Pergeseran Kemiringan pada *Vigènere Chiper*

YulieAnneria Sinaga – NIM :13504085 [1)]
1) Jurusan Teknik Informatika ITB, Bandung 40116, email: if14085@students.if.itb.ac.id

Abstract – *Terdapat metode-metode untuk menentukan kunci Vigènere chiper, seperti Metode Kasiski untuk menentukan panjang kunci (n). Setelah mendapatkan panjang kunci, pemecahan kunci dapat dilanjutkan dengan teknik analisis frekuensi. Teknik ini dimulai dengan mengelompokan seluruh chiper berdasarkan urutan huruf dari kelompok huruf pertama sampai kelompok huruf ke-n. Kemudian teknik analisis frekuensi dilakukan pada setiap kelompok huruf. Metode dalam memecahkan chiperteks ini dapat dipersulit dengan melakukan metode penggeseran kemiringan pada Vigènere chiper.*

Pergeseran kemiringan pada Vigènere chiper dilakukan dengan menyusun plainteks menjadi bentuk segitiga siku-siku yang membesar di bagian bawah. Jumlah pergeseran menentukan kemiringan segitiga, semakin besar jumlah pergeseran maka kemiringan semakin besar. Tinggi segitiga dibatasi sebanyak 4 baris, apabila jumlah huruf plainteks melebihi 4 baris maka dibentuk segitiga baru lagi sampai akhir plainteks.

Tujuan dilakukan pergeseran ini adalah untuk mempersulit kriptanalis pada saat menentukan panjang kunci dan melakukan pengelompokan huruf pada teknik analisis frekuensi. Sehingga untuk dekripsi chiper tidak hanya dibutuh kunci tetapi juga jumlah pergeseran m. Pada makalah akan dibahas mengenai konsep, implementasi dan pengujian metode penggeseran kemiringan pada Vigènere chiper ini. Serta dilakukan perbandingan-perbandingan kekuatan chiperteks dengan variasi-variasi lainnya pada metode ini yaitu dengan mencoba berbagai nilai m.

Kata Kunci*: Vigènere chiper, pergeseran, plainteks, chiperteks, metode kasiski.*

1. PENDAHULUAN

Vigènere chiper merupakan contoh terbaik dari *chiper* abjad-majemuk (*polyalphabetic subtitution chiper*) 'manual'. Algoritma ini ditemukan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16. *Vigènere chiper* digunakan oleh tentara Konfiderasi (*Confiderate Army*) pada Perang Sipil Amerika (*American Civil War*). Perang Sipil terjadi setelah *Vigènere Chiper* berhasil dipecahkan[1].

Vigènere chiper menggunakan bujursangkar *Vigènere* untuk melakukan enkripsi (lihat gambar 1). Kolom paling kiri dari bujursangkar menyatakan huruf-huruf kunci, sedangkan baris paling atas menyatakan huruf-huruf plainteks[2].

Plaintext (X-Axis)

Key (Y-Axis)

	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 1 : Bujursangkar *Vigènere*

Setiap baris bujursangkar menyatakan huruf-huruf chiperteks yang diperoleh dengan *Caesar chiper*, yang mana jauh pergeseran huruf plainteks ditentukan oleh nilai desimal dari huruf kunci tersebut (di sini, a=0, b=1, c=2,…,z=25). Sebagai contoh huruf kunci c (=2) menyatakan huruf plainteks digeser sejauh 2 huruf ke kanan (dari susunan alfabetisnya) [1]. Kunci digunakan secara berulang-ulang, misalnya kunci yang digunakan adalah KEY maka :

Kunci: `KEYKEYK`
Plainteks: `MESSAGE`
Cipherteks: `WIRCEEO`

Vigènere chiper tidak menerapkan teknik *diffusion* sama sekali, *chiper* ini hanyalah variasi dari *Caesar chiper*. *Chiper* ini diperkirakan tidak dapat dipecahkan selama kurang lebih 300 tahun, sampai akhirnya pada tahun 1863, Feidrich Kasiski berhasil menemukan metode untuk memecahkannya [3]. Metode ini ditemukan berdasarkan kenyataan bahwa kunci mengalami perulangan dan bahasa pada umumnya mengalami perulangan juga. Apabila diberikan pesan yang jauh lebih panjang dari pada kunci, maka kunci akan beberapa kali mengenkripsi himpunan huruf yang sama dengan himpunan huruf sebelumnya yang dienkripsi dengan kunci yang sama [4]. Hal ini menciptakan pola yang sederhana dari perulangan sekumpulan huruf. Dengan mencari frekuensi antara sekumpulan huruf yang berulang tersebut dan memfaktorkannya kita dapat

menemukan panjang kunci yang diiginkan. Dengan didapatkannya panjang kunci, maka kunci akan mudah ditemukan dengan menggunakan teknik analisis frekuensi.

Teknik analisis frekuensi pada sekumpulan huruf *Caesar chiper* dapat digunakan untuk menemukan kunci, dengan didapatkannya panjang kunci melalui metode Kasiski.

Dengan adanya komputer, *Vigènere chiper* menjadi semakin mudah untuk dipecahkan. Kebanyakan chiperteks dapat dipecahkan dalam waktu singkat meskipun memiliki kunci yang panjang. Akibatnya *Vigènere chiper* tidak lagi dipercaya dapat memberikan standar keamanan. Oleh karena itu, kriptanalis dapat dipersulit dalam menentukan kunci dengan menggunakan metode penggeseran kemiringan pada *Vigènere chiper*.

Pergeseran kemiringan pada *Vigènere chiper* dilakukan dengan menyusun plainteks menjadi bentuk segitiga siku-siku yang membesar di bagian bawah. Jumlah pergeseran menentukan kemiringan segitiga, semakin besar jumlah pergeseran maka kemiringan semakin besar. Tinggi segitiga dibatasi sebanyak 4 baris, apabila jumlah huruf plainteks melebihi 4 baris maka dibentuk segitiga baru lagi sampai akhir plainteks.

Tujuan dilakukan pergeseran ini adalah untuk mempersulit kriptanalis pada saat menentukan panjang kunci dan melakukan pengelompokan huruf pada teknik analisis frekuensi. Sehingga untuk dekripsi *chiper* tidak hanya dibutuh kunci tetapi juga jumlah pergeseran.

2. PERBANDINGAN ANTARA *VIGÈNERE* MURNI DENGAN *VIGÈNERE* YANG MENGGUNAKAN PERGESERAN

2.1. *Vigènere Chiper*

Pada *chiper* abjad majemuk, subtitusi huruf diambil dari alfabet yang berbeda, tergantung dari lokasi huruf plainteks saat ini. Berikut akan diberikan ilustrasi dalam melakukan enkripsi dengan *Vigènere chiper*. Untuk penjelasan mengenai metode ini kita gunakan angka 0-25 untuk mensubtitusikan huruf A-Z [5]. Semua tanda baca dan spasi diabaikan.

a	b	C	d	e	f	g	h	i	j	k	l	m
00	01	02	03	04	05	06	07	08	09	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

Untuk setiap huruf ke-i plainteks Pi yang diberikan memiliki subtitusi huruf chiperteks ke-i Ci dengan rumus sebagai berikut :

$$Ci = (Pi + ki) \bmod 26 \qquad (1)$$

Dimana Ki adalah huruf ke-i pada kunci. Akan tetapi Sebagai contoh, terdapat plainteks yang berisi “A quick brown fox jumps” dan kunci yang digunakan adalah “my key sequence”. Di bawah ditunjukan perulangan kunci yang dituliskan di bawah huruf plainteks dengan urutan yang sama. Di bawah plainteks dan kunci dituliskan angka-angka yang berkorespondensi dengan setiap hurufnya.

A	Q	U	I	C	K	B	R	O	W	N	F	O	X	J	U	M	P	S
00	16	20	08	02	10	01	17	14	22	13	05	14	23	09	20	12	15	18
K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K
10	04	24	10	04	24	10	04	24	10	04	24	10	04	24	10	04	24	10

K	U	S	S	G	I	L	V	M	G	R	D	Y	B	H	E	Q	N	C
10	20	18	18	06	08	11	21	12	06	17	03	24	01	07	04	16	13	02

Sekumpulan huruf di bawah garis horizontal adalah chiperteks. Sebagai contoh, huruf ketiga plainteks U (=20) dan huruf pertama kunci Y (=24) bila dijumlahkan jumlahnya adalah 44 kemudian dimodulo 26 sesuai persamaan (1) sehingga menghasilkan 18 yang berdistribusi dengan huruf S .

Untuk dekripsi chiperteks digunakan rumus sebagai berikut:

$$Pi = (Ci - ki) \bmod 26. \qquad (2)$$

Sebagai contoh, huruf terakhir dari chiperteks C(=02), dikurangi huruf K(=10) pada kunci menghasilkan nilai -8 dengan menggunakan mod 26 sesuai persamaan (2), kita tambahkan 26 sehingga hasil yang diperoleh adalah 18 yaitu huruf S.

Selain cara di atas, proses enkripsi dan dekripsi dapat dilakukan dengan menggunakan bujursangkar *Vigènere*. Bujursangkar *Vigènere* sangat membantu proses *chipering* yang dilakukan secara manual karena setiap huruf plainteks dan kunci sudah dipetakan menjadi sebuah huruf chiperteks [4]. Sehingga tidak diperlukan perhitungan matematis dalam *chipering* secara manual.

2.2. *Vigènere* dengan Pergeseran

Vigènere dengan pergeseran kemiringan merupakan modifikasi dari *Vigènere chiper* biasa. Letak perbedaan dari kedua algoritma ini ialah pada subtitusi huruf plainteks dengan huruf kunci. Pada *Vigènere chiper* biasa setiap huruf plainteks dipasangkan dengan huruf kunci dengan urutan yang sama. Sedangkan pada metode pergeseran ini plainteks disusun dahulu dalam bentuk segitiga dengan suatu nilai pergeseran m, kemudian setiap barisnya dilakukan subtitusi dengan kunci seperti pada

Vigènere chiper biasa. misalnya :

Dengan pergeseran m = 1:

Plainteks	kunci	chiperteks
A	key	K
QU	key	AY
ICK	key	SGI
BROW	key	LVMG
N	key	X
FO	key	PS
XJU	key	HNS
MPS	key	WTQ

Dengan pergeseran m = 2:

Plaintekeks	kunci	chiperteks
AQ	key	KU
UICK	key	EMAU
BROWNF	key	LVMGRD
OXJUMPS	key	YBHEQNC

Baris pertama segitiga selalu dimulai dengan sebuah huruf pertama plainteks, baris ini kita sebut bi, kemudian baris berikutnya b_{i+1} berjumlah *1+ (m*i)*. Jumlah baris pada sebuah segitiga dibatasi menjadi 4 baris saja. Jumlah baris ditentukan menjadi hanya 4 baris tanpa memiliki maksud tertentu.

Apabila kunci yang digunakan adakah rangkaian huruf yang sama seperti AAAA atau BBBB maka hasil *Vigènere chiper* dengan pergeseran dan tanpa pergeseran akan sama. Hal ini disebabkan oleh pergeseran yang terjadi tidak memiliki pengaruh apapun karena setiap huruf tetap dikenai huruf kunci yang sama.

Pergeseran ini akan menyulitkan kriptanalis pada saat akan menentukan panjang kunci, karena kunci tidak digunakan secara berulang-ulang pada jarak yang sama. Selain itu kriptanalis juga akan mengalami kesulitan dalam melakukan pengelompokan huruf pada metode analisis frekuensi.

2.3. Algoritma

Berikut adalah algoritma enkripsi plainteks dengan metode *Vigènere* dengan pergeseran. Algoritma ini menyusun plainteks ke dalam bentuk segitiga siku-siku dengan jumlah pergeseran jumPeg. Segitiga yang dibentuk akan memiliki tinggi 4 baris dan alas sepanjang 4 * jumPeg. Dan fungsi enkripsi Encrypt adalah fungsi yang melakukan subtitusi antara plainteks (setiap baris yang telah mengalami pergeseran) dengan kunci.

```
int i = 0;
 while (i<plainteks.Length)
 {
  int j = 1;
  while (j<5 & i<plainteks.Length)
  {
   int k =0;
   plainTemp = null;
   chiperTemp = null;
   while ( k < (jumPeg * j) &
i<plainteks.Length)
   {
    plainTemp += plainteks[i];
    i++;
    k++;
   }
   chiperTemp = Encrypt(plainTemp,
kunci);
   chiperTemp2 += chiperTemp;
   j++;
  }
  chiperteks = chiperTemp2;
 }
 return chiperteks;
```

Fungsi Encrypt merupakan fungsi enkripsi yang juga digunakan pada enkripsi dengan menggunakan metode *Vigènere chiper* biasa. Fungsi ini menerima parameter plainteks P dan kunci key.

```
for (int i = 0; i < P.Length; i++)
{
 encrypt     +=     Convert.ToString
 (Convert.ToChar(
 (Convert.ToInt16(key[i%key.Length])
 + Convert.ToInt16(P[i])) % 65536));
}
return encrypt;
```

Berikut adalah algoritma dekripsi plainteks dengan metode *Vigènere* dengan pergeseran. Algoritma ini menyusun plainteks ke dalam bentuk segitiga siku-siku dengan jumlah pergeseran jumPeg. Segitiga yang dibentuk akan memiliki tinggi 4 baris dan alas sepanjang 4 * jumPeg. Dan fungsi enkripsi Decrypt adalah fungsi yang melakukan subtitusi antara chiperteks (setiap baris yang telah mengalami pergeseran) dengan kunci

```
int i = 0;
while (i < chiperteks.Length)
{
 int j = 1;
 while (j< 5 & i <chiperteks.Length)
 {
  int k = 0;
  plainTemp = null;
  chiperTemp = null;
  while (k < (jumPeg * j) & i <
chiperteks.Length)
  {
   chiperTemp += chiperteks[i];
   i++;
   k++;
  }
  plainTemp   =   Decrypt(chiperTemp,
kunci);
```

```
  plainTemp2 += plainTemp;
  j++;
  }
  plainteks = plainTemp2;
 }
 return plainteks;
```

Fungsi Decrypt merupakan fungsi dekripsi yang juga digunakan pada enkripsi dengan menggunakan metode *Vigènere chiper* biasa. Fungsi ini menerima parameter chiperteks C dan kunci key.

```
for (int i = 0; i < C.Length; i++)
 {
   decrypt += Convert.ToString
   (Convert.ToChar(
   ((Convert.ToInt16(C[i]) -
   Convert.ToInt16(key[i
   %key.Length])) % 65536)));
}
```

2.4 Kriptanalisis

Metode Kasiski yang digunakan untuk menetukan panjang kunci pada *Vigènere chiper* adalah dengan mamanfaatkan kuntungan bahwa bahasa inggris tidak hanya mengandung perulangan huruf tetapi juga perulangan pasangan huruf atau triple huruf seperti TH,THE, dan sebagainya [1]. Terdapat kemungkinan perulangan ini menghasilkan kriptogram yang berulang. Perhatikan contoh di bawah ini:

Plainteks : `THE QUICK FOX A QUICK`
Kunci : `KEY KEYKE YKE Y KEYKE`
Chiperteks : `DLC AYGMO DYB Y AYGMO`

Pada contoh diatas, `QUICK` dienkripsi menjadi kriptogram yang sama, yaitu `AYGMO`. Tetapi kasus tersebut tidak selalu terjadi. Hal tersebut bisa terjadi karena jarak antara kata yang berulang adalah kelipatan dari panjang kunci, maka kata yang sama tersebut akan muncul menjadi kriptogram yang sama pula pada chiperteks. Untuk kasus di atas, jarak antara Q dengan Q adalah 9 yang merupakan kelipatan dari panjang kunci yaitu 3.

Untuk mendapatkan panjang kunci, semua jarak antara kriptogram yang berulang dihitung. Setelah mendapatkan jarak-jarak antara kriptogram yang berulang, tentukan faktor pembagi yang beririsan dari jarak-jarak tersebut. Kemungkinan besar irisan tersebut merupakan panjang kunci atau kelipatannya[1].

Setelah mendapatkan panjang kunci kita dapat memecahkan kunci dengan teknik analisis frekuensi. Plainteks dibagi-bagi menjadi kelompok huruf sebanyak panjang kunci. Kelompok huruf pertama merupakan huruf-huruf dengan urutan pertama pada kelompok huruf yang telah dikelompok sepanjang kunci. Pengelompokan ini terus dilakukan sampai kelompok huruf dengan urutan ke-panjang kunci. Analisis frekuensi terus dilakukan sampai kelompok huruf terakhir sehingga didapatkan kunci yang dicari.

Metode pergeseran kemiringan pada *Vigènere chiper* dapat mempersulit kriptanalis pada saat akan menentukan panjang kunci karena kunci tidak digunakan secara berulang-ulang pada jarak yang sama. Akan tetapi bukan berarti *chiper* ini tidak dapat dipecahkan. Pola yang sama dapat terjadi apabila ukuran chiperteks cukup panjang dan jumlah pergeserannya besar. Misalnya dengan jumlah pergeseran lebih besar atau sama dengan panjang chiper atau pergeseran sebanyak panjang kunci, metode ini menjadi tidak berguna, karena plainteks kembali menggunakan kunci secara berulang-ulang pada jarak yang sama, sehingga sifat *chiper* menjadi kembali seperti *Vigènere* biasa.

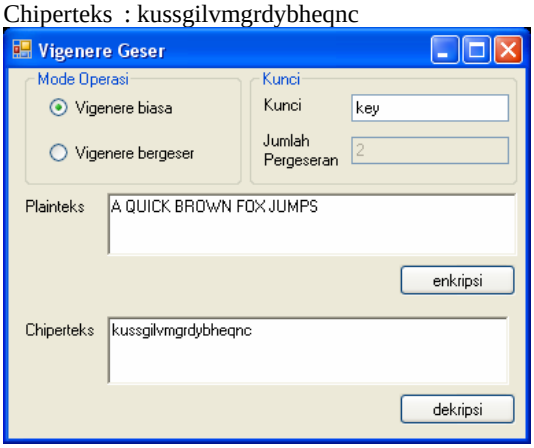
2.5 Implementasi

Aplikasi *Vigènere* Geser merupakan implementasi dari metode *Vigènere chiper* dengan pergeseran kemiringan. Aplikasi ini menerima dua mode operasi yaitu *Vigènere* biasa dan *Vigènere* bergeser untuk memperlihatkan perbandingan antara chiperteks yang dihasilkan dengan kedua metode tersebut. Aplikasi ini membaca plainteks, chiperteks, dan kunci sebagai huruf kecil dan mengabaikan spasi. Hal ini ditujukan untuk memudahkan subtitusi urutan huruf A- Z dengan urutan angka dari 0-25.

3. HASIL DAN PEMBAHASAN

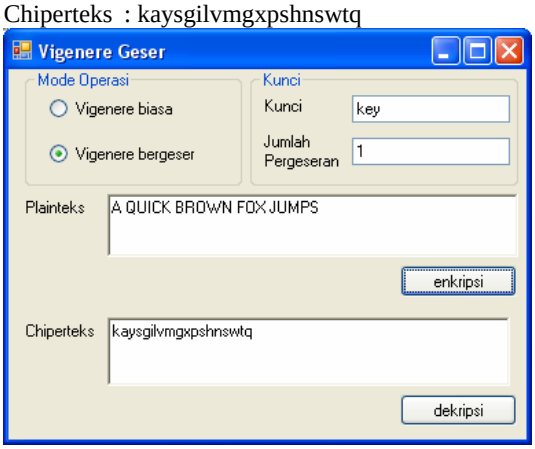
Berikut adalah hasil penggunaan aplikasi yang telah diimplementasi dengan dua mode operasi yaitu *Vigènere* biasa dan *Vigènere* bergeser. Hasil dari penggunaan aplikasi ini dapat menunjukan perbandingan antara mode *Vigènere* biasa dan *Vigènere* dengan pergeseran, selain itu juga akan dilakukan perbandingan antara penggunaan jumlah pergeseran yang berbeda-beda.

Berikut ditunjukan metode *Vigènere* biasa
Plainteks : A QUICK BROWN FOX JUMPS
Kunci : key
Chiperteks : kussgilvmgrdybheqnc



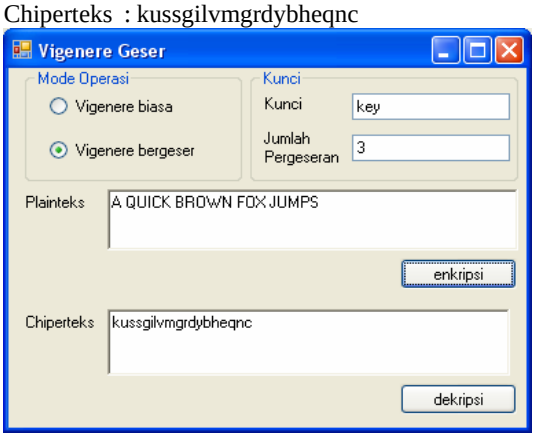
Gambar 2 : Metode *Vigènere* biasa

Berikut ditunjukan metode *Vigènere* bergeser dengan jumlah pergeseran 1.
Plainteks : A QUICK BROWN FOX JUMPS
Kunci : key
Chiperteks : kaysgilvmgxpshnswtq



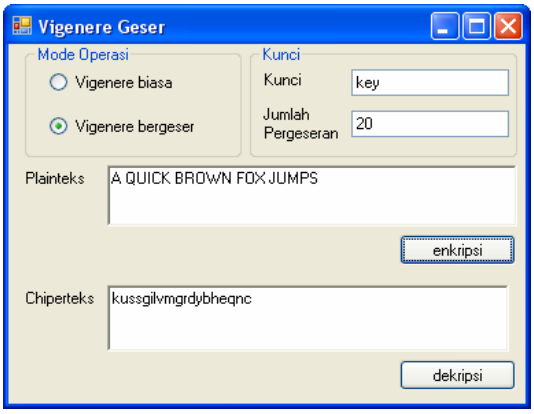
Gambar 3 : *Vigènere* bergeser dengan pergeseran 1

Berikut ditunjukan metode *Vigènere* bergeser dengan jumlah pergeseran = jumlah huruf kunci.
Plainteks : A QUICK BROWN FOX JUMPS
Kunci : key
Chiperteks : kussgilvmgrdybheqnc



Gambar 4 : *Vigènere* bergeser dengan pergeseran = panjang kunci

Hasil enkripsi dari *Vigènere* dengan pergeseran 3 atau sama dengan panjang kunci menunjukan hasil yang sama dengan hasil enkripsi *Vigènere* biasa. Hal ini disebabkan oleh jumlah huruf pada setiap baris segitiga adalah kelipatan panjang kunci, sehingga kunci digunakan berulang-ulang pada plainteks tanpa pergeseran. Sehingga dapat disimpulkan bahwa metode pergeseraan akan tidak berguna apabila dilakukan pergeseran sebanyak panjang kunci.
Berikut ditunjukan metode *Vigènere* bergeser dengan jumlah pergeseran =20.
Plainteks : A QUICK BROWN FOX JUMPS
Kunci : key
Chiperteks : mcssoilvmilpsvbyybq



Gambar 5 : *Vigènere* bergeser dengan pergeseran > panjang plainteks

Dari hasil pergeseran sebanyak 20 huruf di atas dapat disimpulkan apabila pergeseran dilakukan sama besar atau lebih besar dari panjang plainteks maka pergeseran tidak akan berarti apa-apa karena plainteks habis pada baris pertama sehingga tidak terjadi pembentukan segitiga.

4. KESIMPULAN

Metode pergeseran kemiringan ini merupakan modifikasi dari *Vigènere chiper* yang dilakukan untuk menutupi kelemahannya yaitu perulangan kunci dengan jarak yang sama. Metode ini digunakan untuk mempersulit kriptanalis dalam menentukan kunci dengan metode pemecahan yang sudah ada. Akan tetapi metode ini menjadi tidak berguna apabila jumlah pergeseran yang dilakukan lebih besar atau sama dengan panjang chiper dan sama dengan panjang kunci. Jumlah pergeseran yang disarankan untuk mendapatkan manfaat maksimal dari metode ini adalah lebih kecil dari panjang kunci.

DAFTAR REFERENSI

[1] Munir, Rinaldi. *Diktat Kuliah IF5054 Kriptografi*. Program Studi Teknik Informatika, Institut Teknologi Bandung. 2006.

[2] *How The Vigènere Chiper Works : A Detailed Explanation into an Important Cryptographic HistoricalDiscovery.* https://www.securetrust.com/resources/vigenereciipherdetails/. Tanggal akses 18 Oktober 2007, pukul 17.00

[3] Wilson, I. Philip, M. Garcia. “A Modified Version of the Vigenère Algorithm”, IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.3B, March 2006

[4] Schineier, B. *Applied Cryptography*. John Wiley and Sons Inc. New York, New York, 1995.

[5] Faith, Chao. *The Vigènere Chiper*. Department of Mathematics, Golden Gate Universitiy. 2006.