NAMA :NURHIKMAH

NIM :D0216015

KELAS : B

Vigenere Cipher

Vigenere Cipher adalah contoh terbaik dari chipher alfabet ‘manual’. Algoritma ini dipublikasi oleh diplomat (sekaligus seorang kriptologis) Prancis balaise de Vigenere pada abad 16, meskipun giovan batista Belaso telah menggambarkannya pertama kali pada tahun 1553 seperti ditulis dalam bukunya la cifra del sig. Giovan Batista Belaso. Vigenere cipher dipublikasikan pada tahun 1586, tetapi algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemuaanya cipher tersebut kemudian dinamakan vigener cipher. Cipher ini berhasil di pecahkan oleh babbage dan kasiski pada pertengahan abad 19 [PIP02] Viginer cipher digunakan oleh tentara konfderasi (Confiderate Army) pada perang Sipil Amerika (American Civil war). Perang sipil terjadi setelah Vigener berhasil dipecahkan. Vigener Cipher sangat dikenal karena mudah dipahami dan implementasikan. Cipher menggunaan bujursangkar Vigenere untuk malakukan enkripsi. Kolom paling kiri dari bujur sangkar menyatakan huruf-huruf kunci, sedangkan baris palig atas menyataan huruf-huruf plaaintext. Setiap baris didalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dari caesar chipher yang mana jumlahpergeseran huruf plainteks ditentukan nilai numerik huruf kunci tersebut (yaitu, a=0, b= 1 ,c=2,.....z=25)

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 plaiteks THIS PLAINTEXT dan kunci adalah Sony maka pengguna kunci secara periodik adalah sbb

PLAINTEXT : THIS PLAINTEXT

KUNCI : sony sonysony

Sertiap huruf Plainteks akan di enkripsi dengan setiap huruf kunci dibawahnya untuk mengerjakan enkripsi dengan vigenere chipher. Lakukan pada bujursangkar viginere sebagai berikut: tarik garis vertikal dari huruf plainteks ke bawah lalu tarik garis mendatar dari huruf kunci kekanan. Perpotongan kedua garis tersebut menyatakan hurf chiperteksnya.

Contoh

Misalkan plainteks THIS PLAINTEXT dienkripsi dengan kunci Sony karena panjag unci tidak sama maka kunci diulang secara periodik.

PLAINTEXT : THIS PLAINTEXT

KUNCI : sony sonysony

Chiphertext:LVVQ HZNGFHRVL

Secara matematis, misalkan kunci dengan panjag k1K1,.....Km . Plainteks aslah rangkaian p1 p1.... pn. Dan chipherteksadalah arangkaian p c1, c1..... cn maka enkripsi vigenere cipher dapat dinyatakan sebagai:

c1=( pi+ kr) md 26 (1≤i≤i≤t)

dan

i=r(mod ) (1≤r ≤t)

contoh:

(T+S) mod 26 =(19+14)mod 26 = 11= L

(H+o) mod 26 =(7+18)mod 26 = 21 =V

viginer chipher dilakukan dengan cara berkebalikan yang menarik garis sampai periodik.untuk memecahkan vigenere cipher, cukup menentukan kunci jika kunci tidak teralalu panjang. Kunci dpt ditemukan dengan menuis program komputer untuk melakukan exhaustive ke search. Sebagai contoh jika chiperteks yang dihasilkan dengan vigenere hada.

p1=( c1- k1) Mod 26.

Kelemahan vigenere cipher adlah kuncinya yang pendek diulang secara periodik. Untuk memecah vigenere cipher untuk menentukan kuncinya dan tidak terlalu jika hasil deskripsi dengan kunci tersebut menyataan kata yang berarti. Cara ini membutuhkan usaha pecobaan sebanyak 26n kali. Semkin panjang kunci (semakin besar periode) semakinbanyak usaha percobaan yang harus dilakukan.

Metode Kasiski untuk menentukan panjang knci.

Metode kasiski membantu menemukan panjang kunci. friedrichKasiski adalah orang yang pertama kali memecahkan Vigenere Cipher pada tahun 1863 tetapi Charles Babbage telah mengembangkan cara yang serupa tahu 1854.[WIKA06. Metode Kasiski memanfaatkan keuntugan bahwa bangsa inggris tida hanya mengandung perulangan huruf double huruf atau tripel hururf. Seperti TH,the dan sebagainya. Perulangan kelompo huruf ini ada kemungkinan menghasilkan kriptogma yangberulang.

Plainteks : CRIPTO IS SHORT FOR CRYPTOGRAPHY

Kunci : abcdab cd abcda bcd abcdabcdabcd

Cipherteks : CSASTP KV SIQUT SQU CSASTPIUAQJB

Pada contoh ini CRIPTO dienkripsi menjadi kriptogramyang sama, yaitu CSATP, tetapi kasus seerti ini tidak selalu demikian misalnya pada contoh berkut:

Plainteks : CRIPTO IS SHORT FOR CRYPTOGRAPHY

Kunci : abcdab cd abcda bcd abcdabcdabcd

Cipherteks : CSASTP KV SIQUT SQU CSASTPIUAQJB

Pada contoh diatas. CRYPTO tidak di enkripsi menjadi kriptogma yang sama. Secara intutif kita dpat membuat argumentas bahwa jika jarak antara dua buah string yang berulang didalam plainteks merupakan kelipatan dari panjang kunci, maka string yang tersebut akn muncul menjadi kriptogma yang sama pula di dalam cipheteks. Hal ini ditunjukkan pada contoh pertama, yang mana kunci adalah abcd dengan panjang 4. Sementara stirng CRYPTO muncul berulang di dalam plainteks dan jarak antara dua buah kemunculan ini (dihitung dari awal setiap perulanagan string) adalah 16 karakter (tidak termask spasi) dan 16 adalah kelipatan 4. Sedangkan pada contoh kedua uncinya abcdef dengan panang . tetapi 6 bukan kelipatan 16.

Untu menentukan panjang kunci langkah-langkahnyaadaala sebagai berikut[WI06]

Kriptanalis mengitun semua kriptogma yang berulang did alam cipherteks. (pesan yang panjang biasanya mengundang kriptogma yang berulang ) kemudiank jarak antara kriptogram yang berulang dihitung.

Kriptanalis menghitung semua faktor 9pembaki0 dari jarak tersebut. Faktor pembaki menyatakan kunci yang mungkin. Tentukan irisan dari impunan faktor pembagi tersebut. Nilai yang muncul didalam irisan menyataan aknka yang muncul pada semua faktor ebagi dari jarak-jarak tersbut. Nilai tersebut mungkin adalah panjang kunci hal ini karen string yang berulang dapat muncul bertindihan coincidence) tetapi sangat mungkin terjadi huruf yang sam dienkripsi dengan hruf kunci yang sama huruf-huruf kunci diulang pada kelipatan panjang kunci sehingga jarak yang ditemukan pada langkah satu sangat mungkin merupakan kelipta panjang kunci.

Misalkan kriptanalis memperoleh cipherteks

**DYDUXRM**HTVDV**NQD**QNW**DYDUXRMH**ARTJGW**NQD**

Kripto yang berulang adalah **DYDUXRM** dan NQD jarak antara dua buah perulangan **DYDUXRM** adalah 18. Semua aktor pembagi 18 adlaah {18, 9, 6, 3, 2} (1 tidak dimasukkan) yang menyiratkan baha panjang kunci kemungkinan adalah faktor-faktor tersebut. Jarak antara dua buah **NQD** adalah 20. Semua aktr pembagi 20 adalah{20, 10, 5, 4, 2,} irisan dari kedua buahn himpunan tersebut adlah 2 sehingga kita mentimpulkan anang kunci kemungkinan besar adalah 2.

Variasi vigenere cipher

Terdapat sejumlah farian Vigenere Cipher yang pada dasarnya perbedaanya terletak pada cara membentuk tabel atau cara menghasilkan kuncinya sedangkan enkripsi dan diskripsi tidak berbeda dengan viginere cipher standar. Beberapa varian diantaranya:

1. Full vigenere cipher

pada varian ini setiap baris didalam tabel tidak menyatakan pergeseran huruf, tetapi merupakan permutasi huruf-huruf alfabet. Mislanya pada baris A sususnan huruf-huruf alfabet adaalah acak seerti dibawah ini.

1. Auto Key Vigenere Cipher

Idealnya kunci tidak digunakan secara berulang, pada auto-key vigenere cipher, jika panjang kunci lebih kecil dari panjang plainteks. Maka kunci dismabng dengan plainteks tersebut. Misalnya untuk mengengkripsi pesan.

NEGARA PENHASIL MINYAK

Dengan Kunci

INDO

Maka kunci tersebut disambung dengan plainteks semula sehingga panjang kunci menjadi plainteks:

Plainteks : NEGARAPENGHASILMINYAK

Kunci : INDONEGARAPENGHASILMI

1. RUNNING-KEY VIGENERE CIPHER

Pada varian ini, kunci bukan string pendek yang diulang secra periodik seperti pada vigenere Cipher standard. Tetapi kunci adalah string yang sangat panang yang diambil dari teks bermakna (misalnya naskah roklamasi, naskah pembukaan UUD 1945, terjemahan ayat didalam kitab suci, dan lain-lain). Untuk menengkripskan plainteks:  
NEGARA PENGHASIL MINYAK

Dapat digunakan kunci berupa sila ke-2 Pancasila:

KEMASNUSIAAN YANG ADIL DAN BERADAB

Selanjutnya enkripsi dan deskripsi dilakukan seperti biasa.