

$c_{11} = a_{11}b_{11} + a_{12}b_{21} + \cdots + a_{1r}b_{r1}$

dan secara umum dapat dinyatakan

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \cdots \quad (2.3)$$

$a_{ik}b_{kj} = \sum_{k=1}^{n} a_{ik}b_{kj}$.

Definisi 2.3 [2] Determinan adalah suatu fungsi khusus yang mengasosiasikan suatu bilangan rill dengan suatu matriks bujur sangkar. Determinan dari matriks A dinotasikan dengan $\det(A)$ atau $|A|$.

Definisi 2.4 [2] Jika A adalah sebarang matriks bujur sangkar, dan jika dapat ditemukan suatu matriks bujur sangkar B sehingga berlaku $AB = BA = I$, maka A dikatakan dapat dibalik (*invertible*) dan B dinamakan invers dari A, dinyatakan sebagai $B = A^{-1}$.

2.5 Aritmatika Modulo

Aritmatika modulo, yang juga dikenal sebagai *modular arithmetic*, memiliki peranan yang signifikan dalam aplikasi kriptografi. Operator yang digunakan dalam aritmetika modulo adalah mod. Operator mod digunakan untuk menghasilkan sisa pembagian. Misalnya 31 dibagi 5 memberikan hasil $= 6$ dan sisa $= 1$, sehingga kita tulis $31\ mod\ 5 = 1$

Definisi 2.6 [15] Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi $a\ mod\ m$ (dibaca "$a\ modulo\ m$") memberikan sisa jika a dibagi dengan m. Dengan kata lain, $a\ mod\ m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$

Notasi: $a\ mod\ m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$

Bilangan m disebut modulus atau modulo dan hasil aritmatika modulo m terletak di dalam himpunan $\{0,1,2,3, \ldots, m-1\}$.

2.6 Relasi Rekurensi

Metode penyelesaian relasi rekurensi dengan iterasi merupakan pendekatan yang paling mendasar. Prinsipnya adalah dengan menghitung suku-suku barisan secara berurutan secara terus-menerus hingga pola tertentu teridentifikasi. Berdasarkan pola tersebut, kita dapat menyusun rumus eksplisit untuk mendapatkan suku-suku barisan dengan mudah. Untuk mengidentifikasi polanya, barisan dapat dihitung secara menaik $(a_0, a_1, a_2, \ldots)$ atau menurun $(a_n, a_{n-1}, a_{n-2}, \ldots)$.

Untuk mengatasi kendala dalam menemukan rumus eksplisit dari relasi rekurensi, ada metode yang disebut "Persamaan Karakteristik" [11].

2.7 Bilangan Fibonacci

Pada tahun 1634, matematikawan Albert Girard menulis formula untuk barisan Fibonacci pada karyanya *L'Arithmetique de Simon Stevin de Bruges*. Bilangan Fibonacci dimulai dengan 2 suku: $F_1 = 1$ dan $F_2 = 1$, meskipun terkadang dapat definisikan $F_0 = 0$. Bilangan Fibonacci dapat dirumuskan sebagai berikut [14].

$$F_n = F_{n-1} + F_{n-2}, n \geq 3 \quad (2.4)$$

Sehingga dengan menggunakan Persamaan (2.8) maka akan diperoleh rumus:

$F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, F_6 = 8, F_7 = 13, \ldots$

2.8 Matriks Fibonacci

Matriks adalah salah satu alat utama yang digunakan untuk memberikan solusi untul permasalahan yang berasal dari hubungan rekurensi linear. Versi matriks dari hubungan rekurensi linear pada deret Fibonacci dapat ditulis sebagai berikut [13]

$$\begin{bmatrix} F_n \\ F_{n+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} F_{n-1} \\ F_n \end{bmatrix}$$

Misalkan:

$$Q = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & F_1 \\ F_1 & F_2 \end{bmatrix}$$

dengan menggunakan induksi matematika, maka matriks Q dapat ditulis sebagai berikut.

$$Q^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}$$

dari persamaan $Q^{n+1}Q^n = Q^{2n+1}$, diperoleh:

$$\begin{bmatrix} F_n & F_{n+1} \\ F_{n+1} & F_{n+2} \end{bmatrix} \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix} = \begin{bmatrix} F_{2n+2} & F_{n+1} \\ F_{2n+1} & F_{2n} \end{bmatrix}$$

dengan perkalian matriks, diperoleh identitas untuk setiap bilangan Fibonacci di sisi kanan. Maka akan diperoleh Persamaan (2.9) sebagai berikut.

$$F_{n+1}^2 + F_n^2 = F_{2n+1} \quad (2.5)$$

hasil penjumlahan kuadrat dari n bilangan Fibonacci pertama pada Persamaan (2.9) sama dengan penjumlahan n suku pertama, yang ditulis dalam Persamaan (2.10) berikut.

$$F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1} \quad (2.6)$$

Secara umum, terdapat beberapa identitas dasar Fibonacci seperti berikut ini.

$$F_1F_2 + F_2F_3 + F_3F_4 + \cdots + F_{n-1}F_n = \frac{F_{2n-1} + F_nF_{n-1} - 1}{2} \quad (2.7)$$

Sedemikian sehingga akan mendefinisikan matriks baru. Matriks Fibonacci ber-ordo $n \times n$ yang didefinisikan sebagai berikut.

$$\mathcal{F}_n = [f_{ij}] = \begin{cases} F_{i-j+1}, & i-j+1 \geq 0, \\ 0, & i-j+1 < 0. \end{cases} \text{untuk } i,j \in \mathbb{Z}^+ \quad (2.12)$$

2.9 Entropy

Entropy digunakan untuk mengukur tingkat ketidakpastian antara variabel acak dalam suatu file data. Claude E. Shannon telah mengembangkan konsep entropy untuk variabel acak. Satuan yang digunakan untuk mengukur nilai entropy adalah bit [19].

Semakin tinggi nilai entropy, maka tingkat keacakan semakin meningkat, sehingga pesan menjadi lebih sulit untuk diprediksi. Shannon memberikan definisi pengukuran untuk entropy informasi (dalam bit) sebagai:

$$Entropy = H(X) = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i) \quad (2.13)$$

Keterangan:
$H(X) =$ Nilai entropy
$P(x_i) =$ Probabilitas kemunculan karakter ke-x_i

2.10 Analisis Korelasi *Pearson (Product Moment)*

Analisis korelasi adalah metode statistika yang digunakan untuk menentukan suatu besaran yang menyatakan seberapa kuat hubungan suatu variabel dengan variabel lain dengan tidak mempersoalkan apakah suatu variabel tertentu tergantung kepada variabel lain. Semakin nyata hubungan linier (garis lurus), maka semakin kuat atau tinggi derajat hubungan garis lurus antara kedua variabel atau lebih [22].

Koefisien korelasi adalah ukuran yang dipakai untuk mengetahui derajat hubungan antara variabel-variabel. Koefisien korelasi digunakan sebagai indeks untuk menilai seberapa besar hubungan antar variabel. Simbol (r) digunakan untuk menggambarkan besarnya koefisien korelasi antara dua variabel. Nilai koefesien korelasi berada pada interval $-1 < 0 < 1$, yaitu apabila $r = -1$ korelasi negatif sempurna, artinya taraf signifikansi dari pengaruh variabel X terhadap variabel Y sangat lemah dan apabila $r = 1$ korelasi positif sempurna, artinya taraf signifikansi dari pengaruh variabel X terhadap variabel Y sangat kuat, maka terdapat hubungan linier yang kuat antara *ciphertext* dan *plaintext* [22].

Pedoman untuk memberikan penilaian kuat/erat tidaknya hubungan sebuah variabel terdapat pada tabel berikut [24] :

Tabel 2.1 Pedoman Derajat Hubungan Dua Variabel

Interval Koefisien	Derajat Hubungan
0,00 – 0,20	Sangat Lemah
0,21 – 0,40	Lemah
0,41 – 0,60	Sedang
0,61 – 0,80	Kuat
0,81 – 1,00	Sangat Kuat

Adapun prosedur menggunakan analisis korelasi *Pearson* yaitu sebagai berikut:

1. Hipotesis:
   $H_0 : r = 0$ (tidak terdapat korelasi/hubungan yang signifikan antara *Plaintext* dan *Ciphertext*)
   $H_1 : r \neq 0$ (terdapat korelasi/hubungan yang signifikan antara *Plaintext* dan *Ciphertext*)
2. Statistik Uji:
   Uji statistik yang digunakan adalah Korelasi *Pearson* (r), dengan menggunakan Persamaan 2.14 berikut ini:

$$r = \frac{n\sum xy - \sum x \sum y}{\sqrt{n\sum x^2 - (\sum x)^2}.\sqrt{n\sum y^2 - (\sum y)^2}} \quad (2.14)$$

Keterangan :
$r =$ Koefisien korelasi *Pearson*
$n =$ Banyaknya data
$x =$ Nilai ASCII *Plaintext*
$y =$ Nilai ASCII *Ciphertext*

3. Kriteria Uji:
   Dalam menguji korelasi ini, taraf signifikansi yang digunakan yaitu $\alpha = 5\%$, dengan kriteria pengujian sebagai berikut [24]:
   - Jika nilai signifikansi $< 0{,}05$, maka berkorelasi
   - Jika nilai signifikansi $> 0{,}05$ maka tidak saling berkorelasi

3. Metode

Penelitian ini dilakukan dengan menggunakan metode penelitian kepustakaan *(library research)* atau studi literatur dengan urutan kerja sebagai berikut:

1. Studi literatur yang berkaitan dengan Kriptografi *Hill Cipher*
2. Pembentukan matriks kunci dari matriks bilangan Fibonacci
3. Menguji kelayakan matriks kunci yang dibentuk dari matriks bilangan Fibonacci
4. Merumuskan algoritma enkripsi dan dekripsi Kriptografi *Hill Cipher*
5. Menguji kualitas *ciphertext* hasil enkripsi menggunakan Kriptografi *Hill Cipher* dengan menghitung nilai *entrophy* dan analisis korelasi *Pearson*
6. Membuat program untuk mengenkripsi *plaintext* dan mendekripsikan *ciphertext* dengan bantuan *software Visual Studio Code* dalam hal ini menggunakan bahasa pemrograman *python.*

4. Hasil dan Pembahasan

4.1 Pembuatan Matriks Kunci dari Matriks Fibonacci

Dengan penggunaan Persamaan (2.8) akan menghasilkan entri-entri matriks kunci Kriptografi *Hill Cipher* sebagai berikut.

Matriks ukuran $3 \times 3 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix}$

Matriks ukuran $4 \times 4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 3 & 2 & 1 & 1 \end{bmatrix}$

Matriks ukuran $5 \times 5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 2 & 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 1 & 0 \\ 5 & 3 & 2 & 1 & 1 \end{bmatrix}$

Tabel 4.2 Determinan Matriks Kunci

Ordo Matriks Kunci	Nilai Determinan
Kunci 3×3	1
Kunci 4×4	1
Kunci 5×5	1

4.2 Operasi Matriks Untuk Kriptografi

4.2.1 Algoritma Enkripsi Kriptografi *Hill Cipher*

Langkah pertama : Pilih matriks A berukuran $n \times n$ yang mempunyai determinan tidak sama dengan 0. Setiap elemen dari matriks A merupakan elemen $\mathbb{Z}_{95}$ (bilangan bulat modulo 95). Matriks A adalah kunci rahasia dan harus disepakati dulu antara penerima dan pengirim pesan.

Langkah kedua : Membagi *plaintext* menjadi blok-blok yang berisi n huruf dimana n sesuai dengan ordo matriks. Misalnya matriks berordo 2×2 maka akan menghasilkan $P_1 = \begin{pmatrix} \rho_1 \\ \rho_2 \end{pmatrix}$. Apabila bagian blok terakhir memiliki sisa karakter yang tidak memiliki pasangan maka akan ditambahkan sembarang *dummy* untuk melengkapi.

Langkah ketiga : Mengkonversi *plaintext* yang telah dibagi menjadi blok-blok ke dalam bilangan ASCII yang ada pada Tabel 2.1.

Langkah keempat : Selanjutnya lakukan operasi perkalian antara matriks *A* dengan matriks *P*.

Langkah kelima : Setiap elemen matriks yang diperoleh di Langkah 4 dijadikan bilangan bulat modulo 95 karena jumlah karakter konversi pada Tabel 2.1 dan hasilnya ditambahkan dengan 32 pada tiap elemen agar hasil enkripsi masih tetap berada dalam lingkup karakter pada Tabel 2.1.

Langkah keenam : Konversikan angka yang diperoleh kedalam karakter yang bersesuaian pada kode ASCII (*American Standart Code for Information Interchange*) yang dapat diliat pada Tabel 2.1.

4.2.2 Algoritma Dekripsi Kriptografi *Hill Cipher*

Algoritma dekripsi sejalan dengan proses enkripsi, namun untuk matriks kunci yang digunakan adalah matriks invers dari matriks *A*.

Langkah pertama : Membagi *Ciphertext* menjadi blok-blok yang berisi n huruf dimana n sesuai dengan ordo matriks kemudian mengkonversikannya ke dalam bilangan ASCII yang bersesuaian pada Tabel 2.1.

Langkah kedua : Menghitung invers dari matriks kunci.

Langkah ketiga : Melakukan pengurangan elemen C_i pada langkah pertama dengan 32 dan menjumlahkan hasilnya dengan kelipatan 95 berdasarkan indeks karakter hasil bagi pada proses enkripsi.

Langkah keempat : Melakukan perkalian, matriks C_i yang diperoleh pada langkah ketiga dengan invers matriks K.

Langkah kelima : Mengkonversikan hasil pada langkah keempat ke dalam karakter yang bersesuaian pada Tabel 2.1.

4.3 Hasil Enkripsi dan Dekripsi Pesan

Pengirim pesan akan mengirimkan pesan **"Mabar Yuk?"** ke penerima. Pesan tersebut akan dienkripsi dan dekripsi menggunakan metode Kriptografi *Hill Cipher* dengan bantuan *software Visual Code Studio.*

4.3.1 Enkripsi dan Dekripsi Pesan dengan Matriks Kunci 3×3

Membagi *plaintext* menjadi blok-blok yang berisi 3 huruf serta mengkonversikannya ke dalam bilangan ASCII yang bersesuaian pada Tabel 2.1 sehingga diperoleh sebagai berikut.

$P_1 = (M \quad a \quad b) = (77 \quad 97 \quad 98)$
$P_2 = (a \quad r \quad space) = (97 \quad 114 \quad 32)$
$P_3 = (Y \quad u \quad k) = (89 \quad 117 \quad 107)$
$P_4 = (? \quad . \quad .) = (63 \quad 46 \quad 46)$

Diperoleh matriks $P = \begin{bmatrix} 77 & 97 & 98 \\ 97 & 114 & 32 \\ 89 & 117 & 107 \\ 63 & 46 & 46 \end{bmatrix}$

Tabel 4.3 Perkalian *Plaintext* dengan Matriks Kunci 3×3

Konversi Huruf ke Angka	Matriks Kunci	Hasil Perkalian Matriks Kunci
$\begin{bmatrix} 77 & 97 & 98 \\ 97 & 114 & 32 \\ 89 & 117 & 107 \\ 63 & 46 & 46 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 77 & 174 & 349 \\ 97 & 211 & 340 \\ 89 & 206 & 402 \\ 63 & 109 & 218 \end{bmatrix}$

Dari hasil perkalian *plaintext* dengan matriks kunci, akan di modulokan dengan 95 dan menjumlahkan hasilnya dengan 32 sehingga diperoleh matriks *ciphertext.* Maka:

$$C = \left(\begin{bmatrix} 77 & 174 & 349 \\ 97 & 211 & 340 \\ 89 & 206 & 402 \\ 63 & 109 & 218 \end{bmatrix} mod\ 95 \right) + \begin{bmatrix} 32 \\ 32 \\ 32 \\ 32 \end{bmatrix} = \begin{bmatrix} 109_0 & 111_1 & 96_3 \\ 34_1 & 53_2 & 87_2 \\ 121_0 & 48_2 & 54_4 \\ 95_0 & 56_1 & 60_2 \end{bmatrix}$$

Mengonversikan matriks C ke dalam karakter yang bersesuaian pada Tabel 2.2, maka:

$$C = \begin{bmatrix} 109_0 & 111_1 & 96_3 \\ 34_1 & 53_2 & 87_2 \\ 121_0 & 48_2 & 54_4 \\ 95_0 & 56_1 & 60_2 \end{bmatrix} = \begin{bmatrix} m & o & ' \\ " & 5 & W \\ y & 0 & 6 \\ \_ & 8 & < \end{bmatrix}$$

Sehungga diperoleh *ciphertext* dari hasil konversi yaitu **mo'"5Wy06_8<**

Membagi *ciphertext* menjadi blok-blok yang berisi 3 huruf dan mengkonversikannya ke dalam bilangan ASCII yang bersesuaian pada Tabel 2.2 sehingga diperoleh :

$C_1 = (m \quad o \quad ') = (109 \quad 111 \quad 96)$
$C_2 = (" \quad 5 \quad W) = (34 \quad 53 \quad 87)$
$C_3 = (y \quad 0 \quad 6) = (121 \quad 48 \quad 54)$
$C_4 = (\_ \quad 8 \quad <) = (95 \quad 56 \quad 60)$

Maka diperoleh matriks $C = \begin{bmatrix} 109 & 111 & 96 \\ 34 & 53 & 87 \\ 121 & 48 & 54 \\ 95 & 56 & 60 \end{bmatrix}$

Berdasarkan indeksi karakter hasil bagi pada proses enkripsi sehingga dieroleh matriks *ciphertext* sebagai berikut

$$C = \begin{bmatrix} 77 & 174 & 349 \\ 97 & 211 & 340 \\ 89 & 206 & 402 \\ 63 & 109 & 218 \end{bmatrix}$$

Kemudian akan dicari invers dari matriks kunci sebagai berikut.

$$kof(K) = \left((-1)^{i+j} M_{ij}\right) = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$adj(K) = \left(kof(K)\right)^T = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & -1 & 1 \end{pmatrix}$$

Jadi invers dari matriks kunci adalah

$$K^{-1} = \frac{1}{detK} adj(K) = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & -1 & 1 \end{pmatrix}$$

Tabel 4.4 Perkalian *Plaintext* dengan Matriks Kunci **3 × 3**

Matriks *Ciphertext*	Kunci	Hasil Perkalian Matriks Kunci
$\begin{bmatrix} 77 & 174 & 349 \\ 97 & 211 & 340 \\ 89 & 206 & 402 \\ 63 & 109 & 218 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 77 & 97 & 98 \\ 97 & 114 & 32 \\ 89 & 117 & 107 \\ 63 & 46 & 46 \end{bmatrix}$

Mengkonversikan hasil perkalian kunci ke dalam karakter yang bersesuaian pada Tabel 2.2, maka:

$$P = \begin{bmatrix} 77 & 97 & 98 \\ 97 & 114 & 32 \\ 89 & 117 & 107 \\ 63 & 46 & 46 \end{bmatrix} = \begin{bmatrix} M & a & b \\ a & r & space \\ Y & u & k \\ ? & . & . \end{bmatrix}$$

Sehingga diperoleh *plaintext* dari hasil dekripsi yaitu **Mabar Yuk?**

4.3.2 Enkripsi dan Dekripsi Pesan dengan Matriks Kunci 4 × 4

$P_1 = (M \quad a \quad b \quad a) = (77 \quad 97 \quad 98 \quad 97)$
$P_2 = (r \quad space \quad Y \quad u) = (114 \quad 32 \quad 89 \quad 117)$
$P_3 = (k \quad ? \quad . \quad .) = (107 \quad 63 \quad 46 \quad 46)$

Diperoleh matriks $P = \begin{bmatrix} 77 & 97 & 98 & 97 \\ 114 & 32 & 89 & 117 \\ 107 & 63 & 46 & 46 \end{bmatrix}$

Tabel 4.5 Perkalian *Plaintext* dengan Matriks Kunci **4 × 4**

Konversi Huruf ke Angka	Matriks Kunci	Hasil Perkalian Matriks Kunci
$\begin{bmatrix} 77 & 97 & 98 & 97 \\ 114 & 32 & 89 & 117 \\ 107 & 63 & 46 & 46 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 3 & 2 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 77 & 174 & 349 & 620 \\ 114 & 146 & 349 & 612 \\ 107 & 170 & 323 & 539 \end{bmatrix}$

Diperoleh *ciphertext* dari hasil konversi yaitu **mo'r3s'j,kf'**

Membagi *ciphertext* menjadi blok-blok yang berisi 4 huruf dan mengkonversikannya ke dalam bilangan ASCII yang bersesuaian pada Tabel 2.2 sehingga diperoleh:

$C_1 = (m \quad o \quad ' \quad R) = (109 \quad 111 \quad 96 \quad 82)$
$C_2 = (3 \quad S \quad ' \quad J) = (51 \quad 83 \quad 96 \quad 74)$
$C_3 = (, \quad k \quad F \quad ') = (44 \quad 107 \quad 70 \quad 96)$

Maka diperoleh matriks $C = \begin{bmatrix} 109 & 111 & 96 & 82 \\ 51 & 83 & 96 & 74 \\ 44 & 107 & 70 & 96 \end{bmatrix}$

Kemudian akan dicari invers dari matriks kunci sebagai berikut.

$$kof(K) = \left((-1)^{i+j} M_{ij}\right) = \begin{pmatrix} 1 & -1 & -1 & 0 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$adj(K) = \left(kof(K)\right)^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & -1 & 1 & 0 \\ 0 & -1 & -1 & 1 \end{pmatrix}$$

Jadi invers dari matriks kunci adalah

$$K^{-1} = \frac{1}{detK} adj(K) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & -1 & 1 & 0 \\ 0 & -1 & -1 & 1 \end{pmatrix}$$

Tabel 4.6 Perkalian *Plaintext* dengan Matriks Kunci **4 × 4**

Matriks *Ciphertext*	Kunci	Hasil Perkalian Matriks Kunci
$\begin{bmatrix} 77 & 174 & 349 & 620 \\ 114 & 146 & 349 & 612 \\ 107 & 170 & 323 & 539 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & -1 & 1 & 0 \\ 0 & -1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 77 & 97 & 98 & 97 \\ 114 & 32 & 89 & 117 \\ 107 & 63 & 46 & 46 \end{bmatrix}$

Mengkonversikan hasil perkalian kunci ke dalam karakter yang bersesuaian pada Tabel 2.2, maka:

$$P = \begin{bmatrix} 77 & 97 & 98 & 97 \\ 114 & 32 & 89 & 117 \\ 107 & 63 & 46 & 46 \end{bmatrix} = \begin{bmatrix} M & a & b & a \\ r & space & Y & u \\ k & ? & . & . \end{bmatrix}$$

Sehingga diperoleh *plaintext* dari hasil dekripsi yaitu **Mabar Yuk?**

4.3.3 Enkripsi dan Dekripsi Pesan dengan Matriks Kunci 5 × 5

$P_1 = (M \quad a \quad b \quad a \quad r) = (77 \quad 97 \quad 98 \quad 97 \quad 114)$
$P_2 = (space \quad Y \quad u \quad k \quad ?) =$
$(32 \quad 89 \quad 117 \quad 107 \quad 63)$

Diperoleh matriks $P = \begin{bmatrix} 77 & 97 & 98 & 97 & 114 \\ 32 & 89 & 117 & 107 & 63 \end{bmatrix}$

Tabel 4.7 Perkalian *Plaintext* dengan Matriks Kunci **5 × 5**

Konversi Huruf ke Angka	Matriks Kunci	Hasil Perkalian Matriks Kunci
$\begin{bmatrix} 77 & 97 & 98 & 97 & 114 \\ 32 & 89 & 117 & 107 & 63 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 2 & 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 1 & 0 \\ 5 & 3 & 2 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 77 & 174 & 349 & 620 & 1083 \\ 32 & 121 & 270 & 498 & 831 \end{bmatrix}$

$$C = \begin{bmatrix} 109_0 & 111_1 & 96_3 & 82_6 & 70_{11} \\ 64_0 & 58_1 & 112_2 & 55_5 & 103_8 \end{bmatrix}$$

Mengonversikan matriks C ke dalam karakter yang bersesuaian pada Tabel 2.2, maka:

$$C = \begin{bmatrix} 109_0 & 111_1 & 96_3 & 82_6 & 70_{11} \\ 64_0 & 58_1 & 112_2 & 55_5 & 103_8 \end{bmatrix} = \begin{bmatrix} m & o & ' & R & F \\ @ & : & p & 7 & g \end{bmatrix}$$

Sehungga diperoleh *ciphertext* dari hasil konversi yaitu **mo'RF@:p7g**

Membagi *ciphertext* menjadi blok-blok yang berisi 3 huruf dan mengkonversikannya ke dalam bilangan ASCII yang bersesuaian pada Tabel 2.2 sehingga diperoleh:

$C_1 = (m \quad o \quad ' \quad R \quad F) = (109 \quad 111 \quad 96 \quad 82 \quad 70)$
$C_2 = (@ \quad : \quad p \quad 7 \quad g) = (64 \quad 58 \quad 112 \quad 55 \quad 103)$

Maka diperoleh matriks

$$C = \begin{bmatrix} 109 & 111 & 96 & 82 & 70 \\ 64 & 58 & 112 & 55 & 103 \end{bmatrix}$$

Kemudian akan dicari invers dari matriks kunci sebagai berikut.

$$kof(K) = \left((-1)^{i+j} M_{ij}\right) = \begin{pmatrix} 1 & -1 & -1 & 0 & 0 \\ 0 & 1 & -1 & -1 & 0 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$adj(K) = \left(kof(K)\right)^T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ -1 & -1 & 1 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & -1 & -1 & 1 \end{pmatrix}$$

Jadi invers dari matriks kunci adalah

$$K^{-1} = \frac{1}{detK} adj(K) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ -1 & -1 & 1 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & -1 & -1 & 1 \end{pmatrix}$$

Tabel 4.8 Perkalian *Plaintext* dengan Matriks Kunci $\mathbf{5 \times 5}$

Matriks *Ciphertext*	Kunci	Hasil Perkalian Matriks Kunci
$\begin{bmatrix} 77 & 174 & 349 & 620 & 1083 \\ 32 & 121 & 270 & 498 & 831 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ -1 & -1 & 1 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & -1 & -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 77 & 97 & 98 & 97 & 114 \\ 32 & 89 & 117 & 107 & 63 \end{bmatrix}$

Mengkonversikan hasil perkalian kunci ke dalam karakter yang bersesuaian pada Tabel 2.2, maka:

$$P = \begin{bmatrix} 77 & 97 & 98 & 97 & 114 \\ 32 & 89 & 117 & 107 & 63 \end{bmatrix} = \begin{bmatrix} M & a & b & a & r \\ space & Y & u & k & ? \end{bmatrix}$$

Sehingga diperoleh *plaintext* dari hasil dekripsi yaitu **Mabar Yuk?**

4.4 Nilai *Entropy*

4.4.1 Nilai *Entropy* dengan Matriks Kunci Ordo 3×3

Chipertext yang diperoleh dari proses enkripsi dengan menggunakan matriks kunci ordo 3×3 adalah **mo'"5Wy06_8<**.

Tabel 4.9 Probabilitas *Ciphertext* dengan Matriks Kunci $\mathbf{3 \times 3}$

Ciphertext	Frekuensi	Probabilitas $(P) = \frac{frekuensi}{Jumlah\ Karakter}$
m	1	0,08333
o	1	0,08333
'	1	0,08333
"	1	0,08333
5	1	0,08333
W	1	0,08333
y	1	0,08333
0	1	0,08333
6	1	0,08333
_	1	0,08333
<	1	0,08333
Jumlah	**12**	**1**

Kemudian akan dihitung nilai *entropy* menggunakan Persamaan (2.13), maka:

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i)$$
$$= -[-0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987] = 3{,}5844$$

Jadi, nilai *entropy* dari *ciphertext* adalah 3,5844

4.4.2 Nilai *Entropy* dengan Matriks Kunci Ordo 4×4

Chipertext yang diperoleh dari proses enkripsi dengan menggunakan matriks kunci ordo 4×4 adalah **mo'R3S'J,kF'.**

Tabel 4.10 Probabilitas *Ciphertext* dengan Matriks Kunci $\mathbf{4 \times 4}$

Ciphertext	Frekuensi	Probabilitas $(P) = \frac{frekuensi}{Jumlah\ Karakter}$
m	1	0,08333
o	1	0,08333
'	3	0,25
R	1	0,08333
3	1	0,08333
S	1	0,08333
J	1	0,08333
,	1	0,08333
k	1	0,08333
F	1	0,08333
Jumlah	**12**	**1**

Kemudian akan dihitung nilai *entropy* menggunakan Persamaan (2.13), maka: $H(X) = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i)$

$$= -[-0{,}2987 - 0{,}2987 - 0{,}5 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987 - 0{,}2987] = 3{,}7857$$

Jadi, nilai *entropy* dari *ciphertext* adalah 3,7857

4.4.3 Nilai *Entropy* dengan Matriks Kunci Ordo 5×5

Chipertext yang diperoleh dari proses enkripsi dengan menggunakan matriks kunci ordo 5×5 adalah **mo'RF@:p7g**.

Tabel 4.11 Probabilitas *Ciphertext* dengan Matriks Kunci $\mathbf{5 \times 5}$

Ciphertext	Frekuensi	Probabilitas $(P) = \frac{frekuensi}{Jumlah\ Karakter}$
m	1	0,1
o	1	0,1
'	1	0,1
R	1	0,1
F	1	0,1
@	1	0,1
:	1	0,1
p	1	0,1
7	1	0,1
g	1	0,1
Jumlah	**10**	**1**

Kemudian akan dihitung nilai *entropy* menggunakan Persamaan (2.13), maka:

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i)$$

$$= -[-0{,}3321 - 0{,}3321 - 0{,}3321 - 0{,}3321 - 0{,}3321 - 0{,}3321 - 0{,}3321 - 0{,}3321 - 0{,}3321 - 0{,}3321] = 3{,}321$$

Jadi, nilai *entropy* dari *ciphertext* adalah 3,321

4.5 Korelasi *Pearson*

4.5.1 Data Matriks Ordo 3×3

Tabel 4.12 Data Matriks Ordo $\mathbf{3 \times 3}$

No	Nilai ASCII *Plaintext* (x)	Nilai ASCII *Ciphertext* (y)	x^2	y^2	xy
1	77	109	5929	11881	8393
2	97	111	9409	12321	10767
3	98	96	9604	9216	9408
4	97	34	9409	1156	3298
5	114	53	12996	2809	6042
6	32	87	1024	7569	2784
7	89	121	7921	14641	10769
8	117	48	13689	2304	5616
9	107	54	11449	2916	5778
10	63	95	3969	9025	5985
11	46	56	2116	3136	2576
12	46	60	2116	3600	2760
Jumlah	983	924	89631	80574	74176

Dengan menggunakan Persamaan 2.14, diperoleh nilai koefisien korelasi sebagai berikut:

$$r = \frac{n\sum xy - \sum x \sum y}{\sqrt{n\sum x^2 - (\sum x)^2}.\sqrt{n\sum y^2 - (\sum y)^2}}$$

$$= \frac{12(74176) - (983)(924)}{\sqrt{12(89631) - (983)^2}\sqrt{12(80574) - (924)^2}}$$

$$= -0{,}164$$

Berdasarkan Tabel 2.3, oleh karena nilai $-0{,}164$ berada pada interval koefisien $0{,}00 - 0{,}20$, maka *plaintext* dan *ciphertext* memiliki korelasi dengan derajat hubungan yaitu korelasi sangat lemah dengan bentuk hubungannya yaitu negatif.

4.5.2 Data Matriks Ordo 4×4

Tabel 4.12 Data Matriks Ordo 4×4

No	Nilai ASCII *Plaintext* (x)	Nilai ASCII *Ciphertext* (y)	x^2	y^2	xy
1	77	109	5929	11881	8393
2	97	111	9409	12321	10767
3	98	96	9604	9216	9408
4	97	82	9409	6724	7954
5	114	51	12996	2601	5814
6	32	83	1024	6889	2656
7	89	96	7921	9216	8544
8	117	74	13689	5476	8658
9	107	44	11449	1936	4708
10	63	107	3969	11449	6741
11	46	70	2116	4900	3220
12	46	96	2116	9216	4416
Jumlah	983	1019	89631	91825	81279

Berdasarkan Tabel 2.3, oleh karena nilai $-0{,}316$ berada pada interval koefisien $0{,}21 - 0{,}40$, maka *plaintext* dan *ciphertext* memiliki korelasi dengan derajat hubungan yaitu korelasi lemah dengan bentuk hubungannya yaitu negatif.

4.5.3 Data Matriks Ordo 5×5

Tabel 4.13 Data Matriks Ordo $\mathbf{5 \times 5}$

No	Nilai ASCII *Plaintext* (x)	Nilai ASCII *Ciphertext* (y)	x^2	y^2	xy
1	77	109	5929	11881	8393
2	97	111	9409	12321	10767
3	98	96	9604	9216	9408
4	97	82	9409	6724	7954
5	114	70	12996	4900	7980
6	32	64	1024	4096	2048
7	89	58	7921	3364	5162
8	117	112	13689	12544	13104
9	107	55	11449	3025	5885
10	63	103	3969	10609	6489

Berdasarkan Tabel 2.3, oleh karena nilai 0,106 berada pada interval koefisien $0{,}00 - 0{,}20$, maka *plaintext* dan *ciphertext* memiliki korelasi dengan derajat hubungan yaitu korelasi sangat lemah dengan bentuk hubungannya yaitu positif.

Tabel 4.14 Nilai Koefisien Korelasi

Ordo Matriks Kunci	Nilai Korelasi	Tingkat Hubungan
Kunci 3×3	$-0{,}164$	Sangat lemah
Kunci 4×4	$-0{,}316$	Lemah
Kunci 5×5	0,106	Sangat Lemah

5. Penutup

5.1 Kesimpulan

Berdasarkan hasil penelitian dapat disusun kesimpulan sebagai berikut:

1. Implementasi matriks Fibonacci dapat digunakan dalam proses pengamanan (enkripsi) dan membaca pesan (dekripsi) dalam Kriptografi *Hill Cipher*. Dalam proses enkripsi dilakukan dengan mengkonversi pesan atau *plaintext* ke dalam bilangan ASCII kemudian dikalikan dengan matriks kunci, hasilnya dimodulokan dengan 95 dan agar hasil modulo masih tetap berada dalam lingkup karakter tabel ASCII maka ditambahkan 32. Dalam proses dekripsi pesan yang telah di enkripsi memiliki proses yang hampir sama yaitu mengkonversi *ciphertext* ke dalam bilangan ASCII kemudian dikalikan dengan matriks kunci kemudian dikurangi 32 dan dijumlahkan dengan kelipatan 95.
2. Dengan menggunakan matriks Fibonacci sebagai kunci dalam algoritma *Hill Cipher*, dapat meningkatkan keamanan sistem kriptografi. Kombinasi antara konsep matriks Fibonacci dan *Hill Cipher* memungkinkan penggunaan kunci yang dinamis dan sulit dipecahkan, sehingga pesan yang dikirimkan dapat lebih aman dari serangan kriptanalisis. Hal itu dapat diliat pada hasil analisis nilai entrophy, semakin besar ordo matriks kunci dan semakin panjang Plaintext nilai entrophy yang diperoleh semakin baik atau cenderung naik. Serta berdasarkan analisis korelasi person semakin besar ordo matriks kunci diperoleh kecenderungan atau hubungan antara *plaintext* dan *ciphertext* semakin lemah yang menandakan bahwah hasil enkripsi semakin baik. Ini menunjukkan potensi pengembangan dan penerapan metode kriptografi yang lebih kuat dengan memanfaatkan konsep matematika seperti matriks Fibonacci.

5.2 Saran

Adapun rekomendasi untuk penelitian kedepan yaitu:

1. Menggunakan algoritma lain atau menggabungkan dua algoritma untuk melakukan proses enkripsi dan dekripsi pesan.
2. Mengenkripsi dan deskripsi file/dokumen menggunakan algoritma kriptografi.

Ucapan Terima Kasih: Penelitian ini dapat dilaksanakan dengan lancer berkat bantuan dan dukungan dari berbagai pihak, untuk itu peneliti mengucapkan terima kasih kepada Civitas Akademika Universitas Halu Oleo, Dosen Pembimbing, Tim Penguji dan pihak-pihak lain yang telah memfasilitasi dan membantu berjalannya penelitian ini.

Daftar Pustaka

[1] M. Abomhara dan G. M. Køien. 2015. "*Cyber Security and the Internet of Things : Vulnerabilities , Threats , Intruders.*" Journal Of Cyber Security, Volume 4: 65–88.

[2] H. Anton dan C. Rorres. 2004. *Elementary Linear Algebra. American College of Radiology Network*. Volume 9.

[3] N. Buulolo dan A. Sindar. 2020. "Analisis Dan Perancangan Keamanan Data Teks Menggunakan Algoritma Kriptografi DES (Data Encryption Standard)." *Respati* 15 (3): 61.

[4] D. Craigen, N. Diakun-Thibault, R. Purse. 2014. "Defining Cybersecurity." Technology Innovation Management Review 4 (10): 13–21.

[5] H. Fitroti, M. U. Romdhini, N. W. Switrayni. 2021. "*Hill Cipher Algorithm with Generalized Fibonacci Matrix in Message Encoding.*" Eigen Mathematics Journal 4 (2): 51–59.

[6] M. T. Gençoğlu. 2019. "*Importance of Cryptography in Information Security.*" ISOR Journal of Computer Engineering 21 (1): 65–68.

[7] B. S. Hasugian. 2017. "Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah." *Jurnal Warta* : 1–19.

[8] A. Hidayat dan T. Alawiyah. 2013. "Enkripsi Dan Dekripsi Teks Menggunakan Algoritma Hill Cipher Dengan Kunci Matriks Persegi Panjang." *Jurnal Matematika Integratif* 9 (1): 39–51.

[9] G. K. Ijemaru, I. Adeyanju, K. Olusuyi, T. J. Ofusori. 2018. "*Security Challenges of Wireless Communications Networks : A Survey.*" International Journal of Applied Engineering Research. Volume 13: 5680–92.

[10] M. Irwan. 2017. "Pengantar Matlab Untuk Sistem Persamaan Linear." *Jurnal MSA* (*Matematika Dan Statistika Serta Aplikasinya*) 5 (2): 48–48.

[11] R. Jehanshah. 2017. "Bentuk Matriks Untuk Bilangan Fibonacci." *FMIPA Universitas Sumatera Utara* I: 1–42.

[12] J. M. Kizza. 2020. *Guide to Computer Network Security*.

[13] G. Lee, J. Kim, dan S.-G. Lee. 2002. "*Factorizations And Eigenvalues Of Fibonacci And Symmetric Fibonacci Matrices*" Volume 3: 203–11.

[14] A. M. Meinke. 2011. "*Fibonacci Numbers And Associated Matrices*." *Kent State* 1 (8): 1–49.

[15] R. Munir. 2010. "Matematika Disktrit." *Informatika Bandung*, 281–308.

[16] D. Ratnasari dan H. P. Sejati. 2012. "Algoritma Enkripsi Citra Digital Dengan Kombinasi Dua Chaos." *Nasional Aplikasi Teknologi Informasi* 1 (Juni): 1–6.

[17] N. P. Puspita dan N. Bahtiar. 2010. "Kriptografi

Hill Cipher Dengan Menggunakan Operasi Matriks,". *Matematika UNDIP*. Volume 1(1) : 1-5.

[18] A. N. Rahma, R. Rahmawati, S. M. Jauza. 2020. "Determinan Matriks Centrosymmetric Bentuk Khusus Ordo Berpangkat Bilangan Bulat Positif Dengan Kofaktor." *Jurnal Sains Matematika Dan Statistika* 6 (7): 30–41.

[19] D. Ratnasari dan H. P. Sejati. 2017. "Enkripsi Citra Digital Menggunakan Kombinasi Algoritme Hill Cipher Dan Chaos Map Dengan Penerapan Teknik Selektif Pada Bit Msb." *Jurnal Teknologi Technoscientia* 10 (1): 109–17.

[20] Rojali. 2011. "Studi Dan Implementasi Hill Cipher Menggunakan Binomial Newton." *Matematika Dan Pendidikan Karakter Dalam Pembelajaran* 22: 1–7.

[21] Ruminta. 2009. Matriks Persamaan Linier Dan Pemograman Linier. *Rekayasa Sains Bandung*.

[22] W. R. Safitri. 2016. "Analisis Korelasi Dalam Menentukan Hubungan Antara Kejadian Demam Berdarah Dengue Dengan Kepadatan Penduduk Di Kota Surabaya Pada Tahun 2012 - 2014." *Jurnal Kesehatan Masyarakat* 1 (3): 1–9.

[23] W. Stallings. 2017. *Cryptography and Network Secuirty*. England : Pearson Education Limited

[24] Sugiyono. 2016. "Memahami Penelitian Kualitatif," 1–23. Bandung: Alfabeta.

[25] Supiyanto. 2015. "Implementasi Hill Cipher Pada Citra Menggunakan Koefisien Binomial." *Seminar Nasional Informatika* 2015 (November): 284–91.

[26] Y. Zou, J. Zhu, X. Wang, L. Hanzo. 2016. "*A Survey on Wireless Security : Technical Challenges , Recent Advances , and Future Trends.*" Proceedings of the IEEE 104 (9): 1727–65.

Diterima tgl. 19 September 2024
Direvisi tgl. 7 Desember 2024
Disetujui untuk terbit tgl. 15 Desember 2024