Modifikasi Bigram dan Penggunaan Tabel Tiga Dimensi pada Vigenere Cipher

Aji Nugraha Santosa Kasmaji 13510092
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13510092@std.stei.itb.ac.id

***Abstract*—Metode vigenere cipher adalah salah satu dari metode enkripsi klasik yang cukup terkenal. Namun pada metode tersebut telah ditemukan beberapa titik lemah yang dapat digunakan dalam proses kriptanalisis. Pada makalah ini akan dibahas modifikasi lebih lanjut dari metode vigenere cipher dengan tujuan menambah kerumitan dari pola *cipher text* yang dihasilkan. Modifikasi pertama dilakukan dengan mengembangkan tabel vigenere yang digunakan menjadi tabel 3 dimensi, sehingga proses enkripsi akan menjadi lebih kompleks. Modifikasi kedua adalah dengan mengaplikasikan enkripsi secara bigram, seperti yang biasa digunakan dalam playfair cipher sehingga diharapkan dapat mengacaukan metode analisa frekuensi. Akan lebih lanjut dibahas tiga buah algoritma yang diterapkan dengan menggunakan modifikasi yang telah disebutkan. Algoritma pertama adalah penggunaan kunci ganda pada vigenere cipher. Algoritma kedua mengaplikasikan teknik bigram pada vigenere cipher. Dan algoritma ketiga adalah modifikasi lebih lanjut dari teknik kedua. Selain itu akan dilakukan analisa lebih lanjut untuk menguji dan membandingkan ketahanan dari ketiga algoritma tersebut.**

***Index Terms*—kriptografi klasik, modifikasi, vigenere cipher, bigram, kriptanalisis**

I. PENDAHULUAN

Metode *Vigenere cipher* adalah salah satu dari beberapa metode kriptografi klasik yang sering digunakan. Metode ini menggunakan kunci untuk memetakan sebuah *plain text* menjadi *cipher text*, sesuai dengan aturan yang direpresentasikan dalam bentuk tabel. Tujuan dari pengembangan metode ini awal mulanya digunakan untuk mengaburkan pemetaan satu huruf *plain text* ke satu huruf *cipher text*, yang dapat dianalisa dengan mudah dengan menggunakan analisa frekuensi terhadap kemunculan huruf-huruf yang ada.

Namun seiring dengan perkembangan jaman, telah ditemukan beberapa metode yang dapat digunakan untuk melakukan kriptanalisis terhadap *cipher text* yang dihasilkan oleh Vigenere cipher tersebut. Salah satu metode disebut dengan metode Kasiski, yang memanfaatkan lebih lanjut titik lemah Vigenere cipher dan analisa frekuensi secara parsial. Sehingga dengan menggunakan metode-metode tersebut, *cipher text* dapat didekripsi secara paksa oleh pihak ketiga.

Pada makalah ini, akan ditawarkan beberapa modifikasi yang digunakan untuk memperumit penggunaan *Vigenere cipher*. Modifikasi ini dilakukan dengan harapan untuk menambah ketahanan cipher text yang dihasilkan, tanpa mengubah pola pengunaan asal dari *Vigenere cipher* itu sendiri.

II. DASAR TEORI

A. Vigenere Cipher

Vigenere cipher adalah sebuah metode yang digunakan untuk melakukan enkripsi terhadap teks alfabet dengan menggunakan beberapa urutan afabet *Caesar cipher* yang berbeda, yang disesuaikan dengan huruf-huruf yang ada pada kata kunci. *Vigenere cipher* dapat dikatakan sebagai bentuk sederhanda dari enkripsi jenis cipher substitusi abjad majemuk.

Vigenere cipher menggunakan bujursangkar Vigenere untuk melakukan enkripsi. Pada setiap baris bujur sangkar, dituliskan huruf-huruf sesuai dengan urutan yang diperoleh dengan menggeser beberapa huruf seperti yang digunakan pada *Caesar cipher*. Untuk melakukan enkripsi, akan dibutuhkan kunci tertentu. Tiap huruf yang dimiliki oleh kunci akan digunakan untuk menentukan jumlah pergeseran huruf pada teks yang akan dienkripsi. Penentuan huruf cipher pada metode *Vigenere cipher* klasik dapat dituliskan dengan rumus berikut:

$$C_i(p) = (p + k_i) \bmod 26$$

Ketika panjang kunci yang digunakan lebih pendek dibandingkan dengan panjang *plain text*, maka kunci akan digunakan berulang secara periodik. Contoh aplikasi dari vigenere cipher dapat dilihat pada contoh berikut:

Plain text	: `BREAKINGLAW`
Kunci	: `cipherkeyci`
Cipher text	: `DZTHOZXKJCE`

Dapat dilihat bahwa huruf yang sama dapat dipetakan menjadi huruf cipher yang berbeda, pada kasus ini huruf A dapat menjadi huruf H maupun C. hal inilah yang menjadi sifat utama dari cipher substitusi abjad majemuk. Untuk bagaimana cara penggunaan bujursangkar vigenere

dapat dilihat pada gambar 1.

	A	B	C	D	E	F	G	H
a	A	B	C	D	E	F	G	H
b	B	C	D	E	F	G	H	I
c	C	D	E	F	G	H	I	J
d	D	E	F	G	H	I	J	K
e	E	F	G	H	I	J	K	L
f	F	G	H	I	J	K	L	M

Gambar 1. Ilustrasi pemetaan vigenere cipher untuk huruf 'B' dengan kunci 'c'

B. Analisa Frekuensi

Analisa frekuensi adalah sebuah metode pada kriptanalisis yang mempelajari frekuensi dari huruf dan kumpulan huruf pada *cipher text*, yang digunakan untuk melawan jenis enkripsi yang memiliki basis substitusi huruf. Analisa frekuensi pertama kali ditemukan pada abad ke-9 oleh Al-Kindi.

Analisa frekuensi diterapkan dengan memanfaatkan sifat dasar suatu bahasa. Setiap bahasa tentunya memiliki huruf atau kumpulan huruf yang pada penggunaannya memiliki frekuensi yang berbeda-beda pula. Dasar yang lain adalah dengan memperhitungkan fakta bahwa huruf yang sering muncul pada *plain text* suatu bahasa, maka huruf substitusinya juga akan sering muncul pula pada *cipher text*. Dengan melakukan perhitungan statistik, maka kemunculan huruf pada sebuah *cipher text* dapat dianalisa dengan membandingkan dengan kemungkinan huruf atau kumpulan huruf yang pada suatu bahasa.

C. Metode Kasiski

Metode Kasiski adalah sebuah metode yang digunakan dalam kriptanalisis untuk melawan cipher abjad majemuk, seperti contohnya *Vigenere cipher* sendiri. Metode ini ditemukan oleh Friedrich Kasiski pada tahun 1863.

Dengan menggunakan metode Kasiski, proses kriptanalisis pertama kali akan dititikberatkan pada pencarian panjang suatu kata kunci yang digunakan pada proses enkripsi cipher abjad majemuk. Setelah panjang kunci diketahui, maka *plain text* akan dibagi menjadi beberapa bagian sesuai dengan jumlah huruf yang ada pada kata kunci. Barulah tiap bagian tersebut didekripsi masing-masing dengan perlakuan yang sama dengan cipher abjad tunggal, misalnya dengan analisa frekuensi.

Pada metode ini, pertama akan dicari panjang kunci dengan memanfaatkan kemungkinan adanya pengulangan kata, atau mungkin urutan huruf yang ada pada suatu *plain text*. Metode ini juga memanfaatkan sifat *Vigenere cipher*, dimana penggunaan kunci diulang secara periodik. Apabila kata pada *plain text* tersebut dikenai enkripsi dengan urutan kunci yang sama, maka akan menghasilkan *cipher text* yang sama pula. Jarak antara kata yang sama tersebutlah yang dapat dicurigai sebagai kelipatan dari panjang kata kunci yang digunakan. Perlakuan ini diulang beberapa kali untuk urutan kata yang berbeda, dan dari beberapa jarak antar kata berulang yang ditemukan dapat dicari nilai faktor persekutuan yang sama dari beberapa kasus. Contohnya pada kasus sebagai berikut:

Plain : `CRYPTO IS SHORT FOR CRYPTO…`
Kunci : `abcdab cd abcda bcd abcdab…`
Cipher : `CSASTP KV SIQUT GQU CSASTP…`

Dapat dilihat bahwa kata `CRYPTO` dienkripsi menjadi *cipher text* yang sama, yaitu `CSASTP`. Hal ini dikarenakan kedua kata tersebut dienkripsi menggunakan kunci yang sama yang diakibatkan oleh perulangan kunci pada *Vigenere cipher*. Dari data tersebut, kita dapat menemukan jarak antara perulangan kata adalah 16, oleh karena itu dapat kita simpulkan panjang kunci yang digunakan memiliki kemungkinan: 1, 2, 4, 8, 16.

III. DESKRIPSI SOLUSI

Pada bagian ini akan dibahas mengenai modifikasi algoritma yang ditawarkan untuk menambah tingkat kerumitan dan ketahanan Vigenere cipher terhadap serangan yang telah ada. Metode yang digunakan akan menggunakan hasil modifikasi dari bujursangkar Vigenere, yaitu kubus Vigenere. Kubus Vigenere merupakan tabel 3 dimensi yang menampung daftar urutan huruf *Caesar cipher* untuk dua sumbunya.

Kubus vigenere yang digunakan memiliki beberapa pengaturan tambahan. Pengaturan pertama, pada dimensi pertama dan dimensi kedua yang merupakan bujursangkar vigenere pada umumnya, urutan huruf Caesar cipher dibalikan urutannya, dimulai dari huruf Z. Namun untuk dimensi ketiganya, tetap dilakukan terurut sesuai abjad. Hal ini dilakukan mengingat bahwa bujursangkar vigenere telah diketahui luas oleh masyarakat dunia, sehingga dengan melakukan hal ini, para kriptanalisis tidak memliki awalan atau senjata berupa bujursangkar Vigenere tersebut. Gambaran mengenai isi kubus vigenere dapat dilihat pada gambar 2.

Z	Y	X	W	V	U	T	S	R
Y	X	W	V	U	T	S	R	Q
X	W	V	U	T	S	R	Q	P
W	V	U	T	S	R	Q	P	O
V	U	T	S	R	Q	P	O	N

(a)

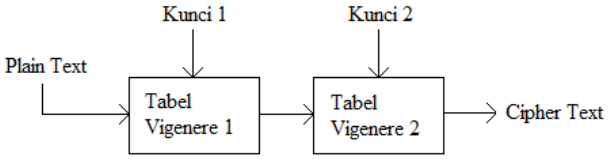
Z	A	B	C	D	E	F	G	H
Y	Z	A	B	C	D	E	F	G
X	Y	Z	A	B	C	D	E	F
W	X	Y	Z	A	B	C	D	E
V	W	X	Y	Z	A	B	C	D

(b)

Gambar 2. Ilustrasi isi Kubus Vigenere (a) Dimensi pertama dan kedua (b) Dimensi kedua dan ketiga

A. Penggunaan Kunci Ganda

Pada proses modifikasi pertama, dimensi ketiga dari kubus Vigenere digunakan sebagai tempat untuk menampung kunci kedua. Sehingga pada satu kali proses enkripsi, digunakan dua kunci yang berbeda. Kunci pertama digunakan untuk melakukan enkripsi terhadap huruf pada *plain text*, sementara kunci kedua akan digunakan untuk melakukan enkripsi terhadap hasil yang didapatkan pada enkripsi sebelumnya. Struktur sistem pada modifikasi ini dapat dilihat pada gambar 3.



Gambar 3. Ilustrasi sistem Vigenere cipher kunci ganda

Proses penggunaan kunci ganda ini sama halnya dengan melakukan proses *Vigenere cipher* sebanyak dua kali. Hanya saja proses enkripsi tiap tahapannya akan menggunakan dua bujursangkar Vigenere yang berbeda akibat dari modifikasi yang dilakukan pada kubus Vigenere sebelumnya. Proses penggunaan kunci ganda ini merupakan modifikasi yang paling umum digunakan pada vigenere cipher, serta dilakukan juga pada kriptografi modern, yaitu *Triple DES*.

Tujuan dari modifikasi yang pertama ini yang pertama adalah untuk meningkatkan keamanan enkripsi, karena pada proses enkripsi pertama akan menggunakan dua kunci, serta seolah-olah menggunakan dua bujursangkar Vigenere yang berbeda. Hal ini dilakukan dengan harapan proses kriptanalisis menjadi dua kali lebih lama, karena harus melakukan perhitungan sebanyak dua kali juga.

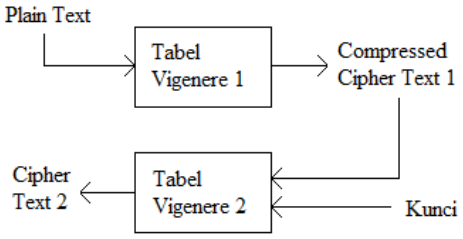
Tujuan kedua adalah untuk mengaburkan hubungan antara *plain text* dengan *cipher text*. Pada analisa frekuensi, dibutuhkan informasi mengenai bahasa yang digunakan pada *plain text*. Hal tersebut diperlukan untuk mengetahui statistik kemungkinan munculnya suatu huruf pada suatu bahasa. Contohnya huruf E,T,A,O,I,N adalah huruf dengan tingkat kemunculan tingga dalam bahasa Inggris. Namun, dengan melakukan enkripsi sebanyak dua kali, maka bagian dari *cipher text* yang didapat dari pembagian metode kasiski berisi hasil enkripsi dari *cipher text* sebelumnya, sehingga harapannya tidak akan bisa dikaitkan terhadap suatu bahasa tertentu.

Contoh proses enkripsi dapat dilihat pada bagian di bawah ini:

Plain text : `VIGENERE`
Kunci 1 : `firstfir`
Kunci 2 : `secondse`
Cipher text : `RNERGTSI`

B. Enkripsi pada Pasangan Huruf (Bigram)

Bentuk modifikasi kedua lebih cenderung mengubah bagaimana cara enkrispi suatu *plain text* dilakukan. Metode ini mengambil tata cara enkripsi terhadap *plain text* dari *Playfair cipher*. Pada modifikasi kedua ini, proses enkripsi akan dilakukan per pasangan huruf. Dimensi pertama dan dimensi kedua digunakan untuk menentukan pada sel dua dimensi mana letak suatu pasangan huruf pada dimensi pertama dan dimensi kedua kubus vigenere. Sementara pada dimensi ketiga digunakan untuk memetakan pasangan huruf menjadi sebuah huruf cipher berdasarkan kunci yang digunakan. Struktur sistem pada modifikasi ini dapat dilihat pada gambar 4.



Gambar 4. Ilustrasi sistem Vigenere cipher pasangan kata

Tujuan dari modifikasi kedua adalah untuk mengatasi masalah analisa frekuensi pada umumnya. Selain itu untuk mempersulit analisa terhadap pasangan kata (bigram). Misalnya saja kata "*THE*" pada *plain text* melalui metode ini dapat dipecah menjadi dua kemungkinan, yaitu "*TH*" dan "*HE*", yang masing-masing dapat dirubah menjadi suatu huruf cipher tertentu, dan dienkripsi lebih lanjut dengan menggunakan kunci yang tertera. Oleh karena itu diharapkan metode ini dapat menyulitkan analisa secara bigram.

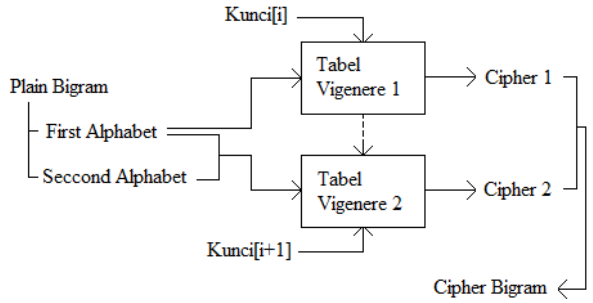
Tujuan yang kedua adalah untuk menerapkan *compressed cipher* pada metode kriptografi klasik. Dengan menggunakan *compressed cipher*, maka ada dua keunggulan yang harapannya dapat diperoleh. Keunggulan pertama adalah menurunnya ukuran berkas yang digunakan untuk mengirim pesan, sehingga pesan rahasia yang cukup panjang akan cukup ditampung dalam ukuran yang lebih kecil. Keunggulan kedua adalah dengan *compressed cipher*, maka secara tidak langsung dapat menciptakan aspek chaos pada kriptografi. Hal ini dikarenakan pada umumnya kriptografi digunakan untuk memetakan satu huruf *plain text* menjadi tepat satu huruf *cipher text*. Sehingga, dengan menggunakan jenis *compressed cipher* atau *expansive cipher* akan memberikan suatu kesulitan tersendiri bagi kriptanalis.

Namun, dalam perancangan modifikasi kedua ini telah ditemukan beberapa titik lemah dari modifiikasi jenis ini. Kelemahan yang pertama adalah metode ini sangat bergantung pada kubus vigenere yang digunakan, sehingga kerahasiaan kubus vigenere haruslah sangat dijaga. Kelemahan yang kedua adalah metode ini cukup rentan terhadap metode Kasiski yang dapat dimodifikasi untuk bigram, sehingga *cipher text* memiliki kemungkinan untuk dipecahkan begitu kriptanalis mengetahui bahwa satu huruf *cipher text* mewakili dua huruf *plain text.*

C. Enkripi Kombinasi pada Pasangan Huruf

Modifikasi ketiga dapat dikatakan sebagai kombinasi antara modifikasi pertama dan modifikasi kedua, dan metode vigenere klasik. Titik berat pada modifikasi ketiga ini adalah bagaimana suatu proses enkripsi dapat terdiri dari lebih dari satu pemrosesan yang berbeda, hanya dengan menggunakan satu kunci saja.

Proses enkripsi dimulai dengan melakukan pemecahan *plain text* menjadi bentuk pasangan dua huruf. Huruf pertama akan digunakan pada tabel vigenere 1 (dimensi pertama dan kedua kubus Vigenere), dengan melakukan proses vigenere cipher klasik. Dari hasil tersebut didapatkan keluaran pertama dari proses enkrispi bigram. Lalu pasangan huruf tersebut dienkripsi dengan menggunakan modifikasi kedua, dengan huruf berikutnya dari kunci yang telah digunakan sebelumnya. Dari proses kedua tersebut akan dihasilkan keluaran kedua. Hasil keluaran pertama dan keluaran kedua yang masing-masing berupa sebuah huruf kemudian disusun menjadi sebuah bigram, dan hasil tersebutlah yang menjadi *cipher bigram* yang nantinya akan disusun kembali menjadi *cipher text* yang utuh. Struktur sistem pada modifikasi ini dapat dilihat pada gambar 5.



Gambar 5. Ilustrais *Vigenere cipher* kombinasi

Contoh proses enkripsi dapat dilihat pada bagian di bawah ini:

Plain text : `VIGENERE`
Kunci 1 : `firstfir`
Cipher text : `JEKHFNQV`

Proses :

- V dienkripsi tabel 1dengan kunci f → J
- VI dikompres dengan tabel vigenere 1→ W
- W dienkripsi tabel 2 dengan kunci I → E
- J dihubungkan dengan E → JE

Tujuan dari pengembangan modifikasi ketiga ini adalah untuk melakukan eksperimen dengan menggabungkan berbagai macam modifikasi *Vigenere cipher* yang telah dibuat sebelumnya. Harapannya, dengan melakukan penggabungan maka fitur dari masing-masing modifikasi mampu menutupi kelemahan dari bagian modifikasi lainnya.

Tujuan lainnya adalah untuk menambah kerumitan pada proses enkripsi, dengan memasukkan dua buah proses yang berbeda, dengan memakai bagian kunci yang berbeda pula untuk satu kali proses enkripsi. Dengan hal tersebut, maka analisa frekuensi harapannya menjadi kurang efektif untuk diterapkan pada cipher text yang dihasilkan, karena cipher text mengandung dua jenis pemetaan, yaitu pemetaan satu huruf ke satu huruf, serta pemetaan terkompresi.

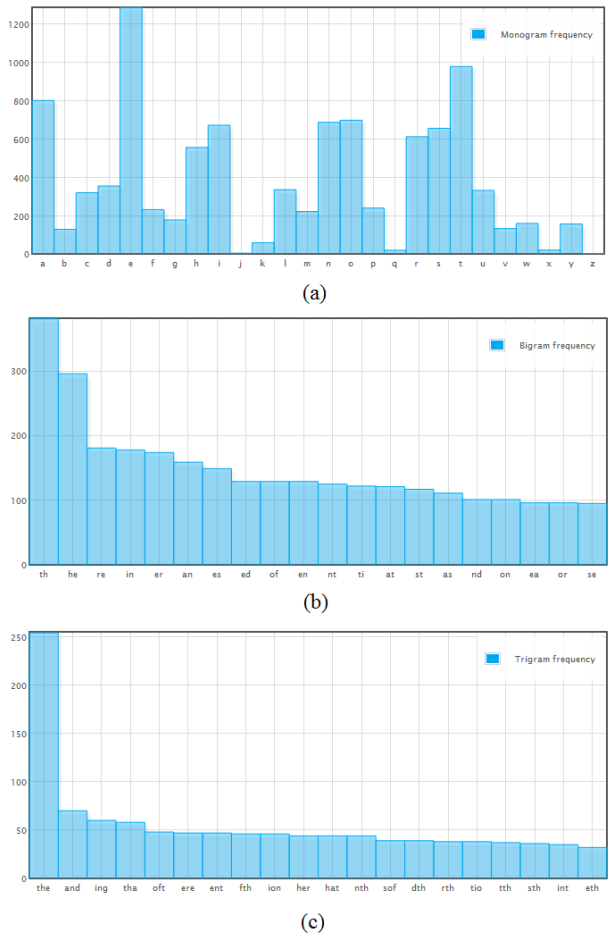
IV. IMPLEMENTASI DAN ANALISIS

A. Target Plain Text

Target *plain text* yang digunakan merupakan sebuah tulisan eksposisi panjang dalam bahsa Inggris yang diambil dari:

http://www.bbc.co.uk/history/ancient/romans/pompeii_portents_01.shtml

Plain text terdiri dari 9823 huruf, dengan sebelumnya telah dihilangkan unsur-unsur berupa angka, spasi dan simbol-simbol lainnya. Data lebih lanjut terkait analisa frekuensi target *plain text* dapat dilihat pada gambar 6.



(a) (b) (c)

Gambar 6. Data terkait analisa frekuensi terhadap target *plain text* (a) monogram (b) bigram (c) trigram

Pada monogram dapat dilihat bahwa huruf yang dominan adalah E, T, A, O, I, N; Bigram yang paling dominan adalah TH dan HE; Trigram yang paling dominan adalah THE, sesuai dengan struktur alami bahasa Inggris

B. Struktur Dasar Kubus Vigenere

Berikut adalah algoritma umum yang digunakan untuk membentuk struktur awal dari kubus vigenere yang digunakan:

```
public int[26][26][26] alphabetMatrix;

for (int i=0; i<alphabetMatrix.length; i++){
   for (int j=0; j<alphabetMatrix[i].length; j++){
      for (int k=0; k<alphabetMatrix[i][j].length; k++){
         if (25 - (i + j - k) >= 0){
            alphabetMatrix[i][j][k] ← (25-(i+j-k)) % 26;
         } else {
            alphabetMatrix[i][j][k] ← (25-(i+j-k)) + 26;
         }
      }
   }
}
```

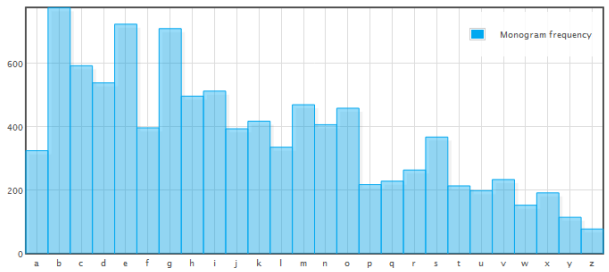
Hasilnya adalah kubus vigenere yang sesuai dengan rancangan pada deskripsi solusi yang ditawarkan sebelumnya.

C. Vigenere Cipher dengan Kunci Ganda

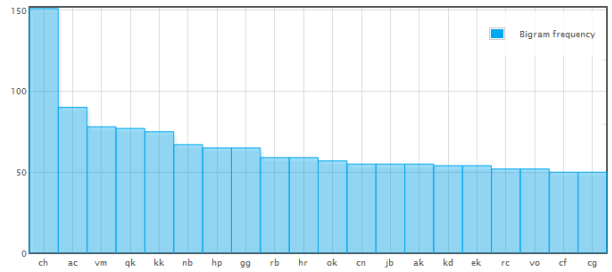
Berikut adalah algoritma umum yang digunakan untuk melakukan enkripsi dengan veigenere cipher kunci ganda:

```
function Encrypt1(input String: text, key1, key2) → String
KAMUS
 Result: String
 i, j, k, iPlain, iKey1, iKey2: integer
ALGORITMA
 i ← 0
 j ← 0
 k ←  0

  while (i < inputText.length()){
  // Merubah karakter ASCII menjadi nomor pada kubus
     iPlain ← text[i]-65
    iKey1 ← key1[j]-65
    iKey2 ← key2[k]-65

  // proses enkripsi
    result ← result +
    (alphabetMatrix[iKey1][iPlain][iKey2]+65)

  // iterator
    i ← i + 1

    if (j < (tKey1.length-1)){
       j ← j + 1
    } else {
       j ← 0
    }

    if (k < (tKey2.length-1)){
       k ← k + 1
    } else {
       k ← 0;
    }
  }

 → result
```

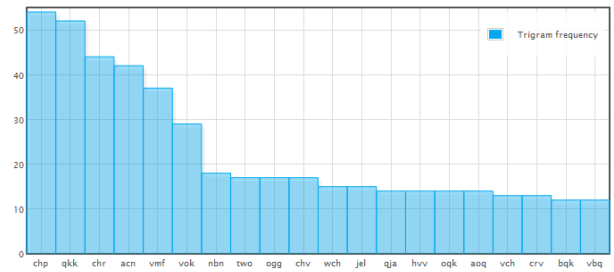
Dari hasil enkripsi menggunakan algortima Vigenere cipher dengan kunci ganda: "*oceano*" dan "*graphy*" analisa frekuensi yang didapatkan dari cipher text hasil dapat dilihat pada gambar 7.



(a)



(b)



(c)

Gambar 7. Data terkait analisa frekuensi terhadap hasil enkripsi modifikasi pertama (a) monogram (b) bigram (c) trigram

Dapat dilihat pada gambar bahwasecara monogram dan trigram, persebaran huruf menjadi lebih landai dibandingkan dengan *plain text*, sementara pada bigram tidak berpengaruh banyak. Sehingga dapat dikatakan cipher text akan lebih sulit dianalisa oleh kriptanalis.

Untuk pengatasan metode Kasiski, pada data frekuensi ditemukan bahwa trigram chp memiliki kemunculan paling banyak, beberapa di antaranya pada urutan huruf ke: 122, 212, 584, 638, 1022, 1034, 1178, 1190, 1334, , 1394, dan seterusnya. Setelah dihitung berapa factor persekutuan terbesarnya, ditemukan hasilnya adalah 6, yang mana tepat dengan "*oceano*" maupun "*graphy*"

yang panjangnya masing-masing adalah 6 huruf. Dengan demikian dapat dikatakan bahwa modifikasi jenis pertama rentan terhadap serangan metode Kasiskidalam pencarian panjang kunci, hanya saja memberikan sedikit kesulitan pada analisa frekuensi setelahnya.

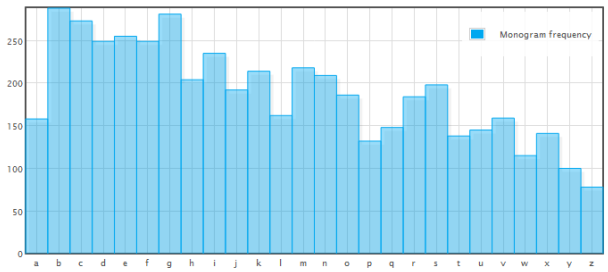
D. Vigenere Cipher pada Pasangan Huruf

Berikut adalah algoritma umum yang digunakan untuk melakukan enkripsi dengan veigenere cipher pada pasangan kata (bigram).

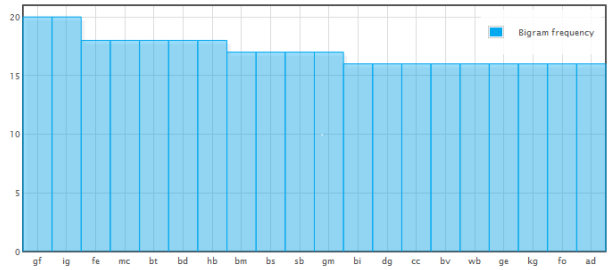
```
function Encrypt2(input String: text, key) → String
KAMUS
  Result: String
  i, j, k, iPlain1, iPlain2, iKey: integer
ALGORITMA
  i ← 0
  j ← 0

  // Menggenapkan panjang target plain text
  if (inputText.length() % 2 != 0){
     inputText ← inputText + inputText[1]
  }

   while (i < inputText.length()){
   // Merubah karakter ASCII menjadi nomor pada kubus
      iPlain1 ← text[i]-65
      iPlain2 ← text[i+1]-65
      iKey ← key[j]-65

   // proses enkripsi
      result ← result +
      (alphabetMatrix[iPlain2][iPlain1][iKey]+65)

   // iterator
      i ← i + 2

      if (j < (tKey1.length-1)){
         j ← j + 1
      } else {
         j ← 0
      }
   }

  → result
```

Dari hasil enkripsi menggunakan algortima Vigenere cipher untuk pasangan huruf dengan kata kunci: "*oceanography*" analisa frekuensi yang didapatkan dari cipher text hasil dapat dilihat pada gambar 8.

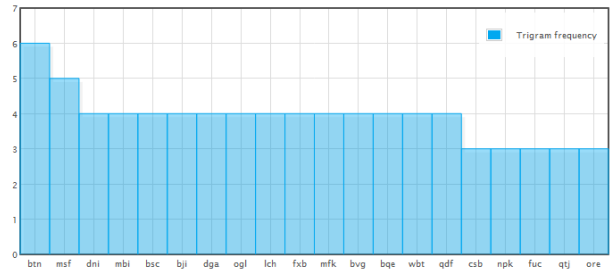
Dapat dilihat pada gambar 8 bahwa persebaran kata pada *cipher text* melandai secara signifikan, baik pada monogram, trigram, dan terutama pada bigram. Hal ini akan mempersulit analisa frekuensi, karena pada bigram sendiri terdapat 6 kata yang memiliki jumlah kemunculan hampir sama, sementara trigram akan berfungsi sebagai jebakan karena tidak ada hubungannya dengan proses enkripsi menjadi *cipher text*.



(a)



(b)



(c)

Gambar 8. Data terkait analisa frekuensi terhadap hasil enkripsi modifikasi kedua (a) monogram (b) bigram (c) trigram

Untuk metode Kasiski paling efektif diberlakukan pada bigram, dan ditemukan bahwa kemunculan GF ada pada urutan huruf ke: 305, 378, 413, 1347, 1489, 1741, dan seterusnya. Dari sampel 5 selisih kemunculan tersebut, ditemukan bahwa factor persekutuan terbesarnya adalah 1, yang mana tidak sesuai dengan "oceanography" yang memiliki panjang kata sebesar 12 huruf. Dari hal tersebut dapat disimpulkan bahwa metode kedua cukup aman dari serangan metode Kasiski untuk teks yang digunakan pada percobaan ini.

E. Vigenere Cipher Kombinasi pada Bigram

Berikut adalah algoritma umum yang digunakan untuk melakukan enkripsi dengan veigenere cipher kombinasi pada pasangan kata (bigram).

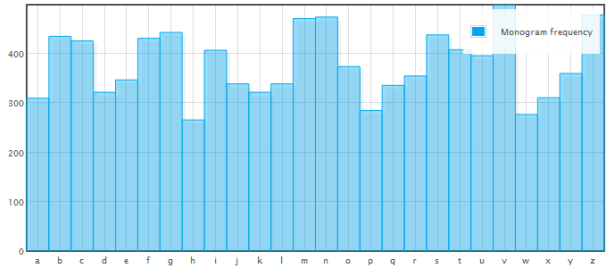
```
function Encrypt3(input String: text, key) → String
KAMUS
  Result: String
  i, j, k, iPlain1, iPlain2, iKey: integer
ALGORITMA
  i ← 0
```

```
j ← 0

// Menggenapkan panjang target plain text
if (inputText.length() % 2 != 0){
   inputText ← inputText + inputText[1]
}

 while (i < inputText.length()){
 // Merubah karakter ASCII menjadi nomor pada kubus
    iPlain1 ← text[i]-65
    iPlain2 ← text[i+1]-65
    iKey ← key[j]-65

  // proses enkripsi 1
    result ← result +
    (alphabetMatrix[0][iPlain1][iKey]+65)

  // iterator 1
    if (j < (tKey.length-1)){
        j ← j + 1
    } else {
       j = 0;
    }

    iKey ← key[j]-65

  // proses enkripsi 2
    result ← result +
    (alphabetMatrix[iPlain2][iPlain1][iKey]+65)

  // iterator 2
    i ← i + 2

    if (j < (tKey1.length-1)){
       j ← j + 1
    } else {
       j ← 0
    }
  }

 → result
```

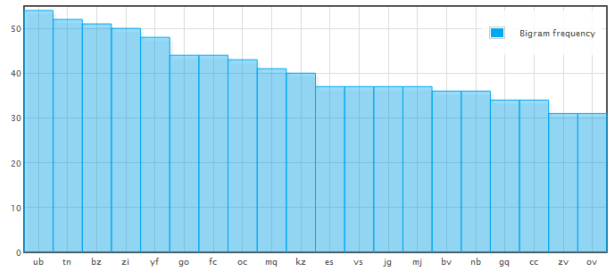
Dari hasil enkripsi menggunakan algortima Vigenere cipher kombinasi untuk pasangan huruf dengan kata kunci: "*oceanography*" analisa frekuensi yang didapatkan dari cipher text hasil dapat dilihat pada gambar 9.

Dari segi data analisa frekuensi pada *cipher text*,metode ketiga memiliki persebaran paling baik dan merata dari segi monogram, dan persebaran yang baik pada bigram, serta persebaran yang cukup baik pada trigram. Oleh karena itu dapat dikatakan bahwa metode kombinasi ini memiliki ketahanan terhadap serangan analisa frekuensi yang baik, dan dapat disaingkan dengan metode kedua (dengan catatan metode kedua tidak diketahui merupakan *compressed cipher*)

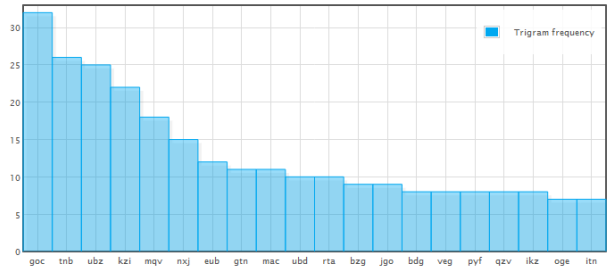
Untuk pendekatan dari metode kasiski, diambil eksperimen dengan memanfaatkan segi paling lemah, yaitu bagian data trigram.



(a)



(b)



(c)

Gambar 9. Data terkait analisa frekuensi terhadap hasil enkripsi modifikasi ketiga (a) monogram (b) bigram (c) trigram

Dari data trigram, ditemukan pasangan huruf yang paling sering muncul adalah "GOC", yang muncul pada urutan ke 212, 584, 1544, 1772, 1820, 1856, dan seterusnya. Dari selisih sampel ke-6 posisi tersebut, ditemukan bahwa factor persekutan terbesarnya adalah 4, yang mana tentunya berbeda dengan "oceanography" yang memiliki panjang 12 huruf.

Dari beberapa eksperimen yang telah ditentukan, dapat dikatakan bahwa metode kombinasi lebih aman dibandingkan dengan kedua metode sebelumnya.

V. CONCLUSION

Dari beberapa percobaan yang telah dilakukan, dapat ditarik kesimpulan bahwa beberapa modifikasi yang dilakukan memberikan peningkatan ketahanan terhadap serangan-serangan kriptografi, khususnya analisa frekuensi dan metode Kasiski. Pada metode pertama masih rentan terhadap metode Kasiski, namun mempersulit pada bagian analisis frekuensi karena keamanannya berlapis dua. Untuk metode kedua memiliki tingkat keamanan cukup tinggi, dengan catatan pihak penyerang tidak mengetahui bahwa pada metode kedua pasangan huruf bigram dienkripsi menjadi satu huruf

tertentu. Sementara sampai pada eksperimen ini selesai, dapat dikatakan bahwa metode kombinasi memiliki tingkat keamanan yang paling konsisten terhadap serangan-serangan tersebut. Namun, tentunya masih banyak ruang untuk modifikasi lebih lanjut dengan harapan peningkatan ketahanan yang lebih baik pada *Vigenere cipher* sendiri.

REFERENCES

[1] Monogram, Bigram, and Trigram Frequency Counts, http://practicalcryptography.com/cryptanalysis/text-characterisation/monogram-bigram-and-trigram-frequency-counts/ (terakhir diakses pada 19/3/2014)

[2] Greatest Common Divisor and Lowest Common Multiplier Calculator, http://www.mathportal.org/calculators/numbers-calculators/gcd-lcm-calculator.php (terakhir diakses pada 19/3/2014)

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 2014

Aji Nugraha Santosa Kasmaji 13510092