MODIFIKASI VIGÈNERE CIPHER DENGAN MENGGUNAKAN MEKANISME CBC PADA PEMBANGKITAN KUNCI

Sibghatullah Mujaddid

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung
Jl. Ganesha No. 10, Bandung
e-mail: if17124@students.if.itb.ac.id

Abstrak – *Vigènere cipher merupakan salah satu algoritma klasik yang digunakan untuk menyembunyikan pesan berupa teks dari pihak yang tidak berhak dengan menggunakan teknik substitusi dimana tiap huruf pada plainteks akan disubstitusi menjadi huruf lain berdasarkan kunci yang digunakan. Berbeda dengan Caesar cipher, Vigènere cipher adalah algoritma substitusi jamak dimana suatu huruf plainteks tidak selalu disubstitusi menjadi huruf yang sama, namun disubstitusi berdasarkan kunci yang digunakan. Algoritma Vigènere cipher klasik ini merupakan algoritma enkripsi yang cukup mudah dipecahkan dengan menggunakan teknik analisis frekuensi terhadap ciphertekstnya.*

Kelemahan utama pada algoritma Vigènere cipher ini yaitu jika panjang kunci lebih pendek dari panjang plainteksnya akan menghasilkan perulangan kunci yang digunakan untuk mengenkripsi plainteks tersebut. Kunci yang berulang tersebut menimbulkan celah berupa jumlah pergeseran yang sama untuk setiap plainteks yang disubstitusi oleh huruf pada kunci yang sama sehingga huruf-huruf pesan atau plainteks dapat dikelompokkan berdasarkan kunci yang digunakan. Karena terdapat kelompok huruf-huruf plainteks yang disubstitusi dengan huruf kunci yang sama karena perulangan kunci, maka tiap kelompok huruf-huruf tersebut dapat dikenakan metode analisis frekuensi terhadapny.

Pada makalah ini, penulis akan membahas perancangan algoritma yang merupakan modifikasi dari Vigènere cipher. Modifikasi yang dilakukan dari algoritma ini adalah dengan menerapkan mekanisme Cipher Block Chaining (CBC) dalam pembangkitan kunci untuk setiap blok plainteks. Mekanisme pembangkitan kunci diadaptasi dari mekanisme operasi Chain Block Chaining (CBC) pada sistem cipher blok. Ide utama dari mekanisme modifikasi ini adalah pembangkitan kunci untuk setiap blok plainteks, di mana setiap blok plainteks berukuran maksimum sama dengan panjang kunci awal, dilakukan dengan mengambil hasil enkripsi (cipherteks) blok sebelumnya. Untuk blok pertama plainteks, dienkripsi dengan menggunakan kunci awal. Dengan demikian, akan dihasilkan kunci dengan panjang yang sama dengan plainteksnya dan kunci baru yang dihasilkan adalah acak berdasarkan kunci awal sehingga algoritma Vigènere cipher akan menjadi lebih kuat.

Kata kunci: *Vigènere cipher*, *Cipher Block Chaining*, kriptografi klasik, analisis kasiski, enkripsi, dekripsi, modifikasi *Vigènere cipher*, pembangkitan kunci, modifikasi algoritma, modifikasi.

1. PENDAHULUAN

Dewasa ini perkembangan teknologi informasi dan komunikasi sudah berkembang sangat pesat. Hampir di setiap bidang kehidupan telah menggunakan teknologi ini sebagai saran pendukung maupun sarana utama. Sehubungan dengan hal ini, aspek keamanan dalam teknologi informasi dan komunikasi tentunya tidak bisa diabaikan. Dalam kegiatan kirim-terima pesan, aspek keamanan yang perlu diperhatikan antara lain kerahasiaan, integritas data, otentikasi, dan nirpenyangkalan. Aspek keamanan tersebut bisa dijaga dengan memanfaatkan kriptografi.

Pada umumnya, algoritma kriptografi bisa dibagi menjadi dua, yakni kriptografi klasik dan kriptografi modern. Kriptografi klasik biasanya menggunakan algoritma yang sederhana dan berbasiskan karakter. Sedangkan kriptografi modern biasanya menggunakan algoritma yang kompleks dan beroperasi dalam mode bit, sehingga lebih susah untuk dipecahkan.

Algoritma kriptografi klasik terdiri dari dua macam, yaitu chiper substitusi dan chiper transposisi. Chiper substitusi menyandikan plainteks dengan cara mengganti setiap karakter dengan karakter lain dalam susunan abjad. Jenis-jenis chiper substitusi ini antara lain chiper abjad-tunggal, chiper abjad-majemuk, chiper substitusi homofonik, dan chiper substitusi poligram. Sedangkan chiper transposisi menyandikan plainteks dengan cara melakukan transpose terhadap rangkaian karakter di dalam plainteks.

Algoritma kriptografi klasik ini menarik untuk dipelajari karena mudah dipahami dan mudah diimplementasikan. Selain itu, kriptografi klasik merupakan dasar dari algoritma kriptografi modern.

2. VIGÈNERE CHIPER

2.1. Konsep Dasar

Vigènere chiper merupakan salah satu contoh chiper abjad-majemuk (polyalphabetic substitution chiper). Chiper abjad-majemuk akan mengganti setiap karakter pada plainteks dengan karakter lain yang mungkin berbeda-beda pada chiperteksnya. Vigènere chiper menggunakan bujur sangkar Vigènere untuk melakukan enkripsi. Setiap baris di dalam bujur sangkar menyatakan huruf-huruf chiperteks yang diperoleh dengan Caesar chiper, di mana jauh pergeseran huruf plainteks ditentukan oleh nilai desimal dari huruf kunci tersebut (A = 0, B = 1, C = 3, ... , Z = 25).

Untuk melakukan enkripsi dengan Vigènere chiper, lakukan pada bujur sangkar Vigènere 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 chiperteksnya.

Pada Vigènere chiper, jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci tersebut akan diulang penggunaannya.

Contoh penggunaan Vigènere chiper:

P : SAYASUKAKRIPTOGRAFI
K : MUSIKMUSIKMUSIKMUSI
C : EUQICGESSBUJLWQDUXQ

Pada contoh di atas, plainteks "SAYASUKAKRIPTOGRAFI" dienkripsi dengan kunci "MUSIK" menghasilkan chiperteks "EUQICGESSBUJLWQDUXQ".

Perhatikan bahwa huruf A pada plainteks disubstitusi dengan huruf yang berbeda-beda pada chiperteks, yakni U, I, S. Hal inilah yang menyebabkan Vigènere chiper termasuk chiper abjad-majemuk.

Aturan enkripsi pada Vigènere chiper bisa dinyatakan juga sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci.

$$C_i \equiv P_i + K_i \pmod{26} \quad \ldots (1)$$

di mana
Pi : karakter plainteks
Ki : karakter kunci
Ci : karakter chiperteks

Dekripsi pada Vigènere chiper dilakukan dengan cara yang berkebalikan, yaitu dengan cara menarik garis horizontal dari huruf kunci sampai ke huruf chiperteks yang dituju, lalu dari huruf cipherteks tarik garis vertikal ke atas sampai ke huruf plainteks. Atau, bisa juga dinyatakan dalam persamaan:

$$P_i \equiv C_i - K_i \pmod{26} \quad \ldots (2)$$

2.2. Kekuatan

Kekuatan algoritma Vigènere chiper ini adalah dapat mencegah frekuensi huruf-huruf di dalam chiperteks yang memiliki pola tertentu yang sama, seperti yang terjadi pada chiper abjad-tunggal. Pada chiper abjad-tunggal, huruf yang paling sering muncul di chiperteks merupakan substitusi dari huruf yang paling sering muncul di plainteks. Karena itu, dengan teknik analisis frekuensi, kriptanalis bisa dengan mudah menebak huruf tersebut. Namun, pada Vigènere chiper hal tersebut tidak bisa dilakukan karena satu macam huruf pada plainteks mungkin dienkripsi menjadi beberapa macam huruf pada chiperteks, seperti pada contoh sebelumnya.

2.3. Kelemahan

Vigènere chiper memungkinkan perulangan huruf atau pasangan huruf pada plainteks terjadi juga pada chiperteksnya. Hal ini dikarenakan kunci yang digunakan untuk melakukan enkripsi juga diulang. Akibatnya, bagian plainteks dan bagian kunci tertentu bisa "berpasangan" lebih dari satu kali. Contoh:

P : SAYACINTAPACARSAYA
K : KASIHKUKASIHKUKASI
C : CAQIJSHDAHIJKLCAQI

Terlihat pada contoh di atas, SAYA dienkripsi menjadi kriptogram yang sama, yaitu CAQI. Namun, perlu diperhatikan bahwa kasus seperti ini tidak selalu demikian, misalnya pada contoh berikut ini:

P : SAYACINTAPACARSAYA
K : SAYANGKUSAYANGKUSA
C : KAWAPOXNSPYCNXCUQA

Pada contoh di atas, SAYA tidak dienkripsi menjadi kriptogram yang sama.

Sifatnya yang mungkin untuk menghasilkan kriptogram yang sama terhadap bagian plainteks yang sama ini menjadi kelemahan Vigènere chiper.

2.4. Metode Kasiski

Metode Kasiski memanfaatkan kelemahan Vigènere chiper yang mungkin menghasilkan kriptogram yang sama untuk bagian plainteks yang sama. Pada contoh di atas, di mana SAYA dienkripsi menjadi kriptogram yang sama, yaitu CAQI, secara intuitif menunjukkan bahwa jika jarak antara dua buah string yang berulang pada plainteks merupakan kelipatan dari panjang kunci, maka string yang sama tersebut akan muncul menjadi kriptogram yang sama pula pada chiperteks. Pada contoh pertama di atas, jarak antara string SAYA adalah 14, dan panjang kunci KASIHKU adalah 7.

Sedangkan pada contoh kedua, jarak antara string SAYA adalah 14, dan panjang kunci SAYANGKU adalah 8.

Dengan metode Kasiski, kriptanalis bisa memperoleh panjang kunci dari suatu Vigènere chiper. Caranya adalah:

1. Mencari semua jarak kriptogram yang berulang pada chiperteks.
2. Mencari faktor pembagi terbesar dari jarak-jarak tersebut. Faktor pembagi ini menyatakan panjang kunci yang mungkin.

Contoh:

QWERTYUIOPASDQWERASDJKLZXCVN

Kriptogram yang berulang adalah QWER dan ASD.

Jarak antara dua perulangan QWER adalah 14. Jarak antara dua perulangan ASD adalah 7. Faktor pembagi 3terbesar 14 dan 7 adalah 7. Dengan demikian, kemungkinan besar panjang kunci adalah 7.

Jika panjang kunci telah diketahui, maka kunci dapat ditentukan dengan beberapa cara, antara lain:

1. Exhaustive key search, yakni dengan membangkitkan semua kemungkinan kunci. Jika panjang kunci adalah p, maka cara ini membutuhkan 26p kali percobaan.
2. Mengelompokkan huruf-huruf pada chiperteks ke sejumlah p kelompok (p = panjang kunci). Lalu, melakukan teknik analisis frekuensi pada tiap-tiap kelompok tersebut.

Dengan demikian, Vigènere chiper merupakan chiper yang bisa terpecahkan (breakable chiper).

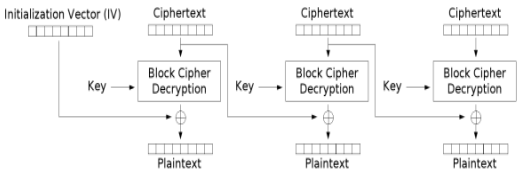
3. CIPHER BLOCK CHAINING

3.1. Konsep Dasar

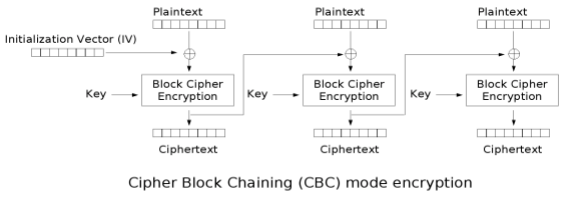
Cipher Block Chaining adalah salah satu mode operasi pada algoritma cipher blok. Algoritma cipher blok sendiri adalah salah satu algoritma kriptografi modern, yaitu algoritma yang beroperasi pada plaintext/ciphertext dalam bentuk blok bit, yang dalam hal ini rangkaian bit dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya. Cipher blok ini dapat beroperasi pada 4 jenis mode. Yaitu Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), dan Output Feedback (OFB).

Konsep yang akan dibahas disini bukan tentang cipher blok, melainkan hanya tentang Cipher Block Chaining (CBC)-nya saja. Mode ini menerapkan mekanisme umpan-balik (feedback) pada sebuah blok, yang dalam hal ini hasil enkripsi blok sebelumnya di-umpan-balik-kan ke dalam enkripsi blok current, yaitu blok yang sedang dioperasikan saat ini. Caranya, blok plainteks yang current di-XOR-kan terlebih dahulu dengan blok cipherteks hasil enkripsi sebelumnya. Selanjutnya hasil peng-XOR-an masuk kedalam fungsi enkripsi. Dengan mode CBC, setiap blok cipherteks bergantung tidak hanya pada blok plainteksnya, tetapi juga pada seluruh blok plainteks sebelumnya.

Dekripsi dilakukan dengan memasukkan blok cipherteks current pada fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok cipherteks sebelumnya. Dalam hal ini, blok cipherteks sebelumnyaberfungsi sebagai umpan-maju (feedforward) pada akhir proses deksipsi. Skema mode CBC dapat dilihat pada gambar 1 dibawah ini. Dalam hal ini, C0 = IV (Initial Vector). IV dapat diberikan oleh pengguna atau dibangkitkan secara acak oleh program. Jadi, untuk menghasilkan blok cipherteks pertama (C1), IV digunakan untuk menggantikan blok cipherteks sebelumnya, C0. Sebaliknya, pada dekripsi, blok plainteks diperoleh dengan meng-XOR-kan IV dengan hasil dekripsi terhadap blok cipherteks pertama.



Cipher Block Chaining (CBC) mode decryption



gambar 1 : Skema Enkripsi dan Dekripsi dengan Mode CBC (sumber: http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation)

3.2 Keuntungan Mode CBC

Karena blok-blok plainteks yang sama tidak menghasilkan blok-blok cipherteks yang sama, maka proses kripanalisis menjadi lebih sulit. Inilah alasan utama penggunaan mode CBC digunakan.

3.3 Kelemahan Mode CBC

Karena blok cipherteks yang dihasilkan selama proses enkripsi bergantung pada blok-blok cipherteks sebelumnya, maka kesalahan satu bit pada sebuah blok plainteks akan merambat pada blok cipherteks yang berkoresponden dan semua blok cipherteks berikutnya. Hal ini berkebalikan dengan proses dekripsi, kesalahan satu bit pada blok cipherteks hanya mempengaruhi blok plainteks yang berkoresponden dan satu bit pada blok plainteks berikutnya (pada posisi bit yang berkoresponden pula).

4. Perancangan Modifikasi Vigènere Cipher

4.1. Konsep Dasar

Modifikasi Vigènere cipher tidak dilakukan pada algoritma utamanya, yaitu enkripsi dan dekripsi, melainkan hanya fokus pada pembangkitan aliran kunci. Algoritma enkripsi dan dekripsi tetap menggunakan algoritma pada Vigènere cipher standar, yaitu dengan rumus aljabar untuk enkripsi:

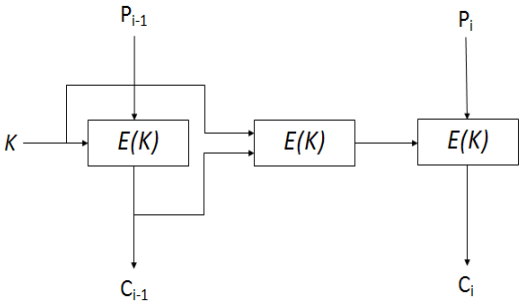
$$C_i \equiv P_i + K_i \pmod{26}$$

dan untuk dekripsi:

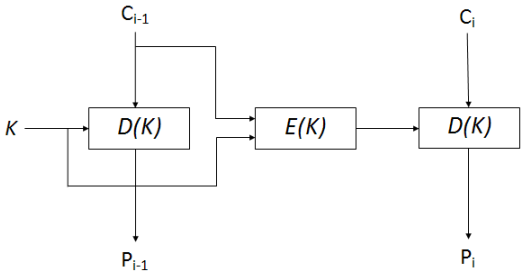
$$P_i \equiv C_i - K_i \pmod{26}$$

Mekanisme modifikasi ini diadaptasi dari mekanisme operasi Cipher Block Chaining (CBC) pada sistem *cipher block*. Namun, pada mekanisme modifikasi ini hanya menerapkan mekanisme umpan-blaik (*feedback*) pada sebuah blok, yang dalam hal ini hasil enkripsi blok sebelumnya di-umpan-balikkan ke dalam enkripsi blok yang *current* sebagai kunci fungsi enkripsi untuk kunci enkripsinya. Dalam modifikasi ini, tidak dilakukan terhadap blok bit plainteks, melainkan terhadap blok karakter plainteks. Selain itu, operasi XOR juga tidak dilakukan seperti pada mode CBC, sehingga dalam modifikasi ini hanya dilakukan proses enkripsi berdasarkan blok plainteks dan kunci. Dalam modifikasi ini, IV yang digunakan adalah kunci awal.

Skema untuk proses enkripsi dan dekripsi pada modifikasi Vigènere cipher adalah sebagai berikut:



(a) enkripsi



(b) dekripsi

Sebelum dienkripsi, plainteks dibagi menjadi beberapa blok dengan panjang tetap, yaitu sama dengan panjang kunci. Setiap blok ini akan dienkripsi dengan kunci yang telah dibangkitkan, yaitu cipherteks hasil enkripsi blok sebelumnya. Untuk blok plainteks pertama, blok plainteks akan dienkripsi dengan cara standar Vigènere cipher yaitu dengan menggunakan kunci awal. Sedangkan untuk blok plainteks berikutnya akan dienkripsi dengan menggunakan kunci yang dihasilkan dari mengenkripsi hasil enkripsi blok (cipherteks) sebelumnya dengan kunci sebelumnya.

Sedangkan dalam proses dekripsinya adalah dengan mendekripsi setiap blok cipherteks dengan menggunakan

kunci yang dihasilkan dari mengenkripsi blok cipherteks sebelumnya dengan kunci sebelumnya. Untuk blok cipherteks pertama, blok cipherteks akan didekripsi dengan cara standar Vigènere cipher yaitu dengan menggunakan kunci awal.

4.2 Algoritma Enkripsi

Secara umum algoritma enkripsi modifikasi Vigènere cipher ini adalah sebagai berikut:

1. Menentukan kunci K. Kunci ini akan digunakan sebagai kunci untuk enkripsi pada blok pertama plainteks.
2. Plainteks P_i dienkripsi menggunakan kunci K.
3. Cipherteks C_i diperoleh dari hasil enkripsi P_i.
4. Enkripsi Cipherteks C_i dengan menggunakan kunci K dan hasilnya simpan sebagai K
5. Lakukan proses enkripsi seperti pada langkah 2 untuk blok plainteks berikutnya yaitu P_{i+1}.
6. Proses berhenti jika tidak ada lagi blok plainteks yang akan dienkripsi.

Contoh:

Diberikan plainteks dan kunci sebagai berikut:

Plainteks: `CINTA MENGALIR SEBENING EMBUN`
Kunci K : `EBIET`

Dengan menggunakan plainteks dan kunci yang sama, Vigènere cipher standar dan Vigènere cipher modifikasi akan dibandingkan.

Plainteks terdiri dari 26 huruf dan kunci terdiri dari 5 huruf. Plainteks kemudian dibagi menjadi blok-blok plainteks dengan panjang blok sepanjang kunci.

Plainteks blok 1: `CINTA`
Plainteks blok 2: `MENGA`
Plainteks blok 3: `LIRSE`
Plainteks blok 4: `BENIN`
Plainteks blok 5: `GEMBU`
Plainteks blok 6: `N`

Pertama, enkripsi blok-blok plainteks tersebut dengan Vigènere cipher standar. Proses enkripsi ini dilakukan dengan menggunakan bantuan progam CryptoHelper dengan hasil sebagai berikut:

`GJVXT QFVKT PJZWX FFVMG KFUFN R`

Kedua, enkripsi blok-blok plainteks tersebut dengan Vigènere cipher modifikasi. Langkah-langkah dalam melakukan enkripsi akan dijelaskan sebagai berikut:

- Lakukan enkripsi blok pertama dengan menggunakan kunci `EBIET` sehingga diperoleh cipherteks berikut:
  Cipherteks blok 1: `GJVXT`

- Lakukan enkripsi cipherteks blok 1 dengan menggunakan kunci K dan simpan sebagai K
  Kunci K: `KKDBM`

- Lakukan enkripsi blok kedua dengan menggunakan kunci K, sehingga diperoleh cipherteks berikut:
  Cipherteks blok 2: `WOQHM`

- Lakukan enkripsi cipherteks blok 2 dengan menggunakan kunci K dan simpan sebagai K
  Kunci K: `GYTIY`

- Lakukan enkripsi blok ketiga dengan menggunakan kunci K, sehingga diperoleh cipherteks berikut:
  Cipherteks blok 3: `RGKAC`

- Lakukan enkripsi cipherteks blok 3 dengan menggunakan kunci K dan simpan sebagai K
  Kunci K: `XEDIA`

- Lakukan enkripsi blok keempat dengan menggunakan kunci K, sehingga diperoleh cipherteks berikut:
  Cipherteks blok 4: `YIQQN`

- Lakukan enkripsi cipherteks blok 4 dengan menggunakan kunci K dan simpan sebagai K
  Kunci K: `VMTYN`

- Lakukan enkripsi blok kelima dengan menggunakan kunci K, sehingga diperoleh cipherteks berikut:
  Cipherteks blok 5: `BQFZH`

- Lakukan enkripsi cipherteks blok 5 dengan menggunakan kunci K dan simpan sebagai K
  Kunci K: `WCYXU`

- Lakukan enkripsi blok keenam dengan menggunakan kunci K, sehingga diperoleh cipherteks berikut:
  Cipherteks blok 6: `J`

Hasil enkripsi selengkapnya bila disusun kembali adalah sebagai berikut:

`GJVXT WOQHM RGKAC YIQQN BQFZH J`

Jika dibandingkan, cipherteks dari hasil modifikasi ini menghasilkan susunan huruf-huruf yang lebih acak Perhatikan blok 2 dan blok 4 pada plainteks, terdapat pola yang sama pada posisi yang sama, yaitu karakter ke-2 dan ke-3 pada masing-masing blok adalah sama.

Plainteks blok 2: MENGA
Plainteks blok 4: BENIN

Hasil enkripsi dari masing-masing blok pada mode Vigènere cipher standar adalah sebagai berikut:

Cipherteks blok 2: QFVKT
Cipherteks blok 4: FFVMG

Perhatikan bahwa pada hasil enkripsi kedua blok memiliki pola yang sama pada posisi karakter ke-2 dan ke-3. Pola yang dimilikinya sama dengan plainteks. Hal ini dapat menunjukkan bahwa FV pada kedua blok cipherteks memiliki plainteks yang sama, yaitu EN.

Bandingkan dengan hasil enkripsi dari masing-masing blok plainteks pada mode Vigènere cipher modifikasi berikut:

Cipherteks blok 2: WOQHM
Cipherteks blok 4: YIQQN

Perhatikan, hasil enkripsi kedua blok menghasilkan pola yang berbeda untuVk posisi karakter ke-2 dan ke-3. Hal ini berbeda dengan mode Vigènere cipher standar yang selalu menghasilkan pola yang sama dengan plainteksnya dengan periode yang sama. Cipherteks hasil modifikasi Vigènere cipher ini menghasilkan susunan huruf-huruf yang lebih acak dan sulit dipecahkan dibandingkan Vigènere cipher standar.

4.3 Algoritma Dekripsi

Secara umum algoritma dekripsi modifikasi Vigènere cipher ini adalah sebagai berikut:

1. Cipherteks C_i didekripsi dengan menggunakan kunci K.
2. Diperoleh plainteks P_i
3. Enkripsi Cipherteks C_i dengan menggunakan kunci K dan hasilnya simpan sebagai K.
4. Lakukan proses dekripsi seperti pada langkah 1 untuk blok cipherteks berikutnya yaitu C_{i+1}.
5. Proses berhenti jika tidak ada lagi blok cipherteks yang akan didekripsi.

Contoh:

Diberikan cipherteks dan kunci sebagai berikut:

Cipherteks: GJVXTWOQHMRGKACYIQQNBQFZHJ
Kunci : EBIET

Untuk proses dekripsi lakukan cara yang sama dengan proses enkripsi, yaitu dekripsi setiap blok. Langkah-langkah dalam melakukan dekripsi akan dijelaskan sebagai berikut:

- Lakukan dekripsi blok pertama dengan menggunakan kunci EBIET sehingga diperoleh plainteks berikut:
  Plainteks blok 1: CINTA
- Lakukan dekripsi cipherteks blok 1 dengan menggunakan kunci K dan simpan sebagai K
  Kunci K: KKDBM
- Lakukan dekripsi blok kedua dengan menggunakan kunci K, sehingga diperoleh plainteks berikut:
  Plainteks blok 2: MENGA
- Lakukan dekripsi cipherteks blok 2 dengan menggunakan kunci K dan simpan sebagai K
  Kunci K: GYTIY
- Lakukan dekripsi blok ketiga dengan menggunakan kunci K, sehingga diperoleh plainteks berikut:
  Plainteks blok 3: LIRSE
- Lakukan dekripsi cipherteks blok 3 dengan menggunakan kunci K dan simpan sebagai K
  Kunci K: XEDIA
- Lakukan dekripsi blok keempat dengan menggunakan kunci K, sehingga diperoleh plainteks berikut:
  Plainteks blok 4: BENIN
- Lakukan dekripsi cipherteks blok 4 dengan menggunakan kunci K dan simpan sebagai K
  Kunci K: VMTYN
- Lakukan dekripsi blok kelima dengan menggunakan kunci K, sehingga diperoleh plainteks berikut:
  Plainteks blok 5: GEMBU
- Lakukan dekripsi cipherteks blok 5 dengan menggunakan kunci K dan simpan sebagai K
  Kunci K: WCYXU
- Lakukan dekripsi blok keenam dengan menggunakan kunci K, sehingga diperoleh plainteks berikut:

Plainteks blok 6: N

Hasil dekripsi selengkapnya bila disusun kembali adalah sebagai berikut:

CINTA MENGA LIRSE BENIN GEMBU N

4.4 Serangan Terhadap Cipherteks

.Contoh pertama, yaitu dengan cara pengubahan salah satu bagian cipherteks. Misal:

Cipherteks asli: GJVXTWOQHMRGKACYIQQNBQFZHJ
Cipherteks hasil serangan:
GJVXTWOBHMRGKACYIQQNBQFZHJ
(*huruf Q pada karakter ke 8 diganti menjadi B*)

Jika didekripsi, menjadi:
Cipherteks: GJVXTWOBHMRGKACYIQQNBQFZHJ
Kunci K: EBIET
Plainteks: CINTAMEYGALIGSEBECINGEBBUN

Contoh kedua, yaitu dengan cara penambahan cipherteks. Misalkan:

Cipherteks asli: GJVXTWOQHMRGKACYIQQNBQFZHJ
Cipherteks hasil serangan:
GJVXTWNOBHMRGKACYIQQNBQFZHJ
(*penambahan huruf N setelah karakter ke 6 (W)*)

Jika didekripsi, menjadi:
Cipherteks: GJVXTWNOBHMRGKACYIQQNBQFZHJ
Kunci K: EBIET
Plainteks: CINTAMDLPVGUPTHKKLPXTPLOQAW

Contoh ketiga, yaitu dengan cara pengurangan satu atau lebih karakter cipherteks. Misal:

Cipherteks asli: GJVXTWOQHMRGKACYIQQNBQFZHJ
Cipherteks hasil serangan:
GJVXTWOQHMRGKACYIQQNBQFZHJ
(*huruf H pada karakter ke 9 dihilangkan*)

Jika didekripsi, menjadi:
Cipherteks: GJVXTWOBHMRGKACYIQQNBQFZHJ
Kunci K: EBIET
Plainteks: CINTAMENLFAMHPVWIXYAWHQFH

Dari ketiga contoh diatas, diperoleh kesimpulan bahwa cipherteks yang telah diserang atau rusak, tidak dapat menghasilkan plainteks yang memiliki arti, sehingga integritas data akan tetap terjamin.

4.5 Metode Kasiski

Metode kasiski dapat digunakan untuk menemukan panjang kunci pada Vigènere cipher dengan cara mencari kriptogram yang sama pada cipherteks.

Dengan menggunakan modifikasi Vigènere cipher ini, kemungkinan adanya kriptogram berulang dapat diperkecil. Dari contoh dibawah ini kita bisa melihat perbedaan antara Vigènere Cipher standar dengan Vigènere cipher modifikasi ini dalam mengenkripsi plainteks yang memiliki pasangan huruf berulang yang jaraknya merupakan kelipatan panjang kunci.

Contoh:
Plainteks:
CRYPTO IS SHORT FOR CRYPTOGRAPHY
Kunci : abcd
Cipherteks menggunakan Vigènere Cipher:
CSASTP KV SIQUT GQU CSASTPIUAQJB
Cipherteks menggunakan modifikasi Vigènere cipher:
CSASVH KN PHAZF MAY TKKUDRCQNJFN

Dapat dilihat bahwa pada Vigènere cipher standar, untuk pola yang sama pada plainteks dengan periode kunci yang sama akan menghasilkan pola kriptogram yang sama.

Sedangkan pada Vigènere cipher modifikasi, pola yang sama pada plainteks tidak menghasilkan pola kriptogram yang sama atau kriptogram yang berulang.

Dengan demikian, kriptanalis akan sulit menemukan korelasi huruf plainteks dengan cipherteks, dan panjang kunci tidak ditemukan walaupun dicari dengan metode kasiski, karena kriptogram berulang tidak ditemukan.

4.6 Kelebihan

Vigènere cipher modifikasi ini memiliki beberapa keunggulan jika dibandingkan dengan Vigènere Cipher standar. Dari segi keamanan, Vigènere cipher modifikasi ini menawarkan penyandian yang lebih aman, dengan pengacakan yang lebih rumit, menggunakan pembangkitan kunci yang acak untuk setiap blok plainteks, dan cipherteks yang dihasilkan tidak mengandung kriptogram yang berulang, seperti terlihat pada contoh diatas. Dari segi lainnya, Vigènere cipher modifikasi memiliki keunggulan dibanding Vigènere Cipher standar, yaitu mendukung integritas data, sehingga aman dari serangan oleh pihak lawan.

4.7 Kekurangan

Walaupun begitu, Vigènere cipher modifikasi tetap memiliki kekurangan. Diantaranya, rumitnya teknik enkripsi dan dekripsi, karena untuk dalam proses enkripsi blok plainteks, enkripsi dilakukan dua kali, pertama enkripsi blok plainteks menggunakan kuncinya, kedua enkripsi cipherteks dengan menggunakan kunci dan simpan sebagai kunci untuk digunakan pada proses enkripsi blok plainteks berikutnya. Demikian halnya dengan teknik dekripsi.

Untuk pengiriman data yang harus sampai walaupun terjadi sedikit cacat, kelebihan Vigènere cipher modifikasi malah menjadi salah satu kekurangannya. Cipherteks yang ternoda karena serangan tidak dapat mengembalikan plainteks utuh, atau plainteks yang sedikit rusak atau ternoda seperti halnya pada Vigènere Cipher. Pada Vigènere cipher modifikasi, bagian setelah Cipherteks ternoda (diubah, dihapus, maupun bagian setelah cipherteks palsu yang ditambahkan) tidak dapat didekripsi dengan benar.

5. KESIMPULAN

Algoritma Vigènere biasa merupakan algoritma yang sangat kuat sebelum dipecahkan oleh Kasiski. Oleh karena itu, dengan menemukan sebuah algoritma berdasarkan pada Vigènere yang diolah sedemikian rupa hingga menyulitkan menemukan panjang kunci dengan menggunakan metode Kasiski akan membuat algoritma tersebut menjadi sebuah algoritma enkripsi yang kuat.

Berdasarkan percobaan dan analisis yang sudah dituliskan di atas, penulis bisa menarik beberapa kesimpulan terkait Vigènere Chiper dengan modifikasi mekanisme CBC:

- Vigènere Chiper dengan modifikasi mekanisme CBC lebih baik daripada Vigènere Chiper standar karena menghilangkan perulangan kunci yang digunakan.

- Vigènere Chiper dengan modifikasi mekanisme CBC menghasilkan cipherteks acak tanpa kriptogram berulang untuk pola yang sama pada plainteks.

- Vigènere Chiper dengan modifikasi mekanisme CBC sangat kuat terhadap serangan chipertext-only, berupa teknik analisis frekuensi ataupun metode Kasiski.

REFERENSI

[1] Munir, Rinaldi, 2005. *Diktat Kuliah IF5054 Kriptografi*. Departemen Teknik Informatika, Institut Teknologi Bandung.

[2] http://en.wikipedia.org/wiki/Vigenère_cipher diakses pada Kamis, 25 Maret 2010.

[3] http://en.wikipedia.org/wiki/Block cipher modes of operation diakses pada Jum'at, 26 Maret 2010.

[4] http://www.informatika.org/~rinaldi/Kriptografi/2009-2010/CryptoHelper.jar

[5] Sugianto, Anggriawan. 2007. *Vigènere Cipher dengan Modifikasi Fibionacci*. Departemen Teknik Informatika, Institut Teknologi Bandung.

[6] Susanto, Eko Budhi. 2007. *Modifikasi Vigènere Cipher Dengan Pendekatan Mode Operasi Cipher Block Chaining*. Departemen Teknik Informatika, Institut Teknologi Bandung.