IMPLEMENTASI ENKRIPSI DATA DENGAN ALGORITMA *VIGENERE CHIPER*

ABSTRAKS

Masalah keamanan data bagi organisasi atau perusahaan merupakan penting pada era informasi. Kerahasiaan data di perusahaan yang bergerak pada produksi, mendapat perhatian dari penulis untuk mengamankan data. Seharusnya data tersebut dapat dirahasiakan, berisi identitas pelanggan, yang didalamnya terdapat harga dan discount yang diberikan untuk pelanggan. Metode algoritma yang digunakan yaitu algoritma vigenere chipper. Keamanan data ini merupakan salah satu aspek yang sangat penting dalam penggunaan computer. Pemilik data tersebut tentunya ingin datanya aman terhadap gangguan dari berbagai tindakan yang tidak di inginkan, baik dari computer pribadi (PC) ataupun jaringan. Dalam kegiatan sehari-hari pelanggan adalah orang-orang yang kegiatannya membeli dan menggunakan suatu produk, baik barang maupun jasa, secara terus-menerus.

Kata Kunci: Vigenere Chiper, Enkripsi, Dekripsi, Chipertext, Plaintext, Harga

1. PENDAHULUAN

Masalah keamanan komputer merupakan sesuatu yang sangat penting dalam era informasi ini terutama bagi suatu organisasi atau perusahaan. Kerahasiaan data

Masalah keamanan komputer merupakan sesuatu yang sangat penting dalam era informasi ini terutama bagi suatu organisasi atau perusahaan. Kerahasiaan data merupakan sesuatu yang penting dalam keamanan data. Data pelanggan menjadi salah satu data yang sangat penting dalam kelangsungan berjalannya perusahaan.

Keamanan merupakan bentuk tindakan untuk mempertahankan sesuatu hal dari berbagai macam gangguan dan ancaman. Aspek yang berkaitan dengan suatu keamanan dalam dunia komputer, antara lain:

- *Privacy/Confidentiality* yaitu usaha menjaga
- informasi dari orang yang tidak berhak mengakses (menggaransi bahwa data pribadi tetap pribadi).
- *Integrity* yaitu usaha untuk menjaga data atau sistem tidak diubah oleh yang tidak berhak.
- *Authentication* yaitu usaha atau metoda untuk mengetahui keaslian dari informasi yang dikirim dibuka oleh orang yang benar (asli).
- *Availability* berhubungan dengan ketersediaan sistem dan data (informasi) ketika dibutuhkan.

Keamanan data ini merupakan salah satu aspek yang sangat penting dalam penggunaan komputer. Pemilik data tersebut tentunya ingin datanya aman terhadap gangguan dari berbagai tindakan yang tidak di inginkan, baik dari komputer pribadi (PC) ataupun jaringan.

1.1 Latar belakang Masalah

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*Cryptography is the art and science of keeping messages secure*). Kata “seni” di dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan. Cara-cara unik tersebut mungkin berbeda-beda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia pesan mempunyai nilai estetika tersendiri. Pada perkembangan selanjutnya, kriptografi berkembang menjadi sebuah disiplin ilmu sendiri karena teknik-teknik kriptografi dapat diformulasikan secara matematik sehingga menjadi sebuah metode yang formal.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, rumusan masalah yang dibuat adalah bagaimana merancang suatu perangkat lunak pengamanan data pelanggan yang dapat membantu mengamankan aplikasi program data pelanggan agar tidak dapat diketahui oleh pihak yang tidak bersangkutan.

1.3 Tujuan Penelitian

Tujuan penelitian antara lain yaitu:

- Untuk membuat system keamanan data pelanggan dengan menggunakan teknik enkripsi.
- Untuk keamanan dan kerahasiaan data pelanggan.

2. TINJAUAN PUSTAKA

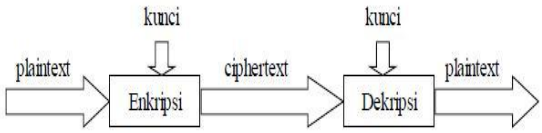
Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan (yang artinya apabila algoritma yang digunakan telah diketahui maka pesan sudah jelas "tidak terlindungi" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut), kriptografi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

2.1 Kriptografi

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/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. Untuk melihat ilustrasi dari proses kriptografi dapat dilihat pada gambar 1, mekanisme kriptografi.



Gambar 1. Mekanisme kriptografi

2.2 Vigenere Cipher

Vigenere Chiper termasuk dalam cipher abjad-majemuk (polyalphabetic substitution Chiper) yang dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigenere pada abad 16 (tahun 1586). *Vigenere Chiper* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kata kunci. *Vigenere Chiper* menggunakan tabel seperti pada tabel 1, *Vigenere Cipher* dengan angka. dalam melakukan enkripsi.

Teknik dari substitusi *vigenere cipher* bisa dilakukan dengan dua cara:

1. Angka
2. Huruf

Tabel 1. Vigenere Cipher dengan Angka

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika ditukar dengan angka, maka kunci dengan huruf " HA"

K = (7, 0, 17, 8)
Dan plaintext nya " SAYA HARIYANTO " akan menjadi
P = (18, 0, 24, 0, 7, 0, 17, 8, 24, 0, 13, 19, 14).

S	A	Y	A	H	A	R	I	Y	A	N	T	O
18	0	24	0	7	0	17	8	24	0	13	19	14
7	0	17	8	7	0	17	8	7	0	17	8	7
25	0	16	8	14	0	9	16	6	0	5	2	21

Chipertext yang dihasilkan:
Chipertext = (25, 0, 16, 8, 14, 0, 9, 16, 6, 0, 5, 2, 2)
Chipertext yang dihasilkan dengan huruf menjadi "

Untuk melakukan deskripsi, bisa juga digunakan modulo 26)

2.3 Vigenere Cipher Huruf

Tabel 2, *Vigenere Cipher dengan huruf* berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser ke kiri dari baris sebelumnya membentuk ke-26 kemungkinan sandi *Caesar* setiap huruf disediakan dengan menggunakan baris yang berbeda-beda sesuai kunci yang diulang.

Tabel 2. *Vigenere Cipher* Dengan Huruf

	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

Plantext: Says Hariyanto
Kunci: Hari
Dari *Plaintext* dengan kata kunci di tabel didapatkan *chipertext* sebagai berikut:

Chipertext: Zapioaiqfaebw
Proses dekripsi, dilakukan dengan mencari huruf chipertext pada baris *plaintext* dari kata kunci.

Dari contoh tabel, maka dapat disimpulkan bahwa rumus dari enkripsi dan dekripsi data *vigenere chiper* adalah:

Enkripsi: Ci = (Pi + Ki) mod 26

Dekripsi: Pi = (Ci – Ki) mod 26; untuk Ci > = Ki

Pi = (Ci+ 26 – Ki) mod 26; untuk Ci < = Ki