IMPLEMENTASI ENKRIPSI DATA DENGAN ALGORITMA *VIGENERE CHIPER*

Putu H. Arjana[1], Tri Puji Rahayu [2],Yakub[3], Hariyanto[4]
Program Studi Teknik Informatika, STMIK Dharma Putra Tangerang
Jl. Otto Iskandardinata No.80 Kota Tangerang 15113
E-mail: contax_tri_puji@yahoo.com

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

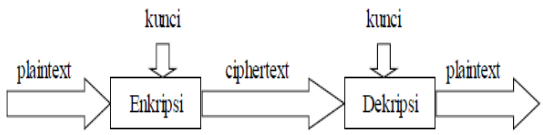
Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan (yang artinya apabila algoritma yang digunakan telah diketahui maka pesan sudah jelas "tidak terlindungi" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut), kriptografi 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

Keterangan:
C = Chiphertext
P = Plaintext
K = Kunci

2.4 Pengertian Pelanggan

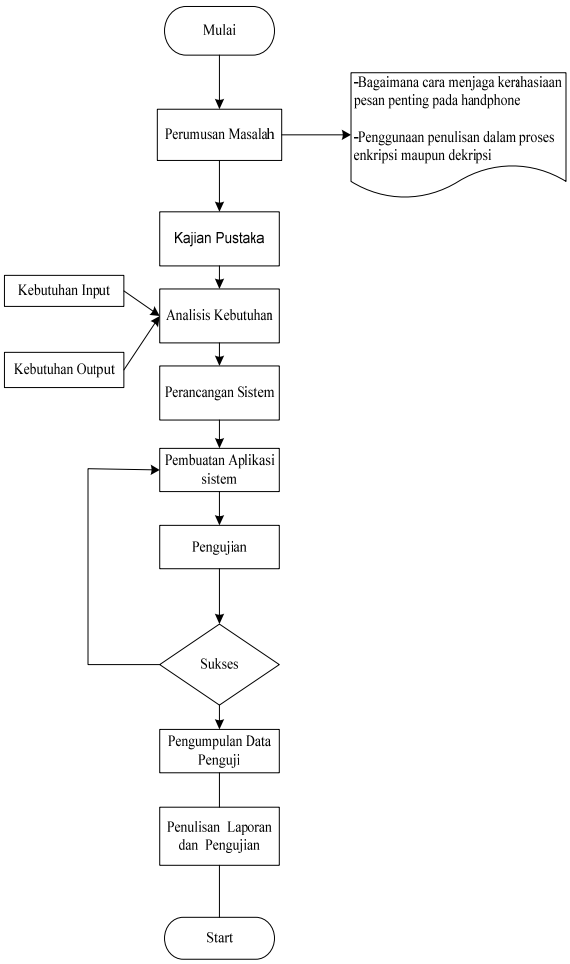
Dalam kegiatan sehari-hari pelanggan adalah orang-orang yang kegiatannya membeli dan menggunakan suatu produk, baik barang maupun jasa, secara terus-menerus.

Dilihat dari segi perbaikan kualitas, sefinisi pelanggan adalah setiap orang yang menuntut pemberian jasa (perusahaan) untuk memenuhi suatu standar kualitas pelayanan tertentu, sehingga dapat memberi pengaruh pada performansi (performance) pemberi jasa (perusahaan) tersebut.

3. METODOLOGI

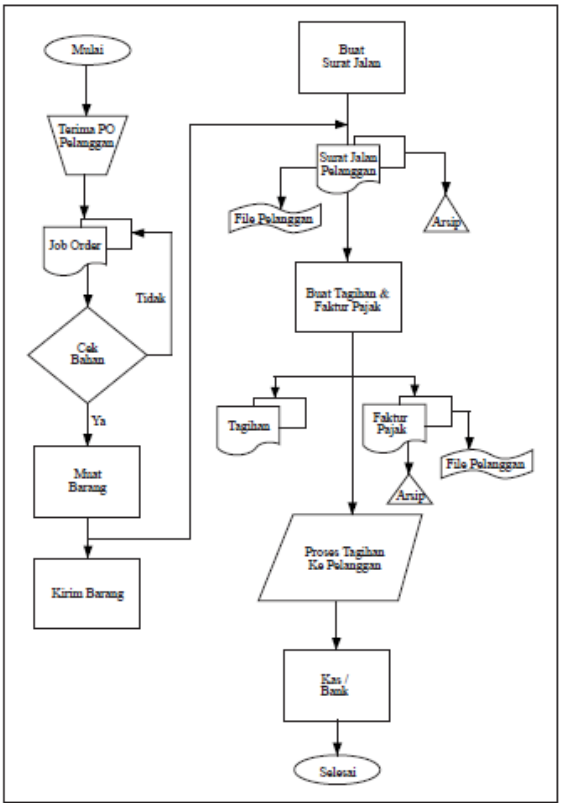
3.1 Kerangka Pemikiran

Secara umum, metode penelitian yang digunakan penulis tersusun dalam suatu diagram alir penelitian seperti dibawah ini. Diagram ini memperlihatkan tahap-tahap proses penelitian yang dilakukan penulis mulai dari tahap awal sampai gerak akhirnya kegiatan penelitian, kerangka pemikiran penelitian ini dapat dilihat pada gambar 2, tentang kerangka pemikiran dan *flowchart* pada gambar 3.



Gambar 2. Keangka pemikiran

Flowchart adalah penggambaran secara grafik dari langkah-langkah dan urut- urutan prosedur dari suatu program. Selain itu juga menggambarkan *file* yang dipakai sebagai input dan *output*, *flowchat* dapat dilihat pada gambar 3 tentang *flowchart.*



Gambar 3. Flowchart

3.2 Rancangan Sistem dan Sistem Yang Diusulkan

Karena lemahnya sistem keamanan dan kerahasiaan data yang masih dilakukan secara manual, maka perlu dibuat sistem informasi yang terkomputerisasi dengan membentuk keamanan dan kerahasiaan datanya dengan melakukan pengenkripsian data, sehingga tidak semua pegawai atau orang lain dapat melihat data pelanggan perusahaan.

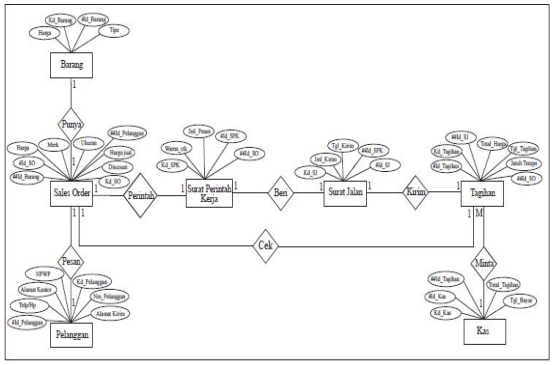
Sistem yang diusulkan penulis adalah, ketika *user* dan *admin* ingin memasukkan atau menambahkan data maka sebelum *admin* atau *user* menyimpan data tersebut maka *user* dan *admin* harus melakukan pengenkripsian data tersebut, sehingga ketka data tersebut tersimpan dalam *database*, maka data telah terenkripsi dan akan sangat sulit terbaca oleh orang yang tidak berkepentingan untuk membaca atau mengetahui informasi yang terdapat pada data yang telah tersimpan dalam database.

Dan ketika *user* atau *admin* ingin melihat data yang telah terenkripsi, maka ia harus mengembalikan kembali data tersebut dengan melakukan deskripsi data, sehingga *user* atau *admin* dapat membaca kembali informasi yang ingin ia

ketahui dari data pelanggan tersebut.

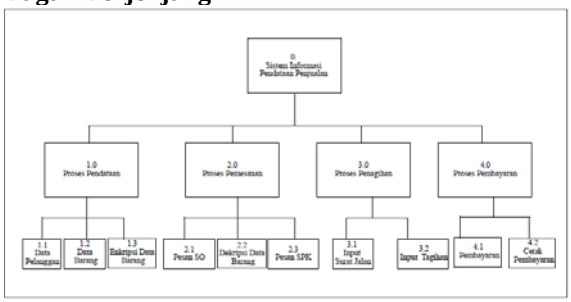
3.3 Entity Relationship Diagram

Entity Relationship Diagram merupakan suatu model jaringan yang menggunakan susunan data yang disimpan pada sistem secara abstrak. *Entity Relationship Diagram* menggambarkan hubungan antara satu entitas yang memiliki sejumlah atribut dengan entitas yang lain dalam suatu sistem yang terintegrasi. *Entity Relatioship Diagram* juga merupakan model konseptual yang dapat mendiskripsikan hubungan antara *file* yang digunakan untuk memodelkan struktur data serta hubungan antar data, *Entity Relatioship Diagram* dapat dilihat pada gambar 4.



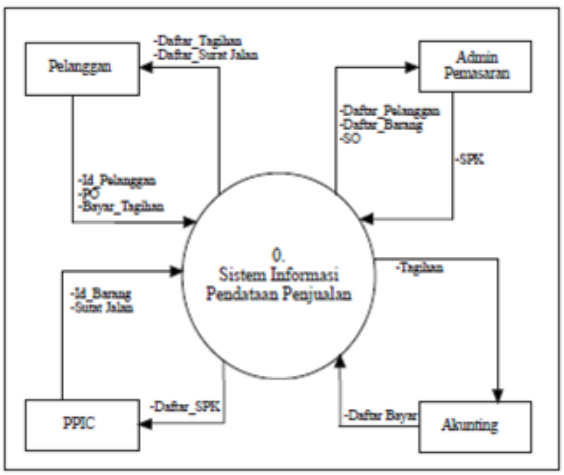
Gambar 4. Entity relatioship Diagram

Bagan Berjenjang

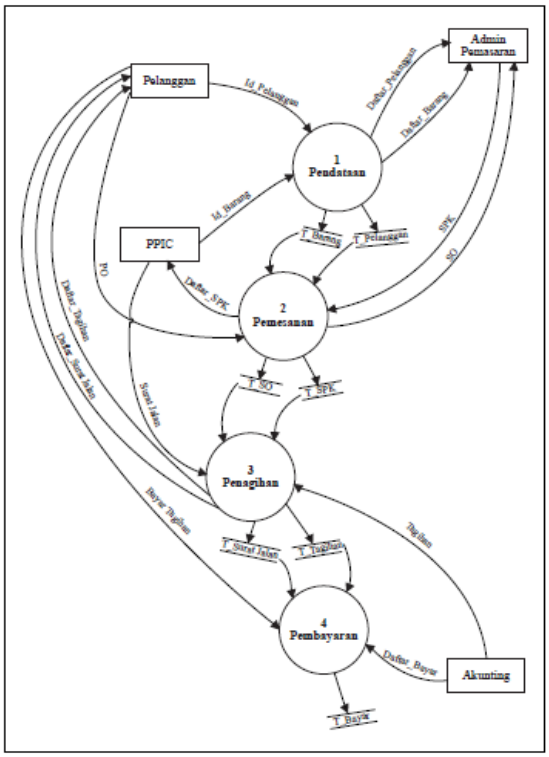


Gambar 5. Bagan Berjenjang

3.4 Contex Diagram

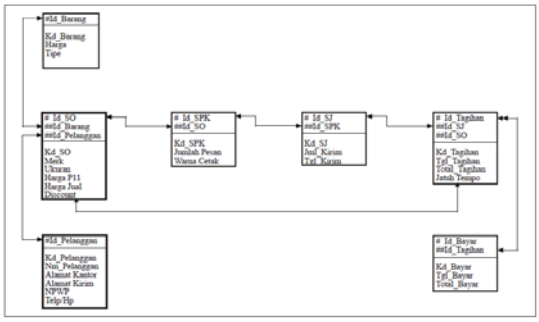


Gambar 6. *Contex Diagram*



Gambar 7. Data Flow diagram (DFD)

3.5 Logical Record Structure (LRS)



Gambar 8. Logical Record Structure (LRS)

4. ANALISA DAN IMPLEMENTASI

Proses Enkripsi

Proses enkripsi mempunyai beberapa langkah yaitu:

Misal: Nama Pelanggan: Prima Indah
Merk Dagang: Tissue Indah
Harga Box: Rp 3.400,-

Langkah 1:

Penggabungan beberapa huruf dari nama pelanggan dan merk dagang. Huruf urutan ke-3 dari depan nama pelanggan, ditambah huruf urutan ke-2 dari belakang merk dagang, ditambah huruf urutan ke -1 dari belakang nama pelanggan, ditambah huruf urutan ke- I dari depan merk dagang. Ini akan menjadi kata kunci pertama, sehingga menghasilkan:

K1 = (I, A, H, T).....(1)

Kunci K1 ini akan melakukan enkripsi vigenere

chiper dan akan menghasilkan enkripsi pertama

E1 = (Pi + K1) mod 26.....(2)
E1 = (XRPGIIUWIH).....(3)

Langkah 2:
Kunci pertama yang telah dihasilkan akan digeser atau ditambahkan sebanyak 3 digit.
Ini akan menjadi kata kunci K2, sehingga menghasilkan:

K2 = (K1 + 3) mod 26.....(4)
K2 = (M, D, K, V).....(5)

Kunci K2 ini akan melakukan enkripsi vigenere chiper dan akan menghasilkan enkripsi kedua.

E2 = (Pi + K2) mod 26.....(6)
E2 =(CUSIMLXYMK).....(7)

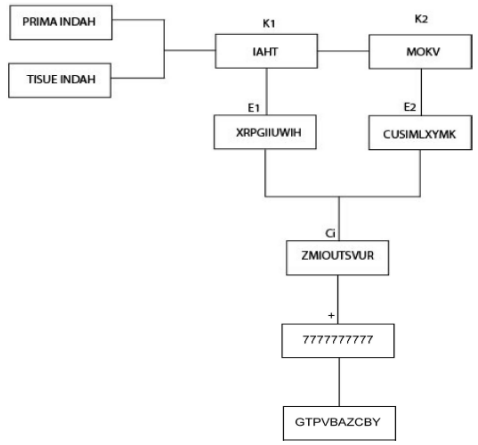
Langkah 3:
Akan dilakukan penggabungan kunci pertama dan kunci kedua.

Ci = (K1 + K2) mod 26.....(8)
Ci = (ZMIOUTSVUR).....(9)

Chipertext akan ditambahkan dengan jumlah harga perkarakter.

(ZMIOUTSVUR) + 7777777777 ....(10)
(GTPVBAZCBY).....(11)

Skema proses enkripsinya yaitu:



Gambar 9. Proses Enkripsi

4.1 Algoritma Enkripsi Vigenere Chiper

Tahapan-tahapan algoritma enkripsi dengan *Vigenere Chiper*:

Tahap 1:
a ← GetTextLen (plainteks)// Hitung jumlah array dari plaintext

Tahap 2:
B ← GetTextlen (kunci)//Hitung jumlah array dari kunci

Tahap 3:
X ← 0// isi variabel x dengan nilai 0
While x <= a
Begin
for j ← 1 to b do
begin

Tahap 4:
P ←Ord (plaintext [x]// Mengubah char menjadi kode ASCII

Tahap 5:
p ← p- 97// Kode ASCII diubah
(a menjadi 0)
Tahap 6:
k ← ord (kunci[j])// key menjadi ASCII

Tahap 7:
k ← k – 97 // Kode ASCII diubah (a menjadi 0) // operasi penambahan *plaintext* dengan *key*-nya.

Tahap 8:
c ←(p + k) mod 26 // operasi vigenere

Tahap 9:
Ciphertext ← Ciphertext + c // Tulis hasil ke dalam Ciphertext inc (x) // nilai x
ditambah 1
end
end

4.2 Algoritma Dekripsi Vigenere Chiper

Tahapan-tahapan algoritma dekripsi dengan *Vigenere Chiper*:

Tahap 1:
a ← GetTextLen (Ciphertext) //Hitung jumlah array dari *Ciph*
Tahap 2:
b ← GetTextLen (kunci) // Hitung jumlah array dari kunci
Tahap 3:
x ← 0 // isi variabel x dengan nilai 0
While x <= a
begin
for j ← 1 to b do
begin
Tahap 4:
c ← Ord (Ciphertext [x]) //Mengubah *char* menjadi kode *AS*
Tahap 5:
c ← c – 97 //Kode *ASCII* diubah (a menjadi 0)
Tahap 6:
k ← ord (kunci[j]) // key menjadi *ASCII*

Tahap 7:

k ← k – 97 //Kode *ASCII* diubah (a menjadi 0)

//operasi pengurangan *Ciphertext* dengan *key*-nya

Tahap 8:

p ← (c - k) mod 26 // operasi *Vigènere*

Tahap 9:

p ← p + 97 // K ode *ASCII* diubah menjadi huruf

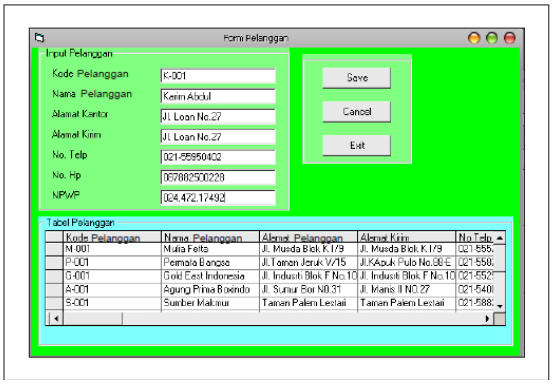
plaintext ← plaintext + p // Tulis hasil ke dalam *plaintext*

inc (x)

end end

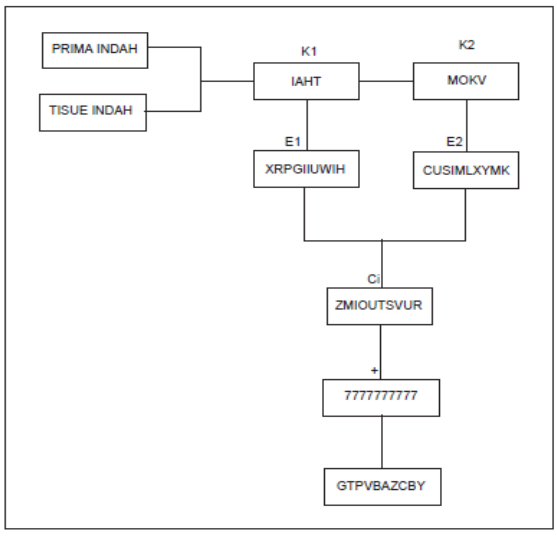
5. HASIL DAN PEMBAHASAN

5.1 Tabel Pelanggan



Gambar 10. Tabel Pelanggan

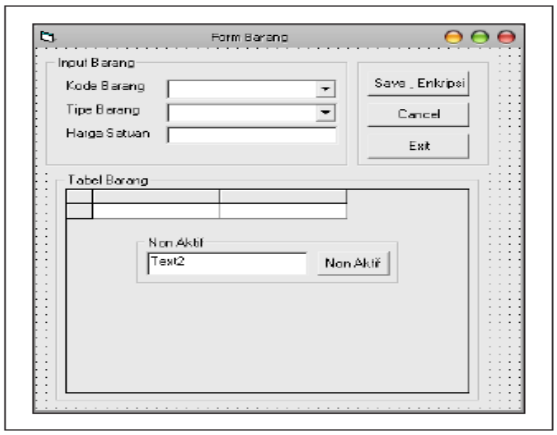
5.2 Proses Enkripsi



Gambar 11. Proses Enkripsi

5.3 Form Data Barang

Form Data Barang digunakan untuk memasukkan data barang. *Form* ini mempunyai kotak isi, kode barang, tipe barang dan harga satuan semua harus terisi dengan lengkap. Untuk menyimpan dan mengamankan data harga yang telah dimasukkan, *user* dapat mengklik tombol " *save & Enkrip* ", dan untuk membatalkan dapat mengklik tombol " *Cancel* " serta untuk keluar dari *form* ini dapat mengklik tombol " *Exit* " atau tanda (X) pada bagian kanan atas *form*.



Gambar 12. Data barang

5.4 Cara Pengujian

Untuk mengimplementasikan dan membuktikan bahwa program dan aplikasi sistem yang dibuat tepat guna maka penyusun melakukan pengujian terhadap aplikasi yang telah dibuat bersama-sama dengan pengguna atau Admin. Pengujian yang dilakukan terhadap program aplikasi ini bertujuan untuk memastikan apakah program aplikasi dapat berfungsi dengan baik dan sesuai dengan keinginan pengguna.

Tujuan lain dilakukan pengujian program aplikasi adalah untuk memperbaiki kesalahan-kesalahan yang ditemukan selama dilakukan pengujian dan selama sistem digunakan oleh pengguna.

6. KESIMPULAN

Setelah melalui tahap demi tahap perancangan program enkripsi data dengan algoritma *Vigenere Chiper* pada perusahaan, maka dihasilkan suatu kesimpulan yaitu:

- Implementasi program nkripsi data dengan *algoritma vigenere chiper* dapat meningkatkan tingkat keamanan pendataan penjualan, khususnya pada data harga.
- Implementasi program enkripsi data dengan *algoritma vigenere chiper* dapat meningkatkan keakuratan informasi, khususnya pada perhitungan harga jual.

DAFTAR PUSTAKA

Aryus, Doni,2007, Keamanan Multimedia, hlm 21, Penerbit Andi.

Aryus, Doni, 2007, Keamanan Multimedia, Penerbit Andi, hlm 191.

Munir, Rinaldi,2006, Kriptografi, Informatika, hlm 12.

Munir, Rinaldi, 2006, Kriptografi, Informatika, hlm 157.