NAMA : NUR SYAHRA

NIM : D02 16 340

**Vigenere Chipher**

Vigenere Chipher adalah contoh terbaik dari copher alphabet-majemuk ‘manual’. Algoritma ini dipublikasikan oleh diplomat(Sekaligus seorang kriptografi) Peransic, Blaise de Vigenere pada abad 16, meskipun Giovan Batisa Belaso telah menggambarkannya pertama kali pada tahun 1553 seperti ditulis di dalam bukunya La Cifra del Sig. Vigenere Chipher dipublikasikan pada tahun 1586, tetapi algoritma tersebut baru dikenal luas 200 tahun kemudian oleh penemunya chipper tersebut kemudian menamakan Vigenere Chipher. Chiper ini berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19[PIP02]. Vigenere Chipher digunakan oleh Tentara Konfiderasi pada Perang sipil Amerika. Vigenere Chipher sangat dikenal karena mudah dipahami dan diimplementasikan. Chiper menggunakan bujursangkat sedangkan Vegenere untuk melakukan ekripsi seperti ditunjukkan pada gambar. Kolom paling kiri dari bujursangkar menyatakan huruf-huruf kunci ,yang mana jumlah pergeseran huruf chiperteks yang diperoleh dengan Caesar cipler,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

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.

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.