TRIPLE VIGENÈRE CIPHER

Satrio Adi Rukmono – NIM : 13506070
Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jalan Ganesha 10, Bandung 40132
E-mail : r.satrioadi@gmail.com

Abstrak

Makalah ini membahas sebuah teknik enkripsi yang penulis kembangkan untuk mempersulit kriptanalis dalam memecahkan cipherteks dan mendapatkan plainteksnya. Teknik ini penulis sebut dengan *Triple Vigenère Cipher* yang merupakan pengembangan dari *Vigenère Cipher*. *Vigenère Cipher* adalah salah satu metode enkripsi klasik berupa subtitusi polialfabetik yang bersifat simetris. Oleh karena itu metode utama dalam melakukan kriptanalisis untuk *Vigenère Cipher* adalah dengan mencari kunci terlebih dahulu, antara lain menggunakan analisis frekuensi. *Triple Vigenère Cipher* penulis rancang untuk mempersulit analisis frekuensi tersebut.

Ada dua metode penguatan enkripsi yang penulis lihat berpotensi untuk diterapkan pada *Vigenère Cipher*, yaitu *super encryption* dan *triple DES*. *Super encryption* adalah metode enkripsi yang bertujuan mempersulit kriptanalisis dengan menggunakan lebih dari satu metode enkripsi yang berbeda. Plainteks dienkripsi menggunakan algoritma enkripsi yang pertama, kemudian cipherteks hasil enkripsi tersebut dienkripsi lagi dengan algoritma enkripsi yang kedua, dan seterusnya. *Triple DES* adalah salah satu teknik untuk memperkuat enkripsi *DES*, yaitu melakukan enkripsi dengan metode *DES* sebanyak tiga kali terhadap plainteks.

Kedua metode tersebut penulis terapkan dengan melakukan *Vigenère Cipher* berulang kali sebagaimana dalam *triple DES*. Jika pada setiap langkah *Vigenère Cipher* digunakan kunci yang berbeda dan masing-masing memiliki panjang kunci yang berbeda, maka seolah-olah teknik enkripsi yang digunakan berbeda, seperti dalam *super encryption*.

Kata kunci: kriptografi, *vigenère cipher, double vigenère cipher, triple vigenère cipher, super encryption*

1. Pendahuluan

Sejak awal mula ditemukannya kriptografi, metode enkripsi selalu berkembang. Di mulai dari algoritma kriptografi klasik hingga kriptografi modern, menggunakan kunci-simetri maupun tidak, semua perkembangan tersebut terjadi karena satu tujuan yang sama: membuat kriptanalisis sesulit mungkin, dengan kata lain untuk alasan keamanan.

Hingga saat ini sudah banyak terdapat metode enkripsi yang diklaim sangat sulit atau bahkan tidak dapat dipecahkan, seperti *Super Encryption* dan *One-Time Pad*. Namun, setiap metode tersebut memiliki kelemahan. Pada *Super Encryption*, misalnya, diperlukan dua modul untuk melakukan enkripsi atau dekripsi, yaitu modul untuk enkripsi/dekripsi *cipher* substitusi sederhana, dan modul untuk enkripsi/dekripsi *cipher* transposisi. Pada *One-Time Pad*, tentu dibutuhkan saluran komunikasi tambahan yang aman dan terpercaya untuk mengirimkan *key* kepada penerima pesan, serta kebutuhan untuk membuat *key* baru setiap kali ingin melakukan enkripsi.

Penulis telah merancang sebuah pengembangan dari salah satu algoritma kriptografi klasik yang cukup populer, yang berpotensi untuk menjadi *unbreakable cipher*, yaitu pengembangan dari *Vigènere Cipher*. Kelebihan metode yang penulis kembangkan ini adalah kemudahan proses enkripsi/dekripsi (cukup menggunakan satu modul untuk enkripsi/dekripsi), kunci yang

relatif pendek sehingga tidak membutuhkan saluran komunikasi lain untuk mengirim kunci kepada penerima pesan, potensi untuk "kebal" terhadap serangan yang memanfaatkan analisis frekuensi, serta proses enkripsi/dekripsi yang relatif fleksibel, mudah digunakan secara manual maupun dengan bantuan program komputer.

2. *Vigenère Cipher* dan Metode Kasiski

2.1. *Vigenère Cipher*

Vigenère Cipher adalah metode enkripsi abjad-majemuk manual. Algoritma ini ditemukan oleh diplomat sekaligus kriptolog Perancis, Blaise de Vigenère, pada abad XVI. Metode ini dipublikasikan pada tahun 1856, dan sekitar dua ratus tahun setelahnya, pada abad XIX. Babbage dan Kasiski berhasil menemukan cara untuk memecahkan *Vigenère Cipher*.

Vigenère Cipher digunakan oleh Tentara Konfederasi pada Perang Sipil Amerika meskipun sebelum Perang Sipil terjadi, metode enkripsi ini telah berhasil dipecahkan.

Pada dasarnya, *Vigenère Cipher* menggunakan teknik yang sama dengan *Caesar's Cipher*. Bedanya, dalam *Vigenère Cipher* setiap huruf dalam plainteks dapat dienkripsikan menggunakan kunci yang berbeda. Huruf pertama pada plainteks dienkripsikan dengan kunci berupa huruf pertama dari kata kunci, dan seterusnya. Jika panjang kunci lebih kecil daripada panjang plainteks, maka kunci dapat diulang penggunaannya (periodik, dengan periode sama dengan panjang kunci). Jika panjang kunci hanya satu huruf, maka enkripsi sama saja dengan *Caesar's Cipher* biasa.

Bujursangkar *Vigenère* (**Tabel 1**) digunakan untuk mempermudah proses enkripsi dengan *Vigenère Cipher*. Kolom paling kiri dari bujursangkar menyatakan huruf kunci, sedangkan baris paling atas menyatakan huruf plainteks. Setiap baris dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar's Cipher*, yang mana jauh pergeseran huruf plainteks ditentukan oleh nilai desimal huruf kunci tersebut (a=0, b=1, c=2, ..., z=25). Sebagai contoh, huruf kunci o (=15) berarti huruf plainteks digeser sejauh 15 huruf ke kanan pada susunan alfabet.

	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

Tabel 1 – Bujursangkar *Vigenère*

Cara menggunakan Bujursangkar *Vigenère* adalah sebagai berikut: tarik garis vertikal dari huruf plainteks ke bawah, lalu tarik garis horizontal dari huruf kunci ke kanan. Perpotongan kedua garis tersebut menyatakan huruf cipherteks dari huruf plainteks yang bersangkutan.

Contoh penggunaan Bujursangkar *Vigenère* untuk plainteks `'KRIPTOGRAFI'` dan kunci `'cipher'`:

Plainteks	`KRIPTOGRAFI`
Kunci	`cipherciphe`

Untuk huruf pertama, tarik garis vertikal dari huruf `K` dan horizontal dari huruf `c`, maka didapatkan cipherteks yaitu huruf `M` (**Tabel 2**). Selanjutnya lakukan hal yang sama untuk huruf kedua (plainteks `R` dengan kunci `i`), didapatkan chiperteks yaitu huruf `Z`. Lakukan lagi untuk seluruh plainteks yang tersisa, hingga didapatkan hasil akhir

Plainteks	`KRIPTOGRAFI`
Kunci	`cipherciphe`
Cipherteks	`MZXWXFIZPMM`

	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

Tabel 2 – contoh penggunaan Bujursangkar *Vigenère*

Dekripsi pada *Vigenère Cipher* dilakukan dengan cara sebaliknya, yaitu menarik garis horizontal ke kanan dari huruf kunci hingga ditemukan huruf cipherteks yag dituju, kemudian dari huruf cipherteks tersebut tarik garis vertikal ke atas sampai ke huruf plainteks.

2.2. Metode Kasiski

Metode Kasiski (Friedrich Kasiski, 1863) membantu kriptanalis dalam menentukan panjang kunci yang digunakan untuk *Vigenère Cipher*. Nama Kasiski populer dengan metode ini, namun sebenarnya Charles Babbage telah menemukan metode serupa pada tahun 1854. Metode ini memanfaatkan keuntungan bahwa bahasa Inggris tidak hanya mengandung perulangan huruf tetapi juga pasangan huruf atau bahkan triplet seperti `TH`, `THE`, dan sebagainya. Perulangan ini memungkinkan adanya kriptogram yang berulang.

Secara intuitif, dapat dibuat suatu argumen bahwa jika jarak antara dua buah *string* yang berulang di dalam plainteks merupakan kelipatan dari panjang kunci, maka *string* yang sama tersebut akan muncul sebagai kriptogram yang sama pula dalam ciherteks. Untuk menentukan panjang kunci, langkah-langkahnya adalah sebagai berikut:

1. Kriptanalis menghitung semua kriptogram yang berulang dalam cipherteks. Kemudian, jarak antara kriptogram yang berulang dihitung.

2. Kriptanalis menghitung semua faktor dari jarak tersebut. Faktor pembagi menyatakan panjang kunci yang mungkin. Tentukan irisan dari himpunan faktor pembagi tersebut. Nilai yang muncul di dalam irisan menyatakan angka yang muncul pada semua faktor pembagi dari jarak-jarak tersebut. Nilai tersebut mungkin adalah panjang kunci.

Metode ini dapat ditangkal dengan menggunakan panjang kunci yang sama dengan panjang plainteks. Namun, tentu sulit untuk mengingat kunci yang begitu panjang (jika plainteksnya panjang) atau perlu mekanisme lain untuk mengirim kunci kepada penerima pesan.

3. *Triple Vigenère Cipher* dan konsep yang mendasarinya

3.1. Konsep yang mendasari *Triple Vigenère Cipher*

3.1.1. Sekilas *Super Encryption*

Super Encryption mengkombinasikan metode *cipher* substitusi dengan *cipher* transposisi. Tujuannya adalah memperoleh *cipher* yang lebih kuat daripada hanya satu *cipher* saja.

Metode ini dilakukan dengan mengenkripsi plainteks menggunakan *cipher* substitusi sederhana seperti *Caesar's Cipher*, lalu hasilnya dienkripsi lagi dengan *cipher* transposisi.

3.1.2. Sekilas *Triple DES*

DES (Data Encryption Standard) adalah salah satu teknik kripografi modern menggunakan *cipher* blok yang populer karena dijadikan standar enkripsi kunci-simetri. Karena *DES* mempunyai potensi kelemahan terhadap *exhaustive key search attack* sebagai akibat panjang kuncinya yang relatif pendek (56 bit), maka orang membuat varian dari *DES* dengan memperbesar ruang kunci tanpa mengubah algoritma. Varian yang paling dikenal adalah

multiple DES, yaitu enkripsi berkali-kali dengan *DES*.

Triple DES atau *TDES* atau *3DES* menggunakan *DES* sebanyak tiga kali. Bentuk sederhana *3DES* yang dikenal dengan mode *EEE* adalah:

Enkripsi:

$C = E_{K3}(E_{K2}(E_{K1}(P)))$

Dekripsi:

$P = D_{K1}(D_{K2}(D_{K3}(C)))$

Selain itu terdapat pula mode *EDE* untuk menyederhanakan *interoperability* antara *DES* dengan *3DES*. Untuk mode ini, dapat digunakan dua buah kunci saja atau tiga buah kunci. Jika hanya menggunakan satu buah kunci, maka hasilnya sama dengan *DES* biasa (*interoperable*).

Dua kunci:

Enkripsi:

$C = E_{K1}(D_{K2}(E_{K1}(P)))$

Dekripsi:

$P = D_{K1}(E_{K2}(D_{K1}(C)))$

Tiga kunci:

Enkripsi:

$C = E_{K3}(D_{K2}(E_{K1}(P)))$

Dekripsi:

$P = D_{K1}(E_{K2}(D_{K3}(C)))$

3.2. *Triple Vigenère Cipher*

3.2.1. Definisi

Triple Vigènere Cipher adalah metode enkripsi dengan cara mengulang teknik *Vigènere Cipher* biasa sebanyak tiga kali dengan menggunakan kunci yang berbeda dengan panjang kunci yang berbeda.

Jika setiap proses enkripsi plainteks P dengan kunci K pada *Vigènere Cipher* dapat disimbolkan sebagai $C=E_K(P)$, maka secara matematis metode *Triple Vigènere Cipher* ini dapat dituliskan sebagai

Enkripsi:

$C = E_{K3}(E_{K2}(E_{K1}(P)))$

Dekripsi:

$P = D_{K1}(D_{K2}(D_{K3}(C)))$

persis seperti pada *3DES*.

3.2.2. Variasi

Seperti pada konsep *3DES*, *Triple Vigènere Cipher* juga dapat divariasikan dengan mode yang berbeda (*EEE* dan *EDE*). Namun perbedaannya adalah pada *Triple Vigènere Cipher*, variasi mode ini tidak mempengaruhi *interoperability* dengan metode *Vigènere Cipher* biasa, sebab berdasarkan definisi yang penulis rancang, setiap tahapan dalam *Triple Vigènere Cipher* dilakukan dengan kunci yang berbeda dengan panjang yang berbeda.

Enkripsi:

$C = E_{K3}(D_{K2}(E_{K1}(P)))$

Dekripsi:

$P = D_{K1}(E_{K2}(D_{K3}(C)))$

Variasi mode ini dikembangkan demi mempersulit proses kriptanalisis lebih jauh lagi.

3.2.3. Contoh

Triple Vigènere Cipher dengan mode *EEE*:

Plainteks (P):
`RUBAH COKELAT YANG LINCAH MELOMPATI ANJING PEMALAS`

Kunci pertama (K_1):
`DELAPAN`

Cipherteks pertama (P'):
`UYMAW CBNIWAI YNQK WICCNK QPLDMCDXT ACJVQK AEBAYDW`

Kunci kedua (K_2):
TUJUH

Cipherteks kedua (P''):
NSVUD VVWCDTC HHXD QRWJGE ZJSWGLXEM ULDCJE JYITSMQ

Kunci ketiga (K_3):
DUA

Cipherteks akhir (C):
QMVXX VYQCGNC KBXG KRZDGH TJVQGOREP OLGWJH DYLNSPK

Triple Vigènere Cipher dengan mode *EDE*:

Plainteks (P):
RUBAH COKELAT YANG LINCAH MELOMPATI ANJING PEMALAS

Kunci pertama (K_1):
DELAPAN

Cipherteks pertama (P'):
UYMAW CBNIWAI YNQK WICCNK QPLDMCDXT ACJVQK AEBAYDW

Kunci kedua (K_2):
TUJUH

Cipherteks kedua (P''):
BEDGP JHEOPH OPTJ RCZIVU QHVEKSTJQA GTPOXQ RKUHEUC

Kunci ketiga (K_3):
DUA

Cipherteks akhir (C):
EYDJJ JKYOSB OSNJ UWZLPU TBVHESWDQD ATSIXT LKXBEXW

3.2.4. Analisis

Pada prinsipnya, mengulang teknik *Vigènere Cipher* sebanyak tiga kali sama saja dengan menjumlahkan setiap kunci terlebih dahulu, kemudian melakukan enkripsi terhadap plainteks menggunakan kunci baru K yang merupakan hasil penjumlahan kunci-kunci tersebut dalam rentang A sampai Z (jika melebihi Z maka kembali ke A dan seterusnya). Pada mode *EDE*, kunci baru K ditentukan dengan mengurangi K_1 dengan K_2 kemudian ditambahkan dengan K_3.

Mode *EEE*:

$K = K_1 + K_2 + K_3$

Mode *EDE*:

$K = K_1 - K_2 + K_3$

Sebagai contoh, perhatikan contoh pertama dari subbagian 3.2.3. Ambil huruf pertama dari plainteks dan masing-masing kunci sebagai sampel. Huruf pertama plainteks adalah R, huruf pertama pada kunci masing-masing adalah D, T, dan D.

```
K = K1 + K2 + K3
  = 'D' + 'T' + 'D'
  = (3 + 19 + 3) mod 26
  = 25 mod 26
  = 25
  = 'Z'
```

Maka hasil enkripsi huruf R dengan kunci Z menghasilkan cipherteks Q. Demikian juga dilakukan dengan seluruh huruf pada kunci sesuai panjang plainteks (45 karakter):

```
K = 'DELAPANDELAPANDELAPANDELAPAN
    DELAPANDELAPANDEL' +
    'TUJUHTUJUHTUJUHTUJUHTUJUHTUJ
    UHTUJUHTUJUHTUJUH' +
    'DUADUADUADUADUADUADUADUADUAD
    UADUADUADUADUADUA'
  = 'ZSUXQTKGYVNJMBKAZJMBGAHFKCUZ
    RLHOYXOWBOUZNHPSS'
```

Terlihat, mengenkripsi plainteks RUBAH COKELAT YANG LINCAH MELOMPATI ANJING PEMALAS menggunakan *Vigènere Cipher* dengan kunci ZSUXQTKGYVNJMBKAZJMBG AHFKCUZRLHOYXOWBOUZNHPSS menghasilkan cipherteks yang sama yaitu QMVXX VYQCGNC KBXG KRZDGH TJVQGOREP OLGWJH DYLNSPK.

Dari sini, terlihat bahwa *Triple Vigènere Cipher* berpotensi untuk mengimbangi kekuatan *One-*

Time-Pad, yaitu mengenkripsi plainteks dengan panjang kunci yang sama dengan panjang plainteks tanpa ada perulangan.

Bagaimana mendapatkan kunci baru K yang panjangnya sama dengan panjang plainteks tanpa adanya perulangan? Penulis merangkum dua syarat untuk ketiga kunci sebagai berikut:

1. Ketiga kunci memiliki panjang yang berbeda dan panjang setiap kunci relatif prima terhadap setiap panjang kunci yang lain. Misalnya pada contoh sebelumnya, K_1 memiliki panjang 7 huruf, K_2 sepanjang 5 huruf, dan K_3 sepanjang 3 huruf.

2. Kelipatan persekutuan terkecil dari panjang ketiga kunci yang digunakan lebih besar dari pada panjang plainteks. Seperti pada contoh sebelumnya, panjang plainteks adalah 45 huruf, sedangkan kelipatan persekutuan terkecil dari 7, 5, dan 3 adalah 105. Oleh karena itu, kunci baru K baru akan mencapai satu periode pada huruf ke-105.

4. Kesimpulan dan Saran

4.1. Kesimpulan

Triple Vigènere Cipher memiliki keunggulan sebagai berikut:

1. Kemudahan proses enkripsi/dekripsi. Proses enkripsi/dekripsi cukup menggunakan satu modul, yaitu modul *Vigènere Cipher* biasa yang digunakan sebanyak tiga kali, tidak seperti *Super Encryption* yang untuk proses enkripsi/dekripsinya dibutuhkan dua modul, yaitu modul untuk *cipher* substitusi dan modul untuk *cipher* transposisi.

2. Proses enkripsi/dekripsi yang relatif fleksibel, mudah digunakan secara manual maupun dengan bantuan program komputer. Untuk proses enkripsi/dekripsi manual cukup digunakan Bujursangkar *Vigènere* sebanyak tiga kali dengan kunci yang berbeda, sedangkan untuk enkripsi/dekripsi dengan bantuan komputer cukup menggunakan perangkat lunak bantuan *Vigènere Cipher yang sudah banyak tersedia di dunia maya dan bebas untuk diunduh*. Pengguna *Vigènere Cipher* tidak perlu membuat perangkat lunak bantu yang khusus.

3. Kekuatan enkripsi sekuat *One-Time-Pad*, jika kunci yang digunakan memenuhi persyaratan yang penulis kemukakan pada subbagian 3.2.4. *One-Time-Pad* merupakan teknik enkripsi yang diklaim tidak dapat dipecahkan menggunakan *exhaustive key search attack*, dan *Triple Vigènere Cipher* pun berpotensi memiliki kekuatan tersebut.

4. Tidak membutuhkan saluran komunikasi lain untuk mengirimkan kunci seperti pada *One-Time-Pad*. Kelemahan pada *One-Time-Pad* adalah panjangnya kunci sehingga tidak mungkin untuk diingat. Oleh karena itu dibutuhkan saluran komunikasi lain yang lebih aman untuk mengirimkan kunci tersebut (dalam bentuk *pad*) kepada penerima pesan. Selain itu, kunci hanya dapat digunakan satu kali, berarti pengiriman kunci harus dilakukan berkali-kali, memperbesar peluang bocornya kunci kepada pihak yang tidak diinginkan. Pada *Triple Vigènere Cipher*, cukup dengan mengingat tiga kunci pendek, asalkan ketiga kunci itu memenuhi persyaratan yang penulis kemukakan pada subbagian 3.2.4., secara virtual sudah didapatkan kunci yang panjangnya sama dengan plainteks dan benar-benar terlihat acak, sehingga begitu serupa dengan kunci pada *One-Time-Pad*.

Namun selain itu *Triple Vigènere Cipher* juga memiliki satu kekurangan, yaitu untuk ukuran plainteks yang besar, sulit untuk dapat menentukan tiga buah kunci yang cukup pendek untuk dapat diingat (tidak perlu dikirim melalui saluran komunikasi yang lain) namun tetap memenuhi syarat kedua untuk kunci yang digunakan bahwa kelipatan persekutuan terkecil dari panjang kunci tidak kurang dari panjang plainteks. Terutama jika plainteks dan kunci berbentuk sedemikian rupa sehingga ada pasangan huruf atau triplet huruf yang sama pada plainteks yang terpisah sejauh kelipatan dari panjang kunci baru K. Dengan demikian, kemungkinan kunci masih dapat dipecahkan oleh kriptanalis menggunakan metode Kasiski.

4.2. Saran

Setelah mempelajari berbagai metode kripografi klasik, penulis melihat bahwa banyak potensi untuk melakukan modifikasi pada algoritma-algoritma yang sederhana tersebut menjadi algoritma baru yang lebih kuat. Secara khusus, potensi tersebut penulis lihat paling besar terdapat pada *Vigènere Cipher*. Oleh karena itu, penulis menyarankan para peminat kriptografi untuk banyak mempelajari dan meng-'oprek' algoritma kriptografi klasik.

DAFTAR PUSTAKA

[1] Munir, Rinaldi, Diktat Kuliah IF5054 Kriptografi, Penerbit ITB 2006