Jurnal Riset Mahasiswa Matematika
Volume 1(2) (2021), Pages 93-104
p-ISSN: 2808-1552; e-ISSN: 2808-4926

Enkripsi dan Dekripsi Pesan Menggunakan Metode Vigenere Cipher dan Route Cipher

Zulfatul Aufia[1], Turmudi[2*] ,Evawati Alisah[3]

[1,2,3]Program Studi Matematika, Fakultas Sains dan Teknologi, Indonesia

Email: szulfia16@gmail.com, turmudi_msi@mat.uin-malang.ac.id*, evawatialisah@mat.uin-malang.ac.id

Abstrak

Keamanan pesan sangat dibutuhkan dalam pertukaran pesan karena pesan memiliki sifat rahasia yang hanya boleh terbaca oleh pihak yang merupakan tujuannya. Kriptografi dapat digunakan untuk mengatasi permasalahan tersebut Penelitian ini menggunakan metode substitusi dan metode transposisi. Metode substitusi yang digunakan adalah vigenere cipher dan metode transposisi yang digunakan adalah route cipher. Terdapat tiga variasi kunci dari metode vigenere cipher yaitu, full vigenere cipher, auto-key vigenere cipher dan running-key vigenere cipher. Tujuan dari penelitian adalah menghasilkan cipherteks dan plainteks menggunakan super enkripsi dengan metode vigenere cipher dan route cipher. Adapun proses enkripsi adalah dengan melakukan enkripsi menggunakan metode vigenere cipher dan selanjutnya dienkripsi lagi menggunakan metode route cipher. Metode vigenere cipher terdiri dari tiga variasi, sehingga setiap variasinya dienkripsi satu persatu yang kemudian dienkripsi lagi dengan metode route cipher. Adapun proses dekripsi adalah dengan melakukan dekripsi menggunakan metode route cipher dan dilanjut dengan metode vigenere cipher. Hasil dari penelitian ini didapatkannya cipherteks pada proses enkripsi dan plainteks pada proses dekripsi dengan menggunakan metode vigenere cipher dengan 3 variasi dan metode route cipher.

Kata kunci: Kriptografi, Super Enkripsi, Enkripsi, Dekripsi, *Vigenere Cipher*, *Route Cipher*

Abstract

Message security is needed in exchanging messages because messages have a secret nature that can only be read by the party who is the destination. Cryptography can be used to overcome these problems. This research uses the substitution method and the transposition method. The substitution method used is the *vigenere cipher* and the transposition method used is the *route cipher*. There are three key variations of the *vigenere cipher* method, namely, *full vigenere cipher*, *auto-key vigenere cipher* and *running-key vigenere cipher*. The purpose of this research is to produce ciphertext and plaintext using super encryption with *vigenere cipher* and *route cipher* methods. The encryption process is to encrypt using the *vigenere cipher* method and then encrypted again using the *route cipher* method. The *vigenere cipher* method consists of three variations, so that each variation is encrypted one by one which is then encrypted again with the *route cipher* method. The decryption process is to perform decryption using the *route cipher* method and followed by the *vigenere cipher* method. The results of this study obtained ciphertext in the encryption process and plaintext in the decryption process using the *vigenere cipher* method with 3 variations and the *route cipher* method.

Keywords: Cryptography, Super Encryption, Encryption, Decryption, *Vigenere Cipher*, *Route Cipher*

PENDAHULUAN

Di era modern seperti saat ini di mana berbagi informasi digital meningkat secara signifikan [1]. Meningkatnya kebutuhan terhadap pertukaran pesan yang semakin tinggi, sehingga aspek keamanan sangat dibutuhkan. Dalam hal ini, dibutuhkan suatu pengamanan sehingga pesan tersebut tidak terbaca oleh pihak lain yang bukan merupakan tujuan dari pesan tersebut. Untuk menangani permasalahan tersebut, maka diperlukan kunci untuk

Submitted: 06 Desember 2021 Reviewed: 08 Desember 2021 Accepted: 10 Desember 2021
DOI: https://doi.org/10.18860/jrmm.v1i1.14207

membukanya, yang mana kunci tersebut hanya dimiliki orang yang berhak membuka pesan tersebut.

Kriptografi (crytography) berasal dari bahasa Yunani "cryptos" artinya "secret" (rahasia) sedangkan "graphein" artinya "writing" (tulisan) [2]. Kriptografi merupakan ilmu yang memiliki hubungan dengan bidang matematika karena memiliki keterkaitan dengan aspek keamanan informasi. Secara umum kriptografi dapat diartikan sebagai suatu bidang ilmu yang memiliki kesenian dalam menjaga kerahasiaan dari suatu data atau informasi [3]. Terdapat dua istilah dalam kriptografi yaitu plainteks (pesan asli) dan cipherteks (pesan yang telah diacak). Adapun proses yang terdapat dalam kriptografi yaitu enkripsi dan dekripsi. Enkripsi yaitu mengubah pesan asli menjadi pesan yang susah dimengerti sedangkan dekripsi merupakan proses mengubah pesan yang tidak dimengerti menjadi pesan bermakna atau pesan asli [4].

Tujuan dari ilmu kriptografi yaitu menjaga keamanan isi dari informasi yang telah disandi, integritas data, autentikasi yang merupakan hubungan identifikasi dan mencegah perilaku tidak teratur dalam pengiriman informasi kepada pengirim [5]. Penerapan kriptografi harus dapat menjamin kerahasiaan, integritas, autentikasi dan nir-penyangkalan [6]. Salah satu metode yang dapat menjaga keamanan pesan adalah gabungan dari metode vigenere cipher dan route cipher atau gabungan tersebut bisa biasa disebut dengan super enkripsi.

Vigenere cipher merupakan algoritma yang dipublikasikan oleh Blaise de Vigenere pada tahun 1586 diabad ke-16. Namun sebenarnya, kode tersebut ditemukan oleh Giovan Batista Belaso pada tahun 1553 dan dimasukkan ke dalam buku La Cifta del Sig [7] Vigenere cipher merupakan pengembangan dari Caesar cipher. Vigenere cipher merupakan algoritma klasik yang menggunakan metode substitusi abjad-majemuk (polyalphabet). Keamanan sandi vigenere tergantung pada banyaknya kunci yang digunakan [8].

Vigenere cipher memiliki tiga variasi yang memiliki perbedaan pada kunci. Variasi vigenere cipher di antaranya yaitu *full vigenere cipher*, *auto-key vigenere cipher* dan *running key vigenere cipher*. *Full vigenere cipher* yaitu pada setiap baris di dalam tabel tidak menyatakan pergeseran huruf, tetapi merupakan permutasi huruf-huruf alfabet. *Auto-key vigenere cipher* yaitu jika panjang kunci lebih pendek dari panjang plainteks maka kunci disambung dengan plainteks tersebut [9]. *Running-key vigenere cipher* yaitu kunci bukan merupakan karakter pendek yang diulang secara periodik seperti pada *Vigenere* standar [10].

Secara matematis, rumus enkripsi dan dekripsi *Vigenere cipher* adalah sebagai berikut:

Enkripsi : $C_i = (P_i + K_i)\ mod\ 26$

Dekripsi : $P_i = (C_i - K_i)\ mod\ 26$

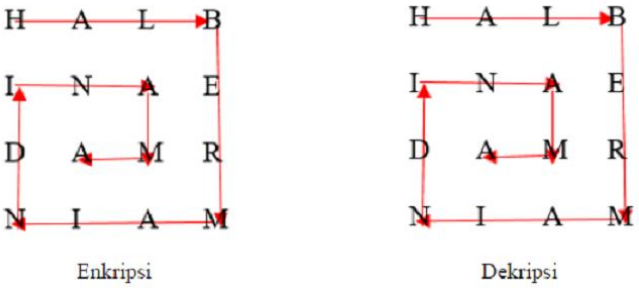
Keterangan

P_i : Nilai karakter plainteks ke-i

C_i : Nilai karakter cipherteks ke-i

K_i : nilai karakter kunci ke-i [11]

Route cipher adalah cipher substitusi di mana kuncinya merupakan rute mana yang akan diikuti saat membaca cipherteks dari blok yang dibuat dengan plainteks. Plainteks ditulis dalam kotak, lalu dibaca mengikuti rute yang dipilih. Berikut ini spiral pada *route cipher* [12].



Algoritma *route cipher* dapat dikatakan mempunyai proses enkripsi yang rumit. Hal tersebut dikarenakan *key* yang lebih membuat proses enkripsi dan dekripsi menjadi fleksibel. Bila panjang karakter tidak habis dibagi dengan panjang karakter, maka penambahan karakter secara *dummy* saat melakukan enkripsi [13].

Super enkripsi adalah suatu konsep yang menggunakan kombinasi dari dua atau lebih teknik substitusi dan permutasi untuk mendapatkan suatu algoritma yang lebih andal (sulit dipecahkan). Teknik dari super enkripsi mudah dilakukan asal sudah memahami teknik substitusi dan permutasi. Langkah-langkah yang perlu dilakukan adalah melakukan enkripsi pesan dengan menggunakan teknik substitusi dan teks kode yang dapat dienkripsi lagi menggunakan teknik transposisi (permutasi) [7].

Berdasarkan uraian di atas sehingga tujuan penelitian ini yaitu untuk mengetahui proses enkripsi pesan menggunakan metode *vigenere cipher* dan *route cipher* dan untuk mengetahui proses dekripsi pesan menggunakan metode *vigenere cipher* dan *route cipher*

Adapun penelitian tentang super enkripsi dilakukan oleh Surya Darma Nasution, Muhammad Syahrizal, Guidio Leonarde Ginting dan Robbi Rahim (2017) berjudul Data Security Using Vigenere Cipher and Goldbach Codes Algorithm yang membahas proses enkripsi dan dekripsi menggunakan metode *vigenere cipher* dan kode *goldbach*. Untuk mencapai cipherteksnya yaitu dengan melakukan enkripsi menggunakan metode *vigenere cipher* dan setelah didapatkan hasilnya (cipherteks) dilanjut dengan enkripsi menggunakan kode *goldbach* Sedangkan untuk proses dekripsinya yaitu dengan melakukan dekripsi menggunakan kode *godbach* dan setelah didapatkan hasilnya (plainteks) dilanjut dengan dekripsi menggunakan metode *vigenere cipher*. Maksud penggabungan 2 metode ini untuk mengatasi kelemahan dari metode *vigenere cipher* yang dapat dilacak dengan metode kasiski. Kode *goldbach* merupakan algoritma yang dapat mengatasi kelemahan pada *vigenere cipher* [14].

Selanjutnya penelitian yang dilakukan oleh Shanny Avelina Halim (2007) berjudul Super Enkripsi Dengan Menggunakan Cipher Substitusi dan Cipher Transposisi membahas tentang proses enkripsi dan dekripsi menggunakan metode substitusi dan transposisi di mana metode substitusi yang digunakan hanya menggunakan 1 kunci yang sama untuk semua karakter dan metode transposisinya menggunakan susunan blok namun metode ini dapat dipecahkan dengan menggunakan metode *brute force* yaitu mencoba semua kemungkinan yang ada [15].

Penelitian lain juga dilakukan oleh Nova Fitri (2019) berjudul Perancangan Aplikasi Penyandian File Teks Menggunakan Algoritma Route Cipher Berbasis Desktop yang membahas proses enkripsi dan dekripsi menggunakan metode *Route cipher* beserta implementasinya. Rute yang digunakan pada metode ini yaitu berbentuk spiral. Rute spiral searah jarum jam digunakan pada proses enkripsi dan untuk proses dekripsi dengan mengisi kolom kosong dari kanan atas ke bawah berbentuk spiral searah jarum jam [12].

METODE

Pada penelitian ini terdapat 2 proses penyelesaian, yaitu proses enkripsi dan dekripsi. Adapun langkah-langkah yang digunakan pada proses enkripsi yaitu melakukan enkripsi menggunakan metode *vigenere cipher*, setelah mendapatkan hasil enkripsinya dilanjut enkripsi menggunakan metode *route cipher*. Langkah-langkah proses dekripsi yaitu dengan melakukan dekripsi menggunakan metode *route cipher*, setelah mendapatkan hasil dekripsinya dilanjut melakukan dekripsi menggunakan metode *vigenere cipher*.
Langkah-langkah proses enkripsi yaitu:

1. Membuat pesan teks asli (plainteks) *vigenere cipher*
2. Menentukan kunci yang digunakan pada *vigenere cipher*
3. Melakukan perhitungan dengan *vigenere cipher* menggunakan rumus $C_i = (P_i + K_i)\ mod\ 26$
4. Mendapatkan hasil enkripsi *vigenere cipher*
5. Menentukan kunci yang digunakan pada metode transposisi *route cipher*
6. Menyusun hasil enkripsi *vigenere cipher* sesuai kunci *route cipher* dari kiri ke kanan secara horizontal
7. Menyusun hasil enkripsi *route cipher* dari kanan atas ke bawah berbentuk spiral searah jarum jam
8. Mendapatkan hasil enkripsi *route cipher* (cipherteks).

Langkah-langkah proses dekripsi yaitu:

1. Menentukan kunci *route cipher* (jumlah karakter cipherteks dibagi kunci pada proses enkripsi)
2. Memasukkan pesan yang sudah disandikan (cipherteks) dan menyusun karakter dari kiri atas ke bawah berbentuk spiral berlawanan dengan arah jarum jam
3. Menyusun plainteks *route cipher* secara horizontal dari kanan ke kiri
4. Menentukan kunci *vigenere cipher*
5. Melakukan perhitungan *vigenere cipher* dengan menggunakan rumus $P_i = (C_i - K_i)\ mod\ 26$
6. Mendapatkan pesan asli *vigenere cipher* (plainteks).

HASIL DAN PEMBAHASAN

Penelitian ini berisi proses enkripsi dan dekripsi pesan menggunakan dua metode atau biasa disebut dengan metode super enkripsi yang mana pada proses ini menggunakan metode substitusi dan transposisi. Metode yang digunakan pada penelitian ini yaitu *vigenere cipher* yang merupakan metode substitusi dan *route cipher* sebagai metode transposisi.

1. Proses Enkripsi Pesan Menggunakan Metode Vigenere Cipher dan Route Cipher
   a. Enkripsi menggunakan variasi *full vigenere cipher*
      1) Menentukan pesan asli (plainteks)
         Pesan asli yang digunakan adalah "JOMBANG KOTA BERIMAN".
      2) Menentukan kunci variasi *full vigenere cipher*
         Kunci yang digunakan adalah "ZFTL". Berikut ini kunci setiap karakter plainteks.

Tabel 1 Kunci Setiap Karakter Plainteks Variasi Full Vigenere Cipher

P_i	J	O	M	B	A	N	G	K	O	T	A	B	E	R	I	M	A	N
K_i	Z	F	T	L	Z	F	T	L	Z	F	T	L	Z	F	T	L	Z	F

3) Melakukan perhitungan menggunakan rumus $C_i = (P_i + K_i)\ mod\ 26$.
$C_1\ (J,Z) = (P_1 + K_1)\ mod\ 26 = (9 + 25)\ mod\ 26 = 34\ mod\ 26 = 8$
$C_2\ (O,F) = (P_2 + K_2)\ mod\ 26 = (14 + 5)\ mod\ 26 = 19\ mod\ 26 = 19$
$C_3\ (M,T) = (P_3 + K_3)\ mod\ 26 = (12 + 19)\ mod\ 26 = 31\ mod\ 26 = 5$
$C_4\ (B,L) = (P_4 + K_4)\ mod\ 26 = (1 + 11)\ mod\ 26 = 12\ mod\ 26 = 12$
$C_5\ (A,Z) = (P_5 + K_5)\ mod\ 26 = (0 + 25)\ mod\ 26 = 25\ mod\ 26 = 25$
$C_6\ (N,F) = (P_6 + K_6)\ mod\ 26 = (13 + 5)\ mod\ 26 = 18\ mod\ 26 = 18$
$C_7\ (G,T) = (P_7 + K_7)\ mod\ 26 = (6 + 19)\ mod\ 26 = 25\ mod\ 26 = 25$
$C_8\ (K,L) = (P_8 + K_8)\ mod\ 26 = (10 + 11)\ mod\ 26 = 21\ mod\ 26 = 21$
$C_9\ (O,Z) = (P_9 + K_9)\ mod\ 26 = (14 + 25)\ mod\ 26 = 39\ mod\ 26 = 13$
$C_{10}\ (T,F) = (P_{10} + K_{10})\ mod\ 26 = (19 + 5)\ mod\ 26 = 24\ mod\ 26 = 24$
$C_{11}\ (A,T) = (P_{11} + K_{11})\ mod\ 26 = (0 + 19)\ mod\ 26 = 19\ mod\ 26 = 19$
$C_{12}\ (B,L) = (P_{12} + K_{12})\ mod\ 26 = (1 + 11)\ mod\ 26 = 12\ mod\ 26 = 12$
$C_{13}\ (E,Z) = (P_{13} + K_{13})\ mod\ 26 = (4 + 25)\ mod\ 26 = 29\ mod\ 26 = 3$
$C_{14}\ (R,F) = (P_{14} + K_{14})\ mod\ 26 = (17 + 5)\ mod\ 26 = 22\ mod\ 26 = 22$
$C_{15}\ (I,T) = (P_{15} + K_{15})\ mod\ 26 = (8 + 19)\ mod\ 26 = 27\ mod\ 26 = 1$
$C_{16}\ (M,L) = (P_{16} + K_{16})\ mod\ 26 = (12 + 11)\ mod\ 26 = 23\ mod\ 26 = 23$
$C_{17}\ (A,Z) = (P_{17} + K_{17})\ mod\ 26 = (0 + 25)\ mod\ 26 = 25\ mod\ 26 = 25$
$C_{18}\ (N,F) = (P_{18} + K_{18})\ mod\ 26 = (13 + 5)\ mod\ 26 = 18\ mod\ 26 = 18$

4) Mendapatkan hasil enkripsi variasi *full vigenere cipher* "ITFMZSZVNYTMDWBXZS".
5) Menentukan kunci *route cipher*. K=3
6) Menyusun hasil enkripsi *vigenere cipher* sesuai kunci *route cipher* secara horizontal.

I	T	F
M	Z	S
Z	V	N
Y	T	M
D	W	B
X	Z	S

7) Menyusun hasil enkripsi dari kanan atas ke bawah berbentuk spiral searah jarum jam.

I	T	F
M	Z	S
Z	V	N
Y	T	M
D	W	B
X	Z	S

8) Mendapatkan hasil enkripsi dari metode *route cipher* "FSNMBSZXDYZMITZVTW".

b. Enkripsi menggunakan variasi *auto-key vigenere cipher*
1) Menentukan pesan asli (plainteks) *vigenere cipher*
Pesan asli yang digunakan adalah "JOMBANG KOTA BERIMAN".
2) Menentukan kunci variasi *auto-key vigenere cipher*
Kunci yang digunakan adalah "ZFTLJOMBANGJOTABER" yang kemudian disambung dengan plainteks. Berikut ini kunci setiap karakter plainteks.

Tabel 2 Kunci Setiap Karakter Plainteks Variasi Auto-key Vigenere Cipher

P_i	J	O	M	B	A	N	G	K	O	T	A	B	E	R	I	M	A	N
K_i	Z	F	T	L	J	O	M	B	A	N	G	K	O	T	A	B	E	R

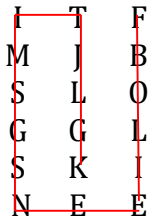
3) Melakukan perhitungan menggunakan rumus $C_i = (P_i + K_i)\ mod\ 26$ dengan kunci K=ZFTLJOMBANGKOTABER

$C_1\ (J,Z) = (P_1 + K_1)\ mod\ 26 = (9 + 25)\ mod\ 26 = 34\ mod\ 26 = 8$
$C_2\ (O,F) = (P_2 + K_2)\ mod\ 26 = (14 + 5)\ mod\ 26 = 19\ mod\ 26 = 19$
$C_3\ (M,T) = (P_3 + K_3)\ mod\ 26 = (12 + 19)\ mod\ 26 = 31\ mod\ 26 = 5$
$C_4\ (B,L) = (P_4 + K_4)\ mod\ 26 = (1 + 11)\ mod\ 26 = 12\ mod\ 26 = 12$
$C_5\ (A,J) = (P_5 + K_5)\ mod\ 26 = (0 + 9)\ mod\ 26 = 9\ mod\ 26 = 9$
$C_6\ (N,O) = (P_6 + K_6)\ mod\ 26 = (13 + 14)\ mod\ 26 = 27\ mod\ 26 = 1$
$C_7\ (G,M) = (P_7 + K_7)\ mod\ 26 = (6 + 12)\ mod\ 26 = 18\ mod\ 26 = 18$
$C_8\ (K,B) = (P_8 + K_8)\ mod\ 26 = (10 + 1)\ mod\ 26 = 11\ mod\ 26 = 11$
$C_9\ (O,A) = (P_9 + K_9)\ mod\ 26 = (14 + 0)\ mod\ 26 = 14\ mod\ 26 = 14$
$C_{10}\ (T,N) = (P_{10} + K_{10})\ mod\ 26 = (19 + 13)\ mod\ 26 = 32\ mod\ 26 = 6$
$C_{11}\ (A,G) = (P_{11} + K_{11})\ mod\ 26 = (0 + 6)\ mod\ 26 = 6\ mod\ 26 = 6$
$C_{12}\ (B,K) = (P_{12} + K_{12})\ mod\ 26 = (1 + 10)\ mod\ 26 = 11\ mod\ 26 = 11$
$C_{13}\ (E,O) = (P_{13} + K_{13})\ mod\ 26 = (4 + 14)\ mod\ 26 = 18\ mod\ 26 = 18$
$C_{14}\ (R,T) = (P_{14} + K_{14})\ mod\ 26 = (17 + 19)\ mod\ 26 = 36\ mod\ 26 = 10$
$C_{15}\ (I,A) = (P_{15} + K_{15})\ mod\ 26 = (8 + 0)\ mod\ 26 = 8\ mod\ 26 = 8$
$C_{16}\ (M,B) = (P_{16} + K_{16})\ mod\ 26 = (12 + 1)\ mod\ 26 = 13\ mod\ 26 = 13$
$C_{17}\ (A,E) = (P_{17} + K_{17})\ mod\ 26 = (0 + 4)\ mod\ 26 = 4\ mod\ 26 = 4$
$C_{18}\ (N,R) = (P_{18} + K_{18})\ mod\ 26 = (13 + 17)\ mod\ 26 = 30\ mod\ 26 = 4$

4) Mendapatkan hasil enkripsi variasi *auto-key vigenere cipher* "ITFMJBSLOGGLSKINEE".
5) Menentukan kunci *route cipher*. K=3
6) Menyusun hasil enkripsi *vigenere cipher* sesuai kunci *route cipher* secara horizontal.

I	T	F
M	J	B
S	L	O
G	G	L
S	K	I
N	E	E

7) Menyusun hasil enkripsi dari kanan atas ke bawah berbentuk spiral searah jarum jam.



8) Mendapatkan hasil enkripsi dari metode *route cipher* "FBOLIEENSGSMITJLGK".

c. Enkripsi menggunakan variasi *running-key vigenere cipher*
1) Menentukan pesan asli (plainteks) *vigenere cipher*
Pesan asli yang digunakan adalah "JOMBANG KOTA BERIMAN".
2) Menentukan kunci variasi *running-key vigenere cipher*

Kunci yang digunakan adalah Pancasila sila ke 5 yang berbunyi "KEADILAN SOSIAL BAGI". Berikut ini kunci dari setiap karakter plainteks.

Tabel 3 Kunci dari Setiap Karakter Plainteks Variasi Running-key Vigenere Cipher

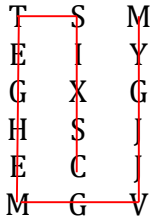
P_i	J	O	M	B	A	N	G	K	O	T	A	B	E	R	I	M	A	N
K_i	K	E	A	D	I	L	A	N	S	O	S	I	A	L	B	A	G	I

3) Melakukan perhitungan menggunakan rumus $C_i = (P_i + K_i)\ mod\ 26$.
$C_1\ (J,K) = (P_1 + K_1)\ mod\ 26 = (9 + 10)\ mod\ 26 = 19\ mod\ 26 = 19$
$C_2\ (O,E) = (P_2 + K_2)\ mod\ 26 = (14 + 4)\ mod\ 26 = 18\ mod\ 26 = 18$
$C_3\ (M,A) = (P_3 + K_3)\ mod\ 26 = (12 + 0)\ mod\ 26 = 12\ mod\ 26 = 12$
$C_4\ (B,D) = (P_4 + K_4)\ mod\ 26 = (1 + 3)\ mod\ 26 = 4\ mod\ 26 = 4$
$C_5\ (A,I) = (P_5 + K_5)\ mod\ 26 = (0 + 8)\ mod\ 26 = 8\ mod\ 26 = 8$
$C_6\ (N,L) = (P_6 + K_6)\ mod\ 26 = (13 + 11)\ mod\ 26 = 24\ mod\ 26 = 24$
$C_7\ (G,A) = (P_7 + K_7)\ mod\ 26 = (6 + 0)\ mod\ 26 = 6\ mod\ 26 = 6$
$C_8\ (K,N) = (P_8 + K_8)\ mod\ 26 = (10 + 13)\ mod\ 26 = 23\ mod\ 26 = 23$
$C_9\ (O,S) = (P_9 + K_9)\ mod\ 26 = (14 + 18)\ mod\ 26 = 32\ mod\ 26 = 6$
$C_{10}\ (T,O) = (P_{10} + K_{10})\ mod\ 26 = (19 + 14)\ mod\ 26 = 33\ mod\ 26 = 7$
$C_{11}\ (A,S) = (P_{11} + K_{11})\ mod\ 26 = (0 + 18)\ mod\ 26 = 18\ mod\ 26 = 18$
$C_{12}\ (B,I) = (P_{12} + K_{12})\ mod\ 26 = (1 + 8)\ mod\ 26 = 9\ mod\ 26 = 9$
$C_{13}\ (E,A) = (P_{13} + K_{13})\ mod\ 26 = (4 + 0)\ mod\ 26 = 4\ mod\ 26 = 4$
$C_{14}\ (R,L) = (P_{14} + K_{14})\ mod\ 26 = (17 + 11)\ mod\ 26 = 28\ mod\ 26 = 2$
$C_{15}\ (I,B) = (P_{15} + K_{15})\ mod\ 26 = (8 + 1)\ mod\ 26 = 9\ mod\ 26 = 9$
$C_{16}\ (M,A) = (P_{16} + K_{16})\ mod\ 26 = (12 + 0)\ mod\ 26 = 12\ mod\ 26 = 12$
$C_{17}\ (A,G) = (P_{17} + K_{17})\ mod\ 26 = (0 + 6)\ mod\ 26 = 6\ mod\ 26 = 6$
$C_{18}\ (N,I) = (P_{18} + K_{18})\ mod\ 26 = (13 + 8)\ mod\ 26 = 21\ mod\ 26 = 21$

4) Mendapatkan hasil enkripsi variasi *running-key vigenere cipher* "TSMEIYGXGHSJECJMGV".
5) Menentukan kunci *route cipher*. K=3
6) Menyusun hasil enkripsi *vigenere cipher* sesuai kunci *route cipher* secara horizontal.

T	S	M
E	I	Y
G	X	G
H	S	J
E	C	J
M	G	V

7) Menyusun hasil enkripsi dari kanan atas ke bawah berbentuk spiral searah jarum jam.

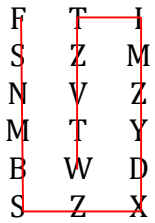


8) Mendapatkan hasil enkripsi metode *route cipher* "MYGJJVGMEHGETSIXSC".

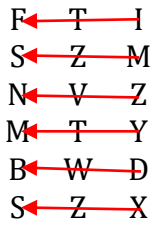
2. Proses Dekripsi Pesan Menggunakan Metode Vigenere Cipher dan Route Cipher
   a. Dekripsi menggunakan variasi *full vigenere cipher* dan *route cipher*
      1) Menentukan cipherteks *route cipher*

Cipherteks dari metode *vigenere cipher* variasi *full vigenere cipher* dan *route cipher* adalah "FSNMBSZXDYZMITZVTW".

2) Menentukan kunci *route cipher*. K=6
3) Memasukkan cipherteks dan menyusun karakter dari kiri atas ke bawah berbentuk spiral berlawanan dengan arah jarum jam.



4) Menyusun cipherteks secara horizontal dari kanan ke kiri.



5) Mendapatkan hasil dekripsi metode *route cipher* "ITFMZSZVNYTMDWBXZS".
6) Menentukan kunci variasi full *vigenere cipher*. Berikut ini kunci setiap karakter cipherteks.

Tabel 4 Kunci dari Setiap Karakter Cipherteks Variasi Auto-key Vigenere Cipher

C_i	I	T	F	M	Z	S	Z	V	N	Y	T	M	D	W	B	X	Z	S
K_i	Z	F	T	L	Z	F	T	L	Z	F	T	L	Z	F	T	L	Z	F

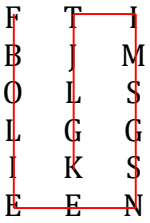
7) Melakukan perhitungan *vigenere cipher* menggunakan rumus $P_i = (C_i - K_i)\ mod\ 26$

$C_1\ (I,Z) = (P_1 - K_1)\ mod\ 26 = (8-25)\ mod\ 26 = -17\ mod\ 26 = 9$
$C_2\ (T,F) = (P_2 - K_2)\ mod\ 26 = (19-5)\ mod\ 26 = 14\ mod\ 26 = 14$
$C_3\ (F,T) = (P_3 - K_3)\ mod\ 26 = (5-19)\ mod\ 26 = -14\ mod\ 26 = 12$
$C_4\ (M,L) = (P_4 - K_4)\ mod\ 26 = (12-11)\ mod\ 26 = 1\ mod\ 26 = 1$
$C_5\ (Z,Z) = (P_5 - K_5)\ mod\ 26 = (25-25)\ mod\ 26 = 0\ mod\ 26 = 0$
$C_6\ (S,F) = (P_6 - K_6)\ mod\ 26 = (18-5)\ mod\ 26 = 13\ mod\ 26 = 13$
$C_7\ (Z,T) = (P_7 - K_7)\ mod\ 26 = (25-19)\ mod\ 26 = 6\ mod\ 26 = 6$
$C_8\ (V,L) = (P_8 - K_8)\ mod\ 26 = (21-11)\ mod\ 26 = 10\ mod\ 26 = 10$
$C_9\ (N,Z) = (P_9 - K_9)\ mod\ 26 = (13-25)\ mod\ 26 = -12\ mod\ 26 = 14$
$C_{10}\ (Y,F) = (P_{10} - K_{10})\ mod\ 26 = 24-5\ mod\ 26 = 19\ mod\ 26 = 19$
$C_{11}\ (T,T) = (P_{11} - K_{11})\ mod\ 26 = (19-19)\ mod\ 26 = 0\ mod\ 26 = 0$
$C_{12}\ (M,L) = (P_{12} - K_{12})\ mod\ 26 = (12-11)\ mod\ 26 = 1\ mod\ 26 = 1$
$C_{13}\ (D,Z) = (P_{13} - K_{13})\ mod\ 26 = (3-25)\ mod\ 26 = -22\ mod\ 26 = 4$
$C_{14}\ (W,F) = (P_{14} - K_{14})\ mod\ 26 = (22-5)\ mod\ 26 = 17\ mod\ 26 = 17$
$C_{15}\ (B,T) = (P_{15} - K_{15})\ mod\ 26 = (1-19)\ mod\ 26 = -18\ mod\ 26 = 8$
$C_{16}\ (X,L) = (P_{16} - K_{16})\ mod\ 26 = (23-11)\ mod\ 26 = 12\ mod\ 26 = 12$
$C_{17}\ (Z,Z) = (P_{17} - K_{17})\ mod\ 26 = (25-25)\ mod\ 26 = 0\ mod\ 26 = 0$
$C_{18}\ (S,F) = (P_{18} - K_{18})\ mod\ 26 = 18-5\ mod\ 26 = 13\ mod\ 26 = 13$

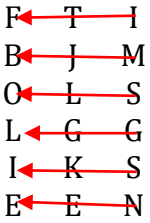
8) Mendapatkan hasil dekripsi metode *vigenere cipher* variasi *full vigenere cipher* "JOMBANG KOTA BERIMAN"

b. Dekripsi menggunakan variasi *auto-key vigenere cipher* dan *route cipher*

1) Menentukan cipherteks *route cipher*
Cipherteks dari metode *vigenere cipher* variasi *auto-key vigenere cipher* dan *route cipher* adalah "FBOLIEENSGSMITJLGK".
2) Menentukan kunci *route cipher*. K=6
3) Memasukkan cipherteks dan menyusun karakter dari kiri atas ke bawah berbentuk spiral berlawanan dengan jarum jam.



4) Menyusun cipherteks secara horizontal dari kanan ke kiri.



5) Mendapatkan hasil dekripsi metode *route cipher* "ITFMJBSLOGGSLSKINEE".
6) Menentukan kunci variasi *auto-key vigenere cipher*. Berikut ini kunci setiap karakter cipherteks.

Tabel 5 Kunci dari Setiap Karakter Cipherteks Variasi Auto-key Vigenere Cipher

C_i	I	T	F	M	J	B	S	L	O	G	G	L	S	K	I	N	E	E
K_i	Z	F	T	L	J	O	M	B	A	N	G	K	O	T	A	B	E	R

7) Melakukan perhitungan *vigenere cipher* menggunakan rumus $P_i = (C_i - K_i)\ mod\ 26$

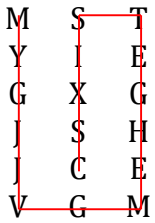
$C_1\ (I,Z) = (P_1 - K_1)\ mod\ 26 = (8-25)\ mod\ 26 = -17\ mod\ 26 = 9$
$C_2\ (T,F) = (P_2 - K_2)\ mod\ 26 = (19-5)\ mod\ 26 = 14\ mod\ 26 = 14$
$C_3\ (F,T) = (P_3 - K_3)\ mod\ 26 = (5-19)\ mod\ 26 = -14\ mod\ 26 = 12$
$C_4\ (M,L) = (P_4 - K_4)\ mod\ 26 = (12-11)\ mod\ 26 = 1\ mod\ 26 = 1$
$C_5\ (J,J) = (P_5 - K_5)\ mod\ 26 = (0-0)\ mod\ 26 = 0\ mod\ 26 = 0$
$C_6\ (B,O) = (P_6 - K_6)\ mod\ 26 = (1-14)\ mod\ 26 = -13\ mod\ 26 = 13$
$C_7\ (S,M) = (P_7 - K_7)\ mod\ 26 = (18-12)\ mod\ 26 = 6\ mod\ 26 = 6$
$C_8\ (L,B) = (P_8 - K_8)\ mod\ 26 = (11-1)\ mod\ 26 = 10\ mod\ 26 = 10$
$C_9\ (O,A) = (P_9 - K_9)\ mod\ 26 = (14-0)\ mod\ 26 = 14\ mod\ 26 = 14$
$C_{10}\ (G,N) = (P_{10} - K_{10})\ mod\ 26 = (6-13)\ mod\ 26 = -7\ mod\ 26 = 19$
$C_{11}\ (G,G) = (P_{11} - K_{11})\ mod\ 26 = (0-0)\ mod\ 26 = 0\ mod\ 26 = 0$
$C_{12}\ (L,K) = (P_{12} - K_{12})\ mod\ 26 = (11-10)\ mod\ 26 = 1\ mod\ 26 = 1$
$C_{13}\ (S,O) = (P_{13} - K_{13})\ mod\ 26 = (18-14)\ mod\ 26 = 4\ mod\ 26 = 4$
$C_{14}\ (K,T) = (P_{14} - K_{14})\ mod\ 26 = (10-19)\ mod\ 26 = -9\ mod\ 26 = 17$
$C_{15}\ (I,A) = (P_{15} - K_{15})\ mod\ 26 = (8-0)\ mod\ 26 = 8\ mod\ 26 = 8$
$C_{16}\ (N,B) = (P_{16} - K_{16})\ mod\ 26 = (13-1)\ mod\ 26 = 12\ mod\ 26 = 12$

$C_{17}\ (E,E) = (P_{17} - K_{17})\ mod\ 26 = (0-0)\ mod\ 26 = 0\ mod\ 26 = 0$
$C_{18}\ (E,R) = (P_{18} - K_{18})\ mod\ 26 = (4-17)\ mod\ 26 = -13\ mod\ 26 = 13$

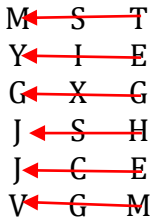
8) Mendapatkan hasil dekripsi metode *vigenere cipher* variasi *auto-key vigenere cipher* "JOMBANG KOTA BERIMAN"

c. Dekripsi menggunakan variasi *running-key vigenere cipher* dan *route cipher*

1) Menentukan cipherteks *route cipher*
Cipherteks dari metode *vigenere cipher* variasi *running-key vigenere cipher* dan *route cipher* adalah "MYGJJVGMEHGETSIXSC".
2) Menentukan kunci *route cipher*. K=6
3) Memasukkan cipherteks dan menyusun karakter dari kiri atas ke bawah berbentuk spiral berlawanan dengan jarum jam.



4) Menyusun cipherteks secara horizontal dari kanan ke kiri.



5) Mendapatkan hasil dekripsi metode *route cipher* "TSMEIYGXGHSJECJMGV".
6) Menentukan kunci variasi *running-key vigenere cipher*. Berikut ini kunci setiap karakter cipherteks.

Tabel 6 Kunci dari Setiap Karakter Cipherteks Variasi Running-key Vigenere Cipher

C_i	I	T	F	M	J	B	S	L	O	G	G	L	S	K	I	N	E	E
K_i	K	E	A	D	I	L	A	N	S	O	S	I	A	L	B	A	G	I

7) Melakukan perhitungan *vigenere cipher* menggunakan rumus $P_i = (C_i - K_i)\ mod\ 26$
$C_1\ (T,K) = (P_1 - K_1)\ mod\ 26 = (19-10)\ mod\ 26 = 9\ mod\ 26 = 9$
$C_2\ (S,E) = (P_2 - K_2)\ mod\ 26 = (18-4)\ mod\ 26 = 14\ mod\ 26 = 14$
$C_3\ (M,A) = (P_3 - K_3)\ mod\ 26 = (12-0)\ mod\ 26 = 12\ mod\ 26 = 12$
$C_4\ (E,D) = (P_4 - K_4)\ mod\ 26 = (4-3)\ mod\ 26 = 1\ mod\ 26 = 1$ \
$C_5\ (I,I) = (P_5 - K_5)\ mod\ 26 = (0-0)\ mod\ 26 = 0\ mod\ 26 = 0$
$C_6\ (Y,L) = (P_6 - K_6)\ mod\ 26 = (24-11)\ mod\ 26 = 13\ mod\ 26 = 13$
$C_7\ (G,A) = (P_7 - K_7)\ mod\ 26 = (6-0)\ mod\ 26 = 6\ mod\ 26 = 6$
$C_8\ (X,N) = (P_8 - K_8)\ mod\ 26 = (23-13)\ mod\ 26 = 10\ mod\ 26 = 10$
$C_9\ (G,S) = (P_9 - K_9)\ mod\ 26 = (6-18)\ mod\ 26 = -12\ mod\ 26 = 14$
$C_{10}\ (H,O) = (P_{10} - K_{10})\ mod\ 26 = (7-14)\ mod\ 26 = -7\ mod\ 26 = 19$
$C_{11}\ (S,S) = (P_{11} - K_{11})\ mod\ 26 = (0-0)\ mod\ 26 = 0\ mod\ 26 = 0$
$C_{12}\ (J,I) = (P_{12} - K_{12})\ mod\ 26 = (9-1)\ mod\ 26 = 1\ mod\ 26 = 1$
$C_{13}\ (E,A) = (P_{13} - K_{13})\ mod\ 26 = (4-0)\ mod\ 26 = 4\ mod\ 26 = 4$
$C_{14}\ (C,L) = (P_{14} - K_{14})\ mod\ 26 = (2-11)\ mod\ 26 = -9\ mod\ 26 = 17$

$$C_{15}\ (J, B) = (P_{15} - K_{15})\ mod\ 26 = (9 - 1)\ mod\ 26 = 8\ mod\ 26 = 8$$
$$C_{16}\ (M, A) = (P_{16} - K_{16})\ mod\ 26 = (12 - 0)\ mod\ 26 = 12\ mod\ 26 = 12$$
$$C_{17}\ (G, G) = (P_{17} - K_{17})\ mod\ 26 = (0 - 0)\ mod\ 26 = 0\ mod\ 26 = 0$$
$$C_{18}\ (V, I) = (P_{18} - K_{18})\ mod\ 26 = (21 - 8)\ mod\ 26 = -13\ mod\ 26 = 13$$

Mendapatkan hasil dekripsi metode *vigenere cipher* variasi *running-key vigenere cipher* "JOMBANG KOTA BERIMAN"

KESIMPULAN

Dari penelitian yang telah dilakukan, dapat ditarik kesimpulan:

1. Pada proses enkripsi menggunakan metode *vigenere cipher* variasi *full vigenere* didapatkan hasil "DFOJZFAUELXJJGASRJ", hasil enkripsi dari metode *vigenere cipher* variasi *auto-key vigenere cipher* dan *route cipher* adalah "DBOLIEENSGSJJGJLGK" dan hasil enkripsi dari metode *vigenere cipher* variasi *running-key vigenere cipher* dan *route cipher* adalah "MYGJJVGMEHGETSIXSC".
2. Sesuai dengan plainteks awal, hasil dekripsi menggunakan metode *vigenere cipher* dengan tiga variasi dan *route cipher* adalah "JOMBANG KOTA BERIMAN"

DAFTAR PUSTAKA

[1] C. Irawan and D. R. I. M. Setiadi, "Implementasi ALgoritma Autokey Cipher dan AES-128 Pada Enkripsi File," *Prosiding SENDI_U,* pp. 335-339, 2019.

[2] D. Ratna, "Implementasi ALgoritma Rail Fence Cipher Dalam Keamanan Data Gambar 2 Dimensi," *Jurnal Pelita Informatika,* vol. 7, no. 1, pp. 38-42, 2018.

[3] M. A. Maricar and N. P. Sastra, "Efektivitas Pesan Teks dengan Cipher Subtitusi, Vigenere Cipher dan Cipher Transposisi," *Majalah Ilmuah teknologi Elektro,* vol. 17, no. 1, pp. 59-65, 2018.

[4] H. Mukhtar, Kriptografi untuk Keamanan Data, Yogyakarta: Deepbublish, 2018.

[5] Efrandi, Asnawati and Yupiyanti, "Aplikasi Kriptografi Pesan Menggunakan ALgoritma Vigenere Cipher," *Jurnal Media Infotama,* vol. 10, no. 2, pp. 120-128, 2014.

[6] A. Hariati, K. Hardayanti and W. E. Putri, "Kombinasi Algoritma PLayfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks," *Publikasi Jurnal & Penelitian Teknik Informatika,* vol. 2, no. 2, pp. 13-17, 2018.

[7] A. Doni, Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi, Yogyakarta: CV: Andi Offset, 2008.

[8] S. Rifqi, Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java, Yogyakarta: CV Andi Offet, 2012.

[9] T. T. Safei, "Pengukuran dan Pengujian Kekuatan Algoritma Auto-key Vigenere Cipher," *Makalah IF3058,* pp. 1-6, 2012.

[10] A. Fauzi, A. Septiana and I. P. Aliansa, "Analisis Perbandingan Full Vigenere Cipher, Auto-key Vigenere Cipher dan Running-key Vigenere Cipher," pp. 3-4, 2016.

[11] R. Munir, Kriptografi Untuk Keamanan Data, Yogyakarta: Deepublish, 2018.

[12] N. Fitri, "Perancangan Aplikasi Penyandian File Teks Menggunakan Algoritma Route Cipher Berbasis Desktop," *Jurnal Pelita Informatika,* vol. 8, no. 1, 2019.

[13] N. D. Girsang, H. Siagian, M. H. Santoso, A. Wahyudi and B. A. Sitorus, "Kombinasi Algoritma Kriptografi Transposisi Rail Fence Cipher dan Route Cipher," *Prosiding Seminar Nasional Teknologi Informatika,* vol. 2, no. 1, pp. 1-4, 2019.

[14] S. D. Nasution, M. Syahrizal, G. L. Ginting and R. Rahim, "Data Security Using Vigenere Cipher dan Goldbach Codes Algorithm," *Internationa Journal of Engineering Research & Technology (IJERT),* vol. 6, no. 1, pp. 360-363, 2017.

[15] S. A. Halim, "Super Enkripsi Dengan Menggunakan CIpher Subtitusi dan Cipher Transposisi," *Makalah F5054-2007-A-080,* 2007.