Vigènere Cipher Rotasi Berlapis

Ripandy Adha - NIM 13507115

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jalan Ganesha nomor 10
e-mail: if17115@students.itb.ac.id, ree_p_and_y@yahoo.com

ABSTRAK

Algoritma Kriptografi *Vigènere Cipher* adalah salah satu teknik kriptografi klasik. Algoritma ini menerapkan metode substitusi polialfabetik yang bersifat simetris. *Vigènere Cipher* menggunakan Bujursangkar *Vigènere* untuk melakukan enkripsi, dengan setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar Cipher*. Tujuan awal algoritma *Vigènere Cipher* adalah agar mampu mengurangi korelasi antara frekuensi huruf pada *plainteks*. Akan tetapi, algoritma *Vigènere Cipher* cukup rentan dipecahkan, khususnya ketika plainteks yang akan dienkripsi cukup panjang, sehingga menyebabkan pola yang berulang. Kriptanalis dapat menemukan kunci enkripsi terlebih dahulu dengan cara menganalisa pola yang berulang tersebut, disesuaikan dengan sifat kalimat khususnya pada bahasa inggris. Dalam makalah ini, akan dilakukan sedikit modifikasi terhadap algoritma *Vigènere Cipher*, dengan tujuan untuk meningkatkan keamanan enkripsi dan mempersulit kriptanalis dalam memecahkan cipherteks maupun kunci enkripsi yang menjadi inti dalam enkripsi dengan *Vigènere Cipher*.

Modifikasi terhadap *Vigènere Cipher* adalah dengan melakukan pengulangan enkripsi dengan menggunakan kunci yang sama. Pengulangan dilakukan dengan mengenkripsi satu karakter dengan seluruh karakter pada kunci, sehingga kunci berotasi untuk setiap tahap enkripsinya. Metode enkripsi ini penulis sebut dengan *Vigènere Cipher* Rotasi Berlapis. Algoritma yang digunakan sama seperti Algoritma *Vigènere Cipher*, modifikasi dilakukan terhadap pemanfaatan kunci dalam enkripsi. Metode ini dapat didasari oleh ide Triple DES yang melakukan enkripsi yang berulang sebanyak tiga kali, tetapi disini pengulangan dilakukan sebanyak panjang kunci.

Kata kunci: Kriptografi, *Vigènere Cipher*, Enkripsi berulang, plainteks, cipherteks.

1. PENDAHULUAN

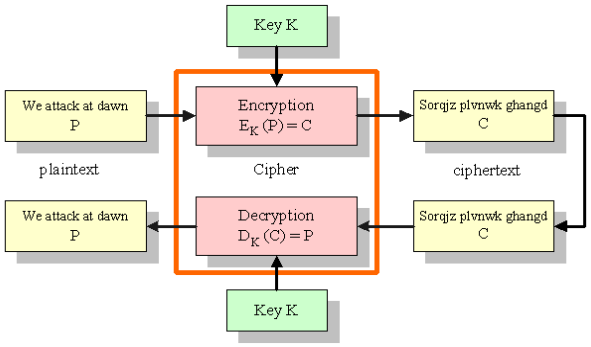
Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Cryptography berasal dari bahasa yunani. Crypto berarti *hidden / secret* (tersembunyi / rahasia) dan Graphy berarti *writing* (tulisan), sehingga kriptografi secara harfiah adalah *secret writing* (tulisan rahasia). Ilmu kriptografi diterapkan untuk keperluan pengiriman pesan agar tidak dapat dibaca dan dimengerti oleh pihak yang tidak berkepentingan.

Ilmu kriptografi semakin banyak digunakan seiring dengan berkembangnya ilmu pengetahuan dan teknologi. Khususnya di dunia informatika, ilmu kriptografi sangat diperlukan dalam pengiriman dan penerimaan pesan yang banyak dikirim melalui jaringan. Pengiriman informasi ini seringkali membutuhkan kerahasiaan yang tinggi, misalnya kode-kode pribadi seperti *password* atau kode PIN.

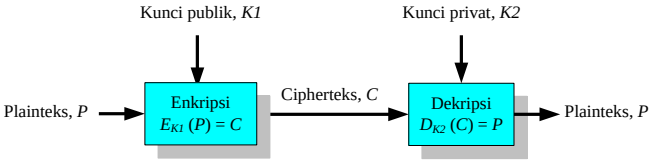
Ilmu kriptografi secara umum dapat dikategorikan menjadi dua, yaitu kriptografi kunci simetri, dan kriptografi kunci nirsimetri. Pada kriptografi kunci simetri, kunci yang digunakan untuk melakukan enkripsi sama dengan kunci yang digunakan untuk melakukan dekripsi. Algoritma kriptografinya disebut dengan algoritma simetri. Sementara itu, pada kriptografi kunci asimetri, kunci yang digunakan untuk melakukan enkripsi tidak sama dengan kunci yang digunakan untuk melakukan dekripsi. Kunci untuk enkripsi diketahui secara publik, dan disebut dengan *public key*, sementara kunci untuk dekripsi hanya diketahui oleh pihak yang berkepentingan dan bersifat privat, dan disebut dengan *private key*. Kriptografi ini disebut juga dengan kriptografi kunci-publik.

Akan tetapi, Ilmu kriptografi telah berkembang sejak jaman dahulu kala. Algoritma kriptografi klasik umumnya berupa algoritma enkripsi yang berbasiskan karakter, yaitu enkripsi terhadap kalimat sehari-hari, kata-kata, atau huruf alfabet. Algoritma kriptografi klasik cukup sederhana dan

mudah digunakan. Beberapa algoritma kriptografi klasik yang cukup terkenal antara lain algoritma cipher substitusi dan algoritma cipher transposisi. Algoritma *Caesar Cipher* yang mendasari *Vigènere Cipher* termasuk dalam algoritma cipher substitusi.



Gambar 1. Skema algoritma simetri



Gambar 2. Skema algoritma nir-simetri

Ide dasar algoritma *Caesar Cipher* adalah dengan menggeser urutan abjad sebanyak n karakter pada setiap huruf di plainteks. Algoritma ini rentan dipecahkan dengan *exhaustive search* karena karakter dalam huruf alfabet hanya ada 26. Rumusan untuk enkripsi dan dekripsi pada *Ceasar Cipher*, dengan pergeseran huruf sejauh *k*, dengan asumsi huruf A = 0, B = 1, ... , Z = 25, adalah sebagai berikut :

Enkripsi: $c_i = E(p_i) = (p_i + k) \bmod 26$ (1)

dan

Dekripsi: $p_i = D(c_i) = (c_i - k) \bmod 26$ (2)

k = kunci rahasia

Kemudian, dikembangkanlah algoritma-algoritma enkripsi lain dengan berdasar pada algoritma *Caesar Cipher*, dengan tujuan meningkatkan keamanan dari enkripsi. Salah satunya algoritma hasil modifikasi dari *Caesar Cipher* adalah *Vigènere Cipher*.

2. *Vigènere Cipher*

Vigènere Cipher termasuk dalam cipher abjad-majemuk yang menerapkan metode substitusi polialfabetik dan termasuk dalam kategori kriptografi kunci simetris. Metode *Vigenere Cipher* ini pertama kali dideskripsikan oleh Giovan Battista Bellaso seperti tertulis di dalam bukunya *La Cifra del Sig. Giovan Batista Belas*. Akan tetapi, *Vigènere Cipher* dipublikasikan oleh Blaise de Vigènere, seorang diplomat Perancis sekaligus seorang kriptologis, pada abad ke-16 yaitu tahun 1586. Oleh karena itu pula metode cipher tersebut dikenal sebagai *Vigènere Cipher*.

Pada masanya, yaitu sekitar abad 16, *Vigènere Cipher* termasuk salah satu algoritma enkripsi terkuat. Tetapi, *Vigènere Cipher* berhasil dipecahkan oleh Babbage dan Kasiski pada petengahan abad ke-19. Selain itu pula, setelah *Vigènere Cipher* dipecahkan, saat itu pulalah terjadinya perang sipil di Amerika.

2.1. Algoritma *Vigènere Cipher*

Pada dasarnya setiap enkripsi huruf pada *Vigènere Cipher* adalah enkripsi huruf pada *Caesar Cipher* dengan kunci yang berbeda-beda. Huruf yang sama pada plainteks tidak selalu dienkripsi dengan kunci yang sama dan menjadi cipherteks yang sama. Hal inilah yang dimaksud dengan karakteristik dari cipher abjad-majemuk, dimana setiap huruf cipherteks dapat memiliki banyak kemungkinan huruf plainteks. Kekuatan dari *Vigènere Cipher* ini yaitu dapat mencegah frekuensi huruf-huruf di dalam cipherteks yang mempunyai pola tertentu yang sama seperti pada cipher abjad-tunggal. Akan tetapi, jika periode kunci telah diketahui dan kunci yang digunakan tidak terlalu panjang, maka kunci dapat diketahui dengan menulis program komputer untuk melakukan *exhaustive key search*.

Algoritma *Vigènere Cipher* bekerja dengan cara mensubstitusikan setiap huruf di plainteks dengan bujursangkar *Vigènere* dalam melakukan enkripsi. Bujursangkar *Vigènere* memiliki huruf-huruf di setiap barisnya yang menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar Cipher*. Enkripsi dilakukan menggunakan suatu kata kunci yang menjadi acuan dalam melakukan enkripsi. Kunci dalam *Vigènere Cipher* adalah berupa sebuah kata yang juga merupakan kata-kata dalam bahasa sehari-hari yang terdiri atas huruf-huruf alfabet. Setiap huruf dalam kunci mensubstitusikan huruf yang bersesuaian dengan plainteksnya. Jika panjang plainteks lebih panjang dari panjang kunci, maka enkripsi dilakukan dengan kunci yang berulang hingga akhir plainteks.

	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 3. Bujursangkar *Vigènere* atau dikenal dengan *tabula recta*

Contoh penggunaan Bujursangkar *Vigènere* atau *tabula recta* untuk plainteks 'ENKRIPSI DAN DEKRIPSI' dengan kunci 'kriptografi' adalah dimulai dari huruf pertama yaitu E, tarik garis vertikal dari huruf E, dan tarik garis vertikal dari huruf k, maka akan didapatkan cipherteks di pertemuan garis tersebut, yaitu huruf O (gambar 2). Selanjutnya lakukan hal yang sama untuk huruf N, dengan huruf r, maka didapatkan cipherteks huruf E. Begitu pula yang dilakukan terhadap setiap huruf-huruf pada plainteks, hingga semua huruf pada plainteks terenkripsi dan menjadi suatu cipherteks. Untuk contoh diatas, hasil enkripsi dengan *Vigènere Cipher* adalah 'OESGBDYZ DFV NVSGBDYZ'.

2.2. Metode Kasiski

Algoritma *Vigènere Cipher* telah dapat dipecahkan oleh Babbage dan Kasiski pada pertengahan abad ke-19. Diperkenalkan oleh Friedrich Kasiski pada tahun 1863. Metode ini pada awalnya ditemukan oleh Babbage, akan tetapi nama Kasiski lebih dikenal untuk metode ini. Metode Kasiski membantu kriptanalis dalam menemukan kunci yang digunakan pada enkripsi *Vigènere Cipher*.

Cara kerja metode Kasiski ini memanfaatkan sifat bahasa Inggris yang tidak hanya mengandung perulangan huruf tetapi juga pasangan huruf seperti TH, hingga triplet seperti THE. Dengan plainteks yang cukup panjang, kemungkinan adanya pola berulang pada cipherteks yang dapat digunakan untuk menandakan kemunculan pasangan huruf dan triplet menjadi besar.

	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 4. Contoh Penggunaan Bujursangkar *Vigènere*

Pada dasarnya, jika jarak antara dua buah string yang berulang di dalam plainteks adalah kelipatan dari panjang kunci, maka kemungkinan string tersebut akan muncul sebagai suatu ktiptogram yang sama pula di dalam cipherteks. Sehingga dari hal tersebut, panjang kunci dapat ditentukan dengan langkah-langkah berikut :

1. Tentukan semua kriptogram yang berulang dalam cipherteks.
2. Hitung jarak antar kriptogram yang berulang
3. Hitung semua faktor dari jarak yang didapat pada no.2.
4. Tentukan irisan dari himpunan faktor pembagi tersebut. Nilai yang muncul di dalam irisan menyatakan angka yang muncul pada semua faktor pembagi jarak-jarak tersebut. Nilai ini mungkin adalah panjang kunci, jika string yang berulang tersebut tidak muncul bertindihan.

Setelah menemukan panjang kunci, maka kata kunci dapat ditentukan dengan menggunakan *exhaustive search* atau dengan teknik analisis frekuensi.

3. *Vigènere Cipher* Rotasi Berlapis

Dengan adanya metode kasiski, dapat disimpulkan bahwa algoritma *Vigènere Cipher* sederhana sudah tidak begitu aman lagi melawan serangan dari kriptanalis. Beberapa penelitian untuk mengembangkan dan memodifikasi *Vigènere Cipher* telah banyak dilakukan. Harapannya adalah untuk menyempurnakan *Vigènere Cipher*, untuk mendapatkan suatu algoritma enkripsi yang

tidak mudah untuk dipecahkan, tentunya dengan didasari oleh algoritma *Vigènere Cipher* itu sendiri. Dalam hal ini, penulis juga berusaha melakukan modifikasi dan pengembangan terhadap algoritma *Vigènere Cipher* demi meningkatkan keamanan dari algoritma enkripsi, dengan dasar algoritma dari *Vigènere Cipher*.

Beberapa teori yang menjadi inspirasi untuk modifikasi dan pengembangan ini diantaranya adalah Triple DES, yang melakukan enkripsi sebanyak 3 kali.

3.1. Sekilas Tentang *DES* dan *Triple DES*

Data Encryption Standard adalah suatu standard enkripsi yang telah disetujui oleh *National Bureau of Standard (NBS)* setelah penilaian kekuatan oleh *National Security Agency (NSA)* Amerika Serikat. DES adalah standard, sedangkan algoritmanya adalah DEA (*Data Encryption Algorithm*), akan tetapi istilah DES sering disalahartikan dan lebih dikenali sebagai algoritmanya. DES tergolong dalam kriptografi kunci-simetri dan tergolong dalam jenis cipher blok. DES beroperasi pada ukuran blok 64 bit.

Karena DES mempunyai potensi kelemahan pada *brute-force attack*, maka dibuat varian dari DES. Varian dari DES yang cukup banyak digunakan adalah DES berganda, yaitu enkripsi berulang-ulang dengan DES dan dengan kunci ganda. Salah satu DES berganda ini yaitu Triple DES.

Triple DES melakukan DES sebanyak 3 kali. Terdapat beberapa mode Triple DES yang dikenali. yaitu mode EEE dan mode EDE. Mode EEE adalah mode dengan melakukan enkripsi sebanyak 3 kali, dengan kunci yang berbeda-beda. Bentuk umum Triple DES mode EEE adalah sebagai berikut :

Enkripsi: $C = E_{K3}(E_{K2}(E_{K1}(P)))$ (3)

Dekripsi: $P = D_{K1}(D_{K2}(D_{K3}(C)))$ (4)

Sedangkan mode EDE adalah mode dengan melakukan enkripsi, kemudian dilakukan dekripsi dengan kunci yang berbeda, dan selanjutnya dilanjutkan dengan enkripsi sekali lagi. Untuk mode EDE, terdapat dua versi, yaitu dengan 2 kunci dan dengan 3 kunci.

Untuk Triple DES dengan mode EDE mnggunakan 2 kunci, memiliki bentuk umum seperti berikut :

Enkripsi: $C = E_{K1}(D_{K2}(E_{K1}(P)))$ (5)

Dekripsi: $P = D_{K1}(E_{K2}(E_{K1}(C)))$ (6)

Sedangkan untuk Triple DES dengan mode EDE menggunakan 3 kunci memiliki bentuk umum seperti berikut :

Enkripsi: $C = E_{K3}(D_{K2}(E_{K1}(P)))$ (7)

Dekripsi: $P = D_{K1}(E_{K2}(D_{K3}(C)))$ (8)

3.2. Algoritma *Vigènere Cipher* Rotasi Berlapis

Algoritma *Vigènere Cipher* Rotasi Berlapis bekerja berdasarkan algoritma dasar *Vigènere Cipher*, dengan menambahkan konsep enkripsi berganda seperti pada DES berganda. Konsep yang digunakan cukup mirip dengan DES berganda, yang pada triple DES menggunakan mode EDE. Disini, metode yang digunakan adalah dengan mengenkripsi plainteks menggunakan algoritma *Vigènere Cipher* dan kemudian dilakukan dekripsi yang merupakan metode dekripsi *Vigènere Cipher*, kemudian dilakukan lagi metode enkripsi yang selanjutnya diikuti dengan metode dekripsi. Hal ini dilakukan berulang-ulang dengan jumlah enkripsi-dekripsi yang dilakukan adalah sama dengan panjang kunci.

Cara kerja metode baru ini adalah dengan mengenkripsi plainteks dengan kunci pertama adalah kunci asli, kemudian untuk enkripsi kedua adalah mendekripsi cipherteks dari hasil enkripsi pertama dengan kunci berupa kunci asli yang setiap karakternya digeser ke kiri sejauh satu karakter. Setelah itu, enkripsi dilanjutkan dengan mengenkripsi cipherteks kedua, yang juga dengan kunci yang bergeser satu karakter ke kiri dari kunci sebelumnya. Enkripsi diulang dengan cara yang sama, berulang sebanyak panjang kunci. Metode ini, selain mengenkripsi plainteks, juga mengenkripsi kunci dengan metode cipher transposisi.

3.3. Contoh Penggunaan

Contoh penerapan algoritma *Vigènere Cipher* Rotasi Berlapis untuk plainteks '`Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan`' dengan kunci '`crypto`'.

`P = Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan` (9)

k_1 = `crypto` (10)

`P' = Migemciiyub ofrjpa wnds stb uvlx nbvli bxblrep dscdyctb rvqpg` (11)

k_2 = `ryptoc` (12)

P" = Vkrlyarkjbn motuwm uwfd zfz dxwe zzent ijzutpw pqlfjjfz axbws (13)

k_3 = yptocr (14)

P"' = Tzkzarpzcpp dminko luuw nhq bmps bqccm wlqsiik rhjucxhq ymuku (15)

k_4 = ptocry (16)

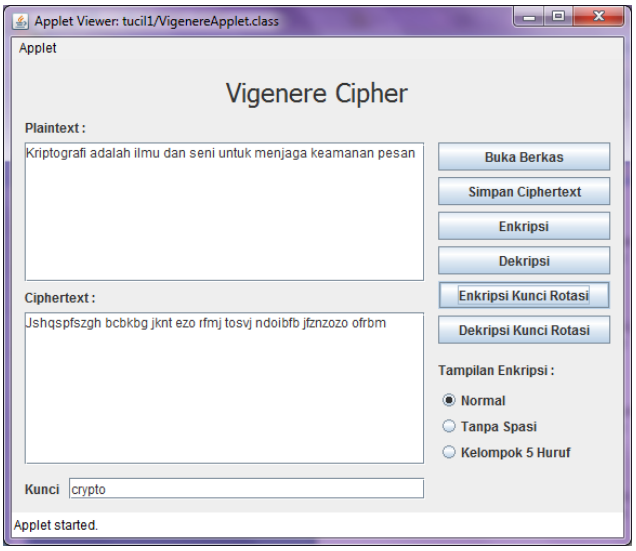
P"" = Egwxjtagony fxpzix nfbi lqs mtbq ksnjy uusdpui ajubovqs jtgid (17)

k_5 = tocryp (18)

P""" = Xuyohituqew uqdbzv cypk coh fhdh ihgxa lshwdwz yynpqmoh chizb (19)

k_6 = ocrypt (20)

C = Jshqspfszgh bcbkbg jknt ezo rfmj tosvj ndoibfb jfznzozo ofrbm (21)



Gambar 5. *Screenshot* program aplikasi untuk enkripsi *Vigènere Cipher* Rotasi Berlapis

3.4. Analisis Terhadap Metode

Dapat dilihat dari contoh, metode yang digunakan mirip seperti algoritma Triple DES dengan mode EDE. Akan tetapi, pada metode diatas, enkripsi diulang sebanyak n kali, dimana n adalah panjang kunci enkripsi. Kunci yang digunakan untuk enkripsi pada setiap tahapnya adalah kunci yang mengalami cipher transposisi pergeseran 1 huruf ke kiri.

Dapat dilihat pada contoh, langkah-langkah enkripsi adalah dengan pertama-tama mengenkripsi plainteks (9) dengan kunci awal (10). Kemudian, cipherteks pertama hasil enkripsi tersebut (11) didekripsi dengan kunci yang telah sedikit dimodifikasi (12), yang menghasilkan cipherteks kedua (13). Hal ini dilakukan berulang kali sebanyak panjang kunci. Pada kasus diatas, panjang kunci adalah 6, sehingga enkripsi dilakukan sebanyak 6 kali. Setelah dilakukan enkripsi sebanyak enam kali, maka didapatkan hasil cipherteks akhir (21), yaitu C = 'Jshqspfszgh bcbkbg jknt ezo rfmj tosvj ndoibfb jfznzozo ofrbm'.

Jika dilihat dari metodenya, cara enkripsi ini masih rentan hanya dengan metode kasiski. Hal ini karena panjang kunci setiap enkripsi adalah sama, dan metode enkripsi dan dekripsi untuk setiap huruf pada plainteks masih merupakan metode *Caesar Cipher*. Akan tetapi, jika menerapkan metode kasiski untuk menyerang cipherteks enkripsi dari metode ini, kunci yang didapat adalah kunci dengan huruf-huruf yang tidak beraturan, yang tidak membentuk kata yang cukup familiar. Akan sulit untuk menentukan kunci, jika pola pikir dalam pencarian kunci adalah bahwa kunci merupakan suatu kata dalam bahasa sehari-hari. Meskipun begitu, walaupun panjang kunci dapat diketahui dengan metode kasiski, kata kunci tidak akan mudah untuk diketahui.

Untuk melakukan enkripsi didapatkan algoritma sebagai berikut :

$$C = E_{Kn}(D_{Kn-1}(E_{Kn-2}(\ldots(E_{K1}(P))\ldots))) \quad (22)$$

untuk jumlah huruf kunci ganjil, dan

$$C = E_{Kn}(D_{Kn-1}(E_{Kn-2}(\ldots(D_{K1}(P))\ldots))) \quad (23)$$

untuk jumlah huruf kunci genap.

Sedangkan untuk melakukan dekripsi, dapat digunakan algoritma berikut :

$$P = D_{K1}(E_{K2}(D_{K3}(\ldots(E_{Kn-1}(D_{Kn}(C)))\ldots))) \quad (22)$$

untuk jumlah huruf kunci ganjil, dan

$$P = D_{K1}(E_{K2}(D_{K3}(\ldots(D_{Kn-1}(E_{Kn}(C)))\ldots))) \quad (23)$$

untuk jumlah huruf kunci genap.

Akan tetapi, ketika metode ini berdasarkan metode Triple DES dengan mode EEE, metode ini tidak akan memperbaiki masalah yang dihadapi oleh *Vigènere Cipher*, melainkan dapat memperburuk keamanan enkripsi. Hal ini karena, ketika dilakukan perhitungan untuk mencari kunci akhir, hasil dari kunci akhir adalah

suatu susunan huruf dengan panjang kunci yang sama seperti kunci aslinya, tetapi dengan semua huruf pada kunci adalah sama. Hal inilah yang menyebabkan metode ini tidak pantas jika mencontoh mode EEE pada Triple DES, karena tidak mencapai sasaran untuk meningkatkan keamanan dan kekuatan dari algoritma enkripsi.

IV. KESIMPULAN

Kesimpulan yang bisa didapat dari studi pengembangan dan modifikasi metode enkripsi yang didasarkan dari metode enkripsi *Vigènere Cipher*, antara lain :

1. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan

2. Metode enkripsi *Vigènere Cipher* adalah metode enkripsi yang sederhana tetapi cukup kuat.

3. Metode enkripsi *Vigènere Cipher* dapat dipecahkan dengan metode Kasiski untuk mencari panjang kuncinya.

4. Algoritma *Vigènere Cipher* cukup berpotensi untuk dikembangkan agar menjadi lebih kuat terhadap serangan dengan mempertahankan kesederhanaan algoritmanya.

5. Algoritma *Vigènere Cipher* Rotasi Berlapis dapat memperkuat algoritma *Vigènere Cipher*.

6. Algoritma *Vigènere Cipher* Rotasi Berlapis lebih cocok jika mengikuti mode EDE yang digunakan dalam metode enkripsi triple DES.

7. Jika Algoritma *Vigènere Cipher* Rotasi Berlapis mengikuti mode EEE yang digunakan dalam metode enkripsi triple DES, justru akan memperlemah kekuatan enkripsi.

REFERENSI

[1] Munir, Rinaldi. *Kriptografi*, Institut Teknologi Bandung, 2006.

[2] Rukmono, Satrio Adi. "*Triple Vigènere Cipher*" http://www.informatika.org/~rinaldi/Kriptografi/2008-2009/Makalah1/MakalahIF30581-2009-a035.pdf Tanggal akses 20/03/2010.

[3] Respationo, Unggul Satrio. "*Venigmare Cipher* dan *Vigènere Cipher*" http://www.informatika.org/~rinaldi/Kriptografi/2008-2009/Makalah1/MakalahIF30581-2009-a054.pdf Tanggal akses 23/03/2010

[4] http://en.wikipedia.org/wiki/Cryptography Tanggal akses 23/03/2010.

[5] http://www.total.or.id/info.php?kk=Cryptography Tanggal akses 23/03/2010.

[6] http://www.lulu.com/items/volume_36/553000/553543/1/print/553543.pdf Tanggal akses 24/03/2010.

[7] http://www.total.or.id/info.php?kk=Data%20Encryption%20Standard Tanggal akses 24/03/2010.