INFORMATIKA Mulawarman | Februari 2014 Vol. 9 | No. 1
ISSN 1858-4853

APLIKASI *CHATTING* RAHASIA MENGGUNAKAN ALGORITMA *VIGENERE CIPHER*

Pricilia Yulianingsih[1)], Hamdani[2)], Septya Maharani[3)]

[1,2,3)]Program Studi Ilmu Komputer, FMIPA, Universitas Mulawarman
Email : tulangikan30@gmail.com[1)], hamdani@unmul.ac.id[2)], septyamaharani@yahoo.com[3)]

ABSTRAK

Pada lingkungan kompetitif sekarang ini,memungkinkan manusia dapat berkomunikasi dan dapat bertukar informasi/data secara jarak jauh. Antar kota, Negara maupun antar benua bukan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi. Algoritma *vigenere cipher* merupakan salah satu metode kriptografi untuk penyandian teks. Penelitian ini bertujuan untuk membuat suatu aplikasi kriptografi yang dapat menyandikan teks dan mengirimkan teks yang terenkripsi melalui jaringan berdasarkan algoritma *vigenere cipher*. Aplikasi ini melakukan kriptografi pada teks berupa huruf, angka dan simbol. Kunci yang digunakan berupa alfanumerik yang merupakan gabungan huruf, angka dan simbol. Hasil dari penelitian ini adalah berupa aplikasi yang dapat melakukan pengiriman pesan teks yang telah terenkripsi melalui jaringan LAN (*Local Area Network*) sehingga kerahasiaan dari pesan tersebut dapat terjaga keamanannya.

Kata kunci: kriptografi, LAN, teks, *vigenere cipher*.

PENDAHULUAN

Kriptografi adalah seni dan ilmu pengetahuan untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan kepada pengguna *(user)* yang hanya memiliki sebuah kunci untuk mengubah kode tersebut. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi *(cipher)* adalah proses dimana informasi atau data yang hendak dikirim dan diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awal dengan menggunakan algoritma tertentu. Dekripsi *(plain)* adalah kebalikan dari enkripsi *(cipher)* yaitu mengubah kembali bentuk informasi atau data tersamar tersebut menjadi informasi awal. [1]

Kriptografi saat ini telah menjadi salah satu syarat penting dalam keamanan teknologi informasi terutama dalam pengiriman pesan rahasia. Pengiriman pesan rahasia sangat rentan terhadap serangan yang dilakukan oleh pihak ketiga, seperti penyadapan, pemutusan komunikasi, pengubahan pesan yang dikirim, dan lain-lain. [3]

Untuk menghindari terjadinya penyadapan tersebut adalah dengan menyandikan pesan sehingga bentuk pesan menjadi teracak dan tidak dimengerti lagi maknanya. Salah satu metode penyandian untuk tujuan di atas adalah menggunakan teknik penyandian dengan algoritma *Vigenere Cipher*.

METODE PENELITIAN

a. Vigenere Cipher

Vigenere Cipher adalah suatu algoritmca yang tergolong ke dalam algoritma subtitusi abjad majemuk. Ini artinya setiap huruf yang sama dalam *plaintext* tidak dipetakan atau disubtitusi oleh satu huruf. Melainkan di subtitusi oleh huruf yang berlainan bergantung dari kunci yang digunakan untuk melakukan enkripsi. *Vigenere Cipher* merupakan bentuk sederhana dari sandi substitusi polialfabetik. Algoritma ini ditemukan oleh diplomat sekaligus kriptologis dari Prancis, *Blaise de Vigenere* pada abad 16. *Vigenere Cipher* dipublikasikan pada tahun 1856, tetapi algoritma ini baru dikenal luas 200 tahun kemudian. *Vigenere Cipher* sangat dikenal karena mudah dipahami dan diimplementasikan. *Cipher* menggunakan bujursangkar *Vigenere Cipher* yang dapat dilihat pada tabel 1. [5]

Kolom paling kiri menyatakan huruf-huruf kunci sedangkan baris paling atas menyatakan huruf-huruf *plaintext*. Setiap baris dalam bujursangkar menyatakan huruf-huruf *ciphertext* yang diperoleh dengan *Caesar Cipher*, yang mana jauh pergeseran huruf *plaintext* ditentukan nilai numerik huruf kunci tersebut (yaitu, a = 0, b = 1, c = 2, …, z = 25).

Bujursangkar *Vigenere* digunakan untuk memperoleh *ciphertext* dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek daripada panjang *plaintext*, maka kunci

diulang penggunaannya (sistem periodik). Bila panjang kunci adalah m, maka periodenya dikatakan m. [2]

	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

Tabel 1. Bujursangkar *Vigenere*

Untuk melakukan enkripsi dengan *Vigenere Cipher*, pada bujursangkar *vigenere* tarik garis vertikal dari huruf *plaintext* ke bawah, lalu tarik garis mendatar dari huruf kunci ke kanan. Perpotongan kedua garis tersebut menyatakan huruf *ciphertext*nya. Secara matematis proses enkripsi dinyatakan dengan persamaan :

$$c_i = (p_i + k_r) \bmod 26$$

keterangan :
c_i = cipherteks (hasil teks terenkripsi)
p_i = plainteks (teks asli)
k_r = kunci

Sebagai contoh kalimat THIS PLAINTEXT akan dilakukan proses enkripsi dengan menggunakan kunci sony. Perhitungan huruf T dienkripsi dengan kunci s :

(T + s) mod 26 = (19 + 18) mod 26 = 11 = L

Hal sama dilakukan untuk semua huruf, sehingga dihasilkan :
Plainteks : THIS PLAINTEXT
Kunci : sony sonysonys
Cipherteks : LVVQ HZNGFHRVL

Dekripsi dilakukan dengan cara yang berkebalikan, yaitu menarik garis mendatar dari huruf kunci sampai ke huruf cipherteks yang dituju, lalu dari huruf cipherteks tarik garis vertikal ke atas sampai ke huruf plainteks. Secara matematis proses dekripsi dinyatakan dengan persamaan :

$$p_i = (c_i - k_r) \bmod 26$$

keterangan :
c_i = *cipher* teks (hasil teks terenkripsi)
p_i = *plain* teks (teks asli)
k_r = kunci

Perhitungan huruf T didekripsi dengan kunci s sebagai :

(L - s) mod 26 = (11 - 18) mod 26 = 19 = T

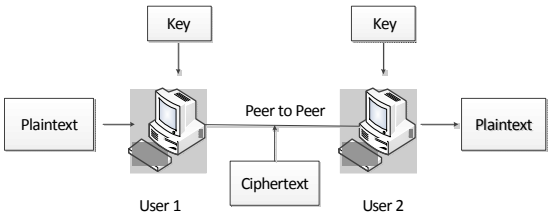
Hal yang sama dilakukan untuk semua huruf, sehingga dihasilkan:
Cipherteks : LVVQ HZNGFHRVL
Kunci : sony sonysonys
Plainteks : THIS PLAINTEXT

b. Jaringan LAN

Jaringan LAN adalah istilah yang digunakan oleh warga Indonesia yang memiliki arti yaitu Jaringan Wilayah Lokal atau dalam bahasa inggris LAN *(Lokal Area Network)*, adalah jaringan komputer yang hanya mencakup wilayah kecil, seperti jaringan komputer kampus, warnet, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil. Jaringan LAN memiliki 2 tipe, yaitu *client/server* dan *peer to peer*. *Client/server* adalah suatu model jaringan komputer yang memiliki *client* dan *server*. Sedangkan *Peer to peer* adalah model jaringan dimana komputer dengan komputer lain saling berhubungan dalam sebuah jaringan dan memiliki kedudukan yang sama. [4]

PENELITIAN DAN PEMBAHASAN

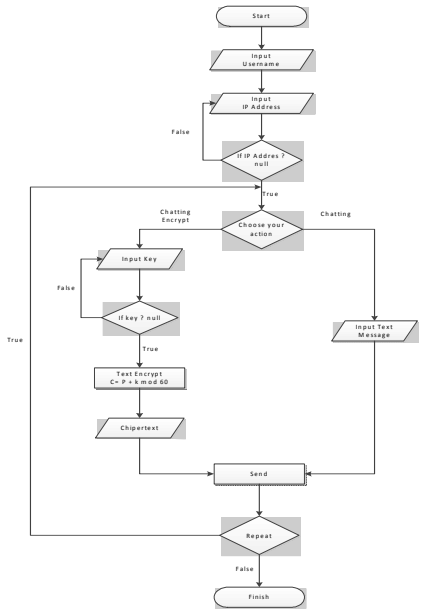
Sistem Kriptografi aplikasi *chatting* rahasia menggunakan algoritma *Vigenere Cipher* merupakan salah satu teknik pengamanan data dari pihak yang tidak berwenang, khususnya berupa data teks yang disebut sebagai pesan. Bentuk pesan yang telah dienkripsi akan menjadi teracak dan tidak dapat dibaca maupun dikenali tanpa proses dekripsi terlebih dahulu. Pesan yang telah diacak berupa *chipertext* dikirimkan melalui jaringan LAN (*Local Area Network*) secara *peer to peer* dari *user* 1 ke *user* 2. Sistem kriptografi teks melalui jaringan LAN terdapat pada gambar 1. [6]



Gambar 1. Sistem Kriptografi Teks

Proses *Sender*

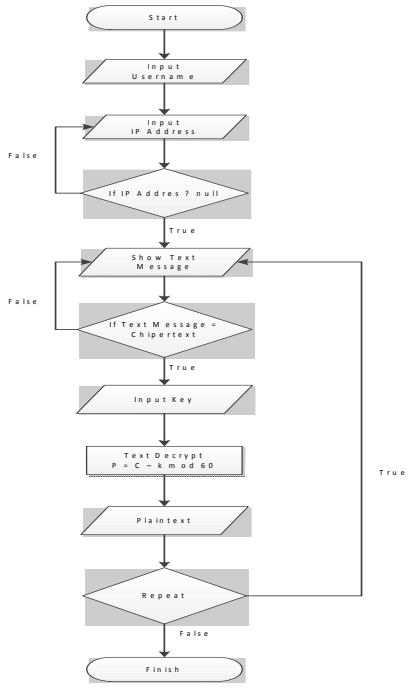
Sender merupakan penggambaran proses enkripsi pada sebuah teks. Pada proses ini teks asli (*plaintext*) disandikan menggunakan sebuah kunci tertentu kemudian dikirim berupa *ciphertext* atau teks yang terenkripsi saat proses pengiriman berlangsung. Proses pada *sender* dapat dilihat pada *flowchart sender* yang ditunjukkan pada gambar 2. [6]



Gambar 2. Flowchart Sender

Proses *Receiver*

Proses *receiver* ini merupakan penggambaran dekripsi teks yang terenkripsi. Dekripsi merupakan kebalikan dari proses enkripsi, yaitu penyandian kembali *cipher*text (teks terenkripsi) menjadi *plain*text (pesan asli) dengan menggunakan kunci yang sama saat melakukan proses enkripsi. Jika kunci yang digunakan tidak sesuai, maka pesan tidak akan kembali seperti semula. Proses pada *receiver* dapat dilihat pada *flowchart receiver* yang ditunjukkan pada gambar 3. [6]



Gambar 3. *Flowchart Receiver*

IMPLEMENTASI SISTEM

a. Impelementasi Proses *Sender*

Proses *sender* menjelaskan cara kerja sistem ketika mengirimkan pesan teks yang terenkripsi. Pada saat menjalankan program, hal yang dilakukan *user* pertama kali adalah memasukkan *username* sebagai identitas pengirim. Kemudian memasukkan alamat IP yang dituju untuk melakukan pertukaran data. Setelah alamat IP *connect* kemudian *user* dapat mengetikkan pesan pada *textbox* yang tersedia, dengan memasukkan kunci pada *textbox key* dan memberi centang pada*cekbox encrypt* maka pesan rahasia dapat dikirimkan. Apabila *user* tidak mencentang *cekbox encrypt*, maka pesan yang dikirimkan berupa *plaintext* (teks asli). Hasil percakapan antara pengirim dan penerima pesan dapat dilihat pada *listbox conversation* yang tersedia. Pada tombol *clear all* berfungsi untuk menghapus semua percakapan antara pengirim dan penerima pesan yang berada di *listbox conversation*. Implementasi antarmuka *sender* dapat dilihat pada gambar 4.

Gambar 4. Implementasi Antarmuka Proses *Sender*

b. Implementasi Proses *Receiver*

Pada *flowchart receiver* menggambarkan bagaimana proses penerimaan pesan. Seperti halnya pada *flowchart sender*, *user receiver* dapat memasukkan *username* terlebih dahulu sebagai identitas penerima pesan. Kemudian *user* memasukkan alamat IP agar terhubung pada *user sender* sebagai pengirim pesan.

Selanjutnya *user* akan menerima pesan yang berupa *plaintext* dan *ciphertext.*

Jika pesan masuk berupa *plaintext* (teks biasa), maka *user* dapat melihat isi pesan tersebut pada *listbox conversation*. Apabila pesan yang diterima berupa pesan *ciphertext* (pesan acak), maka *user* dapat memasukkan kunci terlebih dahulu pada *textbox key*. Agar pesan dapat dibaca atau kembali seperti semula maka kunci yang digunakan adalah kunci yang sama pada saat proses enkripsi dari *user sender.* Selanjutnya *user* dapat memilih percakapan yang akan di dekripsi pada *listbox conversation* dengan menekan tombol dekripsi. *Flowchart receiver* dapat dilihat pada gambar 5. [6].

Gambar 5. Implementasi Antarmuka Proses *Receiver*

KESIMPULAN

Kesimpulan yang dapat diambil berdasarkan penelitian mengenai kriptografi menggunakan algoritma *Vigenere Cipher* untuk aplikasi *chatting* rahasia yaitu kriptografi merupakan salah satu cara yang dapat digunakan untuk mengamankan berbagai tipe file, salah satunya berupa pesan teks. Metode *Vigenere Cipher* merupakan metode perhitungan yang mudah untuk diterapkan dalam penyandian pesan teks baik berupa huruf, angka, maupun simbol. Dengan menggunakan metode *Vigenere Cipher* maka dapat dilakukan percakapan yang bersifat rahasia dengan menggunakan aplikasi *chatting*. Aplikasi *chatting* rahasia ini dapat diimplementasikan pada jaringan LAN.

DAFTAR PUSTAKA

[1] Hamdani. 2012. *Penerapan Metode Vigenere Cipher Pada Kriptografi Klasik Untuk Pesan Rahasia*. Volume 7 nomor 1 halaman 23. Ilmu Informatika Universitas Mulawarman. Samarinda.

[2] Munir, R. 2006. *Kriptografi*. Program Studi Teknik Informatika, ITB. Penerbit Informatika. Bandung.

[3] Nugraha, F. 2012. *Kriptografi Citra Digital Menggunakan Metode Hill Cipher*. Skripsi Ilmu Komputer Universitas Mulawarman. Samarinda.

[4] Tittel, E. 2002. *Computer Networking (JaringanKomputer).* Jakarta. Penerbit Erlangga.

[5] Wilson, I. P. 2006. A Modified Version of the Vigenère Algorithm. Volume 6 nomor 3B. Computing and mathematical Sciences, Texas A&M University-Corpus Christi, 78412 USA.

[6] Yulianingsih, P. 2013. *Kriptografi Menggunakan Algoritma Vigenere Cipher Untuk Aplikasi Chatting Rahasia.* Skripsi Ilmu Komputer Universitas Mulawarman. Samarinda.