

Implementasi Vigenere Chiper dengan Menggunakan MATLAB R2015b

Ayyubi Ahmad

Program Studi Matematika, FMIPA, Universitas Ahmad Dahlan Yogyakarta ayyubiahmad1@gmail.com

Abstrak—Kriptografi merupakan cabang dari ilmu matematika yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak bertanggung jawab. Kerahasiaan dan keamanan suatu pesan menjadi kebutuhan bagi pengirim dan penerima pesan agar informasi tidak disalahgunakan oleh pihak yang tidak bersangkutan. Salah satu jenis metode dari kriptografi adalah *Vigenere Chiper*. Pada artikel ini terdapat modifikasi pada proses enkripsi dan dekripsi kriptografi *Vigenere Chiper* berupa penambahan angka, operasi matematika, dan beberapa tanda baca, juga akan dijelaskan mengenai penerapan enkripsi dan dekripsi kriptografi *Vigenere Chiper* serta membuat program simulasinya menggunakan aplikasi MATLAB R2015b.

Kata kunci: kriptografi, vigenere chiper, matlab R2015b

I. PENDAHULUAN

Perkembangan teknologi informasi dari tahun ke tahun selalu mengalami perkembangan yang sangat pesat sehingga seseorang dapat melakukan pertukaran informasi jauh lebih mudah. Kerahasiaan dan keamanan informasi menjadi kebutuhan terpenting dalam berkomunikasi agar pesan yang dikirim dan diterima tidak disalahgunakan oleh pihak-pihak yang kurang bertanggung jawab.

Kriptografi merupakan cara untuk menjaga kerahasiaan dan keamanan informasi yang ditukarkan dengan mengubah pesan ke dalam bentuk kode-kode yang hanya diketahui oleh pengirim dan penerima pesan yang dimana pesan tersebut mengandung informasi. Selain itu, kriptografi menyediakan sekumpulan teknik yang bertujuan menjaga kerahasiaan dan keamanan informasi sehingga pihak lain tidak dapat mengetahui isi pesan yang dilakukan oleh pengirim dan penerima.

Vigenere chiper merupakan salah satu metode dari kriptografi. *Vigenere chiper* ditemukan oleh seorang diplomat sekaligus kriptolog Prancis, Blaise de Vigenere, pada abad XVI. Pada pengkodean *vigenere chiper*, setiap karakter pada *plaintext* dapat dienkripsikan dengan kunci yang berbeda. Karakter pertama pada *plaintext* dienkripsikan dengan kunci berupa karakter pertama dari kata kunci dan seterusnya. Algoritma pada *vigenere chiper* cukup sederhana dan dapat dikatakan lebih sulit dipecahkan daripada metode lainnya yaitu *caesar chiper*. Proses mengubah informasi menjadi kode disebut enkripsi dan proses mengubah kode menjadi informasi disebut dekripsi.

Pada artikel ini dilakukan modifikasi pada proses enkripsi dan dekripsi *vigenere chiper* dengan menambahkan angka, operasi matematika, dan beberapa tanda baca. Hal ini bertujuan agar pihak yang tidak bersangkutan sulit memecahkan sistem keamanan informasi. Pengujian enkripsi dan dekripsi diimplementasikan menggunakan aplikasi MATLAB R2015b.

II. METODE PENELITIAN

A. Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari kata *crypto* dan *graphia*. *Crypto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Kriptografi juga dapat diartikan ilmu atau seni untuk menjaga keamanan pesan.

Pada prinsipnya kriptografi terdiri dari 4 komponen utama yaitu:

- *Plaintext*, yaitu pesan asli yang ingin dikirimkan dan dijaga keamanannya.
- *Chipertext*, yaitu pesan yang telah dikodekan (disandikan) sehingga siap dikirimkan.

- *Key*, yaitu kunci untuk melakukan teknik kriptografi.
- *Algorithm*, yaitu metode untuk melakukan proses enkripsi dan dekripsi.

Kemudian pada kriptografi terdapat 2 proses dasar yaitu enkripsi dan dekripsi. Enkripsi adalah proses untuk menyandikan pesan yang dapat dibaca (*plaintext*) menjadi pesan acak yang tidak dapat dibaca (*chipertext*), sedangkan dekripsi adalah proses untuk memperoleh kembali *plaintext* dari *chipertext*.



GAMBAR 1. MEKANISME KRIPTOGRAFI

Secara matematis prosesnya dapat dinyatakan sebagai berikut: a.

Proses enkripsi

$$C = E(M) \text{ Keterangan:}$$

- M = pesan asli
- E = proses enkripsi
- C = pesan dalam bahasa sandi

b. Proses dekripsi

$$M = D(C) \text{ Keterangan:}$$

- M = pesan asli
- D = proses dekripsi
- C = pesan dalam bahasa sandi

B. Vigenere Chiper

Vigenere chiper adalah metode enkripsi abjad majemuk manual (*polyalphabetical substitution chiper*). Algoritma ini ditemukan oleh seorang diplomat sekaligus kriptolog Prancis, Blaise de Vigenere, pada abad XVI. Metode ini dipublikasikan pada tahun 1856, dan sekitar dua ratus tahun setelahnya, pada abad XIX, *vigenere chiper* digunakan oleh tentara konfederasi pada Perang Sipil Amerika.

Vigenere chiper pada dasarnya menggunakan teknik yang sama dengan *caesar chiper*. Perbedaannya adalah pada *vigenere chiper* setiap karakter pada *plaintext* dapat dienkripsikan dengan kunci yang berbeda. Karakter pertama pada *plaintext* dienkripsikan dengan kunci berupa karakter pertama dari kata kunci dan seterusnya. Sifat polialfabetik yang dimiliki oleh *vigenere chiper* diimplementasikan dengan bujur sangkar *Vigenere*. Sifat periodiknya terlihat apabila panjang kunci lebih kecil daripada panjang *plaintext*, kunci dapat diulang penggunaannya sampai panjang kunci sama dengan panjang *plaintext*. Jika panjang kunci hanya satu karakter, enkripsinya sama seperti *caesar chiper*.

Bujur sangkar *Vigenere* digunakan untuk mempermudah proses enkripsi dengan *vigenere chiper*. Kolom paling kiri dari bujur sangkar menyatakan karakter kunci, sedangkan baris paling atas menyatakan karakter *plaintext*. Setiap baris dalam bujur sangkar menyatakan karakter-karakter *chipertext* yang diperoleh dengan *caesar chiper* dimana pergeseran karakter *plaintext* ditentukan oleh nilai desimal karakter kunci tersebut.

TABEL 1. BUJUR SANGKAR VIGENERE CHIPER

	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

K u n c i	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

Cara menggunakan bujur sangkar *vigenere chiper* adalah sebagai berikut. Tarik garis vertikal dari karakter *plaintext* ke bawah, lalu tarik garis horizontal dari karakter kunci ke kanan. Perpotongan kedua garis tersebut menyatakan karakter *chipertext* dari karakter *plaintext* yang bersangkutan. Secara matematis, jika kunci K dengan panjang m adalah rangkaian karakter-karakter $K = k_1, \dots, k_m$ dimana k_i didapat dari banyaknya pergeseran pada alfabet ke- i , *plaintext* adalah rangkaian p_1, p_2, \dots, p_m , dan *chipertext* adalah rangkaian c_1, c_2, \dots, c_m , ketiganya dapat dinyatakan dengan formula. Misalkan m menentukan beberapa nilai *integer* positif. Diberikan $P=C=K=(Z_{26})^m$. Untuk sebuah kunci $K = (k_1, k_2, \dots, k_m)$, kita definisikan dengan persamaan berikut:

$$e_k(c_1, c_2, \dots, c_m) = (p_1 + k_1, p_2 + k_2, \dots, p_m + k_m) \text{ mod } 26$$

$$d_k(p_1, p_2, \dots, p_m) = (c_1 - k_1, c_2 - k_2, \dots, c_m - k_m) \text{ mod } 26$$

dimana semua operasi berbasis pada Z_{26} .

Kriptografi *vigenere chiper* menggunakan 26 huruf alfabet, maka kemungkinan pergeseran huruf yang terjadi dari 0 sampai 25. Untuk mengembangkan kriptografi *vigenere chiper* dapat menambahkan angka, operasi matematika berupa penjumlahan (+), pengurangan (-), perkalian (*), pembagian (/), dan beberapa tanda baca berupa titik (.), koma (,), tanda tanya (?), dan tanda seru (!).

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 1 2 3 4 5 6 7 8 9 0 + - * / . , ? !

Adanya penambahan ini mengakibatkan pengujian enkripsi dan dekripsi bekerja pada modulo 44. Karena terdapat 44 kode, maka kemungkinan pergeseran huruf yang terjadi dari 0 sampai 43. Maka persamaan enkripsi dan dekripsi yang digunakan adalah

$$e_k(c_1, c_2, \dots, c_m) = (p_1 + k_1, p_2 + k_2, \dots, p_m + k_m) \text{ mod } 44$$

$$d_k(p_1, p_2, \dots, p_m) = (c_1 - k_1, c_2 - k_2, \dots, c_m - k_m) \text{ mod } 44$$

enkripsi pada *vigenere chiper* dilakukan dengan cara berikut:

- Ubah kunci dan *plaintext* ke dalam urutan bilangan *integer*.
- Tambahkan nilai K dan *plaintext* dengan mereduksinya sebagai penjumlahan modulo 44, dan apabila ukuran *plaintext* lebih panjang daripada kunci, penjumlahan K dilakukan secara periodik. Artinya, bila K sudah mencapai nilai terakhir, proses akan diulang kembali pada K untuk nilai dengan urutan pertama.
- Konversikan kembali urutan bilangan hasil penjumlahan K dan *plaintext*. Proses dekripsi pada *vigenere chiper* dilakukan dengan cara berikut:
 - Ubah kunci dan *chipertext* ke dalam urutan bilangan *integer*.
 - Pada masing-masing urutan bilangan yang merupakan *chipertext*, kurangkan dengan nilai K dan reduksikan sebagai pengurangan modulo 44.
 - Konversikan kembali urutan bilangan hasil pengurangan *chipertext* dan K .

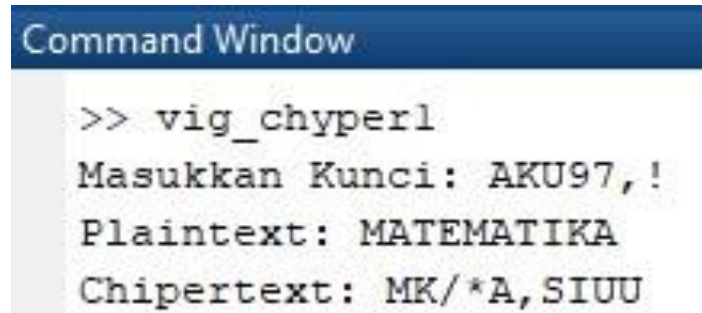
III. HASIL DAN PEMBAHASAN

Dengan perkembangan teknologi yang sangat pesat, pengujian ini dilakukan dengan menggunakan aplikasi MATLAB R2015b agar pembaca mengerti dan memahami bagaimana jika sebuah metode diterapkan dalam menyelesaikan masalah.

A. Pengujian Enkripsi dengan Matlab R2015b dan manual

Bentuk input pada Matlab R2015b untuk enkripsi sebagai berikut:

```
l=['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','1','2','3','4','5','6','7','8','
9','0','+','-','*','/','.','!','?','!'];
k=input('Masukkan Kunci: ','s');
s11=size(k); s1=s11(2);
m=input('Plaintext: ','s');
s22=size(m); s2=s22(2); if s2<=s1
v=1:s2; k=[k(v)]; elseif
(s1<s2) && (s2<2*s1) s3=s2-s1;
v=1:s3; k=[[k],[k(v)]]; else
s2>2*s1 s3=s2-2*s1; v=1:s3;
k=[[k],[k],[k(v)]]; end for i=1:s2
vec1(i)=find(l==(m(i)))-1;
vec2(i)=find(l==k(i))-1; end
vec=vec1+vec2+1; for i=1:s2 if
vec(i)>44
vec(i)=mod(vec(i),44); end end
for i=1:s2 vecf(i)=l(vec(i));
end disp(['Chipertext:
',num2str(vecf)])
```



GAMBAR 2. TAMPILAN HASIL PENGUJIAN ENKRIPSI

Proses secara manual untuk enkripsi sebagai berikut:

Diketahui *plaintext*nya adalah **MATEMATIKA**, dimana pada urutan *chiper* “M” adalah 13, “A” adalah 1, “T” adalah 20, dan seterusnya. Kuncinya adalah **AKU97,!**, dimana pada urutan “A” adalah 0, “K” adalah 10, dan seterusnya, maka dengan transformasi *vigenere chiper*, menjadi

$$\begin{aligned}
 e_1 &= (13 + 0) \bmod 44 = 13, \text{ (artinya 13 pada } \textit{plaintext} \text{ menjadi 13 pada } \textit{chipertext} \text{ yaitu "M")} \\
 e_2 &= (1 + 10) \bmod 44 = 11, \text{ (artinya 1 pada } \textit{plaintext} \text{ menjadi 11 pada } \textit{chipertext} \text{ yaitu "K")} \\
 e_3 &= (20 + 20) \bmod 44 = 40, \text{ (artinya 20 pada } \textit{plaintext} \text{ menjadi 40 pada } \textit{chipertext} \text{ yaitu "}")} \\
 e_4 &= (5 + 34) \bmod 44 = 39, \text{ (artinya 5 pada } \textit{plaintext} \text{ menjadi 39 pada } \textit{chipertext} \text{ yaitu "*"})} \\
 e_5 &= (13 + 32) \bmod 44 = 1, \text{ (artinya 13 pada } \textit{plaintext} \text{ menjadi 1 pada } \textit{chipertext} \text{ yaitu "A")} \\
 e_6 &= (1 + 41) \bmod 44 = 42, \text{ (artinya 1 pada } \textit{plaintext} \text{ menjadi 42 pada } \textit{chipertext} \text{ yaitu ",")} \\
 e_7 &= (20 + 43) \bmod 44 = 19, \text{ (artinya 20 pada } \textit{plaintext} \text{ menjadi 19 pada } \textit{chipertext} \text{ yaitu "S")} \\
 e_8 &= (9 + 0) \bmod 44 = 9, \text{ (artinya 9 pada } \textit{plaintext} \text{ menjadi 9 pada } \textit{chipertext} \text{ yaitu "I")} \\
 e_9 &= (11 + 10) \bmod 44 = 21, \text{ (artinya 11 pada } \textit{plaintext} \text{ menjadi 21 pada } \textit{chipertext} \text{ yaitu "U")} \\
 e_{10} &= (1 + 20) \bmod 44 = 21, \text{ (artinya 1 pada } \textit{plaintext} \text{ menjadi 21 pada } \textit{chipertext} \text{ yaitu "U")}
 \end{aligned}$$

B. Pengujian Dekripsi dengan Matlab R2015b dan manual

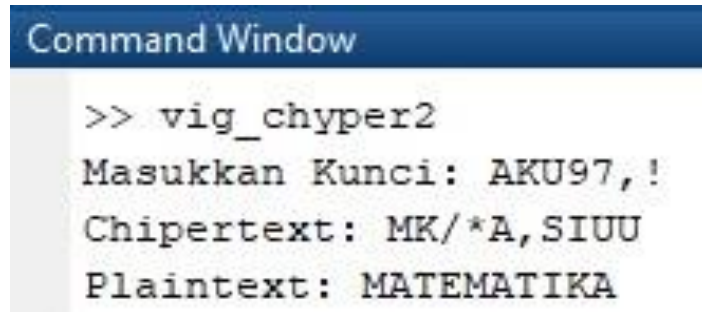
Bentuk input pada Matlab R2015b untuk dekripsi sebagai berikut:

```
l=['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','1','2','3','4','5','6','7','8','
9','0','+','-','*','/','.','!','?','!'];
k=input('Masukkan Kunci: ','s');
s11=size(k); s1=s11(2);
m=input('Chipertext: ','s');
s22=size(m); s2=s22(2); if s2<=s1
v=1:s2; k=[k(v)]; elseif
```

```

(s1<s2) && (s2<2*s1)      s3=s2-s1;
v=1:s3;      k=[[k],[k(v)]]; else
s2>2*s1      s3=s2-2*s1;
v=1:s3;      k=[[k],[k],[k(v)]];
end for i=1:s2
vec1(i)=find(l==m(i))-1;
vec2(i)=find(l==k(i))-1; end
vec=vec1-vec2+1; for i=1:s2      if
vec(i)<44
vec(i)=mod(vec(i),44);      end end
for i=1:s2      vecf(i)=l(vec(i));
end disp(['Plaintext:
',num2str(vecf)])

```



```

Command Window

>> vig_chyper2
Masukkan Kunci: AKU97,!
Chipertext: MK/*A,SIUU
Plaintext: MATEMATIKA

```

GAMBAR 3. TAMPILAN HASIL PENGUJIAN DEKRIPSI

Proses secara manual untuk dekripsi sebagai berikut:

Diketahui *chipertext*nya adalah **MK/*A,SIUU**, dimana pada urutan *chiper* “M” adalah 13, “K” adalah 11, “/” adalah 40, dan seterusnya. Kuncinya adalah **AKU97,!**, dimana pada urutan “A” adalah 0, “K” adalah 10, dan seterusnya, maka dengan transformasi *vigenere chiper*, menjadi

$$d_1 = (13 - 0) \bmod 44 = 13, \text{ (artinya 13 pada } \textit{plaintext} \text{ menjadi 13 pada } \textit{chipertext} \text{ yaitu “M”)}$$

$$d_2 = (11 - 10) \bmod 44 = 1, \text{ (artinya 11 pada } \textit{plaintext} \text{ menjadi 1 pada } \textit{chipertext} \text{ yaitu “A”)}$$

$$d_3 = (40 - 20) \bmod 44 = 20, \text{ (artinya 40 pada } \textit{plaintext} \text{ menjadi 20 pada } \textit{chipertext} \text{ yaitu “T”)}$$

$$d_4 = (39 - 34) \bmod 44 = 5, \text{ (artinya 39 pada } \textit{plaintext} \text{ menjadi 5 pada } \textit{chipertext} \text{ yaitu “E”)}$$

$$d_5 = (1 - 32) \bmod 44 = 13, \text{ (artinya 1 pada } \textit{plaintext} \text{ menjadi 13 pada } \textit{chipertext} \text{ yaitu “M”)}$$

$$d_6 = (42 - 41) \bmod 44 = 1, \text{ (artinya 42 pada } \textit{plaintext} \text{ menjadi 1 pada } \textit{chipertext} \text{ yaitu “A”)}$$

$$d_7 = (19 - 43) \bmod 44 = 20, \text{ (artinya 19 pada } \textit{plaintext} \text{ menjadi 20 pada } \textit{chipertext} \text{ yaitu “T”)}$$

$$d_8 = (9 - 0) \bmod 44 = 9, \text{ (artinya 9 pada } \textit{plaintext} \text{ menjadi 9 pada } \textit{chipertext} \text{ yaitu “I”)}$$

$$d_9 = (21 - 10) \bmod 44 = 11, \text{ (artinya 21 pada } \textit{plaintext} \text{ menjadi 11 pada } \textit{chipertext} \text{ yaitu “K”)}$$

$$d_{10} = (21 - 20) \bmod 44 = 1, \text{ (artinya 21 pada } \textit{plaintext} \text{ menjadi 1 pada } \textit{chipertext} \text{ yaitu “A”)}$$

IV. SIMPULAN DAN SARAN

Pada artikel ini dijabarkan kriptografi *vigenere chiper* yang masih sederhana, kemudian dilakukan modifikasi algoritma *vigenere chiper* untuk mengatasi hal-hal yang masih belum optimal. Modifikasi tersebut dilakukan pada proses enkripsi dan dekripsi dengan menambahkan angka, operasi matematika, dan beberapa tanda baca. Modifikasi tersebut bertujuan agar pihak-pihak yang tidak bersangkutan sulit untuk memecahkan sistem keamanan informasi. Pengujian enkripsi dan dekripsi diimplementasikan dengan aplikasi MATLAB R2015b. Untuk pengembangan lebih lanjut pada kriptografi *vigenere chiper* dapat dilakukan dengan menambahkan tanda baca lainnya dan penggunaan huruf kecil dalam input *plaintext*.

UCAPAN TERIMA KASIH

Syukur Alhamdulillah senantiasa penulis panjatkan kehadiran Allah SWT yang memiliki keistimewaan dan pemberian segala kenikmatan baik iman, kesehatan, dan kekuatan dalam penyusunan makalah ini. Shalawat dan salam senantiasa turunkan kepada nabi Muhammad SAW, keluarga, para sahabatnya, dan umatnya sampai akhir zaman.

Pada kesempatan ini penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada Ibu Dian Ariesta Yuwaningsih, M.Sc. dan Ibu Dian Eka Wijayanti, M.Si. selaku Dosen Pembimbing, di sela-sela rutinitasnya namun tetap meluangkan waktunya untuk memberikan petunjuk, dorongan, saran, dan arahan hingga selesainya penulisan makalah ini.

Ucapan terima kasih juga saya sampaikan kepada Bapak, Ibu, Kakak-kakakku tercinta dengan penuh kasih sayang dan kesabaran yang telah memberikan dukungan dalam penulisan makalah ini.

Akhirnya kepada Allah SWT jualah senantiasa penulis berharap semoga segala sesuatunya dengan tulus dan ikhlas penulis akan selalu mendapat limpahan rahmat dan karunia-Nya, Amin.

DAFTAR PUSTAKA

- [1] Schneier. Bruce, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Second Edition, New York: John Wiley & Sons, Inc.1996.
- [2] Setyaningsih. Emy, "Kriptografi & Implementasinya menggunakan MATLAB", Yogyakarta: Penerbit Andi, 2015.
- [3] Stinson. R. D., "Cryptography Theory and Practice", New York: Chapman & Hall/CRC, 1995.
- [4] Buchmann. J. A., "Introduction to Cryptography", New York: Springer-Verlag, 2000.
- [5] Munir. R., "Kriptografi", Bandung: Informatika, 2006. [6] Rosenthal. J., "Handbook of Cryptography", Zurich: University of Zurich, 2005.