3D Model Vigenere Cipher

Muhammad Anis,13508068
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If18068@students.if.itb.ac.id

Penggunaan algoritma enkripsi klasik masih merupakan salah satu alternative yang masih sering digunakan oleh manusia saat ini walaupun telah ada algoritma modern. Salah satu alasan masih digunakannya algoritma klasik adalah karena terkadang untuk pemecahannya tidak diperlukan suatu program khusus sehingga mudah untuk dideksipsikan.

Salah satu algoritma enkripsi yang sering dipakai adalah vigenere cipher, dimana menggunakan table substitusi dua dimensi untuk mengenkripsikan sebuah pesan dengan menggunakan sebuah kunci .Namun ternyata teknik pengenkripsian ini masih dapat dipecahkan menggunakan analisis kasiski ataupun menggunakan analisis frekuensi, sehingga teknik vigenere cipher ini masih perlu dikembangkan sehingga semakin sulit untuk dipecahkan. Oleh karena itu makalah ini akan membahas mengenai pengembangan lebih lanjut mengenai vigenere cipher dengan menggunakan table substitusi tiga dimensi yang akan menambah kesulitan dari teknik pengenkripsian vigenere cipher.Selain itu akan dibahas juga mengenai sejarah vigenere cipher hingga teknik pengaplikasian vigenere serta mengapa teknik ini mampu dipecahkan menggunakan analisis kasiski serta analisis frequency cipher serta program yang memodelkan vigenere cipher dengan model 3 dimensi ini.

Kata Kunci: Vigenere cipher, table substitusi, tiga dimensi model.

1. PENDAHULUAN

Informasi adalah salah satu hal yang sering dijaga baik dari segi keberadaan, perolehan maupun dari segi pengamanan dari orang-orang atau pihak-pihak yang tidak memiliki akses terhadap informasi tersebut. Begitu pentingnya keamanan atau kerahasiaan sebuah informasi maka dikembangkanlah sebuah ilmu kriptografi. Cabang ilmu ini berusaha untuk mengubah sebuah pesan bermakna sedemikian sehingga tidak dapat dipahami oleh orang-orang yang tidak memiliki hak untuk dengan menggunakan sebuah kata kunci. Kata kunci ini dapat digunakan untuk mendekripsi pesan tersebut sehingga pihak yang berhak dapat mengubah pesan yang tadinya tidak bermakna sehingga pesan tersbut dapat kembali seperti aslinya.

2. LANDASAN TEORI

2.1 Cipher Substitusi

Teknik pengenkripsian data menggunkan cipher substitusi adalah dengan cara mengganti suatu huruf dengan huruf lain menggunakan suatu pola tertentu. Pola ini dapat dibuat sangat sulit sehingga membuat proses pendekripsian akan menjadi sulit pula. Ada dua macam cipher substitusi yaitu *polyalphabetic substitution* dan *monoalphabetic substitution*. *Polyalphabetic substitution* adalah teknik pengenkripsian suatu data dimana satu alphabet dapat dienkripsi menjadi alphabet yang berbeda walaupun menggunakan teknik eknripsi yang berbeda. Hal ini sangat baik dimana dapat mengurangi kemungkinan pemecahan informasi yang kita enkrip menggunakan analisis frekuensi. Sedangkan *monoalphabetic substitution* adalah teknik pengenkripsian suatu informasi dimana sebuah huruf atau alphabet akan menjadi alphabet yang sama jika menggunakan teknik enkripsi yang sama. Salah satu contoh *monoalphabetic substitution* yang sangat terkenal adalah teknik enkripsi *Caesar Cipher*. Inti dari Caesar Cipher adalah menggeser tiap huruf sebanyak n satuan dimana n adalah kunci yang harus dirahasiakan kepada orang lain.

Gambar 1 Caesar Cipher

Sedangkan contoh untuk *polyalphabetical substitution* adalah *vigenere cipher* dimana terdapat sebuah table substitusi yang akan mencocokkan antara sebuah kunci dan plain teksnya. Vigenere Cipher akan dibahas lebih lanjut pada bagian berikutnya.

2.2 Vigenere Cipher

Vigenere Cipher pertama kali ditemukan oleh Giovan Battista Bellaso pada tahun 1553, namun baru dipublikasikan secara luas oleh Blaise de Vigenere pada abad ke 19 sehingga disbut Vigenere Cipher. Cipher ini terkenal karena mudah untuk dimengerti dan diimplementasikan. Untuk mengenkripsikan sebuah informasi menggunakan vigenere cipher digunakan table vigenere yang terdiri atas alphabet yang ditulis pada tiap baris dan kolom. Isi dari table tersebut adalah alphabet yang ditulis sebanyak 26 kali dimana setiap pergantian baris setiap alphabet akan digeser satu bagian ke kiri.

	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 Table Vigenere

Contoh, missal plaintext yang ingin dienkripsi adalah:

ATTACKATDAWN

Kemudian kunci yang akan digunakan untuk mengenkripsi plainteks ini adalah “MAKAN”. Maka teknik enkripsi adalah sebagai berikut:

Pertama-tama kita akan mengulang kunci karena panjang kunci harus sama dengan panjang plainteks yang ingin dienkrip. Sehinggak kunci yang didapatkan adalah MAKANMAKANMA. Kemudian untuk tiap pasangan huruf plainteks dan kunci akan dilihat pada table vigenere untuk mendapatkan karakter hasil enkripsi

{A,M} → M

{T, A} → T

{T, K} → D, dan seterusnya

Sehingga didapatkan hasil enkripsi adalah:

MTDAPWADDNIN

Secara umum vigenere cipher dapat didekripsikan sebagai berikut:

$$E(i) = (P(i) + K(i)) \bmod 26$$

Dimana:

E(i) : Karakter cipher pada posisi ke-i

P(i) : Karakter plain pada posisi ke-i

K(i) : Kunci pada karakter ke-i

Dengan syarat plainteks dan kunci memiliki jumlah karakter yang sama.

Teknik pendekripsian pada vigenere cipher ini juga dilakukan menggunakan table vigenere namun dengan cara terbalik. Pertama-tama kita melihat hasil kuncinya. Kemudian mencari pada baris huruf tersebut nilai cipher teks yang kita ketahui. Maka plainteks yang kita cari adalah indeks kolom yang sesuai dengan posisi tersebut.

Contoh: missal ciphertext yang ingin di dekrip adalah

MTDAPWADDNIN

Lalu kunci yang dimiliki adalah “MAKAN” maka cara mendekripsikan cipher teks tersebut adalah:

Pertama-tama kita harus mencari pada baris table vigenere yang memiliki huruf yang sama dengan huruf yang kita miliki. Lalu kita mencari pada table tersebut cipherteks yang kita cari.

{M,M} → A

{A, T } → T

{K,D} → T, dst

Maka hasil yang didapatkan adalah :

ATTACKATDAWN

Secara umum pendekripsian vigenere cipher dapat didekripsikan sebagai berikut:

$$P(i) = (E(i) - K(i)) \bmod 26$$

Dimana:

E(i) : Karakter cipher pada posisi ke-i

P(i) : Karakter plain pada posisi ke-i

K(i) : Kunci pada karakter ke-i

Dengan syarat plainteks dan kunci memiliki jumlah karakter yang sama.

2.3 Analisis Keamanan Vigenere Cipher

Sama seperti teknik cipher substitusi lainnya, teknik vigenere cipher mencoba untuk memalsukan atau mengubah sebuah karakter pada sebuah plainteks menjadi huruf lain pada cipherteks. Namun kelemahan utama pada vigenere cipher adalah kuncinya yang terkadang memiliki panjang tidak sama dengan plainteksnya harus diulang sehingga memiliki panjang yang sama dengan plainteks. Sehingga jika kita mampu menebak berapa panjang karakter dari sebuah kunci maka kita akan semakin mudah untuk memecahkan cipherteks tersbut. Berikut adalah beberapa teknik yang sering digunakan untuk membantu menentukan panjang kunci.

2.3.1 Analisis Kasiski

Analisis kasiski menggunakan fakta bahwa pada beberapa kata terkadang dienkripsi menggunakan

huruf kunci yang sama sehingga menghasilkan blok-blok yang berulang. Misal untuk kasus seperti ini:

Key:
ABCDABCDABCDABCDABCDABCDABCD
Plaintext:
CRYPTOISSHORTFOR***CRYPTO***GRAPHY
Ciphertext:
CSASTPKVSIQUTGQU***CSASTP***IUAQJB

Pada teks di atas dapat dilihat bahwa terdapat blok kata yang berulang dua kali yaitu CSASTP. Asumsikan bahwa blok yang berulang adalah blok plaintext yang sama. Maka, kita dapat menebak bahwa panjang kunci adalah salah satu diantara bilangan pembagi jarak dua kata itu, yaitu 16. Berarti kemungkinan panjang kunci adalah 16,8,4,2, atau 1. Panjang kunci 2 dan 1 hampir tidak mungkin untuk digunakan karena terlalu pendek, maka menyisakan kemungkinan panjang kunci adalah 16,8, atau 4. Karena kita telah mengetahui kemungkinan panjang kunci tersebut maka kita akan semakin mudah untuk memecahkan cipherteks tersebut

2.3.2 Friedman Test

SFriedman test pertama kali ditemukan oleh William F. Friedman pada tahun1920-an. Metode ini menggunakan *index of coincidence.* Teknik ini membutuhkan dua variable yaitu Kp dan Kr dimana Kp adalah probabilitas dua huruf yang dipilih secara acak pada sebuah bahasa adalah sama. Untuk bahasa inggris nilai ini adalah 0.067. Sedangkan Kr adalah kemungkinan sebuah pemilihan random dari sebuah alphabet (1/26 untuk bahasa inggris)
Maka panjang kunci yang dimaksud dapat diperkirakan sebagai:

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

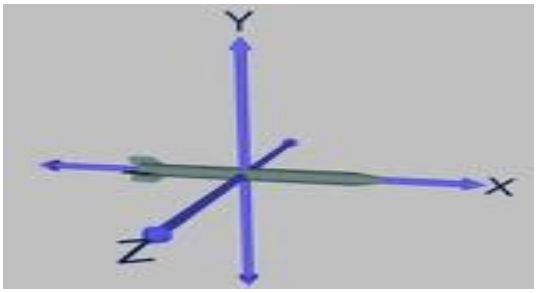
Dengan K_0 adalah

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

Dimana :
C : panjang alphabet (26 untuk bahasa inggris)
N : panjang teks
Ni : Frekuensi kemunculan huruf

3. VIGENERE CIPHER MENGGUNAKAN MODEL 3 DIMENSI

Salah satu kelemahan yang dimiliki oleh vigenere cipher biasa adalah kemungkinan terjadinya perulangan pada cipher teks serta pada kunci. Kemungkinan panjang kunci sama dengan panjang plain teks juga sangat sulit diterapkan pada informasi-informasi yang berukuran sangat besar. Oleh karena itu, untuk mempersulit pemecahan vigenere cipher ini maka akan ditambahkan satu dimensi lagi untuk menambah kemungkinan huruf yang tersedia pada table vigenere ini.



Gambar 3 Sistem Koordinat 3 Dimensi

3.1 Sumbu-Sumbu Pada Vigenere Cipher Model 3 Dimensi

Pertama-tama akan dijelaskan mengenai sumbu-sumbu yang terdapat pada vigenere cipher yang menggunakan model 3 dimensi ini:
Sumbu X : Berisi 26 Point dari A-Z
Sumbu Y : Berisi 26 Point dari A-Z
Sumbu Z : Berisi 26 karakter A-Z dengan satu tambahan karakter yaitu karakter spasi.

3.2 Kunci pada Vigenere Cipher Model 3 Dimensi

Kunci yang digunakan pada teknik enkripsi ini ada dua kunci. Kunci pertama adalah kunci yang digunakan untuk menentukan ketinggian pada sumbu Z, serta menjadi pengenkrip untuk plainteks.. Sedangkan kunci yang satu lagi akan digunakan untuk mengenkrip plainteks sama seperti vigenere cipher biasa.

3.3 Teknik Pengisian Tabel

Pengisian table pada vigenere cipher yang menggunakan model tiga dimensi ini adalah sebagai berikut:

- Setiap pasangan sumbu X dan Y akan direpresentasikan sebagai sebuah table vigenere. Karena

sumbu Z memilki panjang 26, maka akan terdapat 26 tabel vigenere cipher

- Pada sumbu Z = 0, diisi dengan menggunakan vigenere table biasa.
- Pada Vigenere Z=1 sampai dengan Z=26 maka akan diisi dengan bigram yaitu AA,AB,AC,AD. Jumlah bigram yang mungkin adalah permutasi dari 26 dan diambil 2dan ditambahkan 26 karena hurufsama yang berulang tetap diambil yaitu AA, BB,CC dst. Maka jumlah bigram yang mungkin adalah:

$$P_2^{26} = \frac{26!}{(26-2)!} = 650 + 26$$
$$= 676\ Kemungkinan$$

Maka jika dibagi 26, maka dapat terbentuk 26 bagian bigram. Bigram ini dibagi 25 karena baris pertama sudah diambil untuk vigenere cipher biasa. Maka terdapat satu layer yang tidak memiliki pasangan ketinggian pada ketinggian 27. Hal ini disebabkan pada layer awal (layer 0) telah digunakan untuk vigenere cipher biasa. Untuk mengatasai hal ini, maka ditambahkan satu point lagi pada sumbu Z, yaitu karakter yang dapat terbaca pada teks namun tidak termasuk dalam A-Z, yaitu spasi. Sehingga kunci yang diberikan mampu menangkap karakter spasi.

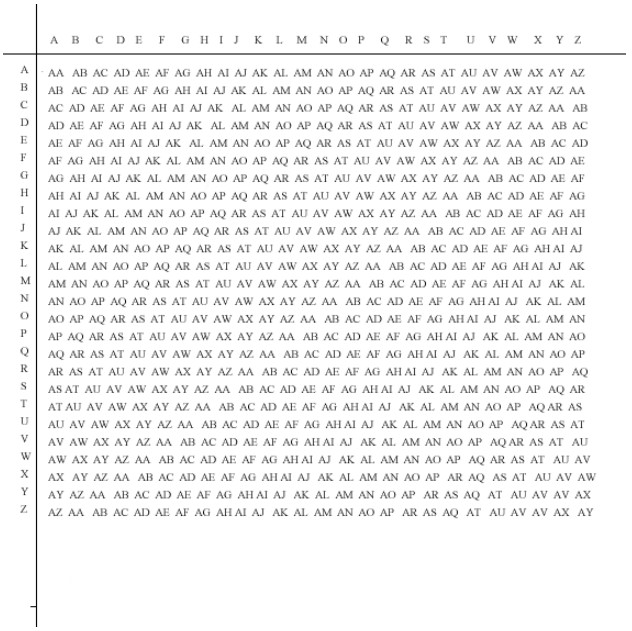
- Setiap table pada setiap layer tetap digeser satu shift setiap perpindahan kolom sesuai teknik vigenere cipher.

Berikut adalah beberapa dari table vigenere cipher yang terbentuk berdasarkan ketinggian Z

a. Z = 0

	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

b. Z = 1



Gambar 4 Model 3 Dimensi Vigenere cipher dengan Z = 1

Tabel Vigenere ini akan terus diulang sebanyak 26 kali hingga mencapai level Z = 26. Setiap pengisian table akan mengikuti pola diatas

3.4 Teknik Enkripsi

Untuk mengenkripsi sebuah plainteks maka dibutuhkan dua kunci. Kunci pertama akan digunakan untuk menentukan ketinggian dari table vigenere cipher yang akan dipakai. Selain itu kan ditambahkan karakter spasi. Karakter spasi ini akan menjadi point ke 26 pada sumbu Z.Dengan adanya karakter spasi ini maka jika kunci pertama mengandung spasi , maka spasi tersebut tidak akan dibuang Kunci kedua akan digunakan untuk pengenkripsi sama seperti vigenere cipher biasa. Plainteks awalnya akan

dienkrip melalui vigenere cipher biasa dengan kunci 2, lalu dicari ketinggiannya dengan menggunakan kunci pertama. Maka itulah hasil enkripsi dari plain teks tersebut.

3.5 Teknik Dekripsi

Untuk mendekripsi sebuah cipherteks, pertama-tama harus dilihat berada pada ketinggian berapa cipherteks tersebut berdasarkan kunci. Jika ternyata ketinggian yang didapat adalah ketinggian 0, maka ambil satu huruf lalu didekrip. Jika ketinggian besar dari 0 maka ambil dua huruf lalu mendekrip. Teknik dekrip yang digunakan adalah sebagai berikut. Ambil satu atau dua karakter (tergantung pada ketinggian yang didapatkan). Setelah mendapatkan ketinggian tersebut, maka pendekripsian sama dengan menggunakan vigenere cipher biasa yaitu mencari pasangan kunci (menggunakan kunci kedua) dan cipherteks yang didapatkan. Maka itulah plainteks yang akan didapatkan.

4. HASIL DAN ANALISIS

4.1 Hasil

Berikut adalah source code untuk mengenerate bigram dan alphabet yang akan digunakan sebagai table vigenere:

```
public static void main(String[] args) {
        // TODO code application logic here
        String[][] model = new String[26][26];
        char[] alphabet = generateAlphabet();
        //generateMatriks();
        String[] tes = generateBigram();
        int putaran =0;
        for(int i=0;i<26;i++){
           for(int j=0;j<26;j++){
              for(int k=0;k<26;k++){
                 model[i][j] += tes[k+26*putaran];
              }
              putaran++;
           }
        }

    }

    public static char[] generateAlphabet() {
        char[] alphabet = new char[26];
        for (int i = 0; i < 26; i++) {
            alphabet[i] = (char) (65 + i);
        }
        return alphabet;
    }

    public static String[] generateBigram() {
        String[] ret = new String[26 * 26*26];
        char[] alphabet = new char[26];


        alphabet = generateAlphabet();
        int putaran = 0;
        StringBuilder sb = new StringBuilder();
        for (int k = 0; k < alphabet.length; k++) {
           for (int i = 0; i < alphabet.length; i++)
{
              alphabet = geserCharKePertama(i,
alphabet);
              for (int j = 0; j < alphabet.length - 1;
j++) {
                 ret[putaran++] =
Character.toString(alphabet[k]) +
Character.toString(alphabet[j + 1]) + "";
              }
           }

        }
        return ret;
     }

     public static char[] geserCharKePertama(int
pos, char[] input) {
        if (pos == 0) {
           return input;
        }
        char temp = input[pos];
        char[] input2 = input;
        for (int i = pos - 1; i >= 0; i--) {
           input2[i + 1] = input[i];
        }
        input2[0] = temp;
        return input2;
  }
```

Berikut adalah beberapa teks yang telah dienkrip dan didekrip dengan menggunakan vigenere cipher bermodel tiga dimensi

a. PlainText: Saya Lapar
b. Kunci1 : halo
c. Kunci2: makan

Kita juga akan mengulang kunci pertama sehingga memiliki panjang yang sama dengan

- halohaloh

Lalu kunci kedua akan diulang sehingga memiliki panjang sama dengan plainteks

- Kunci2: makanmaka

Lalu pengenkripsian
{s,,h,m) → EE
{a,a,a } → A
{y,l,k } → MJ
{a,o,a} → PA, dan seterusnya

Hasil yang didapatkan:
EEAMJPAIYMMPQKIR

Ketika didekripsikan menggunakan kunci yang sama didapatkan pula hasil yang sama namun tidak mengandung spasi yaitu SAYALAPAR.
Teknik pendekripsian:
Pertama-tama kita harus melihat kunci pertama yang dimiliki, dari kunci yang didapatkan adalah h, maka kita akan mengambil dua karakter pertama dari ciphertext yang didapatkan. Kemudian dari dua kata tersebut kita menncocokkan dengan baris pada kunci maka kolom yang bersesuain adalah plainteks yang diinginkan

{EE,h,m} → s

Pada karakter pada kunci kedua, didapatkan bahwa kuncinya adalah huruf a, maka kita hanya mengambil satu huruf dari ciphertext di atas.

{a,a,a} → a, dan seterusnya

4.2 Analisis

Penggunaan teknik vigenere cipher dengan menggunakan model tiga dimensi akan menguatkan pengenkripsian dari vigenere cipher biasa. Hal ini dapat dilihat dari panjang ciphertext yang tidak memiliki panjang sama dengan plain teks. Hal ini dapat menyebabkan para kriptanalis bingung untuk memilih bagian mana dari cipherteks yang akan di dekrip, apakah hanya satu huruf atau dua huruf. Penggunaan dua kunci juga akan memiliki nilai kurang dan lebih. Nilai lebihnya adalah jika salah satu kunci berhasil dicuri, belum tentu cipherteks tersebut dapat dipecahkan. Namun dengan penggunaan dua kunci mengharuskan pengguna untuk ekstar hati-hati dimana jika pengguna kehilangan kunci tersebut maka cipherteks tersebut akan menjadi senjata makan tuan. Selain itu penggunaan model ini akan mengacaukan teknik analisis frekuensi dimana seringnya muncul karakter-karakter yang justru tidak ada hubungannya dengan teks atau informasi asli. Penggunaan teknik ini juga memperbanyak kemungkinan kombinasi huruf sehingga semakin tidak memungkinkan penggunaan teknik bruteforce.

Namun kelemahan dari teknik ini adalah teknik ini lebih sulit untuk diterapkan daripada vigenere cipher biasa, yang sangat mudah digunakan . Hal ini dapat dilihat dari jumlah table yang jauh berbeda 26 tabel (vigenere dengan model tiga dimensi) dan 1 tabel (vigenere cipher biasa).

5. KESIMPULAN

Vigenere cipher adalah salah satu algoritma kriptografi klasik yang masih sering digunakan karena kekuatan dan kemudahan penggunaannya. Namun, dengan menggunakan beberapa metode, seperti analisis kasiski menjadikan algoritma ini menjadi dapat dipecahkan. Oleh karena itu, algoritma ini memerlukan suatu pengembangan dimana dengan tidak menghilangkan identitas vigenere cipher, algoritma ini dapat menjadi semakin kuat.

Salah satu teknik yang dapat digunakan untuk memperkuat lagoritma ini adalah dengan menggunakan vigenere cipher yang menggunakan model tiga dimensi sebagai table vigenerenya. Dalam model ini, digunakan 27 tabel vigenere yang berbeda tergantung pada ketinggian pada model tiga dimensi yang ada (pada kasus makalah ini menggunakan sumbu Z). Dengan menggunakan algoritma ini, maka teknik analisis frekuensi dan metode kasiski akan semakin sulit menebak sebuah cipherteks karenacipher teks yang dihasilkan lebih panjang dari cipherteks. Hal ini mengakibatkan munculnya karakter-karakter yang sebenarnya tidak memiliki hubugan langsung dengan informasi asli.

REFERENCES

[1] Munir, Rinaldi. 2011. Bahan Kuliah IF3054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung..
[2] http://www.java-forums.org/lucene/33082-how-generate-bigram-trigram-unigram-probability.html
[3] http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
[4] Lab exercise: Vigenere, RSA, DES, and Authentication Protocols"
[5] http://sharkysoft.com/misc/vigenere/

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, 23 Maret 2011

ttd

Muhammad Anis, 13508068