Keystream Vigenere Cipher: Modifikasi Vigenere Cipher dengan Pendekatan Keystream Generator

Dwitiyo Abhirama / 135 05 013
Program Studi Teknik Informatika ITB, Bandung
email: if15013@students.itb.ac.id

Abstrak

Pertukaran pesan dalam suatu komukisasi perlu diiringi dengan pengamanan. Kriptografi dapat digunakan dalam pengamanan pesan tersebut. Salah satu metode yang telah lama dikenal adalah Vigenere Cipher, yang termasuk ke dalam algoritma kriptografi klasik.

Makalah ini membahas tentang algoritma Vigenere Cipher dengan modifikasi pada kuncinya. Modifikasi dilakukan dengan pendekatan Keystream Generator pada pembangkitan kunci.

Kata Kunci: kriptografi, vigenere cipher, enkripsi, dekripsi, kunci, keystream, cipherteks, plainteks, algoritma, cipher aliran.

1. PENDAHULUAN

Komunikasi merupakan suatu hal yang tidak bisa dilepaskan dari kehidupan manusia. Suatu bentuk komunikasi adalah dengan saling bertukar pesan. Dengan kemajuan teknologi, pertukaran pesan dapat dilakukan dengan berbagai media.

Pesan yang dipertukarkan tersebut dapat bervariasi, dari jenis, kepentingan maupun tingkat kerahasiaannya. Oleh karena itu, diperlukan pengamanan terhadap pertukaran pesan. Kriptografi, baik dengan algoritma klasik maupun modern, telah banyak digunakan dalam pengamanan pesan.

Aloritma kriptografi tersebut dapat ditelaah berdasarkan indikator keamanannya, yaitu: waktu dan biaya yang diperlukan untuk memecahkannya. Dalam dunia kriptografi, suatu algoritma dapat dikatakan aman jika dibutuhkan waktu dan biaya yang relatif besar untuk memecahkannya.

Vigenere Cipher merupakan salah satu algoritma kriptografi klasik yang telah lama digunakan. Namun, Vigenere Cipher telah dapat dilakukan kriptanalisis terhadap panjang kuncinya dengan metode Kasiski. Diteruskan dengan metode analisis frekuensi, Vigenere Cipher dapat dipecahkan. Oleh karena itu, Vigenere Cipher tersebut dimodifkasi untuk mempersulit pemecahan kunci.

Makalah ini membahas modifikasi Vigenere Cipher tersebut. Modikasi tersebut dilakukan pada kuncinya dengan pendekatan Keystream Generator pada pembangkitan kunci.

2. VIGENERE CIPHER

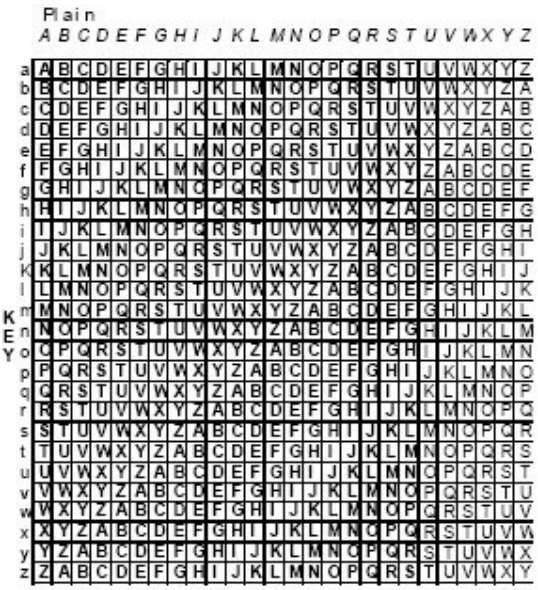
Konsep Dasar

Vigenere Cipher merupakan algoritma kriptografi klasik. Operasi pada algoritma kriptografi klasik berbasis pada operasi karakter, sedangkan operasi pada algoritma kriptografi modern berbasis pada operasi bit. Dalam kriptografi klasik, Vigenere Cipher termasuk ke dalam cipher substitusi abjad majemuk, yang terbuat dari sejumlah cipher abjad tunggal, masing-masing dengan kunci yang berbeda.

Vigenere Cipher telah berkali-kali diciptakan ulang dengan cukup bervariasi. Namun, metode aslinya digambarkan oleh Giovan Batista Belaso pada tahun 1553 seperti tertulis di dalam bukunya La Cifra del Sig. Giovan Batista Belaso. Meskipun demikian, Vigenere

Cipher dipopulerkan oleh Blaise de Vigenere pada tahun 1586.

Vigenere Cipher menggunakan Bujur Sangkar Vigenere (Gambar 1) untuk melakukan enkripsi. Pada bujur sangkar tersebut, kolom paling kiri menyatakan huruf-huruf kunci, dan baris paling atas menyatakan plainteks, sedangkan karakter-karakter lainnya menunjukkan karakter cipherteks. Karakter cipherteks ditentukan dengan menggunakan prinsip Caesar Cipher. Pergeseran huruf menjadi cipherteks ditentukan oleh nilai desimal dari huruf kunci yang bersangkutan (a = 0, b = 1, ..., y = 24, z = 25).



Gambar 1 Bujur Sangkar Vigenere

Bujur Sangkar Vigenere digunakan untuk mendapatkan cipherteks dengan menggunakan kunci yang telah ditentukan. Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang penggunaannya (sistem periodik). Jika panjang kunci adalah m, maka periodenya adalah m. Secara singkat, enkripsi dapat digambarkan sebagai berikut:

```
p (plainteks)   : KRIPTOGRAFI
k (kunci)       : LAMPIONLAMP
c (cipherteks)  : VRUEBCTCARX
```

Penggunaan Bujur Sangkar Vigenere pada enkripsi serupa dengan penjumlahan (dalam desimal) plainteks dengan kunci, lalu modulo 26, sehingga dapat dirumuskan sebagai berikut:

Enkripsi: $c_i = E(p_i) = (p_i + k_i) \bmod 26$
Dekripsi: $p_i = D(c_i) = (c_i - k_i) \bmod 26$

Dekripsi Vigenere Cipher dengan menggunakan Bujur Sangkar Vigenere dilakukan dengan cara berkebalikan enkripsi, yaitu dengan menarik garis mendatar dari huruf kunci sampai ke huruf cipherteks yang dituju, kemudian dari huruf cipherteks tersebut, tarik garis vertikal ke atas sampai ke huruf plainteks.

Untuk memecahkan Vigenere Cipher, perlu mengetahui kuncinya. Jika periode / panjang kunci (m) diketahui, maka kunci dapat diterka dengan *exhaustive search*. Namun, diperlukan hingga 26^m kali percobaan untuk mendapatkan kunci yang menghasilkan plainteks sesuai.

Metode Kasiski telah dapat digunakan untuk menentukan panjang kunci Vigenere Cipher. Dengan diperolehnya panjang kunci, kriptanalisis dapat diteruskan dengan metode analisis frekuensi untuk memecahkan Vigenere Cipher.

Oleh karena itu, berbagai varian Vigenere Cipher bermunculan. Hal tersebut terutama

untuk menutupi kekurangan Vigenere Cipher yang terletak pada pengulangan kunci.

Varian Vigenere Cipher

=> Full Vigenere Cipher
Setiap baris di dalam tabel tidak menyatakan pergeseran huruf, tetapi menyatakan permutasi huruf-huruf alfabet.

=> Auto-Key Vigenere Cipher
Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci disambung dengan plainteks tersebut sehingga panjang kunci menjadi sama dengan panjang plainteks. Misalnya:

```
p (plainteks) : KRIPTOGRAFI
k (kunci)     : LAMPIONKRIP
```

=> Running-Key Vigenere Cipher
Kunci merupakan string panjang yang diambil dari teks bermakna. Misalnya:

```
p(plainteks): KRIPTOGRAFI******
k (kunci)   : KEMANUSIAANYANG..
```

=> One Time Pad
Panjang kunci sama dengan panjang plainteks. Masing-masing karakter kunci diperoleh secara acak.

3. KEYSTREAM GENERATOR

Keystream merupakan bit-bit kunci yang digunakan untuk enkripsi / dekripsi. Keystream umumnya dikenal pada cipher aliran, yang termasuk ke dalam algoritma kriptografi modern.

Keystream tersebut dibangkitkan oleh keystream generator. Keystream generator menerima masukan kunci U dan akan menghasilkan kunci (keystream) yang digunakan untuk enkripsi / dekripsi.

Pengirim dan penerima pesan harus memiliki kunci U yang sama. Kunci U tersebut harus dijaga kerahasiaannya.

Dengan menggunakan keystream generator, kunci U semula akan menghasilkan kunci (keystream) yang akan digunakan untuk enkripsi / dekripsi. Pendekatan terhadap prinsip tersebutlah yang akan digunakan untuk memodifikasi Vigenere Cipher. Penerapan pendekatan tersebut pada Vigenere Cipher dilakukan pada kunci U semula yang panjangnnya lebih pendek daripada panjang plainteks.

4. KEYSTREAM VIGENERE CIPHER

Keystream Vigenere Cipher merupakan perpaduan antara Vigenere Cipher dengan Keystream Generator. Keystream Vigenere Cipher tetap beroperasi pada basis operasi karakter.

Keystream Vigenere Cipher melakukan pedekatan Keystream Generator jika kunci semula U yang merupakan masukan pengguna lebih pendek daripada panjang plainteks. Hal tersebut diwujudkan sebagai berikut:

Untuk karakter kunci (keystream) ke-i, dengan i > m (panjang kunci semula U), karakter kunci (keystream) ke-i ditentukan dengan:

karakter kunci ke-i: $k_i = (k_{i-1} + k_{i-m}) \bmod 26$

Hal tersebut dilakukan hingga panjang kunci (keystream) sama dengan panjang plainteks.

Misalkan kunci semula U adalah WASH, berarti m (panjang kunci) = 4, akan menghasilkan kunci (keystream) sebagai berikut:

```
kunci/keystream: WASH DDVC F...
kar. kunci ke- : 1234 5678 9...
```

Dengan demikian, karakter kunci (keystream) setelah panjang kunci m akan lebih acak. Hal tersebut mengakibatkan kriptanalisis lebih sukar dilakukan

5. KESIMPULAN

Vigenere Cipher, yang termasuk ke dalam algoritma kriptografi klasik, masih memiliki peluang untuk dipecahkan karena penggunaan kunci yang berulang. Pendekatan Keystream

Generator pada Vigenere Cipher dapat menambah kekuatan algoritma.

DAFTAR REFERENSI

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

[2] Bishop, David. *Introduction toCryptography with Java Applets*. Grinnell College. 2003.