Penggunaan Vigenere Cipher untuk menyembunyikan pesan dan informasi

Richard Wellianto - 13514051
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
richard.wellianto@students.itb.ac.id

Abstract*— Semakin berkembangnya zaman, informasi dan pesan makin mudah untuk disampaikan. Proses penyampaian tersebut rawan disusupi oleh para pencuri informasi yang semakin merebak di seluruh penjuru dunia. Untuk menyembunyikan pesan tersebut dari para pencuri informasi, dilakukan enkripsi pada pesan tersebut agar tidak mudah dicermati oleh para pencuri informasi. Makalah ini akan menjelaskan salah satu teknik untuk mengenkripsikan pesan, yaitu *Viginere Cipher.

***Keywords*— Kriptografi, *Vigenere Cipher*, Penyulihan Alfabet, Analisis Frekuensi**

I. PENDAHULUAN

Di zaman modern ini, informasi dan pesan semakin mudah untuk disampaikan. Kemudahan itu juga memudahkan para pencuri informasi seperti hacker untuk mengakses informasi-informasi tersebut. Salah satu cara untuk melindungi informasi dari para pencuri adalah dengan mengenkripsi pesan tersebut dengan menggunakan kriptografi.

Kriptografi adalah ilmu untuk menjaga keamanan pesan. *Crypto* berarti rahasia dan *Graphy* berarti tulisan [3]. Algoritma kriptografik atau yang biasanya disebut dengan *cipher*, adalah persamaan matematika yang digunakan dalam proses enkripsi dan dekripsi [3]. Pesan yang akan disembunyikan biasanya dinamakan dengan plainteks, sedangkan hasil enkripsi pesan pesan dinamakan dengan cipherteks.

Kriptografi harus memenuhi empat aspek dalam menyembunyikan pesan, yaitu kerahasiaan, keutuhan, keabsahan, dan transaksi pesan tak bisa disangkal. Salah satu teknik mengenkripsi pesan dengan kriptografi adalah dengan menyulihkan alfabet dengan alfabet lain, dan *Vigenere Cipher* adalah salah satu kriptografi yang menggunakan teknik tersebut.

II. TEORI BILANGAN

A. Pembagi Bersama

Untuk bilangan a dan b yang tidak bernilai 0, pembagi bersama dari a dan b adalah bilangan-bilangan bulat c yang membagi a juga membagi b.

B. Aritmatika Modular

Aritmatika modular adalah salah satu bagian dari Teori Bilangan. Aritmatika modular cenderung lebih memperhatikan sisa dari pembagian suatu bilangan [7]. Ada banyak jenis aplikasi dari aritmatika modular dalam kehidupan sehari-hari. Salah satu aplikasi dari aritmatika modular adalah ketika ingin mengetahui deadline makalah akan terjadi pada hari apa, yang menggunakan operasi X mod 7, karena jumlah hari dalam satu minggu adalah 7.

Misalnya hari ini adalah hari selasa, tanggal 24 November 2015. Deadline makalah Matematika Diskrit adalah tanggal 11 Desember 2015, yang merupakan 17 hari setelah tanggal 24 November 2015. Karena 17 mod 7 = 3, maka deadline makalah Matematika Diskrit jatuh pada hari jumat karena 3 hari setelah hari selasa adalah hari jumat.

Bentuk operasi aritmatika modular adalah a mod b, yang dibaca “a modulo b” yang memberikan sisa ketika a dibagi dengan b [1]. Persamaan a mod b = c juga berarti, a = b.q + c dengan 0 ≤ c < b [1]. Dalam Matematika Diskrit, aritmatika modular juga dipakai dalam penentuan pembagi bersama terbesar dari dua bilangan menggunakan algoritma Euclid.

III. ENKRIPSI VIGENERE CIPHER

A. *Vigenere Cipher*

Vigenere Cipher, adalah salah satu variasi dari metode enkripsi *Caesar Cipher* [8]. Dalam *Vigenere Cipher*, beberapa *Caesar Cipher* yang berbeda diaplikasikan kepada plainteks untuk menghasilkan cipherteks yang lebih sulit untuk didekripsikan. *Caesar Cipher* yang dilakukan pada plainteks didasari dari sebuah kata kunci. *Vigenere Cipher* adalah salah satu contoh dari enkripsi yang menggunakan penyulihan banyak alfabet [8].

Vigenere Cipher sebenarnya pertama kali dimunculkan oleh Giovan Battista Bellaso di bukunya *La cifra del. Sig. Giovan Battista Bellaso*. Tetapi, pada abad ke 19, *Vigenere Cipher* dinamai dari Blaise de Vigenere, yang mengenalkan teknik enkripsi yang mirip dengan *Vigenere Cipher* pada tahun 1586 [9].

Bagi para pemula, *Vigenere Cipher* terlihat seperti sebuah enkripsi yang tidak bisa dipecahkan. Selama berabad-abad sejak kemunculannya, para matematikawan telah menyatakan bahwa *Vigenere Cipher* tak bisa dipecahkan [9]. *Vigenere Cipher* pertama kali dipecahkan oleh Charles Babbage dan selanjutnya dipecahkan oleh Kasiski, yang mengenalkan metode Kasiski, untuk mengetahui panjang dari kata kunci yang dipakai untuk mengenkripsikan plainteks.

Kelemahan dari *Vigenere Cipher* adalah penggunaan kata kunci yang berulang. Dengan cipherteks yang cukup panjang, analis dapat mengetahui panjang dari kata kunci tersebut dengan menggunakan metode Kasiski. Setelah mengetahui panjang dari kata kunci tersebut, analis dapat menggunakan metode untuk mendekripsikan *Caesar Cipher* kepada cipherteks yang telah dibagi sebanyak panjang kata kunci. Metode ini menggunakan analisis frekuensi yang memakai frekuensi kemunculan sebuah alfabet dalam cipherteks yang kemudian dihubungkan ke suatu bahasa, misalnya bahasa inggris.

B. Tabel Vigenere

Penyulihan dalam enkripsi *Vigenere Cipher* didasari dari 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

Gambar 1 *Vigenere Table*

(sumber: http://www.cs.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html)

Huruf-huruf yang berada di atas tabel merupakan huruf yang berasal dari teks yang akan dienkripsi yang biasanya disebut plainteks. Huruf-huruf yang berada di kiri tabel merupakan huruf yang berasal dari kata kunci.

C. Teknik Enkripsi

Enkripsi dilakukan dengan mengubah huruf-huruf pada plainteks dengan menggunakan kata kunci yang telah ditetapkan, serta dibantu oleh tabel Vigenere pada gambar 1. Asumsikan nilai alfabet ‘A’ (untuk saat ini hanya alfabet kapital yang digunakan pada plainteks, kata kunci, dan cipherteks) adalah 1, nilai alfabet ‘B’ adalah 2, dan seterusnya. Dari tabel Vigenere, dapat disimpulkan bahwa huruf-huruf dari cipherteks dapat didapatkan dengan menggunakan rumus di bawah ini

P[i] = nilai alfabet ke-i dari plainteks
C[i] = nilai alfabet ke-i dari cipherteks
K[i] = nilai alfabet ke-i dari kata kunci
k = panjang kata kunci

$$C[i] = ((P[i] + K[((i-1) \bmod k) + 1] - 2) \bmod 26) + 1$$

Kata kunci yang panjangnya lebih pendek dari plainteks akan diulang sampai panjangnya lebih dari atau sama dengan panjang plainteks (spasi tidak dihitung).. Contoh dari enkripsi *Vigenere Cipher* untuk kalimat “INDONESIA TANAH AIRKU TANAH TUMPAH DARAHKU” dengan kata kunci “MERAH” dapat dilihat di bawah.

Plainteks : INDONESIA TANAH AIRKU TANAH TUMPAH DARAHKU

Kata Kunci : MERAHMERA HMERA HMERA HMERA HMERAH MERAHME

Cipherteks : URUOUQWZA AMRRH HUVBU AMRRH AGQGAO PEIAOWY

Vigenere Cipher dapat menyembunyikan pesan dari analisis frekuensi huruf yang muncul. Kesembilan huruf ‘A’ pada plainteks telah diubah menjadi ‘A’, ‘M’, ‘R’, ‘H’, ‘E’ pada cipherteks. Ini membuat frekuensi ‘A’ yang muncul pada plainteks tak bisa diketahui hanya dengan melihat cipherteks.

IV. DEKRIPSI *VIGENERE CIPHER*

A. Dekripsi dengan kata kunci yang telah diketahui

Dekripsi dengan kata kunci hanya membalikkan teknik enkripsi sebelumnya. Huruf-huruf pada cipherteks didekripsi menggunakan kata kunci yang telah ditetapkan, serta dibantu oleh tabel Vigenere pada gambar 1. Asumsikan nilai alfabet ‘A’ adalah 1, nilai alfabet ‘B’ adalah 2, dan seterusnya. Dari tabel Vigenere, dapat disimpulkan bahwa huruf-huruf dari plainteks dapat didapatkan dengan menggunakan rumus di bawah ini.

P[i] = nilai alfabet ke-i dari plainteks
C[i] = nilai alfabet ke-i dari cipherteks
K[i] = nilai alfabet ke-i dari kata kunci
k = panjang kata kunci

$$P[i] = (C[i] - K[((i-1) \bmod k) + 1]) \bmod 26 + 1$$

Kata kunci yang panjangnya lebih pendek dari cipherteks akan diulang sampai panjangnya lebih panjang atau sama dengan cipherteks (spasi tidak dihitung). Contoh dari dekripsi *Vigenere Cipher* untuk kalimat “URUOUQWZA AMRRH HUVBU AMRRH AGQGAO PEIAOWY” dengan kata kunci “MERAH” dapat dilihat di bawah.

Cipherteks : URUOUQWZA AMRRH HUVBU AMRRH AGQGAO PEIAOWY

Kata kunci : MERAHMERA HMERA HMERA HMERA HMERAH MERAHME

Plainteks : INDONESIA TANAH AIRKU TANAH

Plainteks berhasil didekripsi dari cipherteks.

B. Analisis frekuensi

Beberapa tipe enkripsi mengganti suatu alfabet dengan alfabet lain. *Vigenere Cipher* adalah salah satu enkripsi yang melakukan penggantian alfabet. Perhitungan frekuensi kemunculan alfabet cukup membantu dalam mendekripsikan teks terenkripsi yang menggunakan penyulihan alfabet. Dari frekuensi alfabet yang muncul, alfabet pada plainteks mungkin ditebak sehingga kata kunci yang dicari bisa ditemukan. Analisis frekuensi hanya dapat dilakukan untuk enkripsi dengan satu jenis penggantian, tidak bisa menggunakan beberapa jenis penggantian seperti yang dilakukan pada *Vigenere Cipher.*

Alfabet paling umum yang muncul pada suatu teks dalam bahasa inggris adalah E, diikuti dengan T, A, O, I, N, S, H, R, dan seterusnya. Alfabet paling umum yang muncul pada suatu teks dalam bahasa indonesia adalah A, diikuti dengan N, E, I, T, K, D, dan seterusnya. Alfabet paling umum biasanya digunakan dalam penebakan kode enkripsi karena alfabet tersebut paling banyak muncul di teks yang telah dienkripsi. Misalnya, teks dalam bahasa inggris telah dienkripsi menggunakan enkripsi dengan satu jenis penggantian, seperti *Caesar Cipher* menjadi VQDSBGDC. Perhatikan bahwa alfabet ‘V’, ‘Q’, ‘S’, ‘B’, ‘G’, dan ‘C’ muncul sebanyak 1 kali sedangkan alfabet ‘D’ muncul sebanyak 2 kali. Oleh karena itu dengan analisis frekuensi, kata kunci yang mengubah alfabet ‘E’ menjadi alfabet ‘D’ dianggap sebagai kata kunci enkripsi karena alfabet ‘E’ paling umum dalam bahasa inggris, dan alfabet ‘D’ paling banyak muncul dalam cipherteks. Teks kemudian didekripsi menjadi kata “WRETCHED”.

Tentu saja, metode ini hanya menebak kata kunci enkripsi, sehingga ketepatannya tidak 100 persen. Tetapi, analisis ini bisa membantu dalam penemuan kata kunci enkripsi.

C. Dekripsi tanpa kata kunci yang telah diketahui

Dengan menggunakan analisis frekuensi, kata kunci yang dipakai untuk mengenkripsi plainteks dapat ditemukan sehingga cipherteks dapat didekripsi kembali menjadi plainteks dengan menggunakan kata kunci tersebut. Tetapi, *Vigenere Cipher* merupakan enkripsi yang merupakan enkripsi dengan beberapa jenis penggantian, karena kata kunci merupakan sebuah kata, bukan sebuah alfabet. Oleh karena itu, sebelum menggunakan analisis frekuensi, cipherteks harus dibagi sedemikian rupa sehingga enkripsi yang terjadi dalam tiap bagian cipherteks merupakan enkripsi dengan satu jenis penggantian.

Sebelum membagi cipherteks menjadi beberapa bagian, harus diketahui dulu panjang kata kunci yang digunakan. Untuk mencari panjang kata kunci yang digunakan, diperlukan kemunculan kata yang memiliki lebih dari satu alfabet dalam cipherteks. Pembagi-pembagi dari jarak kemunculan kata tersebut akan dijadikan kemungkinan panjang kata kunci yang dicari. Jika ada lebih dari satu pasang kemunculan kata yang sama, kemungkinan panjang kata kunci yang dicari dipersempit menjadi pembagi-pembagi yang membagi jarak kemunculan pasangan kata pertama sekaligus membagi jarak kemunculan pasangan kata kedua, dan seterusnya. Normalnya, panjang kata kunci *Viginere Cipher* tidak kurang dari tiga.

Akan dicari panjang kata kunci cipherteks URUOUQWZAAMRRHHUVBUAMRRHAGQGAOPEIAOWY untuk menemukan plainteks yang membuat cipherteks tersebut. Perhatikan bahwa kata ‘AMRRH’ muncul sebanyak 2 kali dengan jarak antar kata 10 alfabet. Perhatikan bahwa kata ‘AO’ muncul sebanyak 2 kali dengan jarak antar kata 5 alfabet. Pembagi-pembagi yang membagi 10 sekaligus membagi 5 adalah 5 dan 1. Karena

panjang kata kunci normalnya tidak kurang dari 3, kemungkinan kedua (panjang kata kunci enkripsi sama dengan satu) bisa diabaikan 5 ditetapkan sebagai panjang kata kunci enkripsi. Metode pencarian panjang kata ini disebut dengan metode Kasiski.

Tahap selanjutnya adalah pembagian cipherteks. Karena panjang kata kunci adalah 5, maka cipherteks dibagi menjadi 5 bagian dengan alfabet ke-i dari cipherteks ditempatkan di bagian ke-(((i-1) mod k) + 1). Contoh pembagian cipherteks URUOUQWZA AMRRHHUVBUAMRRHAGQGAPEIAOWY menjadi 5 bagian.

UQMUMGPW
RWRVRQEY
UZRBRGI
OAHUHAA
UAHAAOO

Setelah dibagi menjadi 5 bagian, barulah pada setiap bagian dilakukan analisis frekuensi untuk mendapatkan bagian-bagian dari kata kunci yang dicari. Lalu dari kata kunci yang didapat, cipherteks didekripsi menjadi plainteks kembali.

VII. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Tuhan YME untuk segala karunia dan berkatnya selama penulisan makalah. Penulis juga mengucapkan terima kasih kepada bapak Rinaldi Munir dan ibu Harlili sebagai dosen mata kuliah Matematika Diskrit yang telah memberikan dasar-dasar teori bilangan yang dipakai dalam pembuatan makalah ini. Penulis juga mengucapkan terima kasih kepada Saudara Yusak Yuwono Awondatu yang mengingatkan penulis pada pembahasan enkripsi yang diajarkan bapak Rinaldi Munir pada saat pembahasan teori bilangan dalam kuliah Matematika Diskrit yang menjadi dasar topik dalam makalah ini.

REFERENSI

[1] Slide Presentasi IF 2120 : Teori Bilangan
Diakses pada tanggal 8 Desember 2015, pukul 20.30 WIB

[2] http://www.cs.trincoll.edu/~crypto/historical/vigenere.html
Diakses pada tanggal 8 Desember 2015, pukul 21.04 WIB

[3] http://daniel_rivai.staff.gunadarma.ac.id/Downloads/files/39118/BAB+2+-+KRIPTOGRAFI_.pdf
Diakses pada tanggal 8 Desember 2015, pukul 18.31 WIB

[4] http://www.richkni.co.uk/php/crypta/freq.php
Diakses pada tanggal 9 Desember 2015, pukul 1.09 WIB

[5] http://www.sttmedia.com/characterfrequency-indonesian
Diakses pada tanggal 8 Desember 2015, pukul 21.22 WIB

[6] http://www.richkni.co.uk/php/crypta/vignere.php
Diakses pada tanggal 9 Desember 2015, pukul 1.15 WIB

[7] K. H. Rosen, "Discrete Mathematics and its Applications" 7th ed. New York: McGraw-Hill, 2007, pp. 237 - 244

[8] http://www.cryptomuseum.com/crypto/vigenere/
Diakses pada tanggal 9 Desember 2015, pada pukul 16:20 WIB

[9] http://crypto.interactive-maths.com/vigenegravere-cipher.html
Diakses pada tanggal 9 Desember 2015, pada pukul 16:23 WIB

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, 9 Desember 2015

Richard Wellianto - 13514051