MODIFIKASI VIGENERE CHIPER DENGAN MENGGUNAKAN KUNCI BERGESER

Muhammad Iqbal Faruqi/13507101

Departemen Teknik Informatika

Institut Teknologi Bandung

Jl. Ganesha 10 Bandung 40132

E-mai : said_hawwa@yahoo.com

Abstrak

Vigenere chiper adalah salah satu algoritma kriptografi klasik yang pernah mendapat gelar le chiffre indéchiffrable (bahasa Prancis: 'sandi yang tak terpecahkan'), sampai akhirnya abad ke-19. Pada tahun 1854, Charles Babbage menemukan cara untuk memecahkan sandi Vigenère. Metode ini dinamakan tes Kasiski karena Friedrich Kasiski-lah yang pertama mempublikasikannya.untuk menyulitkan kriptanalis dalam menggunakan metode kasiski, penulis membuat modifikasi dari vigenere chiper yang dinamakan Kunci bergeser, karena salah satu aturan penggunaan kunci adalah menggeser kunci yang akan di bahas pada makalah ini.

***Kata kunci**: Vigenere Chiper, Metode tes kasiski, Kunci bergeser*

I. Pendahuluan

Sebelum adanya komputer kriptografi dilakukan hanya menggunakan secarik kertas dan pena saja, oleh karena itu algoritma kriptografi klasik biasanya cukup sederhana. Metode kriptografi klasik biasanya dibagi berdasarkan dua kategori yaitu chiper subtitusi dan chiper transposisi, yang dimaksud dengan chiper subtitusi ialah, mengganti setiap karakter pada plainteks dengan karakter lain, sehingga plainteks tersebut tidak dapat dibaca lagi, atau diubah menjadi chiperteks. Sedangkan chiper transposisi adalah mengubah susunan huruf pada plaintext sehingga urutannya berubah.

Vigenere chiper adalah suatu metode kriptografi klasik yang dikategorikan sebagai chiper subtitusi, polyalfabetik chiper karena suatu karakter dapat disubtitusi dengan karakter yang berbeda beda. Namun ada suatu kelemahan vigenere chiper, yaitu perulangan yang akan di bahas pada bagian “vigenere chiper”. Dan rentan dengan serangan menggunakan “metode kasiski” yang akan dibahas pada bagian metode kasiski. Oleh karena itu penulis ingin memodifikasi penggunaan metode vigenere chiper agar lebih sulit dipecahkan oleh metode kasiski dengan meminimalkan penggunaan kunci secara berulang, yang akan dibahas dibagian “modifikasi vigenere chiper”.

II. Vigenere Chiper

Sandi Vigenère adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Sandi Vigenère merupakan bentuk sederhana dari sandi substitusi polialfabetik. Kelebihan sandi ini dibanding sandi Caesar dan sandi monoalfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi. Giovan Batista Belaso menjelaskan metode ini dalam buku *La cifra del. Sig. Giovan Batista Belaso* (1553); dan disempurnakan oleh diplomat Perancis Blaise de Vigenère, pada 1586. Pada abat ke-19, banyak orang yang mengira Vigenère adalah penemu sandi ini, sehingga, sandi ini dikenal luas sebagai "sandi Vigenère".

Gambar 1(Blaise de Vigenère,)

Sandi ini dikenal luas karena cara kerjanya mudah dimengerti dan dijalankan, dan bagi para pemula sulit dipecahkan. Pada saat kejayaannya, sandi ini dijuluki **le chiffre indéchiffrable** (bahasa Prancis: 'sandi yang tak terpecahkan'). Metode pemecahan sandi ini baru ditemukan pada abad ke-19. Pada tahun 1854, Charles Babbage menemukan cara untuk memecahkan sandi Vigenère. Metode ini dinamakan tes Kasiski karena Friedrich Kasiski-lah yang pertama mempublikasikannya.

Sandi Vigenère sebenarnya merupakan pengembangan dari sandi Caesar. Pada sandi Caesar, setiap huruf teks terang digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi Caesar dengan geseran 3, A menjadi D, B menjadi E and dan seterusnya. Sandi Vigenère terdiri dari beberapa sandi Caesar dengan nilai geseran yang berbeda.

Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut tabel Vigenère (gambar). Tabel Vigenère berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, membentuk ke-26 kemungkinan sandi Caesar. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang.

	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

Gambar 2(Tabel Vigenere)

Misalkan plainteks yang akan disandikan adalah:

"serbu markas pasukan cumi cumi"

Sedangkan kata kunci(key) adalah:

"takoyaki"

Huruf pertama pada plainteks, S, disandikan dengan menggunakan baris berjudul T, huruf pertama pada kata kunci. Pada baris T dan kolom S di tabel Vigenère, terdapat huruf L. Demikian pula untuk huruf kedua, digunakan huruf yang terletak pada baris A (huruf kedua kata kunci) dan kolom E (huruf kedua teks terang), yaitu huruf E. Proses ini dijalankan terus sehingga

Plainteks: *serbumarkaspasukancumicumi*

Kunci: *takoyakitakoyakitakoyakitakoy*

Chiperteks: *lebpsmkzdacdysestnmikimcfi*

Untuk proses dekripsi, diakukan hal sebaliknya yaitu cari huruf di tengah tabel dengan baris yang ada pada kata kunci, dan seterusnya, secara matematis dituliskan fungsi enkripsi-dekripsi dapat dituliskan dengan:

Enkripsi: $C_i \equiv (P_i + K_i) \mod 26$

Dekripsi : $P_i \equiv (C_i - K_i) \mod 26$

III. Metode Kasiski

Friedrich Kasiski adalah orang yang pertama kali memecahkan *Vigènere cipher* pada Tahun 1863 . metode kasiski membantu untuk menemukan panjang dari kunci yang digunakan pada vigenere chiper dengan memanfaatkan perulangan pasangan huruf atau tripel huruf, seperti TH, THE, dsb. Perulangan kelomok huruf ini menyebabkan ada perulangan dalam kriptogram, contoh:

Plainteks:
CRYPTOISSHORTFORCRYPTOGRAPHY

Kunci: abcdabcdabcdabcdabcdabcdabcd

Cipherteks:
CSASTPKVSIQUTGQU**CSASTP**IUAQJB

Secara intuitif: 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. Pada Contoh diatas:

- kunci adalah "abcd"
- panjang kunci adalah 4
- jarak antara dua CRYPTO yang berulang adalah 16
- 16 adalah kelipatan 4

Kesimpulannya ialah, CRYPTO dienkripsi menjadi kriptogram yang sama. Goal metode Kasiski: mencari dua atau lebih kriptogram yang berulang untuk menentukan panjang kunci. Langkah-langkah metode Kasiski:

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. Hal ini karena *string* yang berulang dapat muncul bertindihan (*coincidence*)

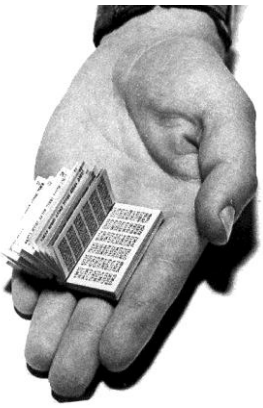
Sampai menemukan panjang kunci, selesailah sudah metode kasiski, lau selanjutnya setelah mengetahui panjang kunci, maka kita dapat menggunakan metode analisis frekuensi untuk menemukan kunci yang bersangkutan. Langkah-langkahnya sbb:

1. Misalkan panjang kunci yang sudah berhasil dideduksi adalah *n.* Setiap huruf kelipatan ke-*n* pasti dienkripsi dengan huruf kunci yang sama. Kelompokkan setiap huruf ke-*n* bersama-sama sehingga kriptanalis memiliki *n* buah "pesan", masing-masing dienkripsi dengan substitusi alfabet-tunggal (dalam hal ini *Caesar cipher*).
2. Tiap-tiap pesan dari hasil langkah 1 dapat dipecahkan dengan teknik analisis frekuensi.
3. Dari hasil langkah 3 kriptanalis dapat menyusun huruf-huruf kunci. Atau, kriptanalis dapat menerka kata yang membantu untuk memecahkan cipherteks

Dengan begitu vigenere chiper dapat dipecahkan oleh metode kasiski dan anailisis frekuensi. Karena jika panjang kunci jauh lebih pendek daripada plainteks maka, hasilnya banyak plainteks yang dienkripsi menjadi chiperteks dengan menggunakan kunci yang sama, inilah kelemahan utama dari vigenere chipper.

IV. Modifikasi Vigenere Chiper dengan Kunci Bergeser

Dengan ditemukannya metode kasiski vigenere chiper dapat dipecahkan. Bila kita teliti dengan seksama, kelemahan dari vigenere chiper terletak pada penggunaan kunci yang berulang, ketika key jauh lebih pendek dari chiperteks, untuk itu ada suatu metode yang bernama "one-time -pad chiper" yang menggunakan panjang key sama dengan panjang plainteks dengan begitu vigenere chiper tidak dapat digunakan untuk memecahkan chiper tersebut.



Gambar3(one-time-pad)

namun banyak masalah mengenai one-time-pad, yaitu key yang terlalu panjang, bagaimana kita memberikan pad kepada target yang kita maksud, intinya amatlah sulit untuk menggunakan chiper ini dalam kehidupan sehari-hari atau dunia nyata. Oleh karena itu penulis mengemukakan sebuah ide untuk meningkatkan keamanan dari vigenere chiper yaitu, dengan mengurangi keberulangan penggunaan kunci dengan menggeser kunci pada bagian tertentu dan pada step tertentu menggunakan aturan yang akan dipaparkan pada uraian selanjutnya.

pada vigenere chiper penggunaan kunci dilakukan secara berulang, pada algoritma kunci bergeser, kunci akan digeser dengan aturan tertentu sebelelum digunakan kembali. Aturannya ialah:

1. Misalkan panjang kunci adalah N
2. Pertama kita geser seluruh kunci ke kiri sebanyak satu karakter dan karakter pertama akan digeser ke posisis N.
3. Selanjutnya setelah kunci diatas dipakai, maka karakter pertama dari kunci pada step 2 tidak digeser, tetapi karakter ke dua akan menepati posisi ke N dan karakter posisi N akan menepati posisis N-1 dan seterusnya sampai pada karakter ke 3 menepati posisi ke dua.
4. Selanjutnya pada step ke 3 posisi karaker ke 1 dan 2 tidak berubah tapi posisi karakter ke 4 sampai N akan berubah, yaitu di geser ke kiri 1 karakter, dan seterusnya
5. Bila telah sampai pada karakter ke N-1 yang tidak berubah, kembali ke step 2.

Contoh, kita memiliki kunci ABCDE.

penggunaan ke-	Kunci yang digunakan
1	ABCDE
2	**B**CDEA
3	**BD**EAC
4	**BDA**CE
5	**BDAE**C
6	**D**AECB
7	**DE**CBA
8	**DEB**AC
9	**DEBC**A

Dst….

Pada tabel diatas huruf yang dicetak tebal dianggap static dan tidak di geser di step selanjutnya. Sedangkan huruf yang tidak dicetak tebal akan bergeser sejauh satu karakter ke kiri, dan huruf yang tidak dicetak tebal paling kiri akan menepati posisi N, dan ketika tinggal satu huruf yang tidak dicetak tebal, maka semua karakter akan bergeser satu karakter ke kiri, dan karakter yang berada pada ujung kiri akan menepati posisi N.

Contoh penerapan: kunci yang digunakan adalah "ABCDE"

plainteks	IQBAL CAKEP IQBAL CAKEP IQBAL CAKEP IQBAL CAKEP IQBAL
Kunci	ABCDE BCDEA BDEAC BDACE BDAEC DAECB DECBA DEBAC DEBCA
chiperteks	IRDDP DCNIP JTFAN DDKGT JTBEN FAOGQ LUDBL FELER LUCCL

Pada contoh di atas, bahkan kata yang berulagpun tidak akan muncul berulang pada chiperteks, namun lama kelamaan kunci yang dipakai akan berulang, misalkan kunci yang akan dipakai dalaha ABCDE, maka berikut adalah pergeseran sampai mencapai kembali perulangan yang sama:

ABCDE **B**CDEA **BD**EAC **BDA**CE **BDAE**C **D**AECB **DE**CBA **DEB**AC **DEBC**A **E**BCAD **EC**ADB **ECD**BA **ECDA**B **C**DABE **CA**BED **CAE**DB **CAEB**D **A**EBDC **AB**DCE **ABC**ED **ABCD**E

Bila kita lihat akan, ada perulangan kunci pada karakter ke seratus satu. dengan menggunakan algoritma kunci bergeser ini, maka penggunaan unci secara berulang akan berkurang, dan semakin panjang kunci akan semakin lama pula pengulangan yang akan terjadi.

Untuk mendekripsi chiperteks, kita akan melakukan hal yang sama kepada kunci seperti pada metode enkripsi, dan mendekripsi sebagaimana vigenere chiper didekripsi.

V. Analisis Kunci Bergeser

Berdasarkan paparan di atas mengenai kunci bergeser, maka kita bisa menganalisis beberapa hal yang berkaitan dengan kekuatan dan kelemahan dari algoritma ini berdasarkan kemungkinan serangan yang dapat dilakukan terhadap chiperteks yang menggunakan algoritma kunci bergeser ini.

Kekuatan:

- tidak mudah dipecahkan melalui metode kasiski, karena pengulangan penggunaan kunci telah dikurangi, dan jika ada pengulangan pun, panjang kunci akan sulit di prediksi karena metode penggeseran yang dilakukan tidak mudah diprediksi.
- Dengan hanya menggunakan panjang kunci 5 karakter, dapat membangkitkan 100 buah karakter kunci yang tidak sama satu sama lain, ketika kita menambah panjang kunci maka, kunci yang dibangkitkan pun akan semakin tidak berulang.
- Belum ditemukan pola hubungan antara panjang kunci dan panjang karakter kunci yang dibangkitkan, sehingga akan mempersulit kriptanalis untuk memecahkan chiperteks tersebut.
- Kunci awal tidak harus panjang untuk membuat variasi key yang banyak contoh: hanya dengan panjang key 5, kita dapat men-enkripsi 100 karakter dengan kunci yang berbeda-beda.

Kelemahan:

- Meskipun penggunaan kunci yang berulang telah dikurangi, namun tidak menutup kemungkinan untuk kemunculan kata yang berulang, misalkan panjang key adalah 5 maka, setiap 100 karakter yang dienkripsi akan mengalami perulangan, oleh karena itu, jika kita melakukan enkripsi untuk plaintks yang panjangnya 10000 karakter, dan dienkripsi dengan key yang panjangnya 5, maka tidak menutup kemungkinan akan terjadi perulangan pada chiperteks, lalu tinggal diselesaikan memakai metode kasiski dan analisis frekuensi dengan menganggap panjang kunci 100.
- Jika kuncinya agak panjang akan terjadi perulangan meskipun formula untuk mencari panjangnya belum ditemukan/tidak bisa dipakai untuk mencari panjang kunci dengan pasti.

VI. Kesimpulan

Berdasarkan analisis yang telah dilakukan, dapat ditarik beberapa kesimpulan mengenai modifikasi vigenere chiper menggunakan kunci bergeser ini yaitu:

- Algoritma kunci bergeser ini lebih aman jika dibandingkan dengan vigenere chiper biasa, karena algoritma kunci bergeser ini dapat mengurangi frekuensi perulangan kunci
- Metode kasiski juga akan sangat sulit untuk mengetahui panjang key sebenarnya, walaupun metode kasiski masih memungkinkan untuk mencari panjang kunci yang dihasilkan oleh algoritma ini.
- Variasi kunci yang dihasilkan oleh algoritma ini bergantung pada kunci yang dimasukkan, sehingga semakin panjang kunci yang dimasukkan, akan semakin rumit pula chiperteks yang dihasilkan.
- Belum adanya formula yang pasti untuk menghitung panjang kunci yang sebenarnya, membuat algoritma kunci bergeser ini semakin kuat.
- Algoritma kunci bergeser ini mudah dipakai, karena tidak membutuhkan suatu kalimat yang panjangnya sama dengan plainteks untuk menghasilkan kunci yang panjangnya sama dengan plainteks.

Daftar Referensi

[1] http://id.wikipedia.org/wiki/Kriptografi

[2]http://id.wikipedia.org/wiki/Sandi_Vigen%C3%A8re

[3]Slide Kuliah IF3058 Kriptografi, Rinaldi Munir

[4]http://sistem-keamanan-komputer.blogspot.com/2009/04/kriptografi-klasik.html

[5] http://en.wikipedia.org/wiki/One-time_pad#Uses

[6] http://www.ranum.com/security/computer_security/papers/otp-faq/otp.jpg

[7] http://egiewendra.blog.upi.edu/2010/01/19/algoritma-kriptografi-klasik/