Perbandingan Tingkat Keamanan *Vigenère Cipher* dengan *Sidewinder Cipher*

William Eka Putra - 13508071
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
striker_system@hotmail.com

***Abstrak*— *Vigenère Cipher* cukup banyak digunakan dalam kehidupan sehari-hari, pada jaman perang dahulu, enkripsi digunakan untuk mengirimkan pesan perang, pada jaman sekarang enkripsi tetap diperlukan, yaitu untuk menjaga keamanan data, file yang dikhususkan untuk orang tertentu saja, dan masih banyak kejadian-kejadian lainnya. Namun keburukan dari *Vigenère Cipher* adalah sudah sangat sering digunakan sehingga mudah untuk dipecahkan, ada banyak sekali cara untuk memecahkan *Vigenère Cipher* dan cara yang paling populer contohnya adalah Metode Kasiski.**

Vigenère Cipher adalah salah satu metode enkripsi berjenis kunci simetrik dengan menggunakan metode subtitusi alfabet yang mampu mengurangi korelasi antara frekuensi huruf pada *plaintext* dan *ciphertext*. Meskipun demikian, cara ini masih mengeluarkan hasil enkripsi yang berpola, apalagi sekarang sudah ditemukan bermacam-macam perangkat lunak untuk mencari pola dalam sebuah teks. Melihat hal tersebut, penulis ingin meningkatkan keamanan dari *Vigenère Cipher* yang diberi nama *Sidewinder Cipher*, yaitu dengan cara membuat sebuah algoritma baru yang menggabungkan berbagai unsur yang telah ada, misalnya penerapan *One Time Pad*, yaitu untuk membuat enkripsi yang tidak dapat dipecahkan dengan kunci yang acak dan panjang kunci sama dengan panjang teks, atau pembangkitan kunci dengan deret bilangan tertentu, dan penggeseran pembacaan pasangan kunci.

Kata Kunci*—Enkripsi, Metode Kasiski, *One Time Pad*, *Vigenère Cipher

I. PENDAHULUAN

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga *message* agar tetap aman (*secure*).

Kriptografi (*cryptography*) berasal dari bahasa Yunani yaitu cryptos artinya rahasia (*secret*) dan graphein artinya tulisan (*writing*). Jadi kriptografi berarti tulisan rahasia (secret writing). Kriptografi tidak hanya ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, nirpenyangkalan, otentikasi tetapi juga sekumpulan teknik yang berguna.

Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

- *Confidelity* (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.
- *Data integrity* (keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
- *Authentication* (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
- *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

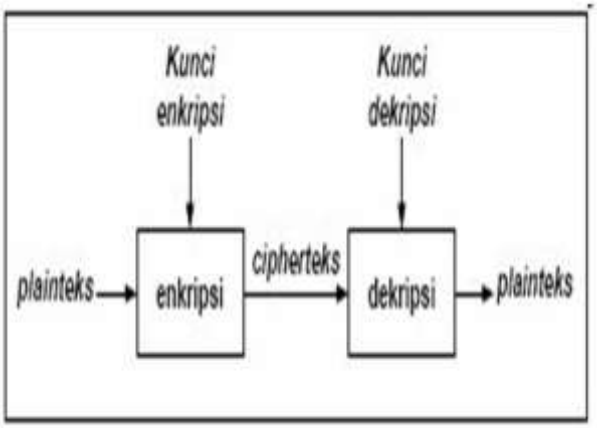
Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan (yang artinya apabila algoritma yang digunakan telah diketahui maka pesan sudah jelas "bocor" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut), kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang digunakan pada algoritma tersebut (oleh pemakainya) sehingga algoritma tersebut dapat saja disebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya.

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi :

- **Plaintext** (M) adalah pesan yang hendak dikirimkan (berisi data asli).

- **Ciphertext** (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
- **Enkripsi** (fungsi E) adalah proses pengubahan *plaintext* menjadi *ciphertext*.
- **Dekripsi** (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal yang asli.
- **Kunci** adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah *plaintext* menjadi *ciphertext* (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti.



Gambar 1. Diagram proses enkripsi dan dekripsi algoritma simetris

Peranan kunci sangatlah penting dalam proses enkripsi dan dekripsi (disamping pula algoritma yang digunakan) sehingga kerahasiaannya sangatlah penting, apabila kerahasiaannya terbongkar, maka isi dari pesan dapat diketahui.

Secara matematis, proses enkripsi merupakan pengoperasian fungsi E (enkripsi) menggunakan e (kunci enkripsi) pada M *(plaintext)* sehingga dihasilkan C *(ciphertext),* notasinya :

$$\mathbf{E_e(M) - C} \qquad (1)$$

Sedangkan untuk proses dekripsi, merupakan pengoperasian fungsi D (dekripsi) menggunakan d (kunci dekripsi) pada C *(ciphertext)* sehingga dihasilkan M *(plaintext),* notasinya :

$$\mathbf{D_d(C) = M} \qquad (2)$$

Di mana fungsi dekripsi D memetakan *ciphertext* P ke plainteks awalnya Adapun fungsi *cipher* yang merupakan komposisi antara enkripsi dan dekripsi dapat ditulis sebagai berikut:

$$\mathbf{D_d(E_e(M)) = M} \qquad (3)$$

II. VIGENÈRE CIPHER

A. Enkripsi dan Dekripsi

Vigenère cipher adalah metode mengenkripsi tulisan yang pertama kali diciptakan oleh seorang yang bernama Blaise de Vigenère pada tahun 1553 dalam bukunya yang berjudul *La cifra del. Sig. Giovan Battista Bellaso*. Metode ini berjenis kunci simetrik dengan menggunakan metode subtitusi polialfabetik dengan mengaplikasikan *Caesar Cipher* yaitu dengan mensubtitusikan huruf pada plainteks dengan kata kunci yang berpadanan letaknya.

Secara matematis, fungsi enkripsi dan fungsi dekripsi dengan mengaplikasikan *Vigenère cipher* dapat dituliskan sebagai berikut:

$$\boldsymbol{C_i = (P_i + K_i) \bmod 26} \qquad (4)$$
$$\boldsymbol{P_i = (C_i - K_i) \bmod 26} \qquad (5)$$

Di mana,
Pi : karakter plainteks
Ki : karakter kunci
Ci : karakter chiperteks

Fungsi enkripsi yang menghasilkan *ciphertext* (C_i) dengan menggunakan (4) dan fungsi dekripsi yang menghasilkan *plaintext* (P_i) dengan menggunakan (5).

Enkripsi dan dekripsi pada *Vigenère cipher* menggunakan bantuan tabel berukuran 26 x 26 berisi huruf alfabet yang biasa disebut sebagai *tabula recta*.

	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. *Tabula recta*

Jika panjang kunci lebih pendek daripada panjang

plainteks, maka kunci diulang secara periodik. Misalkan panjang kunci adalah 20 karakter, maka 20 karakter pertama dienkripsi dengan (4) setiap karakter ke-*i* menggunakan kunci k_i. Untuk 20 karakter berikutnya, kembali menggunakan pola enkripsi yang sama. Misalkan untuk sebuah plainteks alphabet yang berisikan tulisan "MENJADIKUPUYANGSEHAT" dan kunci yang bertuliskan "DIGIMON", maka bisa didapat ciphertext dengan menggunakan (4) sebagai berikut:

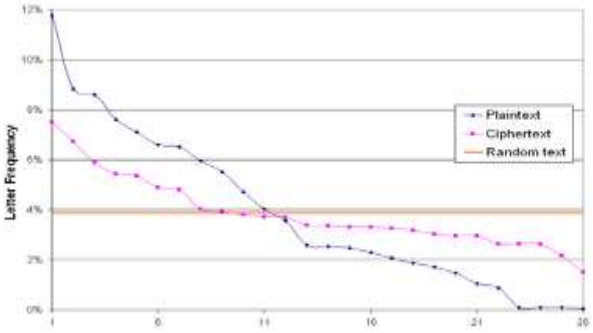
Pi: MENJADIKUPUYANGSEHAT
Ki: DIGIMONDIGIMONDIGIMO
Ci: PMTRMRVNCVCKOAJAKPMH

Dalam hasil enkripsi di atas dapat dilihat bahwa belum tentu satu huruf yang sama dienkripsi menjadi huruf yang sama pula, oleh karena hal ini, algoritma *Vigenère cipher* dikatakan bisa mengurangi frekuensi kemunculan pengulangan huruf dalam sebuah teks.

B. Kriptanalisis pada Vigenère cipher

Ide utama dari *Vigenère cipher*, seperti semua polialfabetik enkripsi lainnya adalah untuk menyamarkan kemunculan frekuensi huruf cipherteks yang bersesuaian dengan plainteks. Sebagai contoh, apabila dengan analisis frekuensi ditemukan bahwa P adalah huruf terbanyak dalam cipherteks dan kriptanalis tahu plainteks dalam Bahasa Inggris maka kriptanalis dapat menyimpulkan bahwa huruf P adalah huruf E yang telah terenkripsi karena dalam Bahasa Inggris huruf E adalah huruf yang paling sering digunakan, dan sisa dari teks akan dapat dipecahkan, hanya masalah waktu saja. Maka, dengan digunakannya *Vigenère cipher* hal ini dapat dikurangi karena satu huruf bisa saja dienkripsi menjadi beberapa huruf lain.

Kelemahan utama dari *Vigenère cipher* adalah kunci yang berulang, apabila seorang kriptanalis dapat menebak dengan tepat panjang kunci, maka cipherteks akan dengan mudah dipecahkan. Memang benar bahwa penggunaan *Vigenère cipher* dapat mengurangi keterlihatan frekuensi pengulangan huruf, akan tetapi, meksipun demikian sedikit dari pola kalimat akan tetap tersisa, hal ini dapat terjadi apabila kunci terlalu pendek atau monoton berulang.



Gambar 3. Grafik perbandingan frekuensi kemunculan huruf

Pada tahun 1863, seorang bernama Friedrich Kasiski dapat memecahkan kode enkripsi dengan Vigenère cipher yang diberi nama Metode Kasiski atau *Kasiski Examination* atau *Kasiski Test*, yaitu dengan mengambil kelemahan sisa pola yang berulang, misalnya sebuah plainteks hendak dienkripsi dengan kunci sepanjang 4 karakter yaitu "ABCD":

Pi: **CRYPTO**ISSHORTFOR**CRYPTO**GRAPHY
Ki: ABCDABCDABCDABCDABCDABCDABCD
Ci: **CSASTP**KVSIQUTGQU**CSASTP**IUAQJB

Dapat dilihat bahwa kata **CRYPTO** secara tidak sengaja terenkripsi menjadi kumpulan kata yang sama yaitu **CSASTP**. Maka secara intuitif kita dapat menyimpulkan bahwa kata **CRYPTO** secara kebetulan dienkripsi dengan sekuens kunci yang sama. Metode Kasiski menyimpulkan bahwa jarak antara kedua kumpulan huruf pada suatu cipherteks memiliki kemungkinan besar adalah merupakan kelipatan dari panjang kunci yang digunakan. Dalam contoh di atas jarak antara kedua kumpulan huruf **CSASTP** adalah 16 karakter, maka bisa ditarik kesimpulan kunci memiliki panjang karakter sebesar 1, 2, 4, 8, atau 16. Dan hipotesis tersebut benar karena panjang kunci adalah 4 karakter yaitu "ABCD".

Metode lainnya adalah penghitungan analisis frekuensi. Sekali waktu panjang kunci enkripsi diketahui, maka cipherteks dapat dipecahkan dengan membaginya ke dalam beberapa kolom dengan masing-masing kolom berkorelasi dengan huruf pada kunci. Tiap kolom berisi plainteks dan kemudian hanya dibutuhkan penggeseran untuk mencoba kunci apa yang tepat dan cipherteks telah terdekripsi. Metode analisis frekuensi ini merupakan pengembangan dari Metode Kasisiki, yang sering juga disebut sebagai Metode Kerckhoffs.

III. ALGORITMA PENDUKUNG

A. One Time Pad

One Time Pad adalah algoritma yang ditemukan oleh Major Joseph Mauborgne pada tahun 1917, yang sampai sekarang adalah algoritma kriptografi sempurna yang tidak dapat dipecahkan. Algoritma ini masih termasuk ke dalam algoritma kriptografi simetri.

Untuk menghindari cara-cara kriptanalisis di atas, terutama Metode Kasiski, konsep *Vigenère Cipher* dapat diperkuat menjadi sebuah *cipher* yang tidak dapat dipecahkan atau *unbreakable cipher*, kecuali tentunya menggunakan metode *brute force* yang dimana selalu menghasilkan jawaban, maka dapat sang pengirim pesan harus memperhatikan berbagai macam hal, contohnya adalah bahwa kunci harus diacak dan panjang kunci harus sama dengan panjang plainteks. Kedua syarat tersebut mengakibatkan plainteks yang sama tidak selalu menghasilkan cipherteks yang sama. Karena panjang

kunci sama dengan plainteks maka tidak ada pengulangan dari kunci.

One Time Pad berisi deretan karakter-karakter kunci yang dibangkitkan secara acak. Satu *pad* hanya digunakan sekali saja untuk mengenkripsi pesan, setelah itu pad yang telah digunakan dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain. Yang memiliki kunci itu hanyalah sang pembuat pesan dan sang penerima pesan.

Metode ini benar-benar membuat sebuah cipherteks memiliki resistansi penuh terhadap Metode Kasiski yang memanfaatkan pola pengulangan huruf untuk mendekripsinya. Meskipun *One Time Pad* adalah algoritma yang aman, namun memiliki kelemahan yang cukup fatal yang mengakibatkan tidak banyak digunakan dalam praktek, yaitu tidak mangkus, karena panjang kunci sama dengan panjang pesan, apabila pesan yang dikirim cukup panjang, maka kunci juga akan mengikuti panjang pesan tersebut dan sulit untuk disimpan, selain itu pendistribusian kunci juga akan merepotkan yaitu bagaimana kunci tersebut dikirmkan secara aman dan tentunya tidak mungkin melalui jalur yang sama dengan jalur pengiriman pesan, kunci harus dikirim karena pembangkitan kunci adalah acak dan sepanjang pesan serta yang mengetahui hanyalah sang pembuat pesan, agar penerima pesan bisa menerima pesan dengan baik, maka kunci tersebut harus dikirimkan melalui jalur yang aman dan biasanya relatif mahal dan lambat.

B. Deret Fibonacci

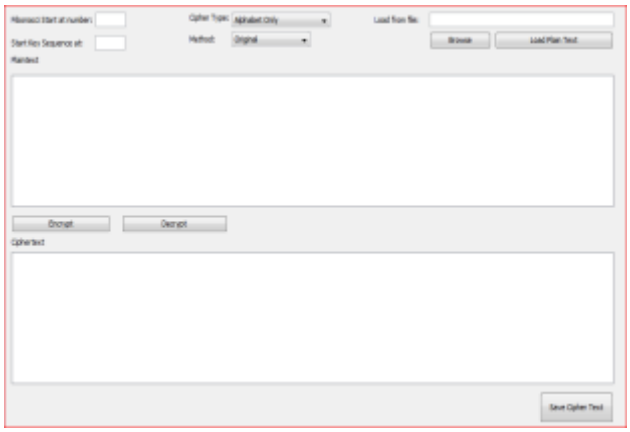
Dalam matematika, bilangan Fibonacci adalah barisan yang didefinisikan secara rekursif sebagai berikut dengan F adalah fungsi yang menghasilkan bilangan dan n adalah indeks dari urutan bilangan:

$$F(n) = \begin{cases} 0, & \text{jika } n = 0; \\ 1, & \text{jika } n = 1; \\ F(n-1) + F(n-2) & \text{jika tidak.} \end{cases} \quad (6)$$

IV. SIDEWINDER CIPHER

Sidewinder cipher adalah algoritma buatan penulis yang bertujuan untuk mengembangkan konsep dan keamanan dari *Vigenère cipher* dengan menggabungkan berbagai konsep, yaitu pembangkitan kunci dengan deret angka dan *One Time Pad*. Algoritma ini memiliki ide utama sebagai berikut:

- Pembangkitan kunci secara acak menggunakan deret *Fibonacci* yang elemen pertamanya ditentukan oleh sang pembuat pesan.
- Pembangkitan kunci dilakukan dengan menerapkan prinsip *One Time Pad*, yaitu panjang kunci sama dengan panjang teks.
- Setelah teks dan kunci terbentuk, dilakukan *Vigenère Cipher* namun tidak dalam indeks array yang sama, jadi teks pada indeks ke-i dipasangkan pada key pada indeks ke-(i+n), dengan n adalah bilangan masukan dari sang pembuat pesan juga.



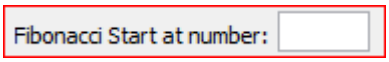
Gambar 4. Tampilan program *Sidewinder Cipher*

A. Pembangkitan Kunci

Tahap awal dari proses enkripsi atau dekripsi ketika menggunakan algoritma ini adalah pembangkitan kunci dengan mengaplikasikan deret bilangan Fibonacci yang angka masukan pertamanya dimasukkan oleh sang pembuat pesan sepanjang plainteks. Apabila F adalah fungsi yang menghasilkan bilangan, n adalah indeks urutan bilangan, dan input adalah angka masukan dari pembuat pesan, maka secara matematis dapat dituliskan:

$$\mathrm{F(n)} = \begin{cases} 0, & jika\ n = 0; \\ input, & jika\ n = input; \\ F(n-1) + F(n-2) & jika\ tidak. \end{cases} \quad (7)$$

Panjang kunci yang dibangkitkan harus sama panjangnya dengan plainteks yang hendak dienkripsi karena diterapkannya konsep *One Time Pad*.



Gambar 5. Tampilan input nilai pertama Fibonacci

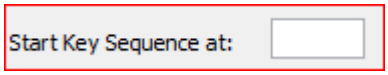
B. Penggeseran Pembacaan Kunci

Setelah kunci dibangkitkan tahap berikutnya adalah enkripsi dengan pembacaan kunci yang berbeda indeksnya, yaitu plainteks pada indeks ke-i dipasangkan pada key pada indeks ke-(i+n), apabila telah mencapai batas ujung kunci, maka pembacaan kunci dimulai kembali dari awal, karena panjang kunci dan plainteks adalah sama, jadi seluruh plainteks mendapatkan pasangan kunci. Yang digunakan tidak hanya 26 alfabet tapi seluruh karakter ASCII, secara matematis ditulis:

$$C_i = (P_i + K_{(i+n) \bmod L}) \bmod 256 \quad (8)$$

$$P_i = (C_i - K_{(i+n) \bmod L}) \bmod 256 \quad (9)$$

Di mana,
Pi : karakter plainteks
Ki : karakter kunci
Ci : karakter chiperteks
n : bilangan geser baca kunci
L : panjang plainteks/kunci



Gambar 6. Tampilan input penggeseran pembacaan kunci

V. PERBANDINGAN KEAMANAN KEDUA ALGORITMA

Untuk dapat membandingkan tingkat keamanan kedua algoritma diperlukan satu sumber plainteks yang sama kemudian dienkripsi menggunakan kedua algoritma tersebut dan kemudian penulis akan mencoba melakukan kriptanalisis terhadap kedua cipherteks yang dihasilkan.

A. Plainteks

Greek mythology is the body of myths and legends belonging to the ancient Greeks concerning their gods and heroes,
the nature of the world, and the origins and significance of their own cult and ritual practices.
They were a part of religion in ancient Greece.
Modern scholars refer to the myths and study them in an attempt to throw light on the religious and political institutions of Ancient Greece,
its civilization, and to gain understanding of the nature of myth-making itself.[1]

Greek mythology is embodied explicitly in a large collection of narratives and implicitly in Greek representational arts,
such as vase-paintings and votive gifts.
Greek myth attempts to explain the origins of the world and details the lives and adventures of
a wide variety of gods, goddesses, heroes, heroines, and mythological creatures. These accounts initially were disseminated in an oral-poetic tradition;
today the Greek myths are known primarily from Greek literature.

The oldest known Greek literary sources, the epic poems Iliad and Odyssey, focus on events surrounding the Trojan War.
Two poems by Homer's near contemporary Hesiod, the Theogony and the Works and Days,
contain accounts of the genesis of the world, the succession of divine rulers, the succession of human ages,
the origin of human woes, and the origin of sacrificial practices.
Myths also are preserved in the Homeric Hymns, in fragments of epic poems of the Epic Cycle,
in lyric poems, in the works of the tragedians of the fifth century BC,
in writings of scholars and poets of the Hellenistic Age and in texts from the time of the Roman Empire by writers such as Plutarch and Pausanias.

B. Cipherteks dengan Vigenère Cipher

Cipherteks di bawah adalah hasil pengenkripsian dengan *Vigenère cipher* biasa yang dimasukkan kata kunci “zeus”.

Fvywj qslgsfgfc ck sly tnhs ge qslgw ufc pyydrxk aifgmkcff xi lgi ufbmyfs Klwdom unrwwqrcff xbwhv agcw ufc lyjnim,
lgi hssylw nj nzd aijkh, ufc xbw nvcyhrm smh mafrcxhgufbi ix slyaq sqf byfl zrx jhxosk tlsbxcudw.
Nzdc qwqi u hzvn ge vydhkcgm mh smgcwmx Ajdiww.
Lsxwqr mugsfsqw lweil ln xbw lcnzr ehv rxovx xbwl mh sm enldqjl ss nzqsq dhkbl nr nzd vydhkcgtw ufc tidhxcuzp cfrxcltxcgmw ix Zrwadrn Yqiyud,
mnk bmpakmtssmif, zrx ln kuam yhvdvmlzrxamk ix sly fzxojd sz exxb-ezocff mnkdpz.[1]

Yqiyc lcnznpiyx mm wlfivhix wwtfabmndx mh s kelyd gidkiwlhsh ge rujqenauim smh ceopcuhxfq hr Ajdie jdtlwrihlzxcgmef sqxm,
ktgb sr zukd-tuamxcffw ufc zilhzy yhjnk.
Fvywj qslg enldqjlr xi wwtfshr nzd slafmhk nj nzd aijkh ufc hylzmfk sly dhzyk zrx sczyfsylwr sz
s vmxw ueladxs ge kivr, kivcimkdw, bwqsyk, gilghryk, zrx exxbgksaabef uqiultvyk. Slykd ewunyhlr mhasmudkc qwqi xarwyehruldh cf zr ijzp-jgdxcu svuvhxcgm;
xivzc nzd Klwdo gqslm sqi efnah hqmgsqmfq evie Fvywj pcldvultvy.

Lgi idciml jriom Klwdo fasilsqc mgtvwwr, xbw dtcu osyer Mfazh ufc Sxqrwyq, eswmr sh wuihlr wojqsofcmhy sly Lqsdsm Auj.
Sai hnigk ac Bglil'k miuj bshldqjgqelq Gimanh, nzd Xbwnkifx ehv sly Onvek zrx Vzcm,
unrnshr uubsofsw ix sly ydrykhw ix sly onvfv, sly ktgwwrwcgm sz vhzcfd voddvm, lgi mmbgykrmif nj bmleh sfim,
lgi ijhkcf nj bmleh onim, smh nzd slafmh ge wuuqmzabmud ovuusmwwr.
Qslgw udrs ujd tlwrilndh cf sly Znqyjhg Bqlrm, am jlsfqyfsw ix dtcu osyer sz lgi Yhhg Wqbpy,
am psjhg jgdqm, am xbw vslcr sz lgi njzkyvhehk nj nzd jcxsl wwmxojx FW,
am alasmhyr sz kblidzvm smh jgdxm ge xbw Gifddrcksmw Sfi ufc mh ldbnk evie sly lhqy ge xbw Qsgsm Ighhvy tx alasilk rywz zw Jdtxujbl ufc Tumrehazw.

C. Cipherteks dengan Sidewinder Cipher

Sedangkan untuk penenkripsian dengan menggunakan *Sidewinder Cipher* dengan masukan angka pertama Fibonacci adalah "3" dan pembacaan kunci yang digeser sejauh "5 karakter" didapat cipherteks (beberapa karakter merupakan karakter yang tidak dapat ditampilkan):

»ÚÊ…ÚæíÜˆÐàãÌæÙçç^ÙÑ□ÉñßÒÎââ^"ÕÖÉŒÍÖÒÓÖ
ÜÅ…ÔèÛÕÜš‡ÝÝÜÍ…ÉÓÏÕÊÜÝºæÎÈ‹ÔÊÔŽ ÄÓÖŽ Ò
Ü‡èÍÝÝå‡ÕÖâÎ□ØÐÊ'ãÎà'*ãÎ…âÉÙ•äÔÜÇâˆÊäßÛÞÉL
Ãç„ëÚÎã×ÛÚ‰áèÄÖ„ÔÜ‡ÞÕÛÝÄÓÑË…ÐÔØ^ÕÊçâØ
ÜÌÖß¢□ÛÓÖÎæã□ßÓÚÐÏÕÛÖ…å"|½ÏÎç—
ÔØ…ÉåÎÓâ • ÝáÒåÝÏÜ□ÏÕáÐ□ÄÛÊ□ä¹×ØÑÄ×•omÒ
ÓÑÞÓÖ×ÑÞÚÆäé×É†Îàèæã^ÕÜÞáÛ"Ãç„ÛãâÉë›Û…ÛÎ
ÏÓ□ÄãâÙÒÝäãáÕÚë□ßÑÜÐ×Ø›□èÐÊ'ÙÔÎÖÐÞãì□ÏÒ
Ô□àÑÙ‰ÚÐÞÔá"Õ×Ø•ØÊèáŸ□†¤ÝÑÝÆ×âgÓÈÒÙš
~Ü"âÉ‰êÑÑ‰áÆâÎâ×LÇàÅÛÜÌÏÝá•ÝÊ…×ãÝÄŽ ÔØ
ÓÔâ†ãÎ…âÉÙ•×ÕØÉ□ÜíË™Ò□‹‰àÏÎá"ÎÚ†□ÉQ¾~~¬
ßÕÙ‹áè"ÜÞÚ□ÛáÎ"×ÒÎØËÒÔÙØ˜ÑÚÍƒÙãØâÝ×ÄÍÍ'Ð
ÓÖãÕàÚ×ÝØÝá□ÕÔ□ÓàÄÝÎäÙ"ÈàÉÎÐÕ˜‰ƒÒèß™Ì×
½ÛÑÎåÓÙÙáÓŸ…ÏâÅ"ÝÞŽ ÈÍÊà"èšnØçÖÜÂáÚÊáÌMß
Ç‰âÜÎŽ ÕÔÕãÖÛ • ãÏ–ÒàÝÎ¡à□u°àÌ…ÔáìÙÔÇ¢Ï–
Ê□"ÚæÔÊã□ÙÚŸÖãÔÔÖë‰ÐÜ□ØÜÈãÌÎÜÓ'ÑÜÑÚÍ
ÇÎëÐÛØ×"ÉÓÐ‰ÚÊçÂ×ÐÔ„êÍÓ"áÛÛØâ†kÏÛ‰ÅÉìÆ
àÝÚæÞâ†ÖÕ„"□‡æÍÈÊ"éÆå•ÍÙë□ÔÙLÏÖÖâ•□Ìâ□ÅÓ
×àÞèÔèŒØÕ‰Ä□ŒÒØ…ÏÕçäÆç—
ÊÍØ"ÆÏÇƒØâÞàÜÌ×Ýàâ□ÕÚ™Þ××ÊÏ‰åØÕßÎáÆâÙÅÝ
×ÐÜÐÞ□ÍŸäâ'"‰ÖéÕÉ„Êç‰åÏ®o¡ßÅÊçèÑÓ®å…ÆÙ
Ñ™ê×çÊèÊ‹ÕØÝâã ‰□□ÚÎÞèÏàÔàs'ÆÓÏŒÖíÙÚÐàäÙ
Î'kvtË×ÔÍØÚåÙÞœ□ëÖ¬åÊ…ÌÏÌãÚàÕå™ÜÝÞæÌÆß˜î^
ÜÊâÎƒÔØØàØ¶Õ×ÂØÆÒ„,Ò™Ôá…è□ÇÛ□âåÔâÎÙ…â
æÔ×ÞæÛÞã©„‰ÕÙÙÍÐtßèÞÉÝÃÐÙ§*½ê□ä×Ê□æ¸è®
• áÍ×GêÝ×ÍÖ• • âÜÊ • ãäÕÄ×ì»Îâ× • Ó'"ÌÎÊÑÓÔ‡áåÆ
à× ^Ù¿Ô'ÞèÄÑÉ·Ôââš*ÒÕ□ÜÖÖÏÏƒÄÖÚá "□ÍæÍÊÒ…
ÛËØÛ"ãÕ"ÜÍÜÔå˜„□âÌ…çÝÈƒÔåÜÐØÜ□ÕÊ‰éÊÑ×
ÚçÛÜ'ß•ÛÐÙ"ÞÉÌÈÜÔÕ□ÞáÇËéÖÄÓÔ•…"LwíÜÍâ'Ê
ÕÍ□âÚÝÙæ□ÝÛÐÞ" ÉÓ„ÛÚÊÔÝ‰Ôââ×Ù"ÂÕ×‰Ñ×
ÒàÏŒàäÊÐÕÛÌÑìNp¿èáˆÚÓàÛÔ□éÔâÞÉŸ…ÓäÉ„ÝÖÙ
ÍÊ³□ÙÎæÎÕ©íâàØZ‰□ÚÚÆ‡ÜÑÒÙæã†ÐÞØÚÞ□ÌßØ
ÔÑ"ÔÎ'ÕÛÄµòƒßÔ¡|ÌÓß¥'ÝËÕ□ÊÝÜ□‰ÞãÍÒê□Û×Ü
ÐÊ"ÉÓØ'ÐËÞ×ÜÆçŸ□ÌãËÚÙ‰Õâ`ÈÛÓâéå™µ¸□|Øãå
ÖÒâÐ□ÛÛÔ†çÕ×ÙÍÏ'êÂà'□□ÙÜØ□ÕæÑÌ±ÓßŒÔÔ
‰çÜÎÅ°ËÞ□ÝÊ‰ÛíÙàç"ÇàÓ□àÍÌÙ×ÑØ□ÈÙÔÔÀÖÖ
ÏÕeáß‰æÍÇ™ØàÌÝÊàç"ÜÕÍÆÞÃŒØãÏÕÈÚÏ×Ò· • éÛÆ
×Û • Ú • n

D. Kriptanalisis pada Vigenère Cipher

Kriptanalisis yang dilakukan akan menggunakan Metode Kasiski dan *Frequency Analysis*, untuk memudahkan penghitungan penulis menggunakan program *CryptoHelper* yang disediakan di situs kuliah.

Menggunakan konsep yang telah dituliskan di bab sebelumnya, dapat dilakukan kriptanalisis sebagai berikut:

- Analisis kemunculan
  - Salah satu Trigraph yang terbanyak muncul adalah "NZD" yaitu sebanyak 6 kali, masing-masing terdapat pada posisi 106,174,278,558,570,742.
  - 6-graph "ENLDQJ" muncul 2 kali yaitu pada posisi 257,541.
  - 10-graph "NJNZDAIJKH" muncul 2 kali yaitu pada posisi 104,568.
  - 10-graph "ZDAIJKHUFC" muncul 2 kali yaitu pada posisi 207,666.
- Penentuan panjang kunci
  - Urutan huruf terdekat dari Trigraph adalah 558 dan 570, sehingga kemungkinan panjang kunci adalah 1, 2, 3, 4, 6, dan 12 karakter.
  - Panjang kunci tersebut diiris dengan kemungkinan panjang kunci 6-graph, yang kemudian menghasilkan panjang kunci adalah 1, 2, 4, 6 atau 12 karakter.
  - Eliminasi panjang berikutnya adalah dengan menggunakan 10-graph yang membuat irisan ketiga kemungkinan panjang kunci adalah 1, 2, atau 4 karakter.
  - Eliminasi terakhir menggunakan 10-graph lagi yang menghasilkan pilihan kemungkinan kunci menjadi 1 atau 4 karakter.
- Asumsi dan nalar
  - Panjang kunci ditentukan 4 karakter karena 1 karakter dianggap terlalu pendek dan tidak mungkin digunakan sebagai kunci.
  - Dari analisis kemunculan juga didapat frekuensi kemunculan satu huruf dan dua huruf yang paling sering muncul, dan diketahui bahwa teks dalam Bahasa Inggris.
  - Mengelompokkan cipherteks karena panjang kunci sudah dapat ditentukan.
  - Asumsikan huruf yang paling sering muncul adalah "E" dan tiga huruf yang sering muncul adalah "THE"
  - Dengan asumsi tersebut dan cipherteks yang telah dikelompokkan, maka pada langkah pertama didapat karakter ketiga dari kunci yaitu "U"
  - Cara yang sama dilanjutkan terus menerus sampai akhirnya terdapat beberapa teks yang dapat dibaca dan diasumsikan sebagai kata tertentu dan didapatkan kunci yang sepanjang 4 karakter dan bertuliskan "ZEUS"
- Tingkat kebenaran
  - Disimpulkan panjang kunci adalah 4 karakter adalah benar.
  - Didapatkan kunci "ZEUS" adalah benar

Jadi, pengenkripsian dengan *Vigenère Cipher* sekarang ini tidak lagi aman karena sudah sangat banyak metode yang dapat digunakan untuk melakukan penyerangan terhadap kunci, panjang kunci, dan langsung ke cipherteksnya. Contoh di atas membuktikan bahwa panjang kunci sangat memengaruhi tingkat kesulitan kriptanalisis, semakin pendek akan semakin mudah untuk dipecahkan.

E. Kriptanalisis pada Sidewinder Cipher

Kriptanalisis untuk algoritma ini dengan menggunakan Metode Kasiski dan *Frequency Analysis* adalah hal yang mustahil, karena diterapkannya *One Time Pad*.

Penulis telah menggunakan aplikasi yang sama yaitu *CryptoHelper* untuk melakukan analisis kemunculan, akan tetapi bigraph yang muncul hanyalah pasangan huruf SS dan memiliki jarak yang cukup jauh sehingga panjang kunci akan sulit untuk ditebak, untuk trigraph pun hanya muncul 5 pasangan huruf yang jaraknya sangat jauh sehingga tidak akan ada kemungkinan untuk menebak dengan melakukan irisan kemungkinan panjang kunci seperti yang telah penulis lakukan untuk melakukan kriptanalisis pada cipherteks *Vigenère cipher*.

One Time Pad memastikan bahwa hasil enkripsi tidak dapat diserang oleh Metode Kasiski dan *Frequency Analysis* karena persentase pengulangan huruf yang kecil dan sulit untuk ditebak, lebih lagi yang digunakan adalah bilangan ASCII yang memiliki jumlah 256 sehingga akan jauh lebih sulit untuk melakukan asumsi dan nalar dalam kriptanalisisnya.

VI. KESIMPULAN

Melihat berbagai perbandingan, penulis dapat menganalisis dan menyimpulkan:

- Tingkat keamanan *Sidewinder Cipher* ini lebih memiliki keunggulan dibanding *Vigenère cipher* yaitu memiliki ketahanan terhadap Metode Kasiski dan *Frequency Analysis* karena mengurangi adanya pola kata yang berulang dan panjang kunci akan sulit untuk ditentukan.
- Meskipun menggunakan konsep *One Time Pad*, tapi algoritma ini tidak perlu menyimpan kunci sepanjang plainteks, cukup bilangan pertama yang ditentukan oleh pembuat pesan.
- Kekurangan yang dimiliki oleh algoritma baru ini adalah membutuhkan biaya dan waktu yang cukup mahal untuk membangkitkan kunci acak karena digunakannya konsep *One Time Pad*. Apabila teks yang hendak dienkripsi cukup besar maka membutuhkan waktu untuk pembangkitan kunci yang cukup besar pula.

VII. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih terutama kepada Tuhan Yang Maha Esa karena berkat anugerah yang diberikan-Nya makalah ini dapat diselesaikan. Penulis juga mengucapkan terima kasih kepada Bapak Ir. Rinaldi Munir, M.T. selaku dosen pengajar kuliah IF3058 Kriptografi karena berkat kuliah dan referensi yang diberikan oleh beliau makalah ini dapat disempurnakan.

REFERENCES

[1] Murphy, Sean dan Fred Piper. 2002. *Cryptography: A Very Short Introduction*. Oxford University Press, ch 4.
[2] Kahate, Atul. 2008. *Cryptography and Security*. Tata McGraw-Hill, pp 95-123.
[3] http://www.informatika.org/~rinaldi/Kriptografi/2010.2011/kripto10-11.htm
[4] http://en.wikipedia.org/wiki/Vigenere_cipher
[5] http://id.wikipedia.org/wiki/Bilangan_Fibonacci
[6] http://supapri.wordpress.com/2009/07/10/otp-one-time-pad/
[7] http://rizalp.blogspot.com/2008/11/algoritma-deret-bilprima-dan-deret.html

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, 12 Maret 2011

ttd

William Eka Putra - 13508071

LAMPIRAN

A. PLAINTEKS

Adalah plainteks yang digunakan penulis untuk melakukan percobaan baru dan kriptanalisisnya.

Greek mythology is the body of myths and legends belonging to the ancient Greeks concerning their gods and heroes,
the nature of the world, and the origins and significance of their own cult and ritual practices.
They were a part of religion in ancient Greece.
Modern scholars refer to the myths and study them in an attempt to throw light on the religious and political institutions of Ancient Greece,
its civilization, and to gain understanding of the nature of myth-making itself.[1]

Greek mythology is embodied explicitly in a large collection of narratives and implicitly in Greek representational arts,
such as vase-paintings and votive gifts.
Greek myth attempts to explain the origins of the world and details the lives and adventures of
a wide variety of gods, goddesses, heroes, heroines, and mythological creatures. These accounts initially were disseminated in an oral-poetic tradition;
today the Greek myths are known primarily from Greek literature.

The oldest known Greek literary sources, the epic poems Iliad and Odyssey, focus on events surrounding the Trojan War.
Two poems by Homer's near contemporary Hesiod, the Theogony and the Works and Days,
contain accounts of the genesis of the world, the succession of divine rulers, the succession of human ages,
the origin of human woes, and the origin of sacrificial practices.
Myths also are preserved in the Homeric Hymns, in fragments of epic poems of the Epic Cycle,
in lyric poems, in the works of the tragedians of the fifth century BC,
in writings of scholars and poets of the Hellenistic Age and in texts from the time of the Roman Empire by writers such as Plutarch and Pausanias.

B. ALGORITMA SIDEWINDER CIPHER

```
public class VigenereCipher extends Cryptography {

   private int mode = 0;
   private int startFib = 1;
   private int startSeq = 0;

   public VigenereCipher(String _plaintext, String _ciphertext, String _key, int _mode, int _startFib, int _startSeq) {
      super(_plaintext, _ciphertext);
      mode = _mode;
      startFib = _startFib;
      startSeq = _startSeq;
   }

   public void crypt() {
      /*
```

```
        * Deklarasi Variable
        * */
       int i = 0; //iterasi seluruh plaintext
       int ec = 0; //iterasi seluruh karakter saja
       int totalLength = plaintext.length();
       char[] cipher;

       /*
        * Enkripsi
        * */
       cipher = new char[totalLength];

       while (i < totalLength) {
              int ptext = plaintext.charAt(i);
              Array[] Fib = Fibo(startFib);
              int ctext = (ptext + Fib[i + startSeq]) % 26;
              cipher[i] = (char) (ctext);
              ec++;
              i++;
       }

       ciphertext = String.valueOf(cipher);
   }

   public void decrypt() {
       /*
        * Deklarasi Variable
        * */
       int i = 0; //iterasi seluruh ciphertext
       int dc = 0; //iterasi seluruh karakter saja
       int totalLength = ciphertext.length();
       char[] plain = ciphertext.toCharArray();

       /*
        * Dekripsi
        * */
       while (i < totalLength) {
              int ctext = ciphertext.charAt(i);
              Array[] Fib = Fibo(startFib);
              int ctext = (ptext - Fib[i + startSeq]) % 26;
              if (ptext < 0) {
                 ptext += 256;
              }
              plain[i] = (char) (ptext);
              dc++;
              i++;
       }       }

       plaintext = String.valueOf(plain);
   }
}
```