Modifikasi *Vigenere Cipher* dengan Menggunakan *Caesar Cipher* dan Enkripsi Berlanjut untuk Pembentukan *Key*-nya

Fatardhi Rizky Andhika 13508092
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18092@students.if.itb.ac.id

***Abstract*—*Vigenere cipher* merupakan salah satu jenis algoritma klasik yang populer dan sering digunakan sebagai metode penyembunyian pesan (kriptografi). *Vigenere cipher* ini menggunakan teknik substitusi dalam pengenkripsian pesannya dimana setiap karakter plainteks pada pesan akan dienkripsi menjadi karakter lain pada cipherteks berdasarkan kunci yang digunakan. Algoritma ini termasuk ke dalam jenis cipher abjad majemuk atau lebih sering disebut sebagai *polyalphabetic subtitution cipher*. Algoritma ini merupakan bentuk pengembangan dari Caesar Cipher yang juga menggunakan metode substitusi karakter untuk melakukan enkripsi pesan. Tujuan utama dari algoritma enkripsi *Vigenere cipher* ini adalah untuk meminimalkan keterhubungan antara karakter plainteks dan karakter cipherteks yang merupakan kelemahan dari jenis substitusi alfabet tunggal seperti Caesar Cipher. Namun, saat ini telah ditemukan metode ampuh yang dapat secara tepat memecahkan pengkodean *Vigenere cipher* yaitu metode Kasiski. Metode kasiski memanfaatkan kelemahan *Vigenere cipher* yang menggunakan kunci yang sama berulang kali dalam pengkodean karakternya. Walaupun begitu, masih ada teknik-teknik tertentu yang dapat dilakukan untuk memperkuat *Vigenere cipher* sekaligus menggagalkan metode Kasiski tersebut. Dalam makalah ini, akan dipaparkan cara memperkuat *Vigenere cipher* dengan melakukan modifikasi terhadap *Vigenere cipher*. Modifikasi dilakukan dengan menerapkan enkripsi Caesar Cipher yang dibangkitkan dari kunci dan teknik pembangkitkan kunci berikutnya dengan menggunakan enkripsi Vigenere berlanjut sehingga kunci yang digunakan untuk pengkodeannya akan berbeda dengan kunci yang digunakan sebelumnya. Dengan penggunaan metode ini, keterhubungan antara plainteks dan cipherteks akan akan menjadi semakin berkurang dan semakin sulit untuk dipecahkan kriptanalis.**

Kata kunci — Caesar Cipher*, dekripsi, enkripsi, Kasiski, *Vigenere cipher

I. PENDAHULUAN

Informasi adalah inti yang dipertukarkan dalam proses berkomunikasi. Jenis informasi yang digunakan dalam komunikasi pun bermacam-macam. Jika dilihat dari isinya, informasi dapat berupa penting atau tidak penting. Bila dilihat dari sifat persebaran atau *privacy*-nya, informasi dapat bersifat rahasia atau tidak rahasia. Sejak dahulu kala, orang-orang senantiasa berusaha untuk melindungi kerahasiaan dari informasi yang dikomunikasikan melalui media tertentu kepada orang yang dimaksud supaya informasi pada pesan tersebut hanya dapat diterima oleh orang yang bersangkutan saja. Semua orang berusaha untuk melindungi kerahasian informasi yang mereka miliki dengan cara apapun.

Adalah kriptografi, ilmu dan seni untuk menjaga kerahasiaan pesan/berita dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Tujuan dari kriptografi adalah supaya sebuah pesan yang disampaikan hanya akan dapat dimengerti oleh orang yang berhak untuk membacanya saja. Kriptografi ini telah digunakan sejak lama. Bangsa atau peradaban masa lalu seperti mesir ribuan tahun lalu dan peradaban lainnya telah menggunakan konsep kriptografi dalam menyamarkan pesan rahasia dengan media tulis berupa kertas yang disampaikan antarmereka. Kerajaan-kerajaan atau pemerintahan juga telah lama menggunakan penyandian untuk menyembunyikan pesan rahasia yang ingin disampaikan kepada pihak-pihak tertentu saja. Kriptografi diterapkan untuk mempertahankan kerahasiaan informasi yang terdapat dalam media pesan.

Saat ini, ilmu kriptografi semakin banyak digunakan dan mulai berubah menjadi kebutuhan. Dengan maraknya perkembangan ilmu dan teknologi, informasi-informasi penting pun tidak lagi hanya berada pada media tulis saja. Banyak benda-benda di sekitar kita yang memuat informasi-informasi penting yang tidak boleh jatuh ke tangan yang tidak berhak seperti PIN dan *password*, informasi kartu ATM, dan lain-lain. Disinilah kirptografi berperan, menyembunyikan informasi-informasi penting tersebut sehingga hanya pengguna atau orang tertentu saja lah yang dapat mengetahui informasi tersebut.

Secara umum, algoritma yang digunakan dalam kriptografi dapat terbagi ke dalam dua macam, yaitu algoritma kriptografi klasik dan algoritma kriptografi modern. Algoritma kriptografi klasik biasanya adalah algoritma penyembunyian teks yang bersifat sederhana,

berbasis pada pemrosesan per-karakter dan dapat dilakukan tanpa menggunakan komputer. Sedangkan algoritma kriptografi modern adalah algoritma kriptografi yang menggunakan algoritma kompleks dan menggunakan pengolahan berbasis bit dalam proses enkripsi pesannya.

Walaupun algoritma yang umum digunakan dalam kriptografi sekarang ini adalah algoritma kriptografi modern yang lebih kuat dan aman, algoritma kriptografi modern yang berkembang sekarang ini tidak lain dan tidak bukan adalah berkat keberadaan algoritma kriptografi klasik yang lebih dulu digunakan dan kemudian dikembangkan serta disesuaikan dengan kebutuhan dan perkembangan zaman.

Algoritma kriptografi klasik ini menarik untuk dipelajari karena mudah dipahami dan dipelajari serta dilakukan modifikasi terhadapnya. Contoh dari algoritma kriptografi klasik adalah algoritma Caesar Cipher dan algoritma *Vigenere cipher*. Meskipun kedua algoritma ini telah dapat dipecahkan oleh para kriptanalis, algoritma kriptografi klasik ini dapat menginspirasi terciptanya teknik-teknik modifikasi tertentu yang dapat memperkuat algoritma kriptografi klasik itu sendiri. Salah satunya yaitu teknik modifikasi pada *Vigenere cipher* yang akan dijelaskan dalam makalah ini.

II. *CAESAR CIPHER*

KONSEP DASAR *CAESAR CIPHER*

Caesar Cipher merupakan salah satu algoritma cipher tertua dan paling diketahui dalam perkembangan ilmu kriptografi. Caesar cipher merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada chiperteks. Teknik seperti ini disebut juga sebagai chiper abjad tunggal.

Gambar 1 Caesar Wheel
digunakan sebagai tabel substitusi masa lampau

Algoritma kriptografi Caesar Cipher sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama.

Adapun langkah-langkah yang dilakukan untuk membentuk chiperteks dengan Caesar Cipher adalah :

1. Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks.
2. Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya.

Berikut adalah contoh penggunaan Caesar Cipher dengan besar pergeseran sebesar 3 karakter. Dengan nilai pergeseran tersebut, didapat tabel pergeseran nilai Caesar Cipher sebagai berikut :
Tabel Subtitusi :

p_i :	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
c_i :	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**

Contoh proses penggunaan Caesar Chiper:

Pesan
AWASI ASTERIX DAN TEMANNYA OBELIX

Dengan enkripsi menggunakan tabel di atas, pesan dienripsi menjadi :

Chiper
DZDVL DVWHULA GDQ WHPDQQBA REHOLA

Penerima yang menerima chiper tersebut kemudian mendekripsi lagi pesan dengan menggunakan tabel yang sama menjadi :

Pesan Hasil Dekripsi
AWASI ASTERIX DAN TEMANNYA OBELIX

Bila setiap abjad pada plainteks dimisalkan sebagai angka dengan urutan A= 0, B=1, C=2, ..., dan Z=25, maka didapat persamaan matematis dari algoritma Caesar Cipher yaitu :

- Persamaan Enkripsi
$$c_i = E(p_i) = (p_i + 3) \bmod 26$$

- Persamaan Dekripsi
$$p_i = D(c_i) = (c_i - 3) \bmod 26$$

dengan
p_i adalah karakter plainteks ke-i, dan
c_i adalah karakter chiperteks ke-i

KELEMAHAN

Caesar Cipher merupakan algoritma kriptografi dengan keamanan yang paling rendah. Penyebab rendahnya keamanan algoritma ini adalah jumlah kuncinya yang hanya 26 kunci saja (sebanyak pegeseran karakter yang mungkin). Teknik pemecahan algoritma ini dapat dilakukan dengan Exhaustive Search saja yaitu melakukan pengecekan terhadap semua kunci yang ada yang berjumlah 26 tersebut.

III. *VIGENERE CIPHER*

KONSEP DASAR *VIGENERE CIPHER*

Vigenere cipher merupakan jenis cipher abjad majemuk yang paling sederhana. *Vigenere cipher* menerapkan metode substitusi poli alfabetik dan termasuk ke dalam kategori kunci simetris dimana kunci yang digunakan untuk proses enkripsi adalah sama dengan kunci yang digunakan untuk proses dekripsi.

Vigenere cipher ditemukan pertama kali oleh Giovan Battista Bellaso. Beliau menuliskan metode enkripsi yang kita kenal sebagai *Vigenere cipher* ini pada bukunya yang berjudul La Cifradel. Sig. Giovan Battista Bellaso pada tahun 1553. Namun, nama "Vigenere" pada *Vigenere cipher* diambil dari seorang yang bernama Blaise de Vigenere, yang juga merupakan penemu metode algoritma ini setelah Giovan Battista Bellaso.

Enkripsi dengan menggunakan algoritma *Vigenere cipher* pada dasarnya adalah menggunakan prinsip Caesar Cipher, yaitu melakukan enkripsi karakter pada plainteks menjadi karakter lain pada cipherteks. Perbedaan antara Caesar Cipher dan *Vigenere cipher* adalah huruf yang sama pada plainteks tidak selalu dienkripsi menjadi huruf yang sama pada cipherteks. Hal ini terjadi karena pada *Vigenere cipher*, pergeseran karakternya ditentukan oleh karakter yang ada pada kata kunci dan kata ini selalu diulang. Akibatnya, karakter yang sama pada plainteks bolehjadi memiliki karakter yang berbeda pada cipherteksnya. Karena hal ini lah, *Vigenere cipher* merupakan cipher substitusi abjad-majemuk. Tujuan utama dari *Vigenere cipher* ini adalah menyembunyikan keterhubungan antara plainteks dan cipherteks dengan menggunakan kata kunci sebagai penentu pergeseran karakternya.

Berikut adalah contoh penggunaan algoritma *Vigenere cipher* dalam enkripsi pesan dan kunci sebagai berikut.

Pesan : SAYA GANTENG SEKALI
Kunci : BENAR

Metode yang digunakan dalam enkripsi dengan menggunakan *Vigenere cipher* adalah menyusun kunci bersesuaian dengan plainteks yang ada di atasnya. Apabila telah sampai di akhir kunci, ulangi kembali penyusunan kunci sampai seluruh plainteks telah memiliki karakter kunci masing-masing. Berikut adalah contoh pesan dan kunci yang telah diurutkan :

Pesan : SAYA GANTENG SEKALI
Kunci : BENA RBENARB ENARBE

Langkah selanjutnya adalah melakukan Caesar Cipher untuk tiap-tiap karakter tersebut dengan nilai pergeseran karakter ditentukan oleh karakter kunci untuk tiap karakternya. Dalam *Vigenere cipher* ini, karakter A menyatakan pergeseran 0, B=1, C=2, D=3, ... , dan Z=25. Dari Caesar Cipher terhadap masing-masing karakter, didapat :

Pesan : SAYA GANTENG SEKALI
Kunci : BENA RBENARB ENARBE
Chiper: TELA XBRGEEH WRKRMM

Perhatikan karakter 'A' memiliki beberapa karakter hasil enkripsi yaitu 'E', 'A', 'B', dan 'K'. Inilah yang membuat *Vigenere cipher* merupakan cipher abjad majemuk.

Untuk teknik dekripsinya, kita hanya tinggal membalikkan proses enkripsinya saja, yang tadinya memajukan karakter menjadi memundurkan karakter.

Teknik *Vigenere cipher* ini dapat pula menggunakan tabel yang menunjukkan hubungan antara huruf plainteks dan huruf cipherteks seperti pada tabel berikut :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Cara menggunakan tabel di atas adalah tarik garis vertikal dari huruf plainteks ke bawah, lalu tarik garis mendatar dari huruf kunci ke kanan. Perpotongan kedua garis tersebut menyatakan huruf chiperteksnya. Untuk dekripsinya adalah kebalikan dari enkripsi.

Rumus matematis dari enkripsi *Vigenere cipher* ini adalah sebagai berikut :

- Enkripsi
  $$C_i = E_K(M_i) = (M_i + K_i) \mod 26$$
- Dekripsi
  $$M_i = D_K(C_i) = (C_i - K_i) \mod 26$$
  Dengan Ci = karakter chiperteks,
  Ki = karakter kunci, dan
  Mi = karakter plainteks

KEKUATAN

Kelebihan yang ditawarkan oleh *Vigenere cipher* adalah dikuranginya keterhubungan antara karakter plainteks dan karakter cipherteksnya. Hal ini ditunjukkan

dengan sifatnya yang merupakan cipher abjad majemuk yang dapat menghasilkan karakter cipherteks yang berbeda untuk plainteks yang sama. Karena sifat tersebut, metode analisis frekuensi yang sebelumnya dapat digunakan untuk memecahkan Caesar Cipher tidak dapat digunakan untuk *Vigenere cipher* ini.

KELEMAHAN

Namun, *Vigenere cipher* ini juga memiliki kelemahan. Kelemahan dari *Vigenere cipher* ini adalah diulangnya kunci yang sama terus menerus sehingga menimbulkan cipherteks yang sama untuk potongan plainteks yang mana posisinya merupakan kelipatan dari panjang kunci sehingga plainteks tersebut akan selalu mendapatkan potongan kunci yang sama untuk enkripsinya.

Contoh kasus:

Plainteks : BILA SAYA BILANG SUKA
Kunci : MANA MANA MANAMA NAMA
Cipherteks : NIYA EALA NIYAZG FUWA

Dari contoh kasus diatas, potongan "BILA" selalu mendapatkan potongan kunci yang sama karena jarak antara dua potongan kata tersebut merupakan kelipatan dari panjang kunci yang digunakan. Kelemahan ini kemudian akan digunakan untuk pemecahan *Vigenere cipher* dengan metode yang disebut metode Kasiski.

IV. METODE KASISKI

Metode Kasiski merupakan metode pemecahan algoritma *Vigenere cipher* yang dikemukakan pertama kali oleh Friedrich Kasiski ketika dia berhasil memecahkan kriptogram *Vigenere cipher* pada tahun 1863. Namun sebenarnya telah ditemukan sendiri oleh Charles Babbage pada tahun 1846.

Metode Kasiski memanfaatkan kelemahan *Vigenere cipher* yang menggunakan kunci yang sama berulang-ulang sehinggan menghasilkan potongan cipherteks yang sama untuk plainteks yang sama.

Cara kerja metode kasiski ini memanfaatkan keuntungan bahwa bahasa Inggris tidak hanya mengandung perulangan huruf, tetapi juga perulangan pasangan huruf atau tripel huruf, seperti TH, THE, dsb. Perulangan kelompok huruf ini ada kemungkinan menghasilkan kriptogram yang berulang.

Pada dasarnya, jika jarak antara dua buah string yang berulang di dalam plainteks merupakan kelipatan dari panjang kunci, maka string yang sama tersebut akan muncul menjadi kriptogram yang sama pula di dalam cipherteks. Langkah –langkah dari metode kasiski adalah sebagai berikut :

1. Temukan semua kriptogram yang berulang di dalam cipherteks (pesan yang panjang biasanya mengandung kriptogram yang berulang).
2. Hitung jarak antara kriptogram yang berulang
3. Hitung semua faktor (pembagi) dari jarak tersebut (faktor pembagi menyatakan panjang kunci yang mungkin).
4. Tentukan irisan dari himpunan faktor pembagi tersebut. Nilai yang muncul di dalam irisan menyatakan angka yang muncul pada semua faktor pembagi dari jarak-jarak tersebut . Nilai tersebut mungkin adalah panjang kunci.

Setelah panjang kunci diketahui, maka langkah berikutnya menentukan kata kunci. Kata kunci dapat ditentukan dengan menggunakan exhaustive key search. Biasanya, para kriptanalis melengkapi metode pemecahan *Vigenere cipher* ini dengan menggunakan teknik analisis frekuensi.

V. MODIFIKASI *VIGENERE CIPHER* DENGAN CAESAR CIPHER DAN ENKRIPSI BERLANJUT UNTUK PEMBANGKITAN KEY

PERANCANGAN MODIFIKASI *VIGENERE CIPHER*

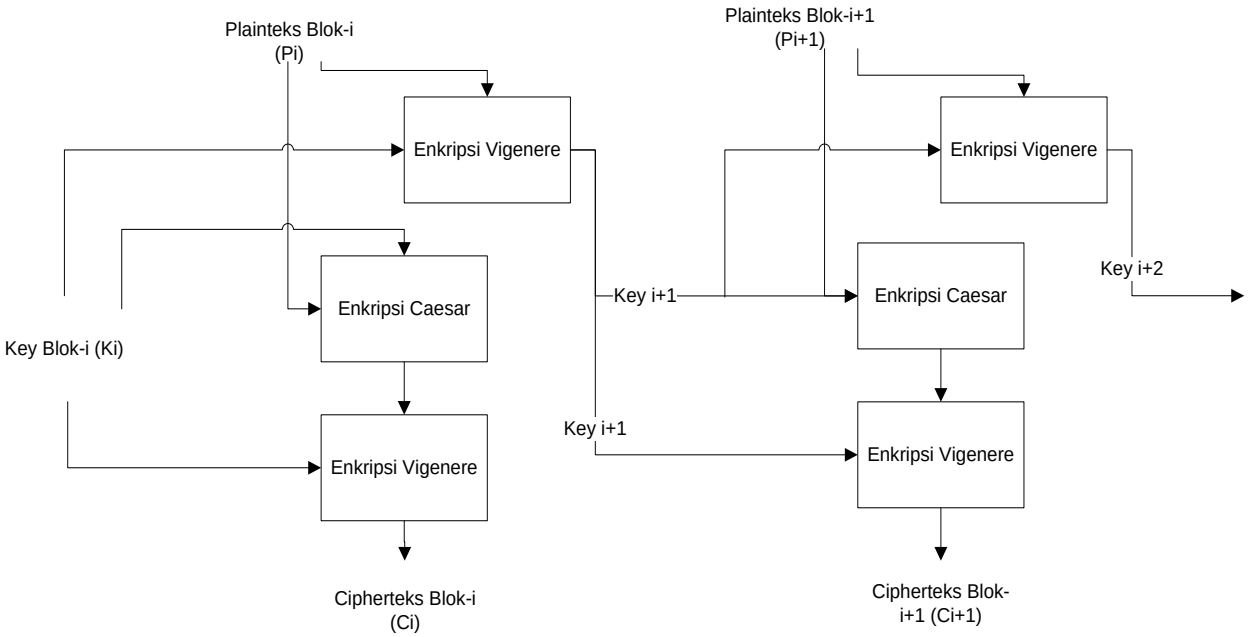
Vigenere cipher bukanlah algoritma kriptografi yang unbreakable. Dengan metode Kasiski yang sudah dijelaskan pada bagian sebelumnya telah dijelaskan bagaimana cara memecahkan cipher yang menggunakan *Vigenere cipher*. Namun, bukan berarti tidak ada hal yang bisa dilakukan untuk memperkuat Vigenerer Cipher dari serangan kriptanalis. Dapat dilakukan teknik-teknik modifikasi tertentu untuk menyamarkan keterhubungan antara plainteks dan cipherteksnya.

Modifikasi yang dilakukan harus dapat mengurangi kemunculan key yang berulang atau bahkan menggunakan pendekatan One-Pad kriptografi yang mana panjang key adalah sama dengan panjang plainteks yang digunakan dimana key akan digenerate berbeda dengan key yang digunakan sebelumnya.

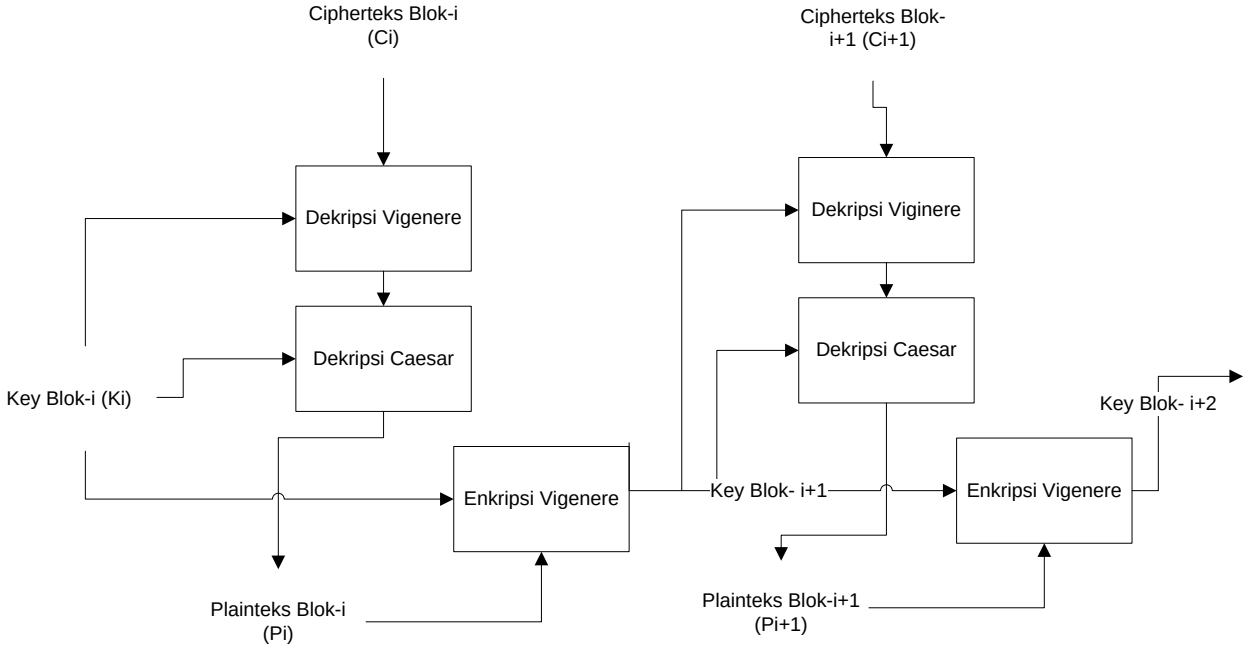
Modifikasi Viginere Cipher yang dilakukan disini adalah bukan modifikasi pada algoritma utamanya.

Bentuk modifikasi yang dilakukan untuk proses ENKRIPSI adalah :

1. Plaintext dibagi menjadi blok-blok dengan panjang blok adalah panjang key yang digunakan
2. Setiap pemrosesan blok-i akan memiliki key K_i masing-masing yang dibangkitkan berdasarkan blok ***i-1*** sebelumnya. Key K_i merupakan hasil *Vigenere cipher* plainteks blok sebelumnya (plainteks P_{i-1}) dengan menggunakan key K_{i-1}. Khusus untuk blok pertama, key-nya adalah key masukan pengguna.
3. Setiap blok plainteks-i (P_i) akan di-enkripsi terlebih dahulu dengan menggunakan algoritma Caesar Cipher. Besar pergeseran Caesar cipher-nya ditentukan berdasarkan key masing-masing blok (K_i) dengan fungsi generate nya adalah :
   Nilai Caesar
   = (K_i karakter1 + K_i karakter2 +...+
   K_i karakter-n) mod 26
4. Hasil enkripsi P_i tadi akan dienkripsi menggunakan *Vigenere cipher* untuk membentuk Cipherteks blok-i (C_i) , key yang digunakan adalah K_i.



Gambar 2 Skema Enkripsi Vigenere Modifikasi



Gambar 3 SkemaDekripsi Vigenere Modifikasi

Bentuk modifikasi yang dilakukan untuk proses DEKRIPSI adalah :

1. Ciphertext dibagi menjadi blok-blok dengan panjang blok adalah panjang key yang digunakan
2. Setiap pemrosesan blok-i akan memiliki key K_i masing-masing yang dibangkitkan berdasarkan blok ***i-1*** sebelumnya. Key K_i merupakan hasil *Vigenere cipher* plainteks blok sebelumnya (plainteks P_{i-1}) dengan menggunakan key K_{i-1}. Khusus untuk blok pertama, key-nya adalah key masukan pengguna.
3. Setiap ciphertext blok-i (C_i) akan didekripsi menggunakan *Vigenere cipher*, key yang digunakan adalah K_i
4. Hasil dekripsi yang diperoleh di langkah-3 akan didekripsikan Caesar Ciphernya dengan nilai Caesar Ciphernya adalah sama dengan pada fungsi enkripsi yang pada akhir langkah ini akan terbentuk blok plainteks-i (P_i)

Penjelasan skematik terhadap algoritma enkripsi dan dekripsinya dapat dilihat di halaman sebelumnya.

Setiap blok plainteks dibentuk berdasarkan panjang key masukan. Pengenkripsian dan pendekripsian dilakukan dalam mode blok.

Fungsi dari pembangkitan key baru dengan metode *Vigenere cipher* pada bentuk modifikasi ini adalah untuk menghilangkan keterkaitan dan keterhubungan antara teks sebelum enkripsi dan teks sesudah enkripsi.

Fungsi dari penggunaan Caesar Cipher sebelum dilakukannya enkripsi adalah untuk merusak tatanan-susunan karakter sebagai bentuk pencegahan terhadap kriptanalis sehingga metode Kasiski dan metode analisis frekuensi tidak dapat dijadikan sebagai acuan untuk memecahkan kode hasil enkripsi.

VI. PENGUJIAN DAN ANALISIS VIGENERE TERMODIFIKASI

Berikut ini adalah source code program yang dibangun dengan modifikasi yang telah dijelaskan sebelumnya. Dalam source code terdapat fungsi enkripsi dan dekripsi yang memanggil fungsi enkripsi/dekripsi *Vigenere cipher* dan *Caesar cipher*

```
  public class Modification {

      public static ArrayList<StringBuilder>
makeBlock(String plain, String key) {
          ArrayList<StringBuilder> stringlist =
new ArrayList<StringBuilder>();
          StringBuilder thisblock = new
StringBuilder();
          for (int i = 0; i < plain.length();
i++) {
              thisblock.append(plain.charAt(i));

              if ((i + 1) % key.length() == 0) {
                  stringlist.add(new
StringBuilder(thisblock));
                  thisblock = new
StringBuilder();
              }
          }
          if (thisblock.length() != 0) {
              stringlist.add(new
StringBuilder(thisblock));
          }

          return stringlist;
      }

      public static String makenewKey(String
plainblok, String oldkey) {
          return
VigenereCipher.encrypt(plainblok, oldkey);
      }

      public static String encrypt(String plain,
String key) {
          //make block with length=key
          ArrayList<StringBuilder> block =
makeBlock(plain, key);
          StringBuilder temp = new
StringBuilder();
          String thiskey = key;
          for (int i = 0; i < block.size(); i++)
{
              String temp1 =
CaesarCipher.encrypt(block.get(i).toString(),
thiskey);

              String cipher =
VigenereCipher.encrypt(temp1, thiskey);

              temp.append(cipher);
              thiskey =
makenewKey(block.get(i).toString(), thiskey);

          }
          return temp.toString();
      }

      public static String decrypt(String
cipher, String key) {
          //make block with length=key
          ArrayList<StringBuilder> block =
makeBlock(cipher, key);
          StringBuilder temp = new
StringBuilder();
          String thiskey = key;
          for (int i = 0; i < block.size(); i++)
{
              String temp1 =
VigenereCipher.decrypt(block.get(i).toString(),
thiskey);

              String plain =
CaesarCipher.decrypt(temp1, thiskey);

              temp.append(plain);
              thiskey = makenewKey(plain,
thiskey);

          }
          return temp.toString();
      }
}
```

Dengan menggunakan program yang dibangun tersebut, dicobakan kasus yang sebelumnya menjadi kelemahan pada *Vigenere cipher* biasa.

Pada *Vigenere cipher* biasa :
Plainteks : BILA SAYA BILANG SUKA
Kunci : MANA MANA MANAMA NAMA
Cipherteks : NIYA EALA NIYAZG FUWA

Pada *Vigenere cipher* modifikasi (pengolahan per blok):
Plainteks : BILA SAYA BILA NGSU KA
Kunci : MANA MANA MANA MANA MA
Cipherteks : MHXZ YBPT PZQJ WZCX LE

Terlihat dari hasil percobaan tersebut bahwa tidak lagi ditemukan cipherteks yang sama untuk hasil enkripsi pada plainteks yang sama dikarenakan key yang sudah diacak ditambah lagi dengan pengacakan plainteks menggunakan Caesar cipher sebelum dilakukan enkripsi dengan *Vigenere cipher*.

Gambar 4 Tampilan Enkripsi Modifikasi

Gambar 5 Tampilan Dekripsi Modifikasi

Berikutnya dilakukan pengujian terhadap file teks berukuran cukup besar berbahasa inggris. Pengujian ini dilakukan untuk mengecek bagaimana keberhasilan metode Kasiski dalam pemecahan cipher modifikasi ini.

File teks yang digunakan adalah file teks yang dulunya sudah pernah dipecahkan dengan menggunakan metode Kasiski. Kali ini, teks tersebut akan dicoba kembali untuk dienkripsi dan dikriptanalisis dengan menggunakan metode Kasiski.

File teks dienkripsi dengan menggunakan key yang sama persis ketika berhasil didekripsikan dengan metode Kasiski, "worldmistery". Hasil enkripsi file teks tersebut, akan dihitung frekuensi terhadap karakter tunggal dan trigraph-nya. Dari penghitungan frekuensi karakter tunggal, kisaran nilai yang diperoleh adalah merata di antara 90-115 dengan tidak ada karakter yang jumlahnya jauh berbeda dengan yang lain. Dari penghitungan frekuensi trigraf, tidak ditemukan trigraf yang ditemukan lebih dari 3 kali (file teks dapat dilihat di http://dl.dropbox.com/u/15952105/fileteks.txt sedangkan file hasil enkripsinya dapat dilihat dilihat di http://dl.dropbox.com/u/15952105/fileterenkripsi.txt).

Dengan hasil penghitungan seperti itu, sudah dapat dipastikan bahwa metoda kasiski yang berlandaskan pada analisis frekuensi akan sangat sulit digunakan dalam pemecahan cipher modifikasi ini.

KELEBIHAN CIPHER MODIFIKASI

Cipher modifikasi ini memiliki keunggulan yang jelas

dibandingkan dengan *Vigenere cipher* biasa. Dari segi keamanannya, cipher modifikasi menyediakan mekanisme penyandian yang lebih rumit dan aman, membangkitkan key acak untuk tiap blok plainteks, dan menerapkan Caesar Cipher untuk menghilangkan keterhubungan antara blok plain asli dan blok ciphernya. Dengan demikian, penggunaan metode Kasiski dan analisis frekuensi dalam pemecahan kodenya akan membutuhkan usaha dan sumber daya yang lebih.

KEKURANGAN CIPHER MODIFIKASI

Cipher modifikasi ini memiliki kekurangan dalam ketersempaian informasi apabila cipherteksnya mengalami serangan. Apabila ada satu saja karakter pada cipherteks yang berubah, maka hasil dekripsi cipher tersebut tidak akan menghasilkan plainteks yang benar karena kerusakan pada salah satu bagian akan merusak pembentukan key untuk blok berikutnya.

Selain itu, tidak tertutup kemungkinan bahwa cipherteks modifikasi ini dapat dipecahkan dengan pendekatan metode kasiski atau dengan metode lain.

VII. KESIMPULAN

Dari analisis dan perancangan modifikasi algoritma kriptografi *Vigenere cipher*, didapat kesimpulan sebagai berikut :

1. Kriptografi merupakan ilmu dan seni yang digunakan untuk menjaga keamanan informasi dengan mengubah informasi tersebut menjadi bentuk yang sulit dimengerti maksudnya.
2. Algoritma *Vigenere cipher* merupakan salah satu algoritma kriptografi klasik yang cukup populer karena mudah dan sederhana penggunaannya.
3. Algoritm *Vigenere cipher* dapat dipecahkan dengan menggunakan metode Kasiski
4. *Vigenere cipher* yang telah dimodifikasi adalah lebih aman dan lebih sulit diserang oleh kriptanalis dibandingkan *Vigenere cipher* biasa.
5. Algoritma *Vigenere cipher* modifikasi ini telah dapat menghilangkan keterhubungan karakter plainteks dan cipherteks sehingga sangat sulit dipecahkan dengan metode Kasiski.
6. Tingkat keamanan dalam penggunaan *Vigenere cipher* modifikasi akan meningkat apabila key yang digunakan lebih panjang.
7. Untuk menambah kerumitan, dapat juga dilakukan modifikasi tambahan terhadap pembangkitan Caesar Cipher nya, jadi tidak hanya berupa fungsi mod 26 dari total karakternya.

REFERENCES

http://en.wikipedia.org/wiki/Friedrich_Kasiski
http://en.wikipedia.org/wiki/Caesar_cipher
http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher.
http://en.wikipedia.org/wiki/Kasiski_examination
http://id.wikipedia.org/wiki/Kriptografi
Rinaldi Munir. Diktat kuliah kriptografi

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Maret 2011

Fatardhi Rizky Andhika
13508092