APLIKASI KRIPTOGRAFI PESAN MENGGUNAKAN ALGORITMA VIGENERE CIPHER

Efrandi, Asnawati, Yupiyanti

Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139

ABSTRACT

The rapid advances in technology now makes a wide variety of communication servicesgrow by leaps and bounds. One of the most important thing in communication using computers and computer networks is to ensure the security of messages, data, orinformation in the data exchange process, thus becoming one of the drivers of the emergence of cryptography technology. Cryptographic algorithms based on dataencoding information that supports the needs of two aspects of information security, namely secrecy (protection of data confidentiality of information) and authenticity (protection against forgery and alteration of information that is not desirable. Application of theory-the theory gained in the college in making this application in order to implement an encrypted message to be more secure. In making the application of this cryptosystem, the method used is the Vigenere Cipher, one other form of encryption of type polyalphabetic. Applications created with Visual Basic 6.0 software and the creation of applications with encryption is expected to settlethe problems mentioned above

Keywords: Keywords: cryptography, Vigenere ciphe, Visual Basic 6.0

INTISARI

Kemajuan pesat dalam teknologi sekarang membuat berbagai layanan komunikasi tumbuh dengan pesat. Salah satu hal yang paling penting dalam komunikasi menggunakan komputer dan jaringan komputer adalah untuk menjamin keamanan pesan, data, atau informasi dalam pertukaran data, sehingga menjadi salah satu pendorong munculnya teknologi kriptografi. Algoritma kriptografi berdasarkan data pengkodean informasi yang mendukung kebutuhan dua aspek keamanan informasi, yaitu kerahasiaan (perlindungan kerahasiaan data informasi) dan keaslian (Perlindungan terhadap pemalsuan dan perubahan informasi yang tidak diinginkan.) Penerapan teori - teori yang diperoleh di perguruan tinggi dalam pembuatan aplikasi ini untuk melaksanakan pesan terenkripsi lebih aman. Dalam pembuatan aplikasi kriptografi ini, metode yang digunakan adalah Vigenere Cipher, salah satu bentuk lain dari enkripsi jenis poly abjad. Aplikasi dibuat dengan perangkat lunak Visual Basic 6.0 dan pembuatan aplikasi dengan enkripsi diharapkan untuk mengatasi permasalahan tersebut

Kata kunci: Kriptografi, Algoritma Vigenere, Visual Basic 6.0

I. PENDAHULUAN

Teknologi informasi berkembang semakin pesat dan mempengaruhi hampir seluruh aspek kehidupan manusia. Perkembangan tersebut secara langsung maupun tidak langsung mempengaruhi sistem perdagangan, transaksi, bisnis, perbankan, industri dan pemerintahan. Tentunya tingkat keamanan yang tinggi juga semakin diperlukan untuk menghindari penyadapan informasi yang mungkin saja terjadi. Terutama di era internet,

Semua informasi dikirim dengan bebas melalui suatu jaringan dengan tingkat keamanan yang relatif rendah. Untuk itulah peranan teknologi keamanan informasi benar-benar dibutuhkan. Salah satu cara yang bisa digunakan adalah menyandikan (mengenkripsi) informasi atau data rahasia yang akan dikirim, sehingga walaupun pihak yang tidak berkepentingan dapat membaca informasi tersebut, pihak tersebut tetap sulit bahkan tidak dapat memahami isi informasi tersebut.

Pada awalnya metode kriptografi pesan yang digunakan masih bersifat umum. Dimana kunci yang digunakan sama untuk proses enkripsi dan dekripsi. Namun terdapat suatu kendala dari metode ini yaitu pentingnya mendistribusikan kunci yang digunakan dalam keadaan aman. Sebuah cara tepat telah ditemukan untuk mengatasi kelemahan ini, yaitu dengan suatu

model enkripsi yang tidak memerlukan sebuah kunci untuk didistribusikan.

Metode ini dikenal dengan nama kunci publik (public-key) yang pertama kali diperkenalkan pada tahun 1976.

Sandi Vigenère sebenarnya merupakan pengembangan dari sandi Caesar. Pada sandi Caesar, setiap huruf teks terang digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi Caesar dengan geseran 3, A menjadi D, B menjadi E and dan seterusnya. Sandi Vigenère terdiri dari beberapa sandi Caesar dengan nilai geseran yang berbeda. Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut tabel Vigenère, tabel Vigenère berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, membentuk ke-26 kemungkinan sandi Caesar. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang. Sandi

ini dikenal luas karena cara kerjanya mudah dimengerti dan dijalankan, dan bagi para pemula sulit dipecahkan.

II. TINJAUAN PUSTAKA

A) Pengertian Aplikasi

Menurut (Supriyanto, 2005,117) "Aplikasi adalah program yang memiliki aktivitas pemrosesan perintah yang diperlukan untuk melaksanakan permintaan pengguna dengan tujuan tertentu". Sedangkan menurut Janner "Aplikasi adalah program atau sekelompok program yang dirancang untuk digunakan oleh pengguna akhir (*end user*)". Aplikasi dapat dimanfaatkan untuk keperluan pembelajaran kepada siswa mengingat dalam suatu proses pembelajaran seharusnya terdapat interaksi antar komponen-komponen pembelajaran. (Irvan, 2013:2).

B) Kriptografi

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mengajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (A. Menezes, P. Van Oorschot and S. Vanstone – Handbook of Applied Cryptography). Sedangkan menurut Kaufman et. al. (2002) menjelaskan bahwa kata Kriptografi berasal dari bahasa yunani dan memiliki makna seni dalam menulis pesan rahasia (*The art of secret writing*), dimana kriptografi terdiri dari 2 kata yaitu *κρυπτο* ψανγ yang berarti *rahasia* atau *tersembunyi* dan *γραφη* yang berarti *tulisan.* (Apriandala, 2013: 114).

Ada empat tujuan mendasar dari ilmu kriptograpi ini juga merupakan aspek keamanan informasi yaitu Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi. Integritas data adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak- pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubtitusian data lain kedalam data yang sebenarnya. Autentikasi adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasiitu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian isi datanya, waktu pengiriman dan lain-lain. Non- repudiasi atau penyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan atau membuat.

Kriptografi memiliki 4 komponen utama yaitu :

1) *Plaintext,* yaitu pesan yang dapat dibaca.
2) *Ciphertext,* yaitu pesan sandi/ pesan acak yang tidak bisa dibaca.
3) *Key,* yaitu kunci untuk melakukan teknik kriptografi.
4) *Algoritma,* yaitu metode untuk melakukan enkripsi dan dekripsi.

Proses – proses dasar kriptografi dibagi menjadi dua bagian, yaitu Enkripsi (*Encryption*) dan Dekripsi (*Decryption*).

Adapun contoh Teknik Kriptografi Klasik, yaitu :

1) Subtitusi yaitu teknik ini mengganti satu atau sekumpulan bit pada blok plainteks tanpa mengubah urutannya.
2) Transposisi yaitu teknik ini memindahkan posisi bit pada blok plainteks berdasarkan aturan tertentu

Sedangkan contoh dari Teknik Kriptografi Modern sendiri yaitu :

1) Kriptografi Simetris, yaitu teknik enkripsi dan dekripsi dengan teknik atau metode atau kunci yang sama.
2) Kriptografi Asimetris, yaitu teknik enkripsi dan dekripsi dengan dua kunci yaitu kunci public (*Public key*) dan kunci rahasia (*Private key*).
3) Kriptografi Hibrid, yaitu teknik enkripsi dan dekripsi dua lapis, maksudnya setelah file di enkripsi kemudian dilakukan enkripsi sekali lagi begitu sebaliknya.

C) Algoritma Vigenere Cipher

Hallim (2010: 3) Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku La Cifra del Sig. Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553.

Cara kerja dari Vigenère cipher ini mirip dengan Caesar cipher, yaitu mengenkripsi plainteks pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet. Vigenère cipher adalah salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjad-majemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda, tidak seperti Caesar cipher yang menerapkan metode substitusi abjad-tunggal yang semua huruf di suatu pesan dienkripsi menggunakan kunci yang sama.

Sebagai contoh Caesar cipher jika terdapat plainteks:

MAKALAH KRIPTOGRAFI

Maka jika dienkripsi dengan dengan nilai kunci 2 akan didapat cipherteks:

OCMCNCJ MTKRVQITCHK

Dari cipherteks yang didapat dapat kita lihat bahwa huruf M dienkripsi menjadi O, huruf A dienkripsi menjadi huruf C, dan seterusnya dimana huruf pada pesan digeser sejauh nilai kunci. Algoritma Caesar cipher sangat sederhana sehingga sangat berisiko untuk dipecahkan karena hanya dibutuhkan pengetahuan satu huruf dari plainteks untuk mengetahui kunci yang digunakan. Vigenère cipher yang menerapkan metode substitusi abjad-majemuk tidak memiliki permasalahan tersebut karena setiap huruf pada pesan yang dienkripsi dengan Vigenère cipher ini akan digeser dengan nilai yang berbeda tergantung dengan kunci yang diberikan. Kunci yang digunakan pada Vigenère cipher berbeda denganyang digunakan pada Caesar cipher. Jika pada Caesar cipher kuncinya hanya satu nilai saja, maka pada Vigenère cipher kunci yang digunakan berbentuk deretan huruf. Kunci yang berbetuk deretan kata tersebut akan memungkinkan setiap huruf plainteks untuk dienkripsi dengan kunci yang berbeda. Jika panjang kunci yang digunakan lebih pendek dari panjang plainteks maka kunci akan diulang sampai panjang kunci sama dengan panjang plainteks. Algoritma ini akan meminimalkan kemungkinan dipecahkannya cipherteks jika satu huruf plainteks diketahui.

Model matematika dari enkripsi pada algoritma Vigenère cipher ini adalah seperti berikut :

$$C_i = E_k (M_i) = (M_i + K_i) \bmod 26$$

Dan model matematika untuk deskripsinya adalah:

$$M_i = D_k (C_i) = (C_i - K_i) \bmod 26$$

Dengan C memodelkan cipherteks, M memodelkan Plainteks, dan K memodelkan kunci.

Contoh dari penerapan algoritma Vigenère cipher adalah jika kita memiliki sebuah plainteks yang ingin dienkripsi:

MAKALAH KRIPTOGRAFI

Dan kita menggunakan kunci:

TUGAS

Maka plainteks akan dienkripsi dengan cara:

Plaintext : MAKALAH KRIPTOGRAFI
Kunci : TUGASTU GASTUGASTUG
Ciphertext : FUQADTB QRAINUGJTZO

Huruf pada kunci akan dikonversi menjadi sebuah nilai, misalnya A = 0, B = 1, sampai dengan Z = 25. Setelah itu prosesnya sama seperti pada Caesar cipher dimana setiap huruf pada plainteks akan digeser sejauh nilai kunci yang posisinya bersesuaian. Pergeseran huruf-huruf ini bisa dipetakan dalam bentuk tabel 26x26 yang memetakan antara huruf pada plainteks dengan huruf pada kunci seperti yang diperlihatkan pada Gambar 1.

	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 1. Tabel pemetaan Vigenère Cipher

Selain menggunakan Algoritma Vigenere Cipher bujur sangkar Vigenere untuk melakukan algoritma ini dapat dilakukan dengan menjumlahkan plaintext dengan kunci kemudian di modulo 26.

Dengan Asumsi a = 0, b = 1, c = 2, ……, z = 25

D) Hardware

Menurut Sutarman (2009:103) Perangkat keras (*Hardware*) yaitu komponen fisik yang digunakan untuk aktivitas *input*, proses, *output*, dan penyimpanan pada suatu sistem komputer.

Berdasarkan fungsinya perangkat keras (*hardware*) komputer dibagi menjadi 3 bagian utama yaitu:

a. Peralatan Masukan (*Input Device*): Peralatan Masukan (*input device*) adalah alat-alat yang digunakan untuk proses memasukan data/informasi ke dalam komputer.

b. Peralatan Proses (*Process Device*): Peralatan proses (*process device*) adalah alat di mana instruksi-instruksi program diproses untuk mengolah data yang sudah dimasukkan lawat alat *input* dan hasilnya akan ditampilkan di alat *output.*

c. Peralatan Keluaran (*Output Device*): Peralatan *Output* adalah peralatan yang dapat menerjemahkan/

mentransformasikan hasil pengolahan data ke pengguna (*user*).

E) Software

Perangkat Lunak (*Software*) adalah serangkaian instruksi yang dipahami oleh perangkat keras pengolahan data atau komputer, sehingga perangkat keras itu dapat melaksanakan pemrosesan data sesuai dengan yang dikehendaki.

Sistem adalah seperangkat elemen-elemen yang terdiri atas manusia, mesin atau alat dan prosedur serta konsep-konsep yang dihimpun menjadi satu guna mencapai tujuan bersama. Secara tradisional, software terbagi menjadi dua katagori dasar yaitu sistem program dan program aplikasi.

F) Flowchart

Menurut Yakub, (2012:162) Bagan alir *(Flowchart)* adalah bagan yang menggambarkan urutan instruksi proses dan hubungan satu proses dengan proses yang lainnya menggunakan simbol-simbol tertentu. Dalam pengoperasian komputer terutama dalam prosess pengolahan data terdapat beberapa simbol yang disebut *Flowchart.*

G) DFD (Data Flow Diagram)

DFD merupakan alat untuk membuat diagram yang serbaguna. Data Flow Diagram terdiri dari notasi peyimpanan data (*data Store*), proses, *Process*), aliran data (*Flow Data)* dan sumber masukan (*entity*). (Yakub,2012:155).

H) Visual Basic

Menurut Daryanto (2003:13) *Visual Basic* adalah salah satu *development tools* untuk membangun aplikasi dalam lingkungan *windows*. Dalam perkembangan aplikasi, *Visual Basic* menggunakan pendekatan visual untuk merancang *user interface* dalam bentuk *form*, sedangkan untuk kodingnya menggunakan dialok bahasa *basic*. *Visual Basic* telah menjadi *tools* yang terkenal bagi para pemula maupun para *developer.*

III. METODOLOGI PENELITIAN

A) Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode pengembangan sistem. Adapun langkah-langkah penelitian adalah:

1) Analisis sistem aplikasi kriptografi pesan menggunakan algoritma vigenere cipher.
2) Implementasi dan pengujian sistem, yakni melakukan pengujian terhadap sistem yang telah dirancang.

B) Perangkat Lunak dan Perangkat Keras

Perangkat Lunak (*Software*): Sistem perangkat lunak merupakan program pendukung yang diperlukan dalam menjalankan perangkat keras. *Software* sebagai penerjemah suatu bahasa mesin (*analog*) yang menghasilkan informasi yang dapat dikenal oleh manusia. Adapun perangkat lunak yang mendukung program ini adalah:

1. Sistem Operasi: Windows 7
2. Program Aplikasi: Visual Basic 6.0,

Perangkat Keras (*Hardware*): Perangkat keras merupakan suatu peralatan fisik komputer yang digunakan untuk menjalankan program yaitu:

1. Monitor 14" WXGA WideScreen
2. Prosesor Intel Centrino M-16
3. Ram 1024 MB
4. Harddisk 80 GB

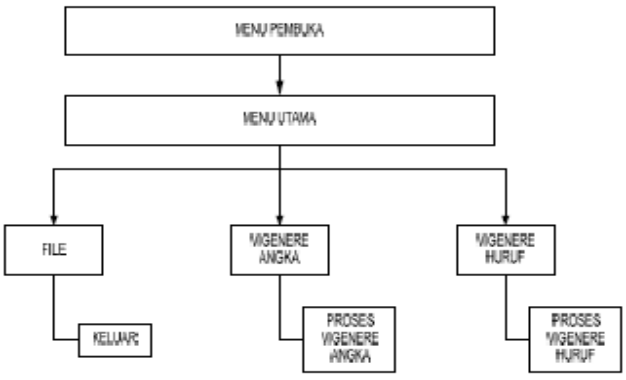
C) Sistem Aktual

Keamanan merupakan aspek terpenting dari sistem operasi *windows* namun pada kenyataannya aspek keamanan berada diurutan terakhir dari sebuah sistem. Sistem lebih menampilkan dari sistem yang dibangun dari pada mengutamakan keamanannya pesan.

D) Sistem Baru

Rancangan Struktur Menu

Rancangan struktur menu adalah sebuah langkah penting yang bertujuan untuk memberikan kemudahan bagi pemakai dalam menjalankan aplikasi ini. Adapun perancangan struktur menu ditunjukkan pada Gambar 2.



Gambar 2. Rancangan Struktur Menu

E) Metode Pengujian Sistem

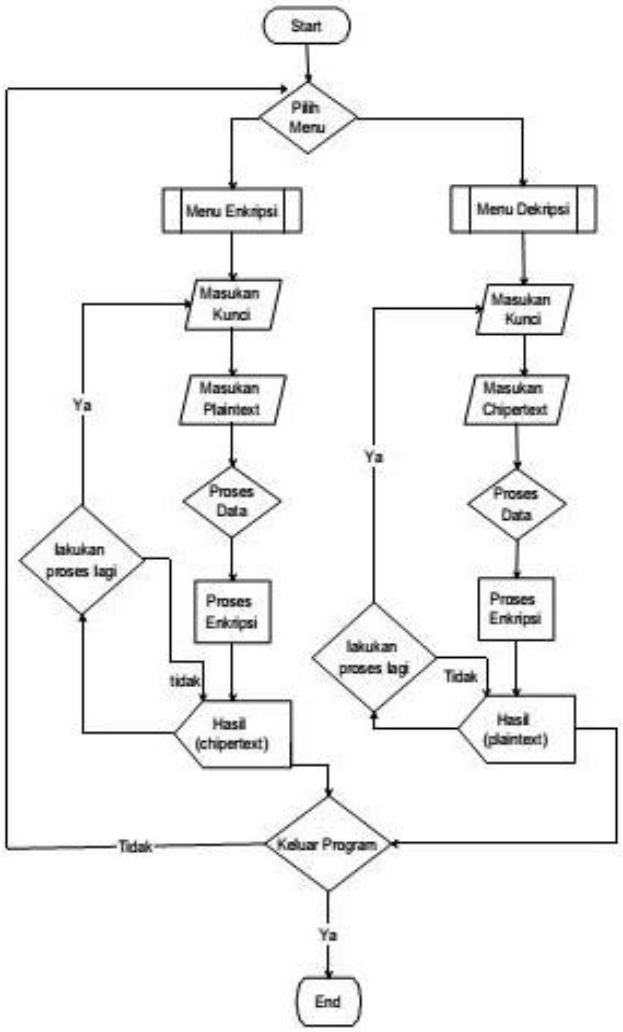
Rancangan pengujian sistem dilakukan setelah aplikasi enkripsi dan deskripsi yang dibuat telah selesai. Proses pengujian sistem dilakukan dengan cara sistematis melalui dua tipe pengujian, yaitu:

a. *Stup Testing* (Pengendalian Stuktur): Yaitu tes struktur kendali sebelum program dijalankan.

b. *Unit Testing* (Pengendalian Unit): Pengujian unit, setiap menu diuji untuk menjamin program tersebut dapat berjalan sesuai dengan fungsinya dengan baik. Ada 2 metode untuk melakukan testing, yaitu:

1. *Black Box Testing* (terfokus pada apakah unit program tersebut memenuhi *requirement*/syarat yang ditentukan dalam spesifikasi).
2. *White Box Testing* (melihat ke dalam program untuk meneliti kode- kode program yang ada, dan menganalisa apakah ada kesalahan atau tidak).

F) Flowchart



Gambar 3. Flowchat

IV. PEMBAHASAN

Pada aplikasi enkripsi dan deskripsi data dengan menggunakan metode Vigenere terdapat beberapa *form* atau *interface* yang di desain untuk mempermudah user atau pemakai dalam menggunakan atau menjalankan aplikasi Vigenere ini.

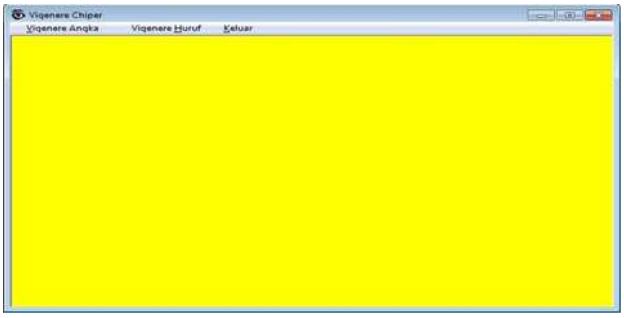
A) Interface Menu Pembuka

Interface menu pembuka ini merupakan tampilan awal yang muncul pada saat aplikasi Vigenere ini dijalankan. Interface menu pembuka ini hanya menampilkan judul aplikasi dan terdapat tombol lanjut untuk menuju ke menu utama, seperti Gambar 4.

Gambar 4. Interface Menu Pembuka

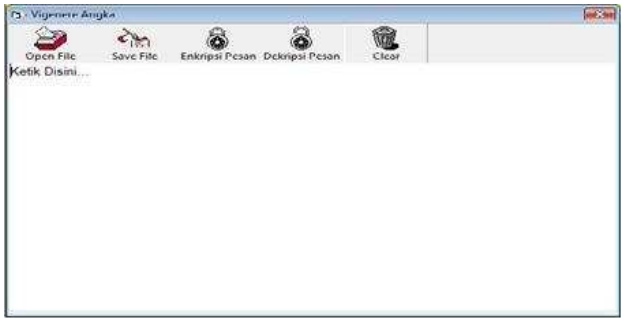
B) Interface Menu Utama

Pada interface menu utama terdapat beberapa menu yaitu menu Vigenere Angka, Vigenere Huruf, dan Keluar, Gambar 5 merupakan tampilan *interface* menu utama.



Gambar 5. Interface Menu Utama

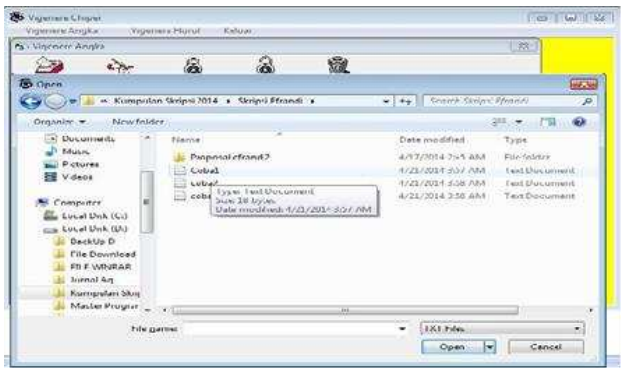
Vigenere Angka



Gambar 6. Interface Vigenere Angka

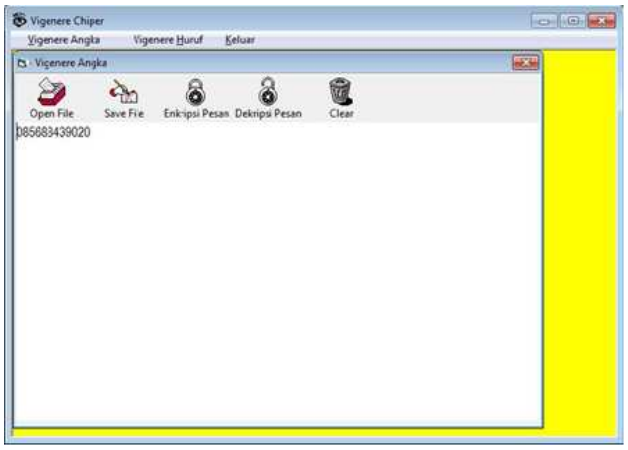
Berdasarkan gambar diatas, terdapat beberapa toolbar yang terdiri dari Open File, Save File, Enkripsi Pesan dan Deskripsi Pesan serta Clear serta "Ketik Disini".

Open File digunakan untuk membuka file yang telah tersimpan pada harddisk atau media penyimpanan lainnya. File yang bisa digunakan pada aplikasi Vigenere ini hanya pada ekstensi file .txt atau notepad, berikut tampilan *open file*.



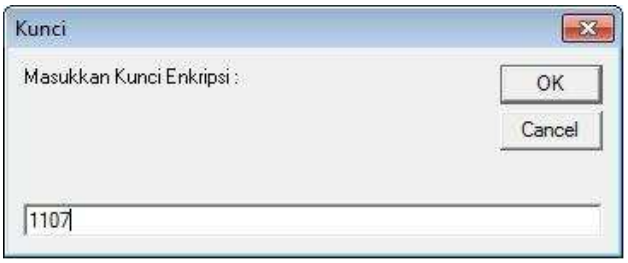
Gambar 7. Tampilan *Open File*

Kemudian pilih *file* yang akan dienkripsi atau di deskripsi, contoh *file* yang dipilih adalah co-baangka.txt, maka *file* yang dipilih tersebut akan muncul pada layar yang terdapat pada aplikasi, seperti gambar berikut ini:



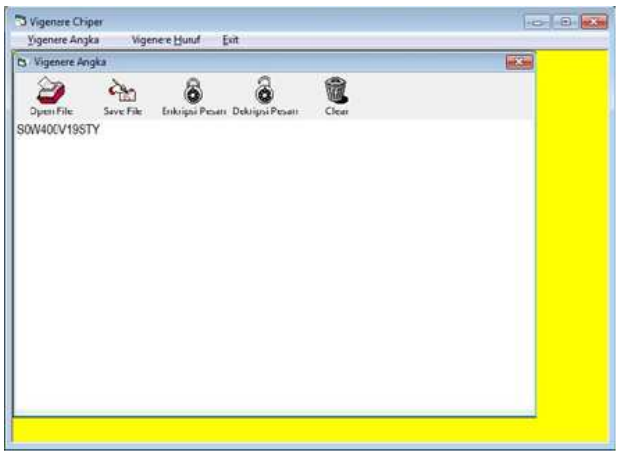
Gambar 8. Tampilan File Angka yang telah dipilih

Pada proses enkripsi pesan, aplikasi atau sistem akan meminta *user* atau pengguna memasukkan kata kunci untuk pesan yang akan dienkripsi, seperti gambar berikut ini.



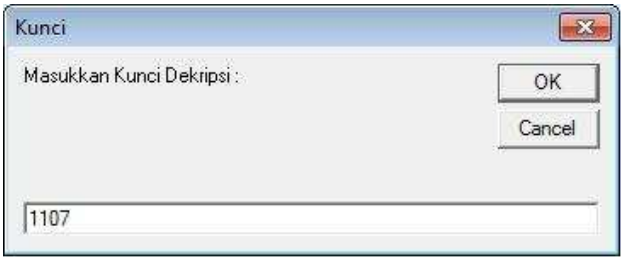
Gambar 9. Tampilan Untuk Memasukkan Kunci Enkripsi

Setelah memasukan kunci enkripsi maka angka-angka tadi akan berubah menjadi seperti gambar dibawah ini.



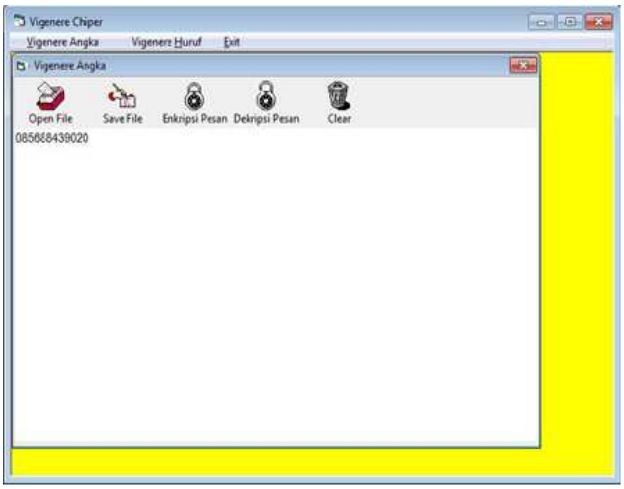
Gambar 10. File Angka yang telah dienkripsi

Deskripsi adalah untuk mengembalikan file yang telah dienkripsi, dengan cara memasukkan kunci enkripsi pada kotak dialog atau kotak pesan seperti gambar dibawah ini:



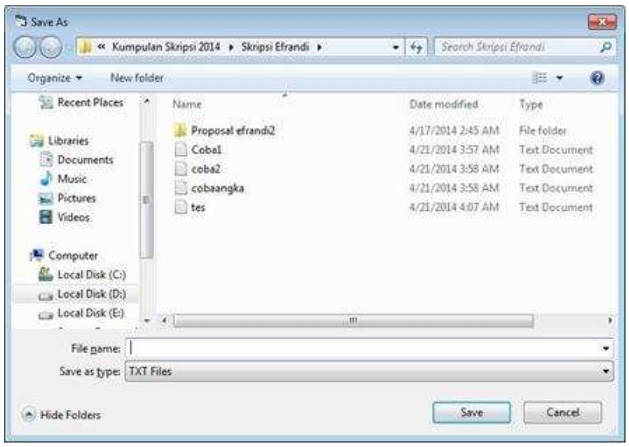
Gambar 11. Kotak Dialog Kunci Deskripsi

Setelah memasukkan kunci pada kotak dialog deskripsi akan file yang telah dienkripsi akan kembali seperti semula seperti gambar dibawah ini.



Gambar 12. File Angka yang telah di deskripsi

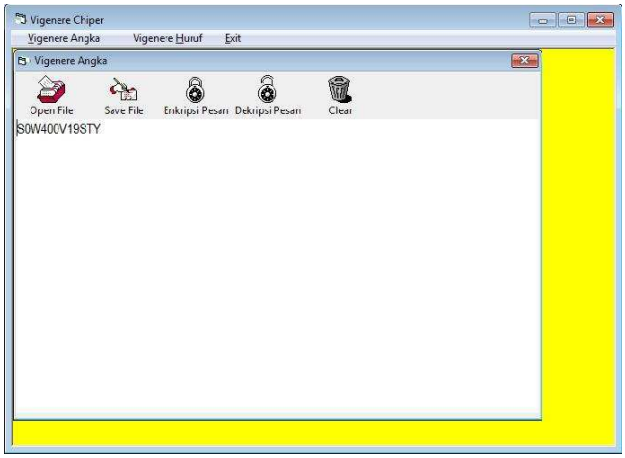
Pada *toolbars save file* berfungsi untuk menyimpan file yang telah dienkripsi atau pun yang sudah di deskripsi, file yang disimpan berupa file .txt, berikut kotak dialog *save file :*



Gambar 13. kotak dialog save file

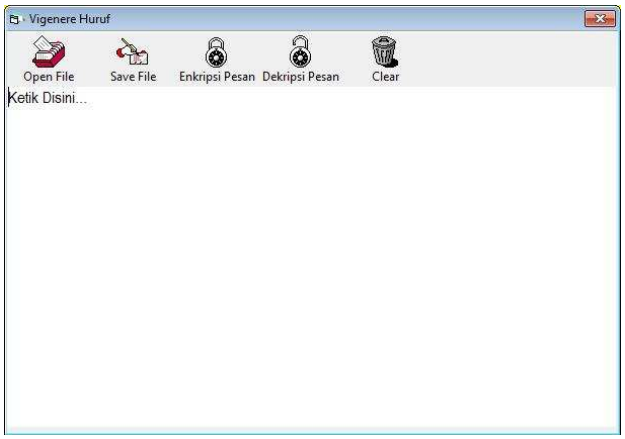
Pada file name ketikan nama file yang akan disimpan kemudian setelah itu klik save atau menekan tombol enter. Misalnya file yang telah dienkripsi disimpan dengan nama *angkaenkripsi.txt*.

Toolbars clear berfungsi untuk membersihkan layar, seperti gambar berikut ini:



Gambar 14. Tampilan Sebelum Diklik Tombol *Clear*

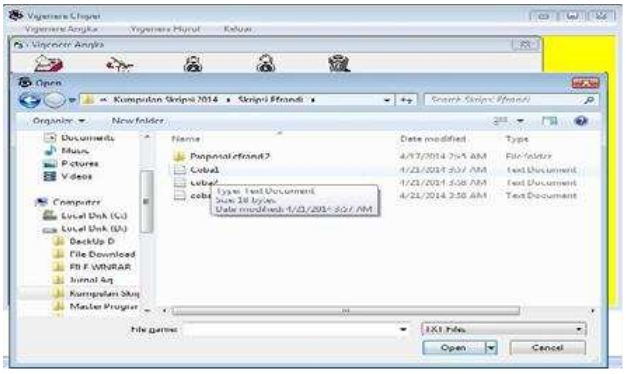
Vigenere Huruf



Gambar 15. Interface Vigenere Huruf

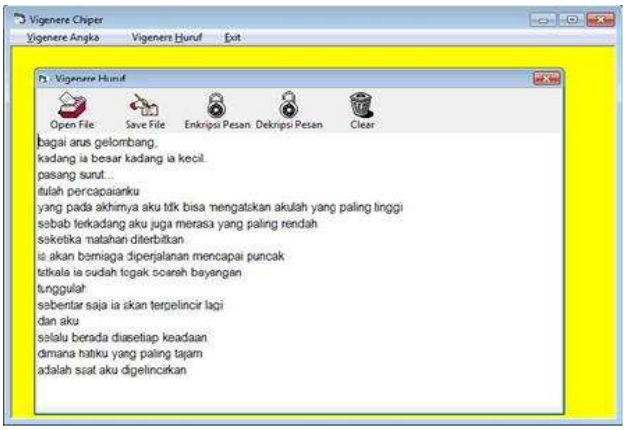
Berdasarkan gambar diatas, terdapat beberapa *toolbar* yang terdiri dari *Open File, Save File,* Enkripsi Pesan dan Deskripsi Pesan serta *Clear* serta "Ketik Disini".

Open File digunakan untuk membuka file yang telah tersimpan pada harddisk atau media penyimpanan lainnya. File yang bisa digunakan pada aplikasi Vigenere ini hanya pada ekstensi file .txt atau notepad, berikut tampilan *open file*.



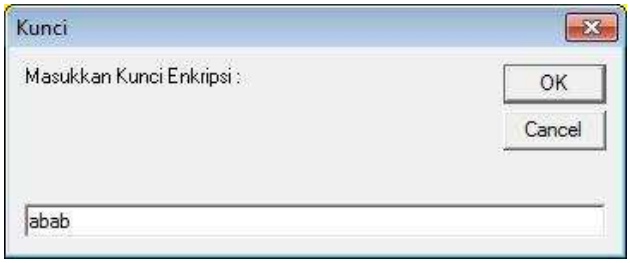
Gambar 16. Tampilan *Open File*

Kemudian pilih *file* yang akan dienkripsi atau di deskripsi, contoh *file* yang dipilih adalah tex.txt, maka *file* yang dipilih tersebut akan muncul pada layar yang terdapat pada aplikasi, seperti gambar berikut ini :



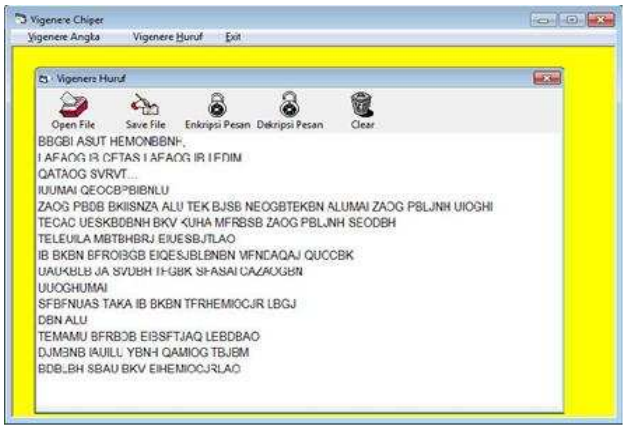
Gambar 17. Tampilan File Huruf yang telah dipilih

Pada proses enkripsi pesan, aplikasi atau sistem akan meminta *user* atau pengguna memasukkan kata kunci untuk pesan yang akan dienkripsi, seperti gambar berikut ini:



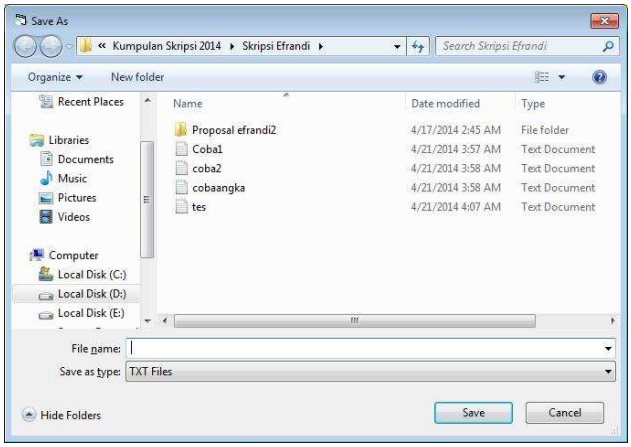
Gambar 18. Tampilan Untuk Memasukkan Kunci Enkripsi

Setelah memasukan kunci enkripsi maka huruf tadi akan berubah menjadi seperti gambar dibawah ini:



Gambar 19. File Huruf yang telah dienkripsi

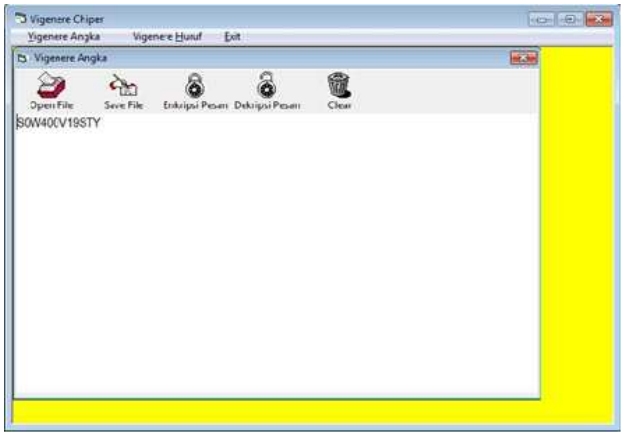
Pada *toolbars save file* berfungsi untuk menyimpan file yang telah dienkripsi atau pun yang sudah di deskripsi, file yang disimpan berupa file .txt, berikut kotak dialog *save file :*



Gambar 20. kotak dialog *save file*

Pada file name ketikan nama file yang akan disimpan kemudian setelah itu klik save atau menekan tombol enter. Misalnya file yang telah dienkripsi disimpan dengan nama *hurufenkripsi.txt.*

Toolbars clear berfungsi untuk membersihkan layar, seperti gambar berikut ini:



Gambar 21 Tampilan Sebelum Diklik Tombol Clear

G) Pengujian Sistem

Pengujian sistem yang dilakukan adalah mencoba memasukkan kata kedalam aplikasi yang telah dibuat dan kemudian disesuaikan dengan perhitungan manual algoritma Vigenere, sebagai contoh:

Plainteks adalah : DEHASEN
Kunci: UNIVED
Hasil: XRPVWH7

Vigenere Table

A	B	C	D	E	F	G	H
0	1	2	3	4	5	6	7
I	J	K	L	M	N	0	P
8	9	10	11	12	13	14	15
Q	R	S	T	U	V	W	X
16	17	18	19	20	21	22	23
Y	Z	0	1	2	3	4	5
24	25	26	27	28	29	30	31
6	7	8	9				
32	33	34	35				

Untuk Pengujiannya sebagai berikut:

(Huruf pertama dari plainteks + huruf pertama dari kunci) mod 36

Jadi = (P+K) mod 36
1. = (D + U) mod 36
= (3 + 20) mod 36
= 23 mod 36
= 23 (X)
2. = (E+N) mod 36
= (4+13) mod 36
= 17 mod 36
= 17 (R)
3. = (H+I) mod 36
= (7 + 8) mod 36
= 16 mod 36
= 15 (P)
4. = (A+V) mod 36
= (0+21) mod 36
= 21 mod 36
= 21 (V)
5. = (S+E) mod 36
= (18+4) mod 36
= 22 mod 36
= 22 (W)
6. = (E+D) mod 36
= (4+3) mod 36
= 7 mod 36
= 7 (H)
7. = (N+U) mod 36

=(13+20) mod 36
= 33 mod 36
= 33 (7)

V. PENUTUP

A) Kesimpulan

1) Untuk merancang aplikasi kripto sistem ini dilalui dalam beberapa tahap yaitu perancangan diagram, *flowchart, layout*/tampilan program, dan pengkodean algoritma Vigenere cipher diimplementasikan pada visual basic 6.0.
2) Pada penulisan *coding* enkripsi dan dekripsi harus melakukan perulangan yang sama tetapi menggunakan objek yang berbeda.
3) Spesifikasi program aplikasi ini dapat dijalankan sesuai dengan spesifikasi teknis yang dirancang.
4) Program aplikasi kripto sistem ini dapat menyembunyikan pesan penting yang bisa dibaca menjadi tidak bisa dibaca dan mencari maksud dari pesan yang rahasia menjadi bisa dibaca.
5) Aplikasi ini dapat diinstal atau diimplementasikan pada sistem operasi windows

B) Saran

1. Dalam pembuatan aplikasi kripto sistem ini diharapkan dapat berguna untuk menjaga dan menjamin kerahasiaan data.
2. Dalam pengisian kunci harus sesuai dengan tipe yang dipilih. Apabila kunci tipe angka hanya bisa dimasukkan angka, dan kunci huruf hanya bisa dimasukkan huruf.

DAFTAR PUSTAKA

Apriandala, Rio, 2013, *Sistem Keamanan Menggunakan Rubik Dengan Algoritma Kriptografi Encryption,* Tugas Besar I Makalah Kriptografi, Universitas Bengkulu. 375 Hal

Daryanto. 2003. *Belajar Komputer Visual Basic*. Yrama Widya. Bandung

Surbakti, Reza, 2013, *Sistem Keamanan Data Menggunakan Algoritma Kriptografi Simetris,* Proposal Skripsi, Unived Bengkulu. 32 Hal

Hadi, Rahadian, 2006, *Pengenalan Visual Basic*. Jakarta. PT. Elex Media Kompetindo.136 Hal

Hallim, Abd, 2010, *Pembuatan Perangkat Lunak Media Pembelajaran Kriptografi Klasik*. Surabaya.Politeknik Eletronika Negeri.11 Hal

Sutarman, 2009 *Pengantar Teknologi Informasi*, Bumi Aksara, Yogyakarta. Hal Yakub, 2012 *Pengantar Sistem Informasi*, Yogyakarta, Graha Ilmu.155 Hal