PENGAMANAN PESAN RAHASIA MELALUI KRIPTOGRAFI VIGENERE CIPHER DENGAN KUNCI BERLAPIS

Benni Purnama,SE,M.Kom
Sekolah Tinggi Ilmu Komputer STIKOM Dinamika Bangsa
Jl. Jendral Sudirman Thehok - Jambi
Email : bennipurnama@stikom-db.ac.id

ABSTRAK

Teknik 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. Dalam melakukan enkripsi pada metode ini dilakukan dengan bantuan table vigenere tableau. Keunggulan dari vigenere cipher dari metode klasik sebelumnya (Caesar cipher) bahwa substitusi untuk ciphrenya bersifat polyalphabetic, dimana satu karakter yang sama mempunyai karakter substitusi yang berbeda. Namun Namun demikian pada metode vigenere ini terdapat beberapa kelemahan yaitu pada plainteks karakter A selalu mendapatkan hasil karakter yang sama antara kunci dan cipherteksnya dan karakter kunci mengalami pengulangan 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. Untuk menghindari kelemahan tersebut di atas, maka perlu adanya teknik untuk dapat meningkatkan kekuatan dari hasil chiperteks vigenere ini. Salah satunya adalah dengan cara membuat kunci lebih dari satu. Dengan dibuatkanya kunci lebih dari satu (kunci berlapis) dimana pada penelitian ini penulis mencoba membuat tiga lapisan kunci, maka kelemahan yang telah penulis uraikan seperti tersebut di atas dapat teratasi. Hasil dari penelitian ini didapat bahwa Hal ini dikarenakan adanya kunci berlapis yang dibuat sebanyak tiga, sedangkan cryptanalyst dapat menduga bahwa kunci yang dibuat pada contoh diatas adalah kunci standar yaitu hanya satu lapisan saja dan menghasilkan plainteks yang masih belum bisa dibaca.

Kata kunci : kunci, plainteks, cipherteks,enkripsi, dekripsi .

ABSTRACT

Techniques Vigenere cipher alphabet cipher is a type of compound that is the most simple. Vigenere cipher applying poly alphabetic substitution method and belongs to the category in which the key is a symmetric key used for encryption is the same as the key used for the decryption process. In carrying out the method of encryption is done with the help of table vigenere tableau. Advantages of vigenere cipher of previous classical methods (Caesar cipher) that is polyalphabetic substitution for ciphrenya, where the same character has a different character substitution. However, the method vigenere However, there are some weaknesses such as the plaintext character A always get the same characters between the key and the character key and cipherteksnya experiencing continuous repetition of the same, giving rise to the same ciphertext to plaintext pieces where its position is a multiple of the key length so that the plaintext will always get the same piece for the encryption key. To avoid the drawbacks mentioned above, the need for techniques for increasing the strength of the results of this vigenere chiperteks. One of them is to make more than one key. With more than one dibuatkanya key (key-plated) which in this study the authors tried to make three key layers, the weakness that has been described as the author of the above can be resolved. The results of this study found that It is because of padded keys made as many as three, while the cryptanalyst can guess that the key is created in the example above is the default key that is only one layer only and generate plaintext which still can not be read.
Keywords : key, plaintext, ciphertext, encrypt, decrypt.

PENDAHULUAN

Dalam perkembangan dunia teknologi komunikasi dan informasi sampai saat sekarang ini peranan akan keamanan system informasi sangatlah penting. Hal ini ditandai dengan banyaknya berbagai temuan tentang kejahatan-kejahatan yang dilakukan oleh pihak tertentu dalam dunia teknologi informasi seperti

Hacking, *Cracking*, *Spy* dan lain sebagainya. Dilain pihak, ada kegiatan yang berupaya untuk mengambil informasi tanpa sepengetahuan si pemilik apakah itu untuk diubah, dimodifikasi atau untuk dipalsukan. Salah satu metode untuk pengamanan tersebut diatas adalah kriptografi. Dimana kriptografi secara sederhana adalah cara merahasikan suatu pesan atau informasi melalui penyandian (*encryption*). Dalam kriptografi teknik penyandian banyak sekali metode yang dilakukan, salah satunya adalah *Vigenere cipher*. Teknik ini dilakukan dengan cara mengacak suatu pesan atau informasi melalui bantuan tabel alfabetis atau lebih dikenal dengan istilah *Vigenere tableau*. Dalam penerapannya, ternyata metode vigenere dapat dipecahkan oleh *cryptanalyst* melalui metode kasiski.
Dengan meli hat hal tersebut di atas, penulis mencoba untuk melakukan enkripsi secara bertingkat dengan cara pemanfaatan kunci yang dipakai lebih dari satu secara bertingkat. Dengan adanya penggunaan kunci secara bertingkat tersebut diharapkan dapat menguatkan enkripsi yang sudah ada sehingga metode kasiski kesulitan untuk mendekripsi pesan yang dienkripsikan melalui kunci bertingkat tersebut.

LANDASAN TEORI

1. Kriptografi

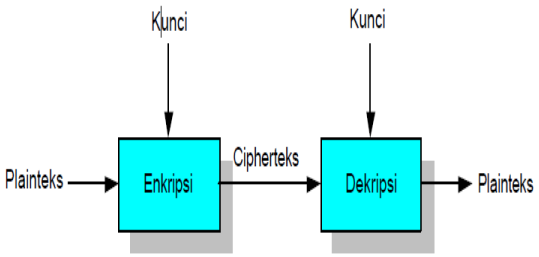
a. Definisi

Menurut Schneier (1996) mengemukakan "*Cryptography is the art and science of keeping messages secure"* yang artinya adalah ilmu dan seni untuk menjaga keamanan pesan. Sedangkan menurut Rinaldi Munir (2006) menyatakan Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Berdasarkan pendapat tersebut dapat disimpulkan bahwa kriptografi adalah ilmu dan seni merahasiakan pesan dengan menggunakan fungsi matematis.

b. Terminologi

Beberapa istilah yang penting untuk diketahui diberikan di bawah ini (Rifki Sadikin, 2012) :
- *Plaintext* adalah data atau informasi yang dapat dibaca dan dimengerti maknanya.
- *Ciphertext* adalah bentuk pesan yang tersandi/pesan tidak terbaca atau tidak dipahami.
- Enkripsi adalah Proses menyandikan plainteks menjadi cipherteks
- Dekripsi adalah proses mengembalikan cipherteks menjadi plainteks semula.
- Key/kunci adalah parameter yang digunakan untuk transformasi *enciphering* dan dechipering. Kunci biasanya berupa string atau deretan bilangan (Ranjan Bose, 2008)

Adapun proses cara kerja kriptografi dapat dilihat pada gambar berikut.



Gambar 1. Topologi Enkripsi dan dekripsi

Pada gambar di atas dapat dijelaskan bahwa pesan asli (plainteks) dienkripsikan melalui kunci. Hasil dari enkripsi adalah berupa cipherteks yaitu pesan yang tidak terbaca. Untuk membuka pesan yang tidak terbaca tersebut (chiperteks) maka pesan tersebut dienkripsikan dengan kunci yang sama sehingga menghasilkan pesan teks yang dapat dibaca (plainteks).

2. 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 boleh jadi 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. Dibawah ini adalah gambar *vigenere tableau* yang digunakan untuk enkripsi dan dekripsi suatu teks.

	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 (vigenere tableau*)

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 =

$$M_i = D_K(C_i) = (C_i - K_i) \mod 26$$

Dimana :
C = Chipertex
K= Key
M = Plaintext
E = encrypt
D = decrypt

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

Pesan : SAYA SUKA KAMU
Kunci : CINTA

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 : S A Y A S U K A K A M U
Kunci : C I N T A C I N T A C I
Cipherteks : U I M T S W S N E A O D

PEMBAHASAN

Teknik Veigenere Cipher

Seperti yang telah diuraikan sebelumnya, dalam melakukan enkripsi pada metode ini dilakukan dengan bantuan table *vigenere tableau*. Keunggulan dari *vigenere cipher* dari metode klasik sebelumnya (*Caesar cipher*) bahwa substitusi untuk ciphrenya bersifat *polyalphabetic*, dimana satu karakter yang sama mempunyai karakter substitusi yang berbeda. Seperti pada contoh di bawah ini :

Plainteks : S A Y A S U K A K A M U
Kunci : C I N T A C I N T A C I
Cipherteks : U I M T S W S N E A O D

Dari karakter plainteks tersebut di atas terdapat karakter yang sama yaitu "A" sebanyak empat. Namun hasil cipherteksnya berbeda (A1=I, A2=t, A3=n, A4=a). Namun demikian pada metode vigenere ini terdapat beberapa kelemahan yaitu pada plainteks karakter A selalu mendapatkan hasil karakter yang sama antara kunci dan cipherteksnya seperti pada contoh di atas (A1:k=I, c=i, A2:k=t,c=t, A3:k=n, c=n dan A4:k=a, c=a). Kelemahan selanjutnya adalah jumlah karakter kunci yang dibuat harus sama dengan jumlah karakter plainteksnya dikarenakan untuk menentukan cipherteks harus melalui perpotongan baris (*key*) dan kolom (*plaintext*) pada table *vigenere*. Akibatnya karakter kunci mengalami pengulangan 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.

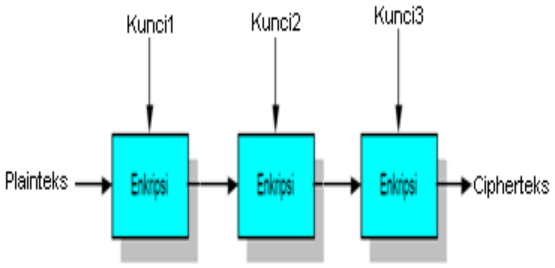
Contoh :
Plainteks : BILA SAYA BILANG SUKA
Kunci : MANA MANA MANAMA NAMA
Cipherteks : NIYA EALA NIYAZG FUWA

Dari contoh diatas dapat diketahui, bahwa 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 (Fatardhi Rizky Andhika,2011).

Teknik Vigenere Cipher dengan Kunci Berlapis

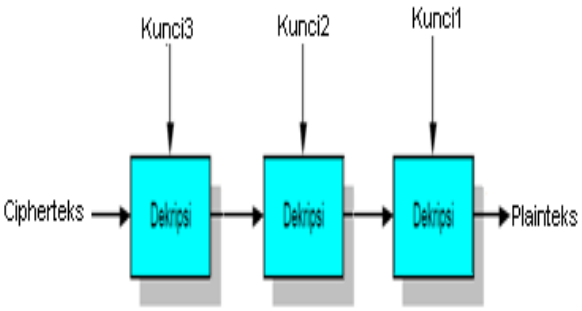
Untuk menghindari kelemahan tersebut di atas, maka perlu adanya teknik untuk dapat meningkatkan kekuatan dari hasil chiperteks *vigenere* ini. Salah satunya adalah dengan cara membuat kunci lebih dari satu. Dengan dibuatkanya kunci lebih dari satu (kunci berlapis) maka kelemahan yang telah penulis uraikan seperti tersebut di atas dapat teratasi. Dalam penelitian ini penulis mencoba membuat lapisan kunci sebanyak tiga lapisan.

Adapun proses enkripsi pada vigenere cipher dengan kunci berlapis dapat dilihat pada gambar di bawah ini :



Gambar3 : Enkripsi dengan tiga lapisan kunci

Sedangkan proses dekripsi dapat dilihat pada gambar berikut ini :



Gambar4 : Dekripsi dengan tiga lapisan kunci

Untuk lebih jelasnya mengenai penerapan *vigenere* dengan tiga lapisan kunci dapat dicontohkan sebagai berikut :

Plainteks : SAYA SUKA KAMU
KUNCI1 : CINTA
KUNCI2 : BENCI
KUNCI3 : SUKA

Dari contoh tersebut dapat diproses sebagai berikut :

Plainteks	: S A Y A S U K A K A M U
Kunci1	: C I N T A C I N T A C I
Enkripsi1	: U I M T S W S N E A O D
Kunci2	: B E N C I B E N C I B E
Enkripsi2	: V M Z V A X W A G I P H
Kunci3	: S U K A S U K A S U K A
Enkripsi3	: N G J V S R G A Y C Z H

Berdasarkan contoh diatas dapat dijelaskan bahwa hasil dari enkripsi dari kunci pertama menjadi plainteks untuk enkripsi pada kunci kedua, hasil enkripsi pada kunci kedua menjadi plainteks pada kunci ketiga. Dan hasil enkripsi kunci ketiga merupakan cipherteks akhir. Dari hasil cipherteks yang terakhir dapat diketahui bahwa pihak-pihak tertentu terutama *cryptanalyst* akan sulit mendekripsikan pesan tersebut diatas. Hal ini dikarenakan adanya kunci berlapis yang dibuat sebanyak tiga, sedangkan *cryptanalyst* dapat menduga bahwa kunci yang dibuat pada contoh diatas adalah kunci standar yaitu hanya satu lapisan saja dan menghasilkan plainteks yang masih belum bisa dibaca.

KESIMPULAN

Keamanan akan suatu informasi patut dirahasiakan sedemikian rupa. Pengamanan pesan dapat dilakukan dengan berbagai metode enkripsi. Dari hasil penelitian ini didapat bahwa pengamanan pesan melalui metode vigenere cipher dengan penggunaan kunci secara berlapis dapat meminimalisir kelemahan yang terjadi pada metode *vigenere cipher* terutama dengan menggunakan metode kasiski. Namun demikian

metode dengan kunci berlapis ini masih memungkinkan dapat dipecahkan jika jumlah lapisan kunci diketahui terlebih dahulu oleh *cryptanalyst.*

DAFTAR PUSTAKA

[1] Andi Kurniawan Dwi.P, 2011, Penerapan Algoritma Vigenere Cipher pada Aplikasi SMS Android, Makalah IF3058 Kriptografi, ITB, Bandung

[2] Dony Ariyus, 2008, Pengantar Ilmu Kriptografi, Teori, Analisis dan Implementasi, Andi Offset, Yogyakarta

[3] Mark .L. Murphy, Android Programming Tutorials, OmmonsWare, 2011

[4] Ranjan Bose, 2008, Information Theory, Coding And Cryptography, Mc Graw Hill

[5] Rifki Sadikin, 2012, Kriptografi Untuk Keamanan Jaringan, Andi Offset, Yogyakarta

[6] Rinaldi Munir,2006, Kriptografi, Informatika, Jakarta

[7] Rudy Hendryanto dan A.Ramadona Nilawati, 2012, Program Aplikasi Enkripsi dan Dekripsi SMS pada Ponsel Berbasis Android dengan Algoritma DES, Prosiding Seminar Nasional Komputer dan Sistem Intelijen (KOMMIT 2012), Universitas Gunadarma, Jakarta

[8] Schneier, Bruce, 1996, Aplied Cryptography 2nd, John Wiley & Son

[9] Fatardhi Rizky Andhika, 2011, Modifikasi Vigenere Cipher dengan Menggunakan Caesar Cipher dan Enkripsi Berlanjut untuk Pembentukan Key-nya, Makalah IF3058 Kriptografi, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.