Vigènere Transposisi

Rangga Wisnu Adi Permana - 13504036 [1)]
1) Program Studi Teknik Informatika ITB, Bandung 40132, email: if14036@students.if.itb.ac.id

Abstract **–** *Seiring dengan pesatnya perkembangan teknologi komunikasi menjadikan penyampaian pesan dapat dilakukan melalui berbagai media. Namun dengan berkembangnya media penyampaian pesan tersebut dibutuhkan pula suatu teknologi untuk menjaga kerahasiaan pesan yang dikirimkan. Teknologi ini disebut dengan kriptografi. Salah satu metode kriptografi klasik yang terkenal adalah vigènere cipher. Vigènere cipher dapat mengubah pesan sederhana menjadi suatu pesan yang sulit dibaca atau pesan lain untuk melindungi kerahasiaan pesan. Namun vigènere cipher ini memiliki kelemahan. Dalam makalah ini, penulis ingin membahas pengembangan algoritma vigènere cipher dengan cara memadukannya dengan algoritma transposisi. Algoritma transposisi adalah suatu algoritma kriptografi yang menngunakan prinsip perubahan letak karakter untuk menyembunyikan arti dari pesan. Makalah ini akan mencakup pembahasan konsep dasar, implementasi dan juga analisis keamanan terhadp bergabai macam serangan dan juga dilakukan beberapa pengujian.*

Kata Kunci*: enkripsi, dekripsi, vigènere, metode kasiski, known plainteks attack, cipherteks, plainteks*

1. PENDAHULUAN

Komunikasi merupakan kebutuhan manusia, salah satu cara melakukan komunikasi ini adalah dengan melakukan pengiriman pesan. Dilatarbelakangi oleh kebutuhan manusia tersebut, teknologi komunikasi dewasa ini maju dengan pesat. Dengan kemajuan teknologi tersebut, manusia dapat melakukan pengiriman pesan dengan mudah di mana saja dan kapan saja dengan menggunakan berbagai media.

Dengan semakin mudahnya manusia dalam melakukan pengiriman pesan, semakin mudah pula pesan tersebut dicuri atau dilihat oleh pihak yang tidak bertanggung jawab. Hal tersebut menjadi masalah yang cukup serius karena pesan yang dikirim dapat merupakan pesan penting yang rahasia.

Salah satu cara untuk menanggulangi permasalahan tersebut adalah dengan menerapkan konsep kriptografi pada pesan yang dikirimkan. Telah banyak algoritma kriptografi, baik kriptografi modern maupun klasik yang sudah diterapkan untuk menjaga keamanan suatu pesan.

Salah satu algoritma kriptografi klasik yang cukup populer adalah vigènere cipher. Algoritma ini cukup sederhana untuk diimplementasikan dan dapat menyembunyikan pesan dengan cukup baik. Namun

algoritma ini memiliki satu kelemahan yang cukup vital, algoritma kriptografi ini dapat dipecahkan dengan menggunakan metode kasiski yang diteruskan dengan penggunaan metode analisis frekuensi.

Berdasarkan kelemahan tersebutlah, maka penulis mencoba menggabungkan vigènere cipher dengan salah satu algoritma kriptografi klasik yang lain yaitu algoritma transposisi, suatu algoritma kriptografi yang menggunakan prinsip perubahan posisi karakter untuk menyembunyikan pesan. Dengan penggabungan ini, diharapkan kelemahan vigènere cipher pada metode kasiski dapat dihilangkan.

Dalam makalah ini, penulis juga ingin melakukan implementasi dari algoritma yang merupakan perpaduan dari vigènere cipher dan algoritma transposisi tersebut. Selain itu akan dilakukan pula analisis keamanan dari algoritma tersebut. Dengan adanya makalah ini, diharapkan pembaca dapat mendapatkan informasi yang sangat berharga dan dapat membantu dalam perkembangan ilmu kriptografi.

2. LANDASAN TEORI

2.1. Vigènere Cipher

Vigènere cipher merupakan algoritma kriptografi klasik, yang menjadi perbedaan utama kriptografi klasik dengan kriptografi modern adalah enkripsi berbasis karakter pada kriptografi klasik dan enkripsi berbasis bit pada kriptografi modern. Dalam kriptografi klasil, vigènere cipher termasuk kedalam cipher substitusi majemuk, yang di mana suatu karakter pada plainteks tidak dipetakan atau disubstitusi menjadi satu karakter saja tetapi bisa menjadi bermacam-macam karakter bergantung kepada kunci. Vigènere cipher ini dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16 (tahun 1586). Namun algoritma ini baru populer 200 tahun kemudian [1].

Untuk melakukan enkripsi, vigènere cipher ini menggunakan bujur sangkar vigènere untuk memetakan karakter cipherteks. Pada bujur sangkar vigènere ini, kolom paling kiri menunjukan karakter

kunci dan baris paling atas menunjukan karakter plainteks, karakter-karakter pada baris lainnya menunjukan karakter cipherteks. Karakter cipherteks tersebut diperoleh dengan menggunakan prinsip *caesar* cipher, yang di mana pergeseran huruf ditentukan dengan nilai desimal dari huruf-huruf yang bersangkutan, di mana untuk karakter berjumlah 26 karakter: a=0, b=1, c=2,d=3,.., z=25.

Vigènere cipher ini juga sering disebut dengan *caesar* k-shift karena penggunaan pemetaan yang dilakukan berdasarkan kunci yang diulang atau dilakukan secara sirkular[2].

Sebagai contoh apabila karakter A beasosiasi dengan kunci karakter c, maka akan menghasilkan karater C. Bujur sangkar vigènere dapat dilihat pada **gambar 1**.

KEY \ Plain	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 Bujur Sangkar Vigenere

Apabila panjang kunci lebih pendek dari plainteks maka kunci akan berulang sehingga dapat memenuhi panjang plainteks. Apabila panjang kunci sama panjang dengan panjang plainteks maka algoritma ini akan sangat mirip dengan algoritma one time pad. Sebagai contoh, plainteks “TUGAS MAKALAH” akan dienkripsi dengan menggunakan kunci “RANGGA”.

P	**T**	**U**	**G**	**A**	**S**	**M**	**A**	**K**	**A**	**L**	**A**	**H**
K	R	A	N	G	G	A	R	A	N	G	G	A
C	**k**	**u**	**t**	**g**	**y**	**m**	**R**	**K**	**l**	**r**	**g**	**H**

Dapat dilihat pada contoh tersebut bahwa vigènere cipher akan sulit dipecahkan dengan menggunakan analisis frekuensi biasa, seperti halnya semua algoritma kriptografi abjad-majemuk. Pada contoh tersebut juga dapat dilihat kalau vigènere cipher menggunakan kunci yang berulang. Penggunaan kunci yang berulang inilah yang menjadikan vigènere cipher memliki kelemahan besar. Babbage dan Kasiski pada pertengahan abad 19 berhasil menemukan kelemahan tersebut. Metode yang mereka gunakan dikenal dengan nama metode Kasiski.

Metode Kasiski digunakan untuk menentukan panjang dari kunci yang digunakan untuk menggunakan vigènere cipher tersebut. Dengan ditemukannya panjang kunci, maka cipherteks akan mudah dipecahkan dengan menggunakan analisis frekuensi.

Metode kasisiki melakukan analisis berdasarkan kemunculan rangkaian huruf yang berulang pada chiperteks. Dari rangkaian huruf yang sering berulang dapat ditemukan panjang kuncinya.

Metode kasiski akan sulit diimplementasikan pada cipherteks yang pendek karena akan sulit menemukan rangkaian karakter yang berulang, sebaliknya pada cipherteks yang panjang akan lebih mudah menemukan rangkaian karakter yang berulang.

2.2. Algoritma Transposisi

Cipher transposisi adalah suatu algoritma enkripsi yang melakukan enkripsi dengan merubah urutan dari plainteks. Pada algoritma ini karakter plainteks tidak dirubah maupun dipetakan menjadi karakter lain. Hasil cipherteks memiliki karakter-karakter yang sama dengan plainteks hanya saja urutannya dirubah.

Cipher transposisi ini memiliki berbagai macam bentuk dan algoritma, diantara contoh dari cipher transposisi ini adalah Rail Fence Cipher, Route Cipher dan Columnar Cipher. Yang akan dibahas pada makalah ini adalah algoritma transposisi yang mirip dengan columnar cipher yang menggunakan prinsip kolom dan baris pada matriks yang memakai kunci berupa angka.

Cara kerja dari cipher transposisi tersebut adalah dengan membangun suatu matriks karakter dari plainteks, kemudian dilakukan *transpose* pada matriks tersebut dan disusunlah cipherteks dari hasil *transpose* tersebut.

Contoh cipher transposisi tersebut adalah melakukan enkripsi plainteks “TUGAS MAKALAH” dengan kunci “3”. Maka akan dibangun matriks seperti berikut:

TUG
ASM
AKA
LAH

Kemudian dilakukan *transpose* sehingga menghasilkan matriks berikut :

TAAL
USKA
GMAH

Dari matriks tersebut disusun kembali teks yang menjadi cipherteks yaitu “TAALUSKAGMAH”.

Untuk melakukan dekripsi yang perlu dilakukan adalah melakukan hal yang sama pada hasil cipher teks, yaitu membangun matriks hanya saja kunci dijadikan jumlah baris, kemudian melakukan *transpose* dan menyusun teks kembali.

3. VIGÈNERE TRANSPOSISI

3.1. Konsep Dasar

Vigènere transposisi merupakan penggabungan dari vigènere cipher dan algoritma transposisi yang telah dibahas pada bagian sebelumnya.

Vigènere transposisi ini melakukan enkripsi dengan cara melakukan vigènere cipher pada plainteks dan hasil cipherteks tersebut dienkripsi kembali dengan menggunakan algoritma transposisi.

Untuk melakukan dekripsi, yang dilakukan adalah melakukan deksripsi algoritma transposisi pada cipherteks, kemudian melakukan dekripsi vigènere cipher.

Karena sebaiknya kunci untuk melakukan enkripsi hanya satu maka kunci untuk melakukan enkripsi transposisi akan diambil berdasarkan panjang dari kunci yang dipakai untuk melakukan vigènere cipher.

Contoh vigènere cipher ini adalah melakukan enkripsi plainteks “TUGASMAKALAH” dengan kunci “RANGGA”.

1. Langkah pertama adalah melakukan enkripsi secara vigènere cipher.

P	**T**	**U**	**G**	**A**	**S**	**M**	**A**	**K**	**A**	**L**	**A**	**H**
K	R	A	N	G	G	A	R	A	N	G	G	A
C	**k**	**u**	**t**	**g**	**y**	**m**	**r**	**k**	**l**	**r**	**g**	**H**

2. Melakukan enkripsi transposisi. Karena kata “RANGGA” memiliki panjang 6 maka kuncinya 6.

KUTGYMRKLRGH => KUTGYM
RKLRGH

=> KRUKTLGRYGMH

Dari contoh tersebut dihasilkan cipherteks “KRUKTLGRYGMH”.

Untuk dekripsi, langkah-langkahnya sebagai berikut :

1. Lakukan dekripsi seperti melakukan dekripsi transposisi dengan kunci yaitu panjang kunci.

KRUKTLGRYGMH => KR
UK
TL
GR
YG
MH

=> KUTGYMRKLRGH

2. Dekripsi dengan dekripsi vigènere cipher.

C	**K**	**U**	**T**	**G**	**Y**	**M**	**R**	**K**	**L**	**R**	**G**	**H**
K	R	A	N	G	G	A	R	A	N	G	G	A
P	**T**	**U**	**G**	**A**	**S**	**M**	**A**	**K**	**A**	**L**	**A**	**H**

Dari proses dekripsi tersebut dihasilkan plainteks “TUGASMAKALAH”.

3.2. Implementasi

Dalam melakukan implementasi, penulis menggunakan bahasa pemrograman java, dengan lingkungan pembangunan sebagai berikut :

1. Java Development Kit (JDK)6.
2. Perangkat pembangunan NetBeans IDE 5.5.

Implementasi yang dilakukan meliputi implementasi enkripsi dan dekripsi vigènere transposisi. Vigènere transposisi yang diimplementasi terdiri dari 2 jenis yaitu yang memakai satu kunci dengan kunci transposisi memakai panjang kunci vigènere cipher dan yang memakai 2 buah kunci yaitu kunci vigènere dan kunci transposisi, hal ini ditujukan untuk melakukan perbandingan keamanan.

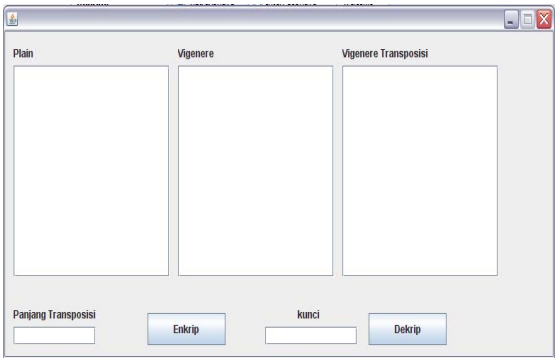
Penulis juga membuat dua buah aplikasi, yaitu yang menggunakan karakter ASCII (berjumlah 256) dan yang menggunakan 26 buah karakter. Untuk memudahkan dalam pembacaan dan penulisan karakter, maka dalam makalah ini difokuskan dengan penggunaan 26 buah karakter.
Aplikasi yang dibangun merupakan aplikasi berbasis desktop dan dapat dijalankan pada desktop dengan berbagai Sistem Operasi dengan penggunaan JRE 6.

Aplikasi yang dibuat oleh penulis terdiri dari dua buah kelas: yang pertama kelas “Interface” yang merupakan kelas antar muka dengan user, kelas ini merupakan kelas turunan dari JFRAME, yang kedua adalah kelas “vigtrans” yang berisi fungsi-fungsi untuk melakukan enkripsi dan dekripsi.

Pada aplikasi yang telah dibangun oleh penulis, terdapat dua buah form untuk memasukan kunci, kunci untuk vigènere cipher dan kunci untuk melakukan tranposisi.

Apabila form kunci untuk melakukan transposisi dikosongkan maka kunci transposisi akan menggunakan panjang String dari kunci untuk melakukan vigènere cipher.

Tampilan dari aplikasi yang telah dibangun dengan menggunakan versi 26 karakter dapat dilihat pada **gambar 2**.



Gambar 2 Tampilan Aplikasi

Pada gambar 2 dapat dilihat bahwa pada aplikasi akan ditampilkan hasil enkripsi vigènere cipher secara per-langkah.

Akan ditampilkan hasil enkripsi terhadap vigènere cipher dan hasil enkripsi vigènere cipher yang sudah ditransposisikan atau vigènere transposisi.

Begitu pula dalam proses dekripsi, akan ditampilkan hasil akhir dekripsi dan hasil dekripsi sebelum didekripsi secara vigènere atau setelah didekripsi secara transposisi.

Kelas "vigtrans" memiliki 4 buah prosedur penting dalam melakukan proses ekripsi dan dekripsi. Berikut penjelasan singkat prosedur-prosedur tersebut:

1. Prosedur vigenere : Prosedur ini berfungsi untuk melakukan vigènere cipher. Prosedur ini dipanggil ketika pengguna meng-klik tombol enkrip. Plainteks yang dimasukan akan dienkripsi secara vigènere cipher oleh prosedur ini.
2. Prosedur transposisi : Prosedur ini berfungsi untuk melakukan transposisi. Prosedur ini dipanggil ketika program telah selesai melakukan vigènere cipher.
3. Prosedur en_vigenere : Prosedur ini berfungsi untuk melakukan dekripsi vigènere cipher. Prosedur ini dipanggil ketika user meng-klik tombol dekripsi.
4. Prosedur en_transposisi : Prosedur ini berfungsi untuk melakukan dekripsi cipher transposisi. Prosedur ini dipanggil ketika program sudah menjalankan prosedur en_vigenere.

Atribut kunci, plainteks dan cipherteks merupakan *private* dari kelas "vigtrans". Kode pada kelas "vigtrans" dibuat penulis sedemikian rupa sehingga mudah untuk dilakukan pengeditan untuk merubah pemakaian jumlah karakter (ASCII atau 26 karakter).

Aplikasi yang telah dibangun telah diuji pada sistem operasi Windows XP Service Pack (SP) 2. Aplikasi berjalan dengan baik pada sistem operasi tersebut.

3. ANALISIS

Berikut akan dibahas analisis keamanan vigènere transposisi terhadap berbagai macam serangan yang disertai beberapa hasil simulasi.

3.1 Metode Kasiski

Metode kasiski adalah suatu metode untuk memecahkan cipherteks yang dibangun dengan vigènere cipher.

Metode kasiski ini dipakai untuk mengetahui panjang kunci yang digunakan dalam vigènere cipher. Dengan diketahuinya panjang kunci tersebut maka vigènere cipher akan mudah dipecahkan dengan menggunakan analisis frekuensi.

Contoh sederhana pemakaian metode kasiski untuk memecahkan vigènere cipher dengan plainteks "HER NAME IS HERA" dengan kunci "RAN" yang setelah dienkripsi akan menghasilkan cipherteks "YEEEAZVIFYEER".

Dengan menggunakan metode kasiski akan ditemukan:

YEEEAZVIFYEER

Kata "YEE" ditemukan 2 kali karena merupakan hasil pemetaan 2 buah "HER" dengan kunci "RAN" dengan ditemukannya kata yang muncul lebih dari satu kali ini dapat diasumsikan bahwa panjang kunci yang dipakai adalah 3 dan pada kasus ini hal tersebut benar. Dengan ditemukannya panjang kunci tersebut, cipherteks akan mudah dipecahkan dengan analisis frekuensi.

Dengan menggunakan vigènere transposisi cipherteks yang dihasilkan adalah "YEVYREAIEEZFE". Pada cipherteks tersebut tidak ditemukan satupun rangkaian huruf yang muncul lebih dari satu kali, dengan begitu metode kasiski tidak dapat menemukan panjang kunci yang digunakan.

3.2. Known-Plaintext Attack

Tidak seperti vigènere cipher biasa, vigènere transposisi cukup kuat terhadap known-plaintext attack, hal ini dikarenakan adanya penggunaan algoritma substitusi dan transposisi secara bersamaan.

Penyerang akan kesulitan menemukan letak hasil pemetaan huruf plainteks pada cipherteks dengan begitu penyerang akan kesulitan mengetahui hasil substitusi huruf yang dicari karena sulitnya mendapatkan huruf hasil pemetaan dari plainteks.
Sebagai contoh enkripsi plainteks "TUGAS MAKALAH" dengan kunci "RAN" akan menghasilkan "KRRCUSKATZNU", dalam hal ini karena penyerang tidak mengetahui kunci yang digunakan, maka penyerang tidak mengetahui jika pada contoh tersebut huruf kedua pada plainteks yaitu A dipertakan menjadi huruf U yang diletakan menjadi huruf kelima pada cipherteks, selain itu juga pada contoh tersebut dapat terlihat bahwa huruf U terdapat 2 buah pada cipherteks, jadi apabila terpecahkan jika huruf kedua plainteks yang berupa A dipetakan menjadi U, penyerang tetap kesulitan mengetahui huruf U yang mana pada cipherteks yang merupakan hasil pemetaan tersebut.

3.3. Chosen-Plaintext Attack

Seperti halnya vigènere cipher, vigènere transposisi ini sangat lemah terhadap chosen-plaintext attack.

Sebagai contoh, penyerang dapat dengan menemukan kunci yang digunakan dengan memiliki "AAAAAAAAAAA" sebagai plainteks. Misal kunci yang digunakan adalah "RAN", maka akan dihasilkan cipherteks "RRRRAAAANNN". Dari hasil enkripsi dapat terlihat jelas kunci yang digunakan adalah "RAN".

Untuk lebih memperkuat dari serangan chosen-plaintext attack. Vigènere transposisi dapat dimodifikasi dengan tidak menggunakan panjang kunci sebagai panjang transposisi. Sebagai contoh digunakan panjang kunci dikurangi 1 sebagai panjang transposisi, maka plainteks "AAAAAAAAAAA" yang dienkripsi dengan kunci "RAN" akan menghasilkan "RNARNAARNAR".

Walaupun dengan modifikasi panjng kunci menjadikan lebih kuat dari chosen-plaintext attack, namun masih dapat dibilang lemah karena dengan pengetahuan penyerang akan algoritma yang dipakai, maka dengan sedikit coba-coba akan mudah diketahui.

Dalam uji coba yang dilakukan penulis, digunakan juga modifikasi panjang kunci dengan memperhitungkan panjang plainteks, namun tetap lemah terhadap serangan chosen-plaintext attack.

3.4. Exhaustive Attack

Kekuatan vigènere transposisi terhadap serangan exhaustive attack pada dasarnya tidak berbeda dengan vigènere cipher biasa. Vigènere transposisi hanya unggul dari hal waktu karena waktu yang digunakan untuk melakukan percobaan menjadi lebih lama karena untuk waktu untuk melakukan transposisi, dengan begitu penyerang akan membutuhkan waktu yang lebih lama untuk memecahkan kunci yang digunakan untuk melakukan enkripsi.

Untuk penggunaan menggunakan kode ASCII dengan panjang kunci n maka jumlah kunci yang mungkin adalah :

$$Jumlah\ kunci = 256^n \quad ....(1)$$

Untuk pemakaian 26 karakter dengan panjang kunci n, maka jumlah kunci yang mungkin adalah:

$$Jumlah\ kunci = 26^n \quad .....(2)$$

Pada dasarnya kekuatan algoritma kriptografi ini pada serangan berjenis exhaustive attack bergantung kepada panjang kunci yang digunakan. Semakin panjang kunci yang digunakan maka akan semakin sulit penyerang menemukan kunci yang digunakan. Namun harus diperhatikan pula panjang kunci yang terlalu panjang tidaklah praktis.

4. KESIMPULAN

Dari keseluruhan isi makalah ini, dapat diambil kesimpulan sebagai berikut:

1. Algoritma vigènere transposisi merupakan penggabungan dari vigènere cipher dan algoritma transposisi.
2. Algoritma vigènere transposisi dapat mengatasi kekurangan vigènere cipher yang dapat dipecahkan dengan menggunakan metode kasiski.
3. Selain menutupi kelemahan vigènere cipher pada metode kasiski, vigènere transposisi juga menutupi kelemahan vigènere cipher pada serangan berjenis known-plainteks attack. Namun vigènere transposisi sangat lemah pada serangan berjenis chosen-plainteks attack.
4. Panjang kunci mempengaruhi kuatnya hasil enkripsi. Semakin panjang kunci yang digunakan maka akan semakin sulit cipherteks yang dihasilkan untuk dipecahkan.
5. Pemakaian karakter ASCII yang berjumlah 256 karakter menjadikan hasil enkripsi lebih kuat dibandingkan pemakaian karakter dengan jumlah 26 karakter.

6. Penggunaan kunci transposisi yang tidak menggunakan panjang kunci, seperti memakai panjang ½ kunci atau penjang cipherteks yang dibagi dengan kunci tidak terlalu berpengaruh pada tingkat keamanan.

DAFTAR PUSTAKA

Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, 2006

http://java.sun.com/ diakses pada Oktober 2007

http://mathdemos.gcsu.edu/mathdemos/vigenere/vigenere.htm diakses pada Oktober 2007

http://www.antilles.k12.vi.us/math/cryptotut/transposition.htm diakses pada Oktober 2007

http://www.cs.fiu.edu./~yehd/cop2210/HW3/ diakses pada Oktober 2007

http://www.math.uscd.edu/~crypto/java/EARLYCIPHER/vigenere .html diakses pada Oktober 2007

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, 2006

[2]http://www.math.uscd.edu/~crypto/java/EARLYCIPHER/vigenere .html diakses pada Oktober 2007