Streamed Key Vigenere Cipher : Vigenere Cipher Menggunakan Penerapan Metode Pembangkitan Aliran Kunci

Faradina Ardiyana
Program Studi Teknik Informatika Institut Teknologi Bandung, Jl.Ganesha 10 Bandung 40132
Email: if14067@students.if.itb.ac.id

Abstract *– Pengguna teknologi semakin beramai-ramai mengembangkan suatu system pengamanan terhadap data yang biasa disebut kriptografi. Salah satu metode yang telah dikenal sejak lama adalah algoritma kriptografi klasik. Walaupun algoritma tersebut sudah using karena mudah dipecahkan namun algoritma tersebut merupakan dasar dari algoritma kriptografi modern. Oleh sebab itu kita harus dapat memahami konsep dasar kriptografi sebelumnya. Pada kesempatan kali ini penulis akan membahas salah satu dari algoritma kriptografi klasik, yaitu Vigenere Cipher dengan modifikasi pada kuncinya yang kemudian akan disebut Streamed Key Vigenere Cipher, yaitu Vigenere Cipher menggunakan penerapan metode pembangkitan aliran kunci untuk membangkitkan kunci dari algoritma vigenere.*

Isi dari makalh ini meliputi konsep dasar, alasan, implementasi dan pengujian, serta perbandingan hasil dengan Vigenere cipher asli. Konsep dasar meliputi landasan teori, implementasi disertai pengujian untuk menguji tingkat keamanan.

Kata Kunci*: kriptografi, vigenere cipher, pembangkit aliran kunci, streamed key vigenere cipher.*

1. PENDAHULUAN

Perkembangan dunia digital saat ini lalu lintas pengiriman data elektronik semakin ramai dan sensitif. Data yang dipertukarkan juga bervariasi dari jenis maupun tingkat kerahasiaannya. Mulai dari data pribadi hingga data negara yang sangat rahasia. Hal ini yang menuntut adanya pengamanan data terhadap proses pengiriman data. Telah banyak ditemukan teknik-teknik pengamanan data, baik teknik klasik maupun modern. Dalam dunia kriptografi, suatu algoritma dikatakan aman jika untuk memecahkannya butuh waktu dan biaya yang relatif besar serta proses algoritma yang rumit. Metode vigenere cipher klasik sudah dapat dilakukan kriptanalisis terhadap panjang kunci dengan metode kasiski, oleh karena itu penulis mencoba mengembangkan metode vigenere cipher dengan memodifikasi kuncinya menggunakan penerapan metode pembangkit aliran kunci untuk membangkitkan kuncinya.

Penggunaan pembangkit aliran kunci dalam vigenere cipher bertujuan untuk mempersulit kriptanalis melakukan pemecahan kunci.

2. VIGENERE CIPHER

2.1 Konsep Dasar

Vigenere cipher merupakan sebuah nama dari seorang yaitu Blaise de Vigenere. Walaupun yang sudah menemukan cipher tersebut terlebih dahulu yaitu Giovan Battista Bellaso. Tetapi Vigenere lah yang sudah menemukan kunci yang lebih kuat lagi dengan nama Autokey cipher. Vigenere cipher adalah suatu metode untuk enkripsi alfabet dari teks dengan menggunakan berbagai macam seri dari caesar cipher berdasarkan huruf-huruf yang ada pada kunci. Cipher ini merupakan bentuk mudahnya dari *polyalphabetic substitution*. Vigenere cipher sudah berkali-kali mengalami penciptaan ulang. Metode asli ditemukan oleh Giovan Battista Bellaso pada bukunya dia *La cifra del. Sig. Giovan Battista Bellaso* pada tahun 1553. Bagaimanapun, skemanya dibuat oleh Blaise de Vigenere pada abad ke-16. Vigenere cipher dipublikasikan pada tahun 1856, tetapi algoritma tersebut baru dikenal luas 200 tahun kemudian dan berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19.

Vigenera Cipher menggunakan Bujursangkar Vigenere untuk melakukan enkripsi (lihat Tabel 1). Kolom paling kiri dari Bujursangkar menyatakan huruf-huruf kunci, sedangkan baris paling atas menyatakan huruf-huruf plainteks. Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar Cipher*, yang mana jauh pergeseran huruf plainteks ditentukan nilai desimal oleh huruf kunci tersebut (a = 0, b = 1, c = 2, …, z = 25). Sebagai contoh, huruf kunci c menyatakan huruf plainteks digeser sejauh 2 huruf ke kanan dari susunan alfabetnya.

	A	B	C	D	E	F	G	H	I	J
a	A	B	C	D	E	F	G	H	I	J
b	B	C	D	E	F	G	H	I	J	K
c	C	D	E	F	G	H	I	J	K	L
d	D	E	F	G	H	I	J	K	L	M
e	E	F	G	H	I	J	K	L	M	N
f	F	G	H	I	J	K	L	M	N	O
g	G	H	I	J	K	L	M	N	O	P
h	H	I	J	K	L	M	N	O	P	Q
i	I	J	K	L	M	N	O	P	Q	R

j	J	K	L	M	N	O	P	Q	R	S
k	K	L	M	N	O	P	Q	R	S	T
l	L	M	N	O	P	Q	R	S	T	U
m	M	N	O	P	Q	R	S	T	U	V
n	N	O	P	Q	R	S	T	U	V	W
o	O	P	Q	R	S	T	U	V	W	X
p	P	Q	R	S	T	U	V	W	X	Y
q	Q	R	S	T	U	V	W	X	Y	Z
r	R	S	T	U	V	W	X	Y	Z	A
s	S	T	U	V	W	X	Y	Z	A	B
t	T	U	V	W	X	Y	Z	A	B	C
u	U	V	W	X	Y	Z	A	B	C	D
v	V	W	X	Y	Z	A	B	C	D	E
w	W	X	Y	Z	A	B	C	D	E	F
x	X	Y	Z	A	B	C	D	E	F	G
y	Y	Z	A	B	C	D	E	F	G	H
z	Z	A	B	C	D	E	F	G	H	I

	K	L	M	N	O	P	Q	R	S
a	K	L	M	N	O	P	Q	R	S
b	L	M	N	O	P	Q	R	S	T
c	M	N	O	P	Q	R	S	T	U
d	N	O	P	Q	R	S	T	U	V
e	O	P	Q	R	S	T	U	V	W
f	P	Q	R	S	T	U	V	W	X
g	Q	R	S	T	U	V	W	X	Y
h	R	S	T	U	V	W	X	Y	Z
i	S	T	U	V	W	X	Y	Z	A
j	T	U	V	W	X	Y	Z	A	B
k	U	V	W	X	Y	Z	A	B	C
l	V	W	X	Y	Z	A	B	C	D
m	W	X	Y	Z	A	B	C	D	E
n	X	Y	Z	A	B	C	D	E	F
o	Y	Z	A	B	C	D	E	F	G
p	Z	A	B	C	D	E	F	G	H
q	A	B	C	D	E	F	G	H	I
r	B	C	D	E	F	G	H	I	J
s	C	D	E	F	G	H	I	J	K
t	D	E	F	G	H	I	J	K	L
u	E	F	G	H	I	J	K	L	M
v	F	G	H	I	J	K	L	M	N
w	G	H	I	J	K	L	M	N	O
x	H	I	J	K	L	M	N	O	P
y	I	J	K	L	M	N	O	P	Q
z	J	K	L	M	N	O	P	Q	R

	T	U	V	W	X	Y	Z
a	T	U	V	W	X	Y	Z
b	U	V	W	X	Y	Z	A
c	V	W	X	Y	Z	A	B
d	W	X	Y	Z	A	B	C
e	X	Y	Z	A	B	C	D
f	Y	Z	A	B	C	D	E
g	Z	A	B	C	D	E	F
h	A	B	C	D	E	F	G
i	B	C	D	E	F	G	H
j	C	D	E	F	G	H	I
k	D	E	F	G	H	I	J
l	E	F	G	H	I	J	K
m	F	G	H	I	J	K	L
n	G	H	I	J	K	L	M
o	H	I	J	K	L	M	N
p	I	J	K	L	M	N	O
q	J	K	L	M	N	O	P
r	K	L	M	N	O	P	Q
s	L	M	N	O	P	Q	R
t	M	N	O	P	Q	R	S
u	N	O	P	Q	R	S	T
v	O	P	Q	R	S	T	U
w	P	Q	R	S	T	U	V
x	Q	R	S	T	U	V	W
y	R	S	T	U	V	W	X
z	S	T	U	V	W	X	Y

Tabel 1 Bujursangkar Vigenere

Bujursangkar Vigenere digunakan untuk memperoleh cipherteks dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang penggunaannya (sistem periodik). Bila panjang kunci adalah m, maka periodenya dikatakan *m*.

Sebagai contoh, jika plainteks adalah BUKU KRIPTOGRAFI dan kuncinya adalah BOY, maka penggunaan kunci secara periodik adalah sebagai berikut :

Plainteks : B U K U K R I P T O G R A F I

Kunci : b o y b o y b o y b o y b o y

Setiap huruf plainteks akan dienkripsi dengan setiap huruf kunci dibawahnya.

Untuk melakukan enkripsi dengan *Vigenere Cipher*, langkah-langkah yang dilakukan pada Bujursangkar *Vigenere* sebagai berikut : tarik garis vertikal dari huruf plainteks ke bawah, lalu tarik garis mendatar dari huruf kunci ke kanan. Perpotongan kedua garis tersebut menyatakan huruf cipherteksnya. Sebagai

contoh dari plainteks sebelumnya, tarik garis vertikal dari huruf B dan tarik garis mendatar dari huruf b, maka perpotongannya adalah pada kotak yang berisi huruf C (lihat Tabel 1). Dengan cara yang sama, tarik garis vertikal dari huruf U dan tarik garis mendatar dari huruf o, maka perpotongannya adalah pada kotak yang berisi huruf I. Hasil enkripsi keseluruhan sebagai berikut :

Plainteks : B U K U K R I P T O G R A F I
Kunci : b o y b o y b o y b o y b o y
Cipherteks : C I I V Y P J D R P U P B T G

Dapat diamati dari hasil diatas bahwa huruf plainteks K dapat dienkripsi menjadi I atau Y, dan huruf cipherteks P dapat merepresentasikan huruf plainteks O dan R. Hal ini merupakan karakteristik dari *cipher* abjad-majemuk. Pada *cipher* substitusi sederhana, setiap huruf cipherteks selalu menggantikan huruf plainteks tertentu, sedangkan pada cipher abjad-majemuk setiap huruf cipherteks dapat memiliki kemungknan banyak huruf plainteks.

Jadi, dengan menggunakan vigenere cipher, kita dapat mencegah frekuensi huruf-huruf di dalam cipherteks yang mempunyai pola tertentu yang sama sebagaimana yang diperlihatkan pada *cipher* substitusi sederhana.

Dekripsi pada vigenere cipher dilakukan dengan cara yang berkebalikan , yaitu menarik garis mendatar dari huruf kunci sampai ke huruf cipherteks yang dituju, lalu dari huruf cipherteks tarik garis vertikal ke atas sampai ke huruf plainteks. Untuk memecahkannya, cukup menentukan kuncinya. Jika periode kunci diketahui dan tidak terlalu panjang, maka kunci dapat ditentukan dengan menulis program komputer untuk melakukan *exhaustive key search*.

Jika diberikan sebuah cipherteks yang dihasilkan dari *Vigenere Cipher* dan diperolah informasi bahwa panjang kunci adalah *n* huruf dan plainteks ditulis dalam bahasa inggris, maka *running* program dengan mencoba semua kemungkinan kunci yang panjangnya *n* huruf, lalu periksa apakah hasil dekripsi dengan kunci tersebut menyatakan kata yang berarti. Cara ini membutuhkan usaha percobaan sebanyak 26^n kali. Semakin panjang kunci (semakin besar periode), semakin banyak usaha percobaan yang harus dilakukan.

2.2 Variant

2.2.1 The Full Vigenere cicpher

The full vigenere cipher mirip dengan vigenere cipher biasa yang menggunakan kunci dengan kata atau frase. Namun *cipher* ini menggunakan keyword yang merupakan permutasi dari rangkaian alfabet daripada deretan huruf saja.

Untuk melakukan enkripsi dan dekripsi caranya sama dengan menggunakan bujursangkar *vigenere cipher* (tabel 1). Keunggulan vigenere cipher sederhana terletak pada kebutuhan akan frekuensi relatif secara keseluruhan yang diperlukan untuk memecahkan pesan.

2.2.2 The Auto-key Vigenere Cipher

Vigenere cipher ini adalah contoh awal dari cipher aliran. Cipher aliran adalah metode enkripsi yang mengenkripsi huruf berdasarkan posisinya dalam teks. Idealnya, kunci yang digunakan tidak pernah berulang. Beberapa cipher aliran menggunakan plainteks dan/atau cipherteks sebagai bagian dari prosesnya, seperti *The Auto-key Vigenere Cipher* ini.

Enkripsi dimulai dengan kunci promer $k_0,k_1,\ldots,k_{i-1}$. Enkripsi karakter sampai karakter ke 1 menggunakan cara yang sama dengan vigenere cipger sederhana. Setelah itu, enkripsi dilanjutkan dengan menggunakan karakter dari plainteks.

Sebagai contoh :

Plainteks : BUKUKRIPTOGRAFI
Kunci : BOYBUKUKRIPTOGR
Cipherteks : CIIVEBCZKWVKOLZ

Untuk mendekripsikannya kita cukup mengetahui kuncinya. Jika sudah mendekripsi dengan kunci, plainteks hasil dekripsinya digunakan sebagai kunci selanjutnya. Kehati-hatian sangat diperlukan saat proses enkripsi, karena kesalahan satu huruf membuat error kepada keseluruhan teks. Hal ini juga berlaku saat pengiriman cipherteks.

2.2.3 The Running-key Vigenere Cipher

Running-key Vigenere Cipher menggunakan teks yang memiliki arti atau cukup dikenal dalam masyarakat. Teks ini bisa berupa buku yang dimiliki oleh pengirim dan penerima pesan. Sebagai contoh :

Plainteks : BUKUKRIPTOGRAFI
Kunci : INDONESIATANAHA
Cipherteks : JHNIXVAXTHGEAMI

Untuk mendekripsinya kita hanya perlu melakukan dekripsi seperti halnya pada metode vigenere cipher sederhana sengan kunci berupa teks yang dimiliki kedua pihak yaitu pengirim dan penerima pesan.

2.2.4 One Time Pad

One time pad menggunakan kunci sepanjang ukuran teks yang ingin dienkripsi secara acak. Setelah dipakai, kertas note dibuang untuk menjaga kerahasiaan dan juga randomisasi kunci selanjutnya. Ditemukan oleh Major Joseph Mauborgne pada tahun 1917. Aturan enkripsi yang digunakan sama persis dengan vigenere cipher biasa. Pengirim pesan mengenkripsi sebuah karakter plainteks dengan sebuah karakter dari kunci. Panjang kunci sama dengan panjang plainteks sehingga tidak terjadi pengulangan. Kekuatan OTP terletak pada kunci yang acak sehingga menghasilkan cipherteks yang seluruhnya acak juga. Selain itu cipherteks yang sama mungkin menghasilkan teks berbeda yang sama-sama memiliki arti sehingga membingungkan kriptanalis.

3. PEMBANGKIT ALIRAN KUNCI

Pembangkit aliran kunci dapat membangkitkan bit-bit kunci berbasis bit per bit atau dalam bentuk blok-blok bit. Untuk yang terakhir ini, *cipher* blok dapat digunakan untuk memperolah *cipher* aliran.

Pembangkit aliran kunci diimplementasikan sebagai prosedur algoritmik, sehingga bit kunci dapat dibangkitkan secara simultan oleh pengirim dan dan penerima pesan. Prosedur algoritmik tersebut menerima masukkan kunci U. keluaran dari prosedur tersebut merupakan fungsi dari U. Pengirim dan penerima pesan harus memiliki kunci U yang sama. Kunci ini harus dijaga kerahasiaanya. *Cipher* aliran menggunakan kunci U yang relatif pendek untuk membangkitkan kunci yang panjang. Namun penulis disini menggunakan huruf alfabet yang diubah ke ascii yang kemudian akan dibangkitkan. Penulis hanya menerapkan metode pembangkitan kuncinya dalam pembangkit aliran kunci ini untuk kemudiaanya digunakan dalam memodifikasi kunci Vigenere Cipher.

4. STREAMED KEY VIGENERE CIPHER

4.1 Konsep Umum

Streamed key Vigenere Cipher adalah paduan antara vigenere cipher dan pembangkit aliran kunci. Maksud adalah algoritma vigenere cipher yang sudah dimodifikasi kuncinya. Kunci di cipher ini diterapkan metode prinsip pembangkit aliran kunci. Kita sudah mengetahui bahwa terdapat kelebihan serta kekurangan dalam vigenere cipher asli, oleh sebab itu penulis berusaha untuk mengambil sisi kelebihannya dan menutupi kekurangannya dengan memodifikasi vigenere cipher tersebut.

Streamed key Vigenere Cipher bekerja pada rangkaian huruf ASCII (di dalam makalah ini hanya 255 karakter, karakter NULL tidak digunakan agar tidak terjadi kesalahan dalam mengenkripsi dan dekripsi). Hal ini bertujuan agar variasi kunci yang memungkinkan semakin banyak sehingga mempersulit kriptanalisis.

Dalam hal ini, kunci dibangkitkan menggunakan bujursangkar vigenere, namun dalam streamed key cigenere cipher ini karakter dalam bujursangkarnya adalah karakter ASCII, dan bujursangkar tersebut terdiri dari 255x255 karakter. Dilihat dari konsep pembangkit aliran kunci, bahwa jika panjang kunci U adalah n bit, maka bit-bit kunci tidak akan berulang sampai 2^n-1 bit, dan dalam Streamed key vigenere cipher yang menggunakan karakter ASCII, maka kunci tersebut tidak akan berulang hingga 255^n-1. Dalam algoritma cipher ini nantinya, semua karakter ascii akan ditulis dalam format heksadesimal.

	0	1	2	3	4	5	6	7	...	253	254
0	1	2	3	4	5	6	7	8	..	254	255
1	2	3	4	5	6	7	8	..	254	255	1
2	3	4	5	6	7	8	..	254	255	1	2
3	4	5	6	7	8	..	254	255	1	2	3
4	5	6	7	8	..	254	255	1	2	3	4
5	6	7	8	..	254	255	1	2	3	4	5
6	7	8	..	254	255	1	2	3	4	5	6
7	8	..	254	255	1	2	3	4	5	6	..
:	..	254	255	1	2	3	4	5	6	..	..
253	254	255	1	2	3	4	5	6	..	..	..
254	255	1	2	3	4	5	6	..	..	..	254

Tabel 2 Bujursangkar Streamed Key Vigenere Cipher

4.2 Algoritma Umum

Pada streamed key vigenere cipher ini, pertama-tama kita memasukkan kunci *K* dangan panjang *n* karakter. Kemudian kunci tersebut akan dibangkitkan dengan menggunakan fungsi GetCipherChar. Pembangkitan kunci tersebut dicari dilihat dari tabel bujursangkar Streamed key vigenere cipher, yang telah dibikin dalam fungsi Table. Setelah memasukkan kunci dengan panjang *n*,kunci setelahnya (n+1) akan dibangkitkan dari kunci sebelumnya dengan melihat ke tabel bujursangkar diatas dan akan digenerete selanjutnya dengan prosedur RotateKeyRiht, menggeser kekanan dengan penggabungan karakter pertama dari panjang kunci 1 dan karakter terakhir dari panjang kunci *n*.

```
private int Table(int row, int col)
    {
      int total = row + col + 1;
      if (total > 0x7F)
        total -= 0x7F
      return total;
    }
private int GetColIndex(int row, char cipherchar)
    {
      int rv = 0;
      for (int i = 0; i < 0x7F; i++)
      {
        if (Table(row, i) == cipherchar)
        {
          rv = i;
          break;
        }
      }
      return rv;
    }
public char GetCipherChar(char key, char plainchar)
    {
      int row = key-1;
      int col = plainchar-1;
      char cipherchar = (char) Table(row, col);
      return cipherchar;
    }
public char GetPlainChar(char key, char cipherchar)
    {
      int row = key-1;
      int col = GetColIndex(row, cipherchar);
      char plainchar = (char) ( col+1);
      return plainchar;
    }
 public char GetKey(int pos, char [] keys)
    {
      char key;
      int N = keys.Length;
      if (pos < N)
        key = keys[pos];
      else
      {  char row = keys[0];
        char col = keys[N - 1];
        key = GetCipherChar(row, col);}
      return key; }
```

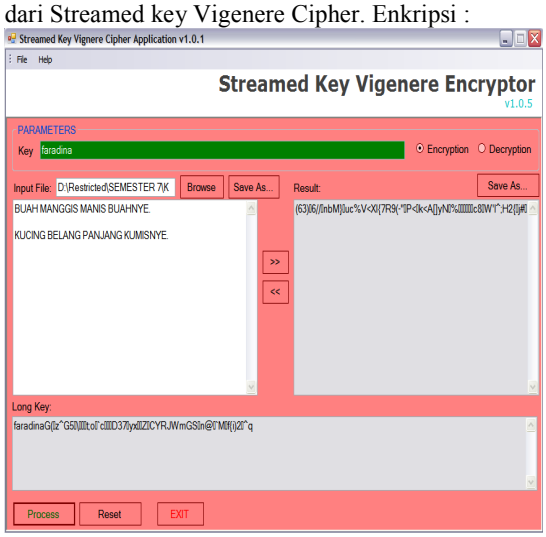
```
private void RotateKeyRight(ref char[] keys, char newkey)
      {
        char[] tmp = new char[keys.Length];
        for (int i = 0; i < keys.Length; i++)
        {
          tmp[i] = keys[i];
        }
        for (int i = 0; i < keys.Length - 1; i++)
        {
          keys[i] = tmp[i + 1];
        }
        keys[keys.Length - 1] = newkey;
      }
```

Untuk enkripsi kita menggunakan metode yang sama dengan Vigenere Cipher, hanya saja pada Streamed Key Vigenere cipher ini menggunakan Bujursangkar nya sendiri dengan karakter ASCII didalamnya. Begitu pula dengan dekripsi, meggunakan cara yang sama dengan dekripsi vigenere cipher tapi dengan tabel bujursangkar ASCII streamed key vigenere cipher.

```
public String Encrypt(string shortkey, string plaintext, ref string longkey)
      {
        int N = plaintext.Length;
        string ciphertext = null;
        int pos=0;
        char[] framekey = shortkey.ToCharArray();
        char currentkey='\0';
        for (int i = 0; i < plaintext.Length; i++)
        {
          char cipherchar = plaintext[i];
            if (i > shortkey.Length)
              RotateKeyRight(ref framekey, currentkey);

            currentkey = lookup.GetKey(i, framekey);
            cipherchar = lookup.GetCipherChar(currentkey, cipherchar);
            longkey += currentkey;
          ciphertext += cipherchar;

        }
        return ciphertext;
      }
 public String Decrypt(string shortkey, string ciphertext, ref string longkey)
      {
        int N = ciphertext.Length;
        string plaintext = null;
        bool warning = false;
        int pos = 0;
        char[] framekey = shortkey.ToCharArray();
        char currentkey = '\0';
        for (int i = 0; i < ciphertext.Length; i++)
        {
          char plainchar = ciphertext[i];
            if (i > shortkey.Length)
              RotateKeyRight(ref framekey, currentkey);

            currentkey = lookup.GetKey(i, framekey);
            plainchar = lookup.GetPlainChar(currentkey, plainchar);
            longkey += currentkey;
          plaintext += plainchar;
        }
        return plaintext;  }
```

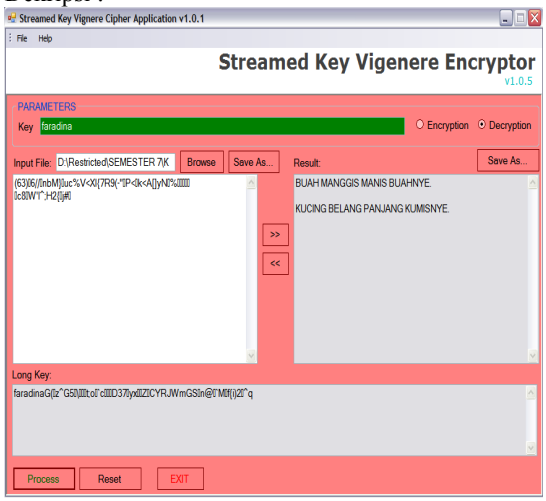
4.3 Hasil Simulasi dan Perbandingan dengan Vigenere Cipher

Berikut akan diperlihatkan hasil enkripsi dan dekripsi dari Streamed key Vigenere Cipher. Enkripsi :



Gambar 1 Enkripsi Streamed Key Vigenere Cipher

Dekripsi :



Gambar 2 Dekripsi Streamed Key Vigenere Cipher

Kekuatan algoritma streamed key vigenere cipher ini terletak pada penggunaan fungsi dalam menghasilkan kunci yang tidak akan berulang hingga 255^n-1. Dengan ini, kriptanalis akan susah untuk memcahkan kuncinya, serta susah untuk mengetahui panjang kunci, karena karakter kunci setelah panjang kunci *n* akan acak dan tidak berulang. Cipher ini membuat

jejak frekuensi dan hubungan antera plainteks dan cipherteks menjadi kabur sehingga mempersulit kriptanalis melakukan kriptanalisis. Algoritma ini juga cukup sederhana sehingga proses enkripsi dan dekripsi dapat dilakukan dengan cepat. Inilah yang membedakan dengan kita menggunakan vigenere cipher asli, karena kuncinya dapat dipecahkan dengan menentukan panjang kunci menggunakan metode kasiski.

4. KESIMPULAN DAN SARAN

Berdasarkan percobaan dan analisis diatas, penulis menarik kesimpulan :

1. Algoritma streamed key vigenere cipher lebih baik dari vigenere cipher yang asli dan variannya, karena menggunakan metode pembangkitan aliran kunci sehingga menghilangkan jejak periodisasi dan frekuensi serta hubungan antera plainteks dengan cipherteks.
2. Jumlah kemungkinan kunci akan berulang adalah 255^n-1.
3. Algoritma streamed key vigenere cipher ini kuat terhadap metode kasiski dalam penentuan panjang kuncinya.
4. Saran bagi yang ingin menggunakan algoritma ini, mungkin masih sederhana sehingga usahakan lebih mempersulit kunci dan proses enkripsi.

DAFTAR REFERENSI

[1] Bishop,David, *Introduction to Cryptography with Java Applet*, Jones and Bartlet Computer Science, 2003

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

[3]http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher, diakses pada bulan Oktober 2007