e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3746

Kombinasi dan Modifikasi Vigenere Cipher dan Hill Cipher Menggunakan Metode Hybrid Kode Pos, Trigonometri, dan Konversi Suhu Sebagai Pengamanan Pesan

Celine Aloyshima Haris [1)], Dony Ariyus [2)]
Magister Teknik Informatika, Universitas AMIKOM Yogyakarta
Jalan Ring Road Utara, Condong Catur, Depok, Sleman, Daerah Istimewa Yogyakarta
E-Mail : celine.haris@students.amikom.ac.id [1)]; dony.a@amikom.ac.id [2)]

ABSTRAK

Seiring perkembangan teknologi yang lebih modern, internet dan jaringan komunikasi juga berkembang pesat. Dalam berkomunikasi kita saling bertukar pesan. Tetapi pesan tersebut harus bisa terjaga kerahasiaan dan keamanan datanya hingga sampai ke penerima pesan. Untuk menjaga pesan tersebut dapat terkirim dengan aman adalah menggunakan teknik kriptografi sebagai pengamanan pesan. Salah satu teknik kriptografi yang digunakan adalah kriptografi klasik dengan menggunakan kombinasi dan modifikasi *vigenere cipher* dan *hill cipher* untuk menyulitkan kriptanalis untuk memecahkan pesan asli. Semakin banyak proses yang diperlukan dan semakin panjang waktu yang dibutuhkan untuk memecahkan pesan yang telah di enkripsi tersebut artinya semakin aman digunakan untuk merahasiakan pesan. Agar semakin sulit memecahkannya maka menggunakan metode hybrid antara kode pos, trigonometri, dan konversi suhu yang diimplementasikan dalam bahasa pemrograman Java.

Kata Kunci – Kriptografi, Pesan, Vigenere Cipher, Hill Cipher, Kode Pos, Trigonometri, Konversi Suhu, Java

1. PENDAHULUAN

Zaman dahulu manusia saling berkomunikasi dengan pertukaran pesan secara tradisional. Seiring perkembangan kemajuan zaman, manusia berkomunikasi menggukan media digital. Penggunaan media digital ini mulai marak digunakan masyarakat pada era Revolusi Industri 4.0 yang mengintegraskan teknologi *cyber* dan teknologi otomatisasi.Hal tersebut juga memberikan dampak kepada keamanan informasi saat pertukaran pesan. Kerahasian dari pesan tersebut harus benar-benar terjaga jangan sampai ada pihak yang menyalahgunakannya. Maka dari itu perlunya upaya untuk mengamankan informasi tersebut, salah satunya dengan memanfaatkan bidang ilmu kriptografi. Kriptografi merupakan cara menyembunyikan pesan dan bagaimana agar orang lain tidak mengetahui isi pesan tersebut (Ariyus, 2008).

Terdapat 2 jenis algoritma dalam kriptografi, yaitu algoritma kriptografi klasik dan modern. Agloritma kriptografi klasik ini adalah yang melatarbelakangi terbentuknya berbagai macam algoritma kriptografi modern. Contoh dari algoritma kriptografi klasik seperti *Caesar Cipher*, *Vigenere Cipher*, *Hill Cipher*, dan *Playfair Cipher*. Sedangkan contoh dari algoritma kriptografi modern seperti MD5, RC4, AES, ElGamal, dan lain sebagainya.

Terdapat beberapa penelitian sebelumnya yang menggunakan kriptografi klasik diantaranya penelitian (U.W.M, Susanto, Rachmawanto, & Setiadi, 2018) yang mengkombinasikan *shift cipher* dan *vigenere cipher*. Penelitian (Hasugian, 2013) yang yang mengimplementasikan algoritma *hill cipher*. Penelitian (Yunita, Hasan, & Ariyus, 2019) yang memodifikasi algoritma *hill cipher* dan *twofish* menggunakan kode wilayah telepon.

Berdasarkan pemaparan diatas, maka kriptografi tidak hanya menyembunyikan pesan, tetapi juga pemecahan masalah dalam keamanan informasi. Maka dari ini tujuan penelitian ini adalah memodifikasi algoritma untuk menyulitkan pemecahan pesan guna mengamankan pesan dengan vigener cipher dan hill cipher menggunakan metode hybrid kode pos, trigonometri, dan konversi suhu

2. TINJAUAN PUSAKA

A. Kriptografi

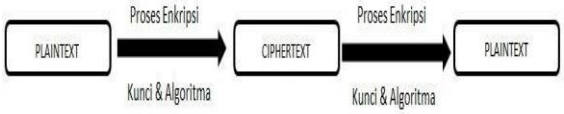
Kriptografi berasal dari bahasa Yunani yang terdiri dalam 2 kata, yaitu "*krytos*" dam "*qraphia*. Arti "*kryptos*" adalah sesuatu yang disembunyikan, tidak dikenal, rahasia, dan misterius. Sedangkan arti "*qrphia*" adalah tulisan. Jadi kriptografi adalah tulisan yang disembunyikan atau tulisan rahasia.

Terdapat beberapa komponen dalam kriptografi (Ariyus, 2008) seperti seperti enkripsi, dekripsi, kunci, ciphertext, plaintext, pesan, dan kriptanalis. Enkripsi merupakan cara untuk merahasiakan dan mengamankan data dengan mengubah teks biasa ke bentuk teks kode dengan menggunakan algoritma yang dapat mengkodekan. Dekripsi merupakan kebalikan dari enkripsi, cara untuk mengembalikan pesan yang telah dienkripsi menjadi bentuk asalnya. Kunci dipergunakan untuk memecahkan enkripsi dan dekripsi, terdapat kunci rahasia dan kunci umum. *Ciphertext* merupakan pesan yang telah melalui proses enkripsi, dan teks tersebut tidak memiliki makna. *Plaintext* merupakan pesan asli yang memiliki makna, pesan asli inilah yang proses menggunakan algoritma kriptografi untuk diproses menjadi *ciphertext*. Pesan merupakan data atau informasi yang ada dalam proses berkomunikasi. Kriptanalis adalah ilmu untuk menganalisis kode, dengan berusaha mendapatkan pesan asli tanpa harus diketahui kuncinya.

Dalam kriptografi mengubah pesan asli yaitu *plaintext* menjadi pesan berkode yaitu *ciphertext*

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3746

menggunakan kunci dan algoritma untuk proses enkripsi dan dekripsinya, seperti pada Gambar 1.



Gambar 1. Alur Kriptografi

Dalam algoritma kriptografi juga terdiri dari 2 jenis, yaitu kriptografi klasik dan modern. Dalam kriptografi klasik biasanya menggunakan teknik subtitusi dan transposisi atau permutasi. Dalam kriptografi modern memerlukan komputerisasi, dan dikelompokkna berdasarkan jenis kuncinya menjadi algoritma simetris dan asimetris. Dengan mengetahui perkembangannya maka kita dapat menentukan kelebihan dan kekurangan dari algoritma kriptografi, sehingga dapat memilih yang benar-benar efektif dan efisien untuk menjaga keamanan pesan atau informasi yang kita miliki.

B. Vigenere Cipher

Vigenere cipher merupakan algoritma untuk mengenkripsi abjad teks dengan subtitusi *polyalphabeti* (Bhardwaj, 2012) .*Vigenere cipher* ini merupakan salah satu dari jenis kriptografi klasik yang sudah diperkenalkan pada sekitar tahun 1986. Algoritma ini dipublikasi oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis yang bernama Blaise de Vigenere. *Vigenere cipher* ini mirip dengan *Caesar cipher*, dengan mengenkripsi *plaintext* pada pesan dengan cara menggeser huruf dalam pesan sejauh nilai kunci pada deret alphabet. Subtitusi polyalphabetik atau subtitusi abjad-majemuk mengenkripsi setiap huruf yang ada dengan menggunakan kunci yang berbeda (Nadhori et al., 2010).Jika panjang kunci yang digunakan lebih pendek dari panjang *plainteks* maka kunci akan diulang sampai panjang kunci sama dengan panjang plainteks. Algoritma *Vigenere cipher* dikenal sangat mudah dipahami dan diimplementasikan, dengan menggunakan tabel bujur sangkar seperti pada Gambar 2. Kolom paling kiri merupakan kumpulan huruf untuk kunci dan bagian atas baris adalah huruf untuk*plaintext.*

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 2. Tabula *Recta Vigenere Cipher*

C. Hill Cipher

Hill cipher termasuk jenis kriptografi klasik yang diciptakan oleh Lester S. Hill pada tahun 1929. Algoritma Hill cipher ini mengganti setiap abjad *plainteks*nya ke dalam bentuk angka numerik yang berkorespondensi dengan 0 sampai 25 (Danny Wowor, 2013). Dalam penerapannya algoritma ini yang menggunakan persamaan aritmatika modulo terhadap matriks, dengan perkalian dan teknik *invers* terhadap matriks. Kuncinya menggunakan matriks n x n dengan n merupakan ukuran blok. *Plainteks* terlebih dahulu dirubah kedalam bentuk angka seperti blok pada Gambar 3 dibawah ini.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 3.*Hill Cipher*

Perhitungan untuk proses enkripsi algoritma *hill cipher* ini menggunakan persamaan (1).

Ciphertext = Matriks Kunci * Matriks *Plaintext*
Modulo 26 .....(1)

Perhitungan untuk proses dekripsi algoritma *hill cipher* ini menggunakan persamaan (2), (3), (4), dan (5).

Plaintext = Matriks Kunci^{-1} * Matriks *Ciphertext*
Modulo 26 .....(2)

$$Adjoin\ K \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \quad \text{.....(3)}$$

Det K = (a x d) – (b x c) .....(4)
|K| = Det K x n Mod 26 = 1 .....(5)

Dimana :
K : matriks kunci ,
n : nilai yang memenuhi agar hasil = 1

D. Kode Pos

Kode Pos terdiri dari serangkaian angka ynag memudahkan pengiriman paket ke wilayah yang dituju. Penomoran kode pos Indonesia terdapat 5 *digit* angka, *digit* pertama menunjukkan wilayah provinsi, *digit* kedua dan ketiga menunjukkan kota atau kabupaten, *digit* keempat menunjukkan kecamatan, dan *digit* kelima menunjukkan kelurahan atau desa (Wahyuningsih & Suryanto, 2015).

E. Trigonometri

Trigonometri berasal dari bahasa Yunani yaitu "*trigonon*" yang artinya tiga sudut dan "*metro*" artinya mengukur. Trigonometri merupakan salah satu cabang ilmu dalam matematika yang berkaitan dengan sudut segitiga yaitu sinus, cosinus, dan tangen. Menurut modul yang dikeluarkan (Direktorat Jenderal PAUD dan Pendidikan Masyarakat, 2017) terdapat persamaan fungsi sinus dan cosinus serta fungsi *invers* sinus dan cosinus (6), (7), (8), dan (9).

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3746

Jika Y = Sin X .....(6)
Maka fungsi *invers* dari sinus
X = Arc Sin Y .....(7)

Jika Y = Cos X .....(8)
Maka fungsi *invers* dari cosinus
X = Arc Cos Y .....(9)

Dimana :
Y : nilai yang dicari atau nilai *plaintext* dan *ciphertext* yang akan digunakan,
X : nilai sudut atau nilai *plaintext* dan *ciphertext* yang akan digunakan.

F. Konversi Suhu

Dalam pengukuran suhu untuk memberikan hasil akurat menggunakan termometer. Dalam suhu terdapat 4 skala yaitu, Celcius, Reamur, Fahrenheit, dan Kelvin (Mundilarto & Istiyono, 2007). Masing-masing skala suhu memiliki titik tetap bawah, titik tetap atas, selang, dan perbandingan dapat dilihat pada Tabel 1.

Tabel 1. Skala Suhu

Skala	Titik Tetap Bawah	Titik Tetap Atas	Selang	Perbandingan
Celcius	0º	100º	100º	5
Reamur	0º	80º	80º	4
Fahrenheit	32º	212º	180º	9
Kelvin	273º	373	100	5

Perubahan suhu atau konversi dari skala celcius ke skala reamur, fahrenheit, dan kelvin dapat dilakukan dengan persamaan (10), (11), dan (12) untuk proses enkripsi. Persamaan (13), (14), dan (15) untuk perubahan suhu atau konversi dari skala reamur, fahrenheit, dan kelvin ke skala celcius untuk proses dekripsi.

$$\text{Celcius ke Reamur} = \frac{4}{5} \times P \quad \text{.....(10)}$$

$$\text{Celcius ke Fahrenheit} = \left(\frac{9}{5} \times P\right) + 32 \quad \text{.....(11)}$$

$$\text{Celcius ke Kelvin} = \left(\frac{5}{5} \times P\right) + 273 \quad \text{.....(12)}$$

$$\text{Reamur ke Celcius} = \frac{5}{4} \times C \quad \text{.....(13)}$$

$$\text{Fahrenheit ke Celcius} = \frac{5}{9} \times (C - 32) \quad \text{.....(14)}$$

$$\text{Kelvin ke Celcius} = \frac{5}{5} \times (C - 273) \quad \text{.....(15)}$$

Dimana :
P : *plaintext*,
C : *ciphertext.*

G. Java

Menurut (Nofriadi, 2015) bahasa pemrograman java pertama kali dibuat oleh James Gosling saat masih bergabung dalam *Sun Microsystems*. Bahasa pemrograman ini merupakan pengembangan dari bahasa pemrograman yang paling populer digunakan dan secara luas dimanfaatkan dalam pengembangan berbagai jenis perangkat lunak aplikasi maupun aplikasi berbasis *web*.

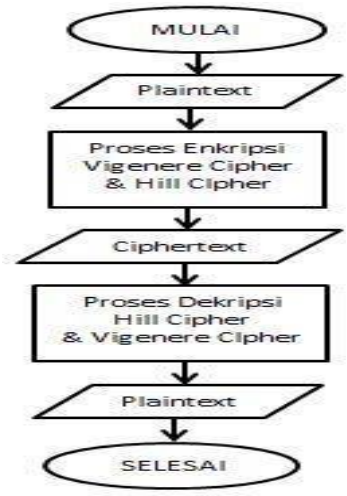
Kelebihan pemgoraman java ini yaitu dapat dijalankan diberbagai sistem operasi sehingga juga merupakan bahasa pemrograman *multiplatform*, bersifat Pemrograman Berorientasi Objek (PBO), serta memiliki *library* yang lengkap. Java ini merupakan pemrograman objek murni karena semua programnya dibungkus dalam kelas (Sukamto & Shalahuddin, 2014).

Salah satu *tools* untuk menjalankan pemrograman java ini, menggunakan editor Netbeans. Netbeans merupakan sebuah aplikasi *Interated Development Environment* (IDE) yang berbasiskan java dari *Sun Microsystems* yang berjalan di atas *swing* dan banyak digunakan sebagai editor berbagai bahasa pemrograman.

3. METODE PENELITIAN

A. Alur Penelitian

Alur dalam penelitian ini seperti pada Gambar 4 dimana pertama kali dengan menginputkan *plaintext*, kemudian pemrosesan enkripsi dengan algoritma *Vigenere cipher* kemudian *Hill cipher* kemudian menghasilkan *ciphertext*. *Ciphertext* tersebut merupakan *plaintext* untuk porses dekripsi yang menggunakan kebalikan dari langkah algoritma yaitu dari *hill cipher* kemudian *vigenere cipher*, akhirnya menghasilkan *ciphertext* yang merupakan *plaintext* asli.

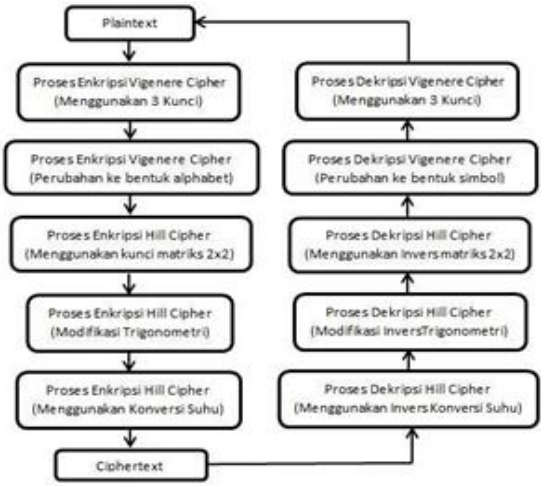


Gambar 4. Alur Penelitian

Untuk lebih memperjelas skema enkripsi dan dekripsi dapat dilihat pada Gambar 5. Untuk proses enkripsi *Vigenere cipher* menggunakan modifikasi 3 kunci, tabel *tabula recta* yang berisi simbol, dan perubahan dari simbol menjadi alphabet. Kemudian proses *Hill cipher* menggunakan modifikasi kunci matriks 2x2 yang menggunakan kunci berdasarkan kode pos, trigonometri sin dan cos, dan konversi

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3746

suhu celcius, reamur, fahrenheit, dan kelvin. Untuk proses dekripsi dimulai dari Hill cipher kemudian *Vigenere cipher*.

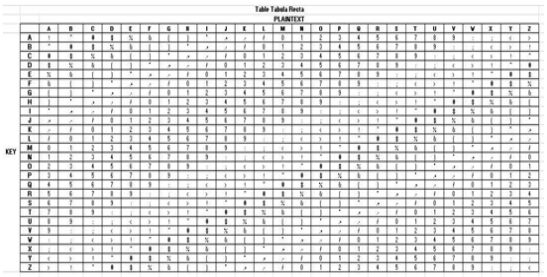


Gambar 5. Skema Enkripsi dan Dekripsi

B. Modifikasi *Vigenere Cipher*

a) Proses Enkripsi

Modifikasi langkah pertama dengan menggunakan tabel *tabula recta* yang berisi simbol, seperti Gambar 6 dibawah ini. Menggunakan 3 kunci, yaitu GEMBOK, EKBMOG, MBEKGO.



Gambar 6. Tabula *Recta*

Modifikasi langkah kedua dengan merubah hasil *plaintext* simbol tersebut menjadi *ciphertext* bentuk alphabet sesuai ketentuan pada Gambar 7 dibawah ini.

!	"	#	$	%	&	(	)	*	+	-	/	0
A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	:	;	<	>
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Gambar 7. Simbol Menjadi *Alphabet*

b) Proses Dekripsi

Proses dekripsi merupakan proses kebalikan dari proses enkripsi yang dimulai dari langkah kedua, yaitu merubah *plaintext* dari *alphabet* menjadi bentuk simbol, sesuai dengan Gambar 7. Kemudian ke langkah kesatu yaitu dari *plaintext* simbol menjadi *alphabet* menggunakan tabel *tabula recta* sesuai pada Gambar 6.

C. Modifikasi *Hill Cipher*

a) Proses Enkripsi

Modifikasi langkah pertama menggunakan Kunci kode pos wilayah Kalimantan, menggunakan 4 digit terakhir dan tidak menggunakan digit pertama karena digit pertama merupakan kode provinsi Kalimantan. Kunci kode pos yang digunakan seperti pada Tabel 2. Selanjutnya merubah *plaintext* menjadi nomor angka sesuai Gambar 8 dengan dimensi matriks 2x1 menggunakan persamaan (1).

Tabel 2. Kode Pos

Propinsi	Kode Pos
Kalimantan Timur	76116
Kalimantan Timur	75121
Kalimantan Timur	76131
Kalimantan Barat	79354
Kalimantan Barat	78716
Kalimantan Tengah	74312
Kalimantan Selatan	72115
Kalimantan Utara	77211

A	B	C	D	E	F	G	H	I	J	K	L	M
25	24	23	22	21	20	19	18	17	16	15	14	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
12	11	10	9	8	7	6	5	4	3	2	1	0

Gambar 8. *Alphabet* Menjadi Numerik

Modifikasi langkah kedua menggunakan trigonometri Sin dan Cos, menghasilkan bilangan desimal dengan 2 digit angka dibelakang koma dan ditambahkan pemisah S untuk Sin menggunakan persamaan (6) dan C untuk Cos menggunakan persamaan (8). Untuk Modifikasi langkah ketiga mengunakan konversi suhu. *Plaintext* dikali kan dengan 100 agar menjadi bilangan bulat.Konversi suhu yang digunakan sesuai dengan Persamaan (10), (11), dan (12), sehingga menghasilkan bilangan desimal dengan 2 digit angka dibelakang koma dan ditambahkan pemisah R untuk Reamur, F untuk Fahrenheit, dan K untuk Kelvin.

b) Proses Dekripsi

Proses dekripsi merupakan proses kebalikan dari proses enkripsi yang dimulai dari langkah ketiga dengan *invers* suhu dengan menggunakan persamaan (15), (16), dan (17) dari skala suhu Reamur, Fahrenheit, dan kelvin ke skala suhu Celsius, penulisan plaintext dengan menggunakan pemisah C untuk Celcius dan ditulis dalam bilangan desimal dengan 2 digit angka dibelakang koma. Langkah kedua yaitu dengan *invers* trigonometri ArcSin dan ArcCos, penulisan plaintext dengan menggunakan pemisah AS untuk ArcSin menggunakan persamaan (7) dan AC untuk ArcCos menggunakan persamaan (9), kemudian ditulis dalam bilangan bulat. Langkah selanjutnya yaitu ke langkah pertama di enkripsi yaitu dengan invers matriks sesuai dengan persamaan (2), (3), (4), dan (5) dengan menggunakan matriks kunci kode pos pada Tabel 2.

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3746

4. HASIL DAN PEMBAHASAN

A. Proses Perhitungan Enkripsi

Proses enkripsi dimulai dengan menggunakan algoritma vigenere cipher. Mengenkripsi plaintext JEBAK TIKUS KANTOR dengan menggunakan tabel tabula recta pada Gambar 6 dan menggunakan modifikasi 3 kunci yaitu GEMBOK, EKBMOG, MBEKGO. Sehingga menghasilkan ciphertext 3*1"<$089%<(>86".

Selanjutnya mengkonversi bentuk simbol dari plaintext 3*1"<$089%<(>86" menjadi bentuk alphabet menggunakan ketentuan dalam Gambar 7. Sehingga menghasilkan ciphertext PINBYDMUVEYGZUSB.

Proses enkripsi berikutnya menggunakan algoritma hill cipher sesuai Persamaan (1), dengan mengubah plaintext

PINBYDMUVEYGZUSB menjadi bentuk numerik sesuai Gambar 8, dan dibentuk menjadi matriks 2x1 pada Tabel 3.

Tabel 3. Matriks *Plaintext*

P	10	N	12	Y	1	M	13	V	4	Y	1	Z	0	S	7
I	17	B	24	D	22	U	5	E	21	G	19	U	5	B	24

Perhitungan matriks menggunakan matriks kunci dari Tabel 2. Diproses menggunakan Persamaan (1) dan seperti pada Tabel 4, menghasilkan *ciphertext* 258410202312712423155252112.

Tabel 4. Perhitungan Matriks *Hill Cipher*

No.	Proses
1.	$\begin{bmatrix}6 & 1\\ 1 & 6\end{bmatrix} * \begin{bmatrix}10\\ 17\end{bmatrix} = \begin{bmatrix}77\\ 12\end{bmatrix} Mod\, 26 = \begin{matrix}25\\ 8\end{matrix}$
…	…
8.	$\begin{bmatrix}7 & 1\\ 2 & 1\end{bmatrix} * \begin{bmatrix}7\\ 24\end{bmatrix} = \begin{bmatrix}73\\ 38\end{bmatrix} Mod\, 26 = \begin{matrix}21\\ 12\end{matrix}$

Perhitungan selanjutkan menggunakan Trigonometri sesuai dengan Persamaan (6) dan (8) ditunjukkan dalam Tabel 5, menghasilkan *ciphertext* 0.42S0.99C0.07S0.98C0.34S0.92C0.21S0.99C0.02S 0.91C0.39S0.97C0.09S0.91C0.36S0.98C.

Tabel 5. Perhitungan Trigonometri

No.	Proses
1.	Sin 25 = 0.42
2.	Cos 8 = 0.99
…	…
16.	Cos 12 = 0.98

Perhitungan berikutnya dengan menggunakan Konversi Suhu sesuai dengan Persamaan (10), (11), dan (12), tetapi terlebih dahulu *plaintext* 0.42S0.99C0.07S0.98C0.34S0.92C0.21S0.99C0.02S 0.91C0.39S0.97C0.09S0.91C0.36S0.98C dikalikan dengan 100, agar menjadi bilangan bulat maka menjadi 42997983492219929139979913698. Perhitungan konversi suhu dari Celcius menjadi Reamur, Fahrenheit, dan Kelvin ditunjukkan dalam Tabel 6 dibawah ini. Maka menghasilkan *ciphertext* 33.81R210.25F279.98K78.78R93.56F365.05K16.63 R210.66F274.25K73.08R102.33F369.59K6.97R195. 14F308.84K78.25R.

Tabel 6. Perhitungan Konversi Suhu

No.	Proses	
1.	Reamur	$\left(\frac{4}{5}\right) * 42 = 33.81$
2.	Fahrenheit	$\left(\frac{9}{5}\right) * 99 + 32 = 210.25$
3.	Kelvin	$\left(\frac{5}{5}\right) * 7 + 273 = 279.98$
…	…	…
8.	Reamur	$\left(\frac{4}{5}\right) * 98 = 78.25$

B. Proses Perhitungan Dekripsi

Proses dekripsi dimulai dari langkah perhitungan kebalikan dari enkripsi, dengan menggunakan algoritma *hill cipher* terlebih dahulu. Mengenkripsi *ciphertext* dari hasil enkripsi yaitu 33.81R210.25F279.98K78.78R93.56F365.05K16.63 R210.66F274.25K73.08R102.33F369.59K6.97R195 .14F308.84K78.25R. Menggunakan persamaan *invers* konversi suhu pada Persamaan (13), (14), dan (15) yang ditunjukkan pada Tabel 7. Sehingga menghasilkan *ciphertext* 42.2699.036.9898.4834.2092.0520.7999.251.7591.3 539.0796.598.7290.6335.8497.81 yang dikalikan dengan 0.01, maka *ciphertext* menjadi 0.42C0.99C0.07C0.98C0.34C0.92C0.21C0.99C0.02 C0.91C0.39C0.97C0.09C0.91C0.36C0.98C .

Tabel 7. Perhitungan *Invers* Konversi Suhu

No.	Proses	
1.	Celcius	$\left(\frac{5}{5}\right) * 33.81 = 42.26$
2.	Celcius	$\left(\frac{5}{9}\right) * (210.25 - 32) = 99.03$
3.	Celcius	$\left(\frac{5}{5}\right) * (279.98 - 273) = 6.98$
…	…	…
8.	Celcius	$\left(\frac{5}{4}\right) * 78.25 = 97.81$

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3746

Perhitungan selanjutnya menggunakan *invers* trigonometri pada Persamaan (7) dan (9), yang ditunjukkan pada Tabel 8 dengan *plaintext* 0.42C0.99C0.07C0.98C0.34C0.92C0.21C0.99C0.02C0.91C0.39C0.97C0.09C0.91C0.36C0.98C. Maka menghasilkan *ciphertext* 25AS8AC4AS10AC20AS23AC12AS7AC1AS24AC23AS15AC5AS25AC21AS12AC.

Tabel 8. Perhitungan *Invers* Trigonometri

No.	Proses
1.	ASin 0.42 = 25
2.	ACos 0.99 = 8
…	…
16.	Acos 0.98 = 12

Perhitungan dekripsi berikutnya menggunakan *invers* matriks sesuai persamaan (2), (3), (4), (5) yang ditunjukkan pada Tabel 9 dibawah ini. Dengan menggunakan *plaintext* 25AS8AC4AS10AC20AS23AC12AS7AC1AS24AC23AS15AC5AS25AC21AS12AC, menghasilkan *ciphertext* 10171224122213542111905724 yang dikonversi menjadi *alphabet* sesuai Gambar 8 maka *ciphertext*nya menjadi PINBYDMUVEYGZUSB.

Tabel 9. Perhitungan *Invers* Matriks *Hill Cipher*

No.	Proses
1.	$\begin{bmatrix}6 & 1\\ 1 & 6\end{bmatrix} * \begin{bmatrix}25\\ 8\end{bmatrix} = \begin{matrix}158\\ 73\end{matrix}$ $\quad \begin{bmatrix}6 & -1\\ -1 & 6\end{bmatrix} * 3 = \begin{bmatrix}18 & -3\\ -3 & 18\end{bmatrix} Mod 26 = \begin{bmatrix}18 & 23\\ 23 & 18\end{bmatrix} * \begin{bmatrix}25\\ 8\end{bmatrix} = \begin{matrix}634\\ 719\end{matrix} Mod 26 = \begin{matrix}10\\ 17\end{matrix}$
…	… …
8.	$\begin{bmatrix}7 & 1\\ 2 & 1\end{bmatrix} * \begin{bmatrix}21\\ 12\end{bmatrix} = \begin{matrix}159\\ 54\end{matrix}$ $\quad \begin{bmatrix}1 & -1\\ -2 & 7\end{bmatrix} * 21 = \begin{bmatrix}21 & -21\\ -42 & 147\end{bmatrix} Mod 26 = \begin{bmatrix}21 & 5\\ 10 & 17\end{bmatrix} * \begin{bmatrix}21\\ 12\end{bmatrix} = \begin{matrix}501\\ 414\end{matrix} Mod 26 = \begin{matrix}7\\ 24\end{matrix}$

Proses dekripsi berikutnya menggunakan algoritma *vigenere cipher* mengubah bentuk *alphabet plaintext* PINBYDMUVEYGZUSB, menjadi simbol sesuai Gambar 7, maka menjadi *ciphertext* 3*1"<$089%<(>86" . Selanjutnya dari *plaintext* berbentuk simbol 3*1"<$089%<(>86" , maka diubah menggunakan tabel *tabula recta* sesuai Gambar 6 dan menggunakan 3 kunci yaitu yaitu GEMBOK, EKBMOG, MBEKGO. Sehingga menghasilkan *ciphertext* JEBAK TIKUS KANTOR yang sesuai dengan *plaintext* asli.

C. Implementasi Program

Pengimplementasian program menggunakan pemrograman Java dengan bantuan *tools* NetBeans IDE versi 8.0.2. Pada Gambar 9 menunjukkan hasil implementasi pemrosesan enkripsi pesan plaintext "JEBAK TIKUS KANTOR" dan Gambar 10 menunjukkan hasil implementasi pemrosesan dekripsi pesan yang mengembalikan ke plaintext atau pesan semula.

Gambar 9. Implementasi Hasil Enkripsi

Gambar 10. Implementasi Hasil Dekripsi

5. KESIMPULAN

Berdasarkan hasil penelitian dan implementasi sistem untuk pengamanan pesan menggunakan algoritma klasik khususnya mengkombinasi dan memodifikasi *vigenere cipher* dan hill cipher menggunakan metode *hybrid* kode pos, trigonometri, dan konversi suhu kelebihannya adalah tidak dapat dengan mudah bagi kriptanalis untuk memecahkan *ciphertext*, karena memiliki tingkat kesulitan yang berlapis untuk mengamankan pesan. Mulai dari modifikasi *vigenere cipher* dengan memodifikasi tabel *tabula recta* dengan simbol dan modifikasi kunci dengan 3 kunci yang digunakan, serta modifikasi matriks *hill cipher* dengan matriks kunci menggunakan nomor kode pos, dan modifikasi berlapis selanjutnya dengan menggunakan perhitungan trigonomteri dan konversi suhu. Pada tahap proses perhitungan trigonometri perlu diperhatikan karena perhitungan ini sangat sensitif jika diimplementasikan pada beberapa bahasa pemrograman.

Untuk pengembangan penelitian selanjutnya dapat memproses enkripsi dengan pesan yang dapat mengkombinasikan alfabet dan numerik secara bersamaan. Selain itu diharapkan dapat mengimplementasikannya menggunakan bahasa pemrograman lainnya dan juga dapat mengenkripsi dan dekprisi pesan dalam bentuk file seperti yang berektensi doc., pdf., bahkan file audio maupun video.

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3746

DAFTAR PUSTAKA

Ariyus, D. (2008). Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi. *Journal of Chemical Information and Modeling*. https://doi.org/10.1017/CBO9781107415324.004

Bhardwaj, C. R. S. (2012). Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols. *IOSR Journal of Computer Engineering*. https://doi.org/10.9790/0661-0423538

Danny Wowor, A. (2013). Modifikasi Kriptografi Hill Cipher Menggunakan Convert Between Base. *Seminar Nasional Sistem Informasi Indonesia*.

Direktorat Jenderal PAUD dan Pendidikan Masyarakat. (2017). *Modul 5 Penerapan Trigonometri dalam Pengembangan Ilmu dan Teknologi dalam Kehidupan Sehari-hari*. Jakarta: Kementrian Pendidikan dan Kebudayaan.

Hasugian, A. H. (2013). Implementasi Algoritma Hill Cipher Dalam Penyandian Data. *Pelita Informatika Budi Darma*.

Mundilarto, & Istiyono, E. (2007). *Seri IPA Fisika 1 SMP Kelas VII*. Jakarta: Yudhitira.

Nadhori, I. U., Jurusan, M., Informasi, T., Pembimbing, D., Elektronika, P., & Surabaya, N. (2010). *Pembuatan perangkat lunak media pembelajaran kriptografi klasik*. 1–11.

Nofriadi. (2015). Java Fundamental Dengan Netbeans 8.0.2. In *DeePublish*.

Sukamto, & Shalahuddin. (2014). Shalahuddin, M. Rosa A.S 2014. Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek. Bandung: Informatika Bandung. *Jurnal Pilar Nusa Mandiri*.

U.W.M, I., Susanto, A., Rachmawanto, E. ., & Setiadi, D. R. I. . (2018). Kombinasi Kriptografi Klasik Pada Media Gambar : Shift Cipher dan Vigenere Cipher. *Prosiding SNATIF Ke-5 Tahun 2018*, 379–384.

Wahyuningsih, S., & Suryanto, J. (2015). Evaluasi Pemanfaatan Kode Pos. *Buletin Pos Dan Telekomunikasi*. https://doi.org/10.17933/bpostel.2011.090304

Yunita, S., Hasan, P., & Ariyus, D. (2019). Modifikasi Algoritma Hill Chiper dan Twofish Menggunakan Kode Wilayah Telepon. *SISFOTENIKA*. https://doi.org/10.30700/jst.v9i2.489