Aplikasi Pewarnaan pada Vigener Cipher

Denver - 13509056
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13509056@std.stei.itb.ac.id

***Abstrak*—Pada jaman dahulu kala, terdapat berbagai negara di masa perang. Mereka memiliki pesan-pesan penting, menyangkut nyawa banyak orang dan menyangkut masa depan berbagai negara tersebut. Adapun berbagai metode penguncian pesan yang digunakan, sampai pada lahirnya metode penguncian Vigenere Cipher. Penggunaan enkripsi pesan ini seperti musiman. Pada tahun sekian sampai sekian, metode yang berlaku metode A, metode ini akan segera tergantikan bila metode ini berhasil dipecahkan. Vigenere Cipher termasuk metode Kriptografi klasik, yang sudah lama terpecahkan oleh metode Kasiski. Titik kelemahan Vigenere Cipher ini dipecahkan oleh metode Kasiski. Disini penulis akan membedah, apa inti dari metode Vigenere Cipher ini, inti yang membedakan Vigenere Cipher dari Caesar Cipher. Apa kelemahan Vigenere Cipher sehingga dapat dipecahkan oleh metode Kasiski dan bagaimana penulis menambahkan elemen pewarnaan untuk menambal kelemahan yang ada pada Vigenere Cipher ini. Penulis juga akan menuliskan modifikasi-modifikasi yang dapat dilakukan pada program pewarnaan Vigenere Cipher yang penulis telah buat.**

***Kata Kunci*—kriptografi, vigener cipher, klasik, warna.**

I. LATAR BELAKANG

Vigener Cipher merupakan salah satu metode Kriptografi klasik yang cukup terkenal. Vigener Cipher merupakan bentuk *polyalphabetic substitution* yang men-enkripsi teks alfabet menggunakan sekumpulan ide dari Caesar Cipher. Vigener Cipher sudah dibuat berulang kali.

Gambar 1. Giovan Battista Bellaso

Pada dasarnya, metode ini dikemukakan pada tahun 1553 oleh Giovan Battista Bellaso dalam bukunya yang bernama *La cifra del. Sig. Giovan Battista Bellaso*.

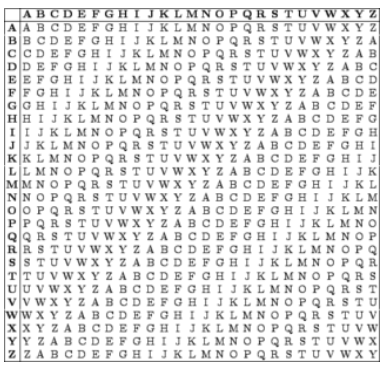
Veginer Cipher ini terkenal karena mudah untuk digunakan dan diimplementasikan. Metode ini juga terkenal karena tidak cukup rentan terhadap analisis frekuensi kemunculan huruf. Pada masa kejayaannya sandi ini dijuluki *le chiffre indechifferable*. Metode ini berhasil dipecahkan oleh metode Kasiski, yang ditemukan oleh Friedrich Kasiski.

Pada tahun 1863 Friedrich Kasiski merupakan orang yang sukses menemukan cara menyerang Vigener Cipher. Penyerangan pertama menggunakan pengetahun dari *plainteks* atau pengenalan kata sebagai kunci.

Pada tahun 1854, Charles Babbage terdorong untuk memecahkan Vigener Cipher ketika John Hall Brock Thwaites memasukan cipher yang baru ke dalam *Journal of the Society of the Arts*. Ketika Babbage menunjukan bahwa Thwaites Cipher menantang Babbage untuk memecahkan ciphernya. Babbage berhasil men-dekripsi sebuah sampel, yang hasilnya merupakan sebuah sajak *The Vision of Sin*, ditulis oleh Alfred Tennyson dengan kuncinya merupakan Emily, nama awal dari istri Tennyson. Babbage tidak pernah menjelaskan bagaimana metode yang ia gunakan sampai pada publikasi yang dilakukan oleh Kasiski.

II. DASAR TEORI

Pada metode Caesar Cipher, setiap huruf teks digantikan dengan huruf lain yang memiliki pergeseran tertentu pada urutan alfabet. Jumlah pergeseran dan arah pergeseran ini bersifat konstan untuk semua alfabet. Sedangkan pada Vigener Cipher, disediakan suatu sandi Caesar dengan nilai geser yang berbeda.



	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 2. Tabel Vigenere Cipher

Untuk men-enkripsi suatu pesan, dapat digunakan tabel Vigenere. Tabel Vigenere ini berisikan semua alfabet yang dituliskan pada lajur horizontal dan vertikal. Setiap kata di-enkripsi dengan menggunakan baris yang berbeda-beda, sesuai kunci yang diulang.

Sebagai contoh kita ingin men-enkripsi kata SAYA SEORANG KAPITEN dengan menggunakan kunci HAI.

Pertama-tama, kunci dibuat berulang-ulang hingga sama panjang dengan panjang *plainteks*, HAIHAIHAIHAIHAIHAIH.

Plainteks: AKU SEORANG KAPITEN
Kunci : HAIHAIHAIHAIHAIHAIH

Setiap huruf pada *plainteks* dipasangkan dengan setiap huruf pada kunci dengan melihat pada tabel vigenere, sehingga menghasilkan:

Cipher teks: HKC SMVRIUG RAXPTMU

Ada cara lain yang dapat digunakan selain menggunakan tabel vigenere. Rumus dibawah ini dapat digunakan untuk me-enkripsi *plainteks*.

$$C_i \equiv (P_i + K_i) \mod 26$$

C: Cipher teks
P: Huruf *plainteks*
K: kunci

Dengan hasil penguncian *plainteks* ini, kita dapatkan serangkaian kalimat yang telah terkunci yang dinamakan Cipher Teks. Proses ini dinamakan enkripsi. Lawan kata dari enkripsi adalah dekripsi. Proses dekripsi ini menggunakan rumus yang ada pada proses enkripsi.

$$P_i \equiv (C_i - K_i) \mod 26$$

(Keteragan simbol sama dengan keterangan simbol pada keterangan enkripsi)

Metode Kriptografi ini tentu mengundang penasaran para ahli Kriptografi untuk menemukan suatu metode untuk memecahkan Vigener Cipher ini. Metode yang berhasil ditemukan bernama metode Kasiski. Ide yang muncul pada metode ini adalah menggunakan frekuensi kemunculan pada *plainteks*. Misalkan kita menemukan bahwa huruf P paling banyak muncul pada cipherteks, dan bila *plainteks* yang dimaksud menggunakan Bahasa Inggris, maka huruf P berkorespondensi dengan E, karena E merupakan huruf yang paling banyak dipakai dalam Bahasa Inggris. Tapi hal ini tidak selamanya berlaku.

Salah satu kelemahan dari Vigener Cipher ini terletak pada kunci yang diberikan. Apabila seorang kriptanalis berhasil menemukan panjang dari kunci kemudian cipherteks dapat dicari sama seperti mendekripsi pada Caesar Cipher. Kasiski dan tes Friedman dapat membantu menemukan panjang dari kunci.

Tes Kasiski meninjau kenyataan bahwa kuncinya merupakan suatu kata yang diulang-ulang. Dibawah ini contoh yang digunakan, menggunakan kunci ABCD, dengan *plainteks* dan cipherteks dibawah ini.

```
Key:        ABCDABCDABCDABCDABCDABCDABCD
Plaintext:  CRYPTOISSHORTFORCRYPTOGRAPHY
Ciphertext: CSASTPKVSIQUTGQUCSASTPIUAQJB
```

Pada cipherteks hasil enkripsi, dapat terlihat dengan mudah suatu pengulangan. Kata CSASTP berulang dengan jarak perulangannya sepanjang 16 huruf. Asumsi bawa pengulangan pada cipherteks merepresentasikan segmen yang sama pada *plainteks*, hal ini mengindikasikan panjang dari kuncinya adalah 16, 8, 4, 2 atau 1 (semua faktor dari jarak pengulangan adalah semua kemungkinan panjang kuncinya). Bila panjang kunci nya 2 atau 1, dianggap tidak masuk akal, pertama-pertama yang perlu kita perhatikan adalah panjang 16, 8, atau 4. Semakin panjang *plainteks*, semakin akurat juga tes yang dilakukan karena pengulangannya itulah.

Tes Friedman (atau dikenal sebagai Tes Kappa) ditemukan pada tahun 1920an oleh William F. Friedman. Dia menggunakan tabel kemunculan, Dengan mengetahui probabilitas bahwa setiap dipilih dua sumber acak yang berbahasa sama (sekitar 0,067 untuk Bahasa Inggris) dan probabilitas kemunculan untuk pilihan acak seragam dari alfabet (0,0385 untuk Bahasa Inggris), panjang kunci dapat diperkirakan sebagai:

$$\frac{\kappa_p - \kappa_r}{\kappa_o - \kappa_r}$$

dimana,

$$\kappa_o = \frac{\sum_{i=1}^{c} n_i(n_i - 1)}{N(N-1)}$$

dan c adalah ukuran dari alfabet (26 untuk Bahasa Inggris), N adalah panjang dari *plainteks*, dan n1 sampai nc huruf-huruf pada cipherteks, dalam *integer*.

Bila panjang kunci telah diketahui, cipherteks dapat dikelompokan sesuai dengan panjang kuncinya. Setiap kolom terdiri dari *plainteks* yang dienkripsi oleh sebuah Caesar Cipher. Gunakan metode untuk memecahkan Caesar Cipher, maka *plainteks* dapat ditemukan.

Penemuan lebih lanjut dari metode Kasiski, dikenal sebagai metode Kerckhoffs. Metode ini menyamakan setiap kolom frekuensi kemunculan huruf bahasa yang dimaksud pada setiap kolom pada frekuensi kemunculan huruf cipherteks.

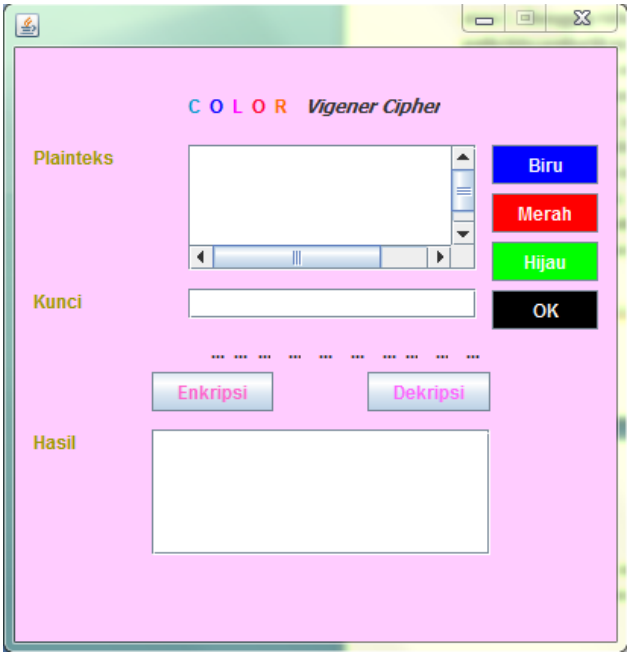
Selanjutnya, bila kunci telah ditemukan, kita dapat melakukan dekripsi pada cipherteks dengan menggunakan kunci yang telah kita temukan. Kunci ini menjadi pusat perhatian para kriptanalis dalam memecahkan Vigenere Cipher.

III. PENERAPAN WARNA PADA VIGENERE CIPHER

Pada bagian ini saya akan menjelaskan bagaimana kelemahan yang ada pada Vigenere Cipher akan saya tutupi dengan penambahan warna pada bagian kuncinya.

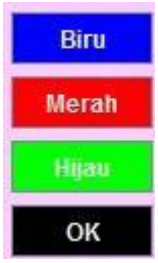
Seperti yang telah dibahas diatas, kelemahan Vigenere Cipher terletak pada kuncinya. Pengulangan kuncinya membuatnya mudah untuk bocor. Dengan penambahan warna pada elemen kuncinya, saya dapat mengacaukan pola perulangan yang ada. Telah dijelaskan bahwa untuk setiap huruf yang ada dalam *plainteks*, bila bertemu dengan suatu huruf dalam kunci, kapan dan dimanapun mereka bertemu, hasil cipherteks akan selalu sama. Itulah kelemahan dalam Vigenere Cipher yang saya maksud.

Dalam Vigenere Cipher yang saya buat, saya akan menambahkan elemen warna pada penguncian. Jadi, akan disediakan sebuah kolom untuk memasukan kunci alfabet seperti biasa, dan akan terdapat sebuah *generate color* untuk memasukan warna pada kunci. Warna-warna yang dipilih akan dimasukan secara berurutan pada kunci yang telah dimasukan. Warna-warna yang telah dipilih, akan dimasukan ke dalam kunci secara berulang, sama seperti kunci masukan. Sebagai contoh kunci masukan AKU, maka kunci akan diulang sepanjang *plainteks* menjadi AKUAKUAKUAKUAK.....dan seterusnya. Sama dengan warna, warna yang telah dipilih, akan diulang terus menerus sampai semua kunci terwarnai. Dibawah ini adalah tampilan secara umum dari program yang saya buat.



Gambar 3. Gambaran keselurahan dari program

Pada gambar diatas terlihat program yang saya buat menggunakan bahasa pemograman Java. Program yang saya buat dinamai Color Vigenere Cipher. Jumlah warna yang saya sediakan hanya 3 warna dasar yang dalam sinar yaitu merah, hijau, dan biru (RGB).

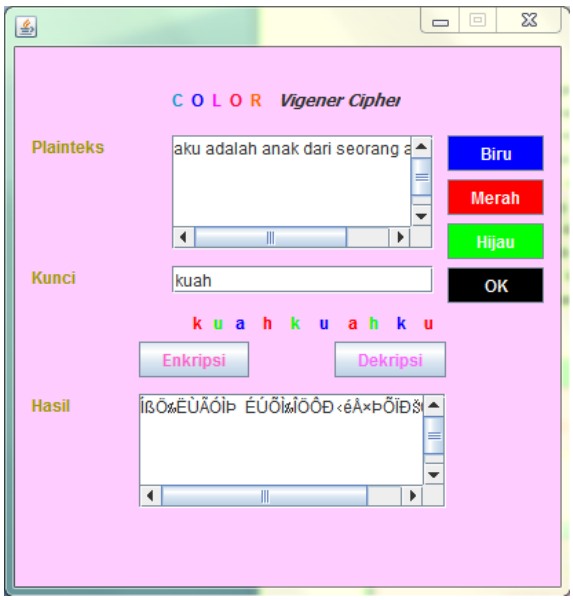


Gambar 4. Generate Color

Gambar diatas adalah alat untuk men-*generate* warna. Dengan mengklik satu per satu pada warna tersebut, dan memencat tombol OK, maka warna akan langsung dimasukan ke dalam kunci. Urutan pemilihan warna juga menjadi perhatian disini karena masing-masing warna memiliki arti yang berbeda-beda. Bila merah ditekan pertama, hijau ditekan kedua, dan biru ditekan terakhir, dan kemudian kita tekan OK, maka urutan pewarnaan kunci akan menjadi Merah – Hijau – Biru – Merah – Hijau – dan seterusnya. Jumlah warna yang saya sediakan dalam program ini dibatasi sejumlah 3 warna saja.

Gambar 5. Tampilan hasil masukan *plainteks* dan kunci beserta hasil *generate color* pada kunci

Kunci pertama yang dimasukan oleh pengguna tertulis biasa dengan warna hitam. Setelah pengguna menekan ketika warna yang ada disamping kanan kolom *plainteks* maka dan menekan OK, maka program akan men-*generate color* yang dipilih oleh penguna dah hasilnya ditampilkan dibawah kunci yang dimasukan pengguna. Kata "kuahkuahku" dibawah kolom kunci, adalah kunci yang telah dimasuki warna setelah pengguna memilih warna pada *generate color*. Kunci inilah yang akan dipakai ke dalam Vigener Cipher untuk menghasilkan cipherteks. Tampilan kunci berwarna tidak ditampilkan sama panjang dengan *plainteks*. Kunci bewarna hanya ditampilkan



Gambar 6. Tampilan keselurahan beserta hasil enkripsi

Diatas merupakan tampilan dari hasil enkripsi *plainteks* dengan kunci berwarna. Langkah enkripsi yang dilakukan pertama-tama adalah mengambil *plainteks* dan kunci berwarna. Untuk kunci berwarna ini, akan ditaruh dalam suatu penyimpan yang berbeda. Kunci tanpa warna disimpan sendiri dan urutan perwarnaan disimpan sendiri. Kemudian *plainteks* dan kunci tanpa warna di-enkripsi dengan metode Vigenere Cipher biasa. Vigenere Cipher yang biasa yang dimaksudkan adalah Vigenere Cipher 256 karatker apa adanya. Maksudnya apa adanya, spasi dikut dienkripsi dengan kunci. Hasil yang ada, sebelum dimasukan ke dalam penampung hasil, akan dimasukan ide dari urutan pewarnaan ini.

Ide yang ada dibalik kunci berwarna ini adalah untuk setiap warna yang ada di dalam kunci, memiliki makna yang berbeda-beda. Untuk kunci yang diberi warna merah, hasil enkripsinya akan digeser maju sebanyak satu kali. Warna hijau akan memberi efek geser mundur sebanyak satu kali dan warna biru dibiarkan untuk tidak diberi efek.

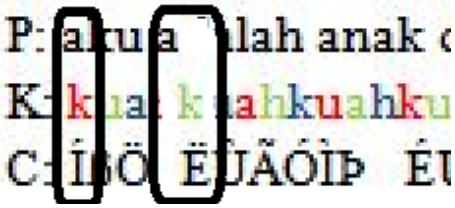
Karena pada setiap kunci diberi warna yang berbeda-beda, maka tiap huruf yang sama pada *plainteks* bila bertemu dengan huruf yang sama pada kunci, maka memungkinkan untuk menghasilkan cipherteks yang berbeda-beda. Sebagai contoh, pada masukan diatas

P: aku adalah anak dari seorang ayah

K: kuahkuahkuahkuahkuahkuahkua

C: ÍßÖ‰ËÙÃÓÌÞ□ ÉÚÕÌ‰ÎÖÔÐ‹éÅ×ÞÕÏÐŠÖÛÈÓ

Pada *plainteks* terdapat aku adalah, ‘a’ pada kata aku dan ‘a’ pada kata adalah, bertemu dengan huruf kunci yang sama ‘k’, tetapi berbeda warnanya, hasil nya berbeda.

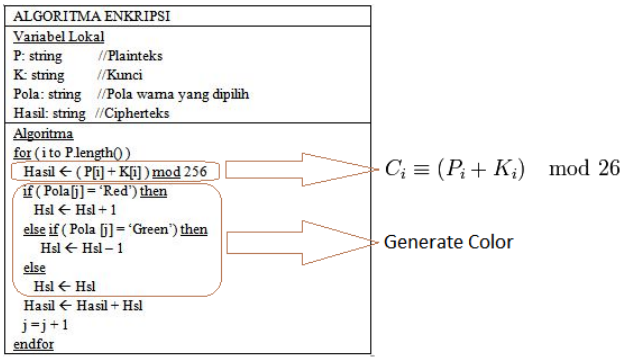


Gambar 7. Huruf yang sama pada *plainteks* dan kunci bisa menghasilkan cipherteks yang berbeda

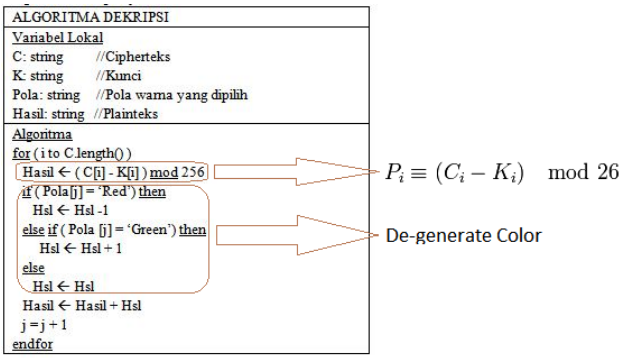
Hal ini disebabkan karena huruf ‘k’ pada kunci berbeda warnanya, ‘k’ yang pertama bewarna merah yang berarti hasil enkripsi biasa digeser maju satu kali, sedangkan ‘k’ yang kedua bewarna hijau yang berarti hasil enkripsi biasa digeser mundur satu kali. Berikut dibawah ini merupakan algoritma enkripsi.

```
ALGORITMA ENKRIPSI
Variabel Lokal

P: string       //Plainteks
K: string       //Kunci
Pola: string    //Pola warna yang dipilih
Hasil: string   //Cipherteks
Algoritma

for ( i to P.length() )
  Hasil ← ( P[i] + K[i] ) mod 256
  if ( Pola[j] = ‘Red’) then
    Hsl ← Hsl + 1
  else if ( Pola [j] = ‘Green’) then
     Hsl ← Hsl – 1
  else
    Hsl ← Hsl
  Hasil ← Hasil + Hsl
  j = j + 1
endfor
```

Proses enkripsi ini dilakukan berdasarkan rumus yang telah diberikan pada awal makalah ini. Hanya saja letak perbedaan ada pada “mod 26”. Karena menggunakan 256 karakter, dengan membedakan antara huruf besar dan kecil, maka dijadikan “mod 256”.



Gambar 7. Algorima enkripsi warna Vigenere Cipher dalam notasi algoritmik



Gambar 8. Algoritma dekripsi warna Vigenere Cipher dalam notasi algoritmik

Pada proses dekripsi, untuk mengembalikan *plainteks* dari cipherteks yang dibuat, hanya dengan melakukan dekripsi Vigener Cipher biasa dan melakukan sedikit modifikasi pada sisi pengaturan warnanya. Berikut adalah algoritma dekripsinya.

```
ALGORITMA DEKRIPSI
Variabel Lokal

C: string       //Cipherteks
K: string       //Kunci
Pola: string    //Pola warna yang dipilih
Hasil: string   //Plainteks
Algoritma

for ( i to C.length() )
  Hasil ← ( C[i] - K[i] ) mod 256
  if ( Pola[j] = 'Red') then
    Hsl ← Hsl -1
  else if ( Pola [j] = 'Green') then
     Hsl ← Hsl + 1
  else
    Hsl ← Hsl
  Hasil ← Hasil + Hsl
  j = j + 1
endfor
```

Untuk melakukan dekripsi cipherteks, kita hanya perlu melakukan perubahan pada sisi rumus Vigenere Ciphernya dan melakukan perubahan pada *generate color*-nya. Rumus dekripsi Vigenere Ciphernya kita dapatkan pada rumusan pada pembahasan pada bab II Dasar Teori diatas. Sedangkan untuk melakukan *degenerate color* kita hanya perlu merubah, apabila warna merah, awalnya dimajukan satu kali, maka disini akan dimundurkan satu kali. Bila warna hijau memundurkan huruf satu kali, maka disini huruf akan dimajukan satu kali. Untuk warna biru dibiarkan sama. Urutan Vigenere Cipher dan *generate color* juga perlu ditukar.

IV. ANALISIS

Dalam pengaplikasian warna pada Vigenere Cipher ini, ada hal yang harus diperhatikan. Perbandingan antara panjang kunci yang dimasukan dengan jumlah pola pewarnaan atau sebaliknya, hasil modulusnya harus bukan merupakan nol. Sebagai misal panjang kunci berjumlah 4, maka panjang pola warna tidak boleh bernilai 2, 4, 8, 12, 16, dan seterusnya. Hal in mencegah pemberian warna pada kunci tidak berulang. Dengan maksud, diharapkan suatu huruf pada kunci diulang-ulang dan mendapatkan warna yang berbeda-beda.

Pemberian warna ini dapat dibilang membuat sulit kriptanilis dalam memecah sandi Vigenere Cipher ini, terutama yang menggunakan metode Kasiski dan metode frekuensi kemunculan huruf. Karena frekuensi kemunculan huruf yang sama untuk pendeteksian *plainteks* semakin jarang dan sulit ditemukan. Huruf yang muncul pada cipherteks menjadi lebih *randomi* ketimbang Vigenere Cipher biasa.

Program pewarnaan Vigenere Cipher yang saya buat ini, sebenarnya dapat dimodifikasi lebih lanjut untuk meningkatkan tingkat keamanan dari enkripsi pesan ini. Dengan menambahkan jumlah pewarnaan yang dapat dipilih, akan membantu kunci untuk lebih mengacak pesan yang akan di-enkripsi. Andaikan saja panjang pola pewarnaan sejumlah warna primer dan warna sekunder total adalah 6 warna. Maka tiap huruf dari kunci akan mendapatkan 6 variasi enkripsi dengan huruf yang sama pada *plainteks*. Bila huruf yang sama ini bertemu dengan huruf lain pada *plainteks*, maka akan memberikan 6 variasi kemunculan cipherteks. Cukup banyak variasi yang diberikan dari hanya 6 warna yang diberikan.

Selain memodifikasi pemberian warna pada kunci, pemberian pola pewarnaan juga dapat diberikan pada *plainteks* dengan tujuan memberikan variasi pada penghasilan cipherteks yang berbeda-beda antara huruf *plainteks* dan huruf pada kunci yang sama.

V. KESIMPULAN

Berikut dibawah ini adalah kesimpulan yang dapat diambil dari makalah secara keseluruhan:

- Memberikan efek pewarnaan pada kunci merupakan salah satu modifikasi kunci yang dapat diberikan pada metode Kriptografi Vigenere Cipher.
- Metode Vigenere Cipher dapat ditambal titik kelemahannya dari penggunaan metode Kasiski dan metode analisis frekuensi kemunculan huruf dengan penambahan warna pada kunci sehingga menghasilkan suatu metode Kriptografi yang lebih amans.
- Beberapa modifikasi dapat dilakukan untuk meningkatkan keamanan Vigenere Cipher bewarna.

REFERENSI

[1] http://buddhawannabe.wordpress.com/2007/09/21/vigenere-cipher-dengan-pembangkitan-kunci-menggunakan-bilangan-euler/ (17/03/12)

[2] http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher (17/03/12)

[3] http://id.wikipedia.org/wiki/Sandi_Vigen%C3%A8re (17/03/12)

[4] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/kripto10-11.htm (18/03/12)

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 19 Maret 2012

Denver - 13509056