RANCANG BANGUN APLIKASI PESAN MENGGUNAKAN ALGORITMA VIGENERE CIPHER DAN ONE TIME PAD

Sugeng Sutrisno[1]
[1]Program Studi Teknik Informatika, Fakultas Ilmu Komputer
Universitas Dian Nuswantoro Semarang
Jl. Nakula I No 5-11 Semarang 50131
Telp : (024) 3517361, Fax : (024) 3520165
Email : sugengsutrisno02@gmail.com[1]

ABSTRAK

Dalam penelitian ini dirumuskan masalah tentang bagaimana merancang dan mengimplementasikan metode Vigenere Cipher dan One Time Pad untuk keamanan pada pesan pesan agar dapat menjadi lebih aman. Sedangkan tujuan dari penelitian ini adalah untuk merancang keamanan Pesan dengan menggunakan metode Vigenere Cipher dan One Time Pad, merancang enkripsi dan dekipsi dengan metode Vigenere Cipher dan One Time Pad pada Pesan agar menjadi lebih aman untuk digunakan serta merancang enkripsi dan dekripsi Pesan agar dapat diterapkan menggunakan bahasa pemrograman PHP. Vigenere cipher dan one time pad adalah bagian dari algoritma kriptografi klasik. Pada kedua algoritma ini menggunakan kunci simetrik untuk proses enkripsi dan dekripsinya, yang mana kunci yang digunakan untuk proses enkripsi sama dengan kunci yang digunakan untuk proses dekripsi. Penggunaan algoritma Vigenere cipher dan one time pad membuat kunci yang digunakan untuk proses enkripsi ataupun dekripsi berjumlah 2 kunci. Dengan adanya 2 kunci ini menjadikan kriptanalisis membutuhkan waktu untuk menemukan kunci yang digunakan sebelum melakukan dekripsi pada ciphertext. Hasil dari keamanan Pesan pada sistem enkripsi Pesan menggunakan algoritma Vigenere Cipher dan One Time Pad untuk membuat Pesan menjadi lebih aman digunakan.

Kata kunci : Vigenere Cipher, One Time Pad, Enkripsi, Dekripsi, Pesan

ABSTRACT

The way to make and apply Vigenere Cipher and One Time Pad has been formulated in this research for making Message became more secure. The main purpose of this reseach is to create Messaging security system using Vigenere Cipher and One Time Pad method, and compile it using PHP so we can encrypt and decrypt in order to make that method work properly. Vigenere Cipher and One Time Pad are part of classic cryptographic algorithm. Both of those algorithm are using symmetrical key on the encryption and decryption progress, which is the key is identical between those two progresses. With the existence of those two key, cryptanalytic needs time for encrypting the Message on ciphertext, the result of this method in to make Message (text, in this case) become more secure.

Keywords: Vigenere Cipher, One Time Pad, Encryption, Decryption, Message

1. Latar Belakang Masalah

Pemanfaatan teknologi dapat kita jumpai dalam kehidupan sehari-hari dimana teknologi memberikan kemudahan untuk melakukan pertukaran informasi. Jaringan komputer dan internet telah mengalami perkembangan yang sangat pesat [1]. Teknologi internet ini mampu menghubungkan semua komputer sehingga bisa saling berkomunikasi dan bertukar informasi berupa data, pesan suara, video dan gambar. Penyampaian pesan dengan menggunakan internet dapat dilakukan dengan memanfaatkan Pesan.

Pesan merupakan komunikasi pengiriman surat secara elektronik yang terhubung melalui jaringan yang saling terkoneksi. Internet yang merupakan media *global* yang dapat dengan mudah diakses oleh siapa saja, hal tersebut menjadikan penyampaian pesan menggunakan Pesan menjadi kurang aman [2]. Kurang amannya pengiriman Pesan dapat terjadi karena ketika dilakukan pengiriman, Pesan yang dikirim berupa pesan asli sehingga apabila dilakukan pengambilan Pesan dari jalur pengiriman maka pesan akan dapat diketahui oleh pihak yang tidak berhak. Maka diperlukan sebuah keamanan pada sebuah data Pesan.

Keamanan merupakan sebuah tindakan untuk menjaga kerahasiaan pada sebuah data Pesan dari berbagai macam gangguan dan ancaman [3]. Semakin banyak data yang akan di kirim atau di proses dengan komputer, maka ancaman terhadap pengamanan Pesan akan semakin dibutuhkan. Salah satu cara untuk menjaga keamanan dan kerahasiaan suatu Pesan adalah dengan teknik enkripsi dan dekripsi [4]. Enkripsi dan dekripsi dapat di gunakan untuk membuat Pesan agar tidak dapat dibaca atau dipahami oleh orang lain yang tidak memiliki hak akses. Teknik pengamanan data dan informasi tersebut dikenal dengan nama Kriptografi. Dengan memanfaatkan kriptografi Pesan yang hendak dikirimkan akan dilakukan enkripsi Pesan terlebih dahulu sehingga Pesan yang dikirim bukan merupakan pesan asli melainkan Pesan yang sudah dienkripsi yang menjadikan kerahasiaan Pesan tetap terjaga. Pesan asli dapat di terima dan dibaca oleh penerima setelah Pesan tersebut diterjemahkan (dekripsi) menggunakan kunci rahasia .

Penggunaan algoritma *Vigenere Cipher* pernah dilakukan tehadap keamanan SMS (*Short Message Service*) agar dapat menjaga integritas dan keamanan pada isi Pesan dan menutupi celah dari keamanan SMS. Pesan yang dikirimkan akan dienkripsi menggunakan *Vigenere Cipher* terlebih dahulu supaya isi dalam Pesan hanya dapat dibaca oleh pengirim dan penerima [5]. Sedangkan penggunaan algoritma *One Time Pad* (*OTP*) pernah di terapkan pada citra digital karena dengan algoritma *One-time pad* secara matematis terbukti sempurna dan aman. *One time pad* dikatakan sempurna dan aman karena didalam penggunaannya barisan pada bilangan diacak sebagai kunci enkripsi dan panjang kunci tersebut sama dengan pesan yang akan dienkripsi dan tidak ada perulangan kunci sebagaimana yang telah diterapkan pada *Vegenere Cipher* [6].

Berdasarkan hal yang sudah dibahas diatas penulis hendak merancang aplikasi Pesan dengan menggabungkan *Vigenere Cipher* dan *One Time Pad* untuk memberikan keamanan pada Pesan dari pihak yang tidak berhak.

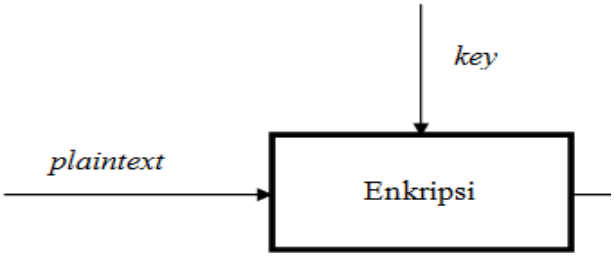
2. Tinjauan Pustaka

2.1 Enkripsi

Enkripsi merupakan bagian dari kriptografi yang digunakan untuk merubah suatu pesan atau informasi menjadi sandi-sandi yang bersifat rahasia. Enkripsi juga dapat diartikan sebagai cipher atau kode. Secara matematis, enkripsi dapat dituliskan sebagai berikut :

EK (M) = C (Proses Enkripsi)

Ketika proses enkripsi dilakukan, pesan *M* disandikan menggunakan kunci *K* kemudian menghasilkan pesan *C*. Pesan M dapat disebut sebagai *plaintext* sedangkan pesan *C* dapat disebut sebagai *ciphertext*. Penyandian pesan atau informasi yang dilakukan menggunakan kunci, yang menjadikan pesan atau informasi tadi dapat dibaca. Tujuan dari enkripsi adalah untuk menyembunyikan pesan atau informasi dari pihak yang tidak berhak.



Gambar 2.1 Proses Enkripsi Pesan

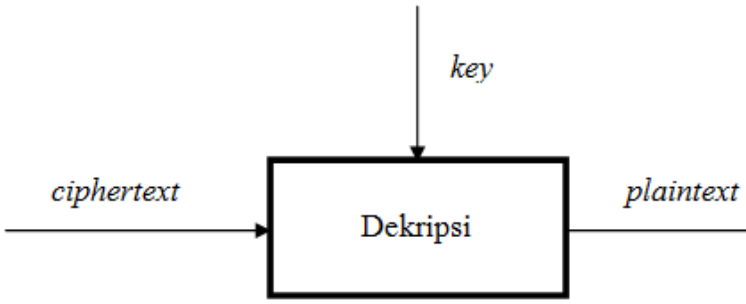
Pada gambar 2.1 menjelaskan bahwa untuk melakukan proses enkripsi dibutuhkan *plaintext* (pesan asli) dan juga kunci yang akan digunakan untuk enkripsi sehingga akan menghasilkan *ciphertext* (pesan rahasia).

2.2 Dekripsi

Dekripsi merupakan kebalikan dari enkripsi. Dekripsi digunakan untuk mengembalikan sandi-sandi atau informasi yang telah diacak menjadi bentuk yang asli dengan menggunakan kunci yang sama untuk proses enkripsi. Secara matematis, dekripsi dapat dituliskan sebagai berikut :

DK (C) = M (Proses Dekripsi)

Ketika proses dekripsi dilakukan, pesan *C* yang merupakan *ciphertext* diuraikan dengan menggunakan kunci *K* sehingga menghasilkan pesan *M* yang berupa *plaintext*. Tujuan dari dekripsi adalah untuk mengembalikan pesan atau informasi kebentuk yang dapat dibaca sesusai pesan atau informasi yang sebenarnya.



Gambar 2.2 Proses Dekripsi Pesan

Pada gambar 2.2 menjelaskan bahwa untuk melakukan proses dekripsi dibutuhkan *ciphertext* (pesan rahasia) dan juga kunci yang akan digunakan untuk dekripsi sehingga akan menghasilkan *plaintext* (pesan asli).

2.3 Algoritma Vigenere Cipher

Vigenere Cipher adalah salah satu jenis kriptografi klasik yang pada dasarnya dilakukan untuk subtitusi cipher abjad majemuk (*polyalphabetic substitution).* Metode ini pertama kali dipublikasikan oleh seorang diplomat (sekaligus seorang

kriptologis) Prancis, *Blaise de Vigenere* pada abad ke-16, tepatnya pada tahun 1586. *Vigenere Cipher* sangat dikenal karena mudah dipahami dan diimplementasikan [5]. Untuk memudahkan dalam proses enkripsi, maka dapat digunakan alat bantu berupa bujur sangkar *Vigenere* (Tabel *Vigenere*) untuk melakukan enkripsi. Adapun bentuk dari perio *vigenere* adalah sebagai berikut :

Tabel 2.2 Bujur Sangkar Vigenere

	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

Penggunaan perio *Vigenere* untuk proses dapat dilakukan dengan menarik garis periodic dari huruf *plaintext* kebawah, lalu perio kekanan secara periodic4l dari huruf kunci. Hasil perpotongan dari kedua garis yang dihasilkan menyatakan huruf *ciphertext*-nya. Sedangkan pada proses dekripsi menggunakan perio *Vigenere* dilakukan dengan menarik kearah huruf *ciphertext* yang dituju secara periodic4l dari huruf kunci. Setelah itu perio garis periodic dari huruf *ciphertext* sampai huruf *plaintext.* Hasil perpotongan dari kedua garis yang dihasilkan menyatakan huruf *plaintext*-nya. Selain menggunakan perio *Vigenere*, proses enkripsi menggunakan *vigenere cipher* dapat dilakukan dengan persamaan matematis sebagai berikut :

- ✓ $C_i = (P_i + K_r) \bmod 26$ …… (1)

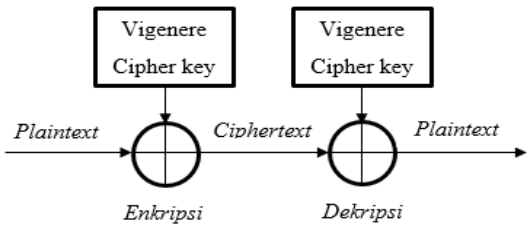
Sedangkan untuk proses dekripsi dapat dilakukan dengan persamaan matematis :

- ✓ $P_i = ((C_i - K_r) + 26) \bmod 26$ ……. (2)

Adapun dari persamaan (1) dan persamaan (2) dapat diketahui :

- C_i = pergeseran karakter pada *ciphertext*
- P_i = pergeseran karakter pada *plaintext*
- K_r= Kunci dalam bentuk decimal yang dihasilkan dari perio konversi.

Untuk melakukan perhitungan dengan persamaan diatas dapat dilakukan dengan merubah terlebih dahulu karakter *plaintext* atau *ciphertext* menggunakan perio konversi sehingga menjadi bentuk decimal. Sedangkan hasil perhitungan menggunakan persamaan (1) dan (2) akan berbentuk periodi untuk kemudian dikonversi menjadi karakter menggunakan perio konversi.



Gambar 2.3 Proses Enkripsi dan Dekripsi Vigenere Cipher

Pada gambar 2.3 menunjukkan bahwa untuk melakukan proses enkripsi dibutuhkan input berupa *plaintext* dan juga kunci dari *vigenere cipher* sehingga dapat menghasilkan *ciphertext* yang diinginkan. Sedangkan untuk proses dekripsi dapat dilakukan dengan menginputkan *ciphertext* dan juga kunci dari *vigenere cipher* sehingga dapat menghasilkan *plaintext* yang diinginkan. Kemudian jika panjang kunci lebih pendek dari *plainext* maka maka kunci akan diulang penggunaannya secara periodic.

2.4 Algoritma One Time Pad

One Time Pad adalah salah satu contoh metode kriptografi dengan algoritma jenis simetri. Seingga kunci yang digunakan untuk proses enkripsi sama dengan kunci yang digunakan untuk proses dekripsi. Ditemukan pada tahun 1917 oleh Major Yoseph Mouborgne dan Gilbert Vernam pada perang dunia ke dua.Metode ini telah diklaim sebagai satu-satunya algoritma kriptografi sempurna yang tidak dapat dipecahkan [6]. Suatu algoritma dikatakan aman, apabila tidak ada cara untuk menemukan plaintext-nya Sampai saat ini, hanya algoritma *One Time Pad (OTP)* yang dinyatakan tidak dapat dipecahkan meskipun diberikan sumber daya yang tidak terbatas. Proses enkripsi dan dekripsi pada *One Time Pad* ini hampir sama dengan proses enkripsi dan dekripsi menggunakan algoritma *vigenere cipher*. Proses enkripsi dapat dilakukan dengan persamaan matematis sebagai berikut :

- ✓ $C_i = (P_i + K_r) \bmod 26$ ……. (1)

Sedangkan untuk proses dekripsi dapat dilakukan dengan persamaan matematis :

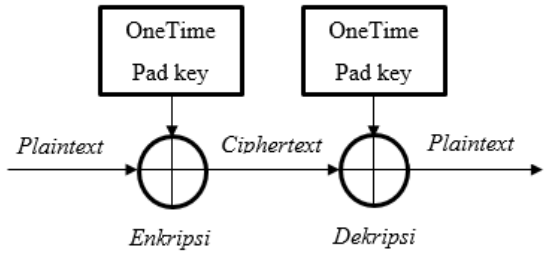
- ✓ $P_i = ((C_i - K_r) + 26) \bmod 26$ ……. (2)

Dari persamaan (1) dan persamaan (2) dapat diketahui :

- C_i = pergeseran karakter pada *ciphertext*
- P_i = pergeseran karakter pada *plaintext*
- K_r= Kunci dalam bentuk decimal yang dihasilkan dari tabel konversi.

Bagian yang membedakan antara *one time pad* dengan *vigenere cipher* adalah pada kunci yang digunakan. Jika penggunaan kunci pada *vigenere* cipher

dapat diulang untuk menyesuaikan dengan panjang *plaintext*, maka pada *one time pad* hal tersebut tidak dapat dilakukan karena jumlah kunci yang digunakan harus sama panjangnya dengan jumlah *plaintext.*



Gambar 2.4 Proses Enkripsi dan Dekripsi One-Time Pad

Pada gambar 2.4 menunjukkan bahwa untuk melakukan proses enkripsi dibutuhkan input berupa *plaintext* dan juga kunci dari *one time pad* sehingga dapat menghasilkan *ciphertext* yang diinginkan. Sedangkan untuk proses dekripsi dapat dilakukan dengan menginputkan *ciphertext* dan juga kunci dari *one time pad* sehingga dapat menghasilkan *plaintext* yang diinginkan. Penggunaan kunci pada *one time pad* setiap pergeseran karakter hanya dapat digunakan tepat satu kali saja.

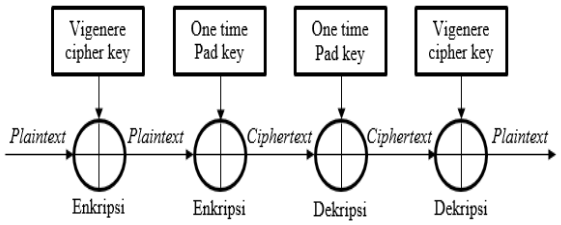
3. Metode

3.1 Instrumen Penelitian

Perkembangan teknologi sangat pesat khususnya internet, dimana dalam pemanfaatannya sangat besar bagi manusia, diantaranya dalam hal pengiriman informasi seperti pesan, suara, gambar, dll. Dalam hal pengiriman pesan melalui internet, Pesan sangat besar di gunakan oleh manusia. Pengunaan Pesan yang mudah untuk hal pertukaran informasi tidak dapat mnejamin suatu kerahasiaan dan integritas dari pesan yang di kirim oleh pengguna. Hal tersebut dapat terjadi karena pemanfaatan Pesan menggunakan media *public* yaitu internet yang penggunaannya dapat diakses oleh siapa saja. Sehingga diperlukan sebuah sistem untuk menjaga kerahasiaan terhadap pesan Pesan tersebut supaya tidak mudah di ketahui atau dibaca oleh orang yang tidak berhak.

Vigenere cipher dan *one time pad* adalah bagian dari algoritma kriptografi klasik. Pada kedua algoritma ini menggunakan kunci simetrik untuk proses enkripsi dan dekripsinya, yang mana kunci yang digunakan untuk proses enkripsi sama dengan kunci yang digunakan untuk proses dekripsi. Penggunaan algoritma *Vigenere cipher* dan *one time pad* membuat kunci yang digunakan untuk proses enkripsi ataupun dekripsi berjumlah 2 kunci. Dengan adanya 2 kunci ini menjadikan kriptanalisis membutuhkan waktu untuk menemukan kunci yang digunakan sebelum melakukan dekripsi pada *ciphertext.*

Proses enkripsi menggunakan algoritma *Vigenere cipher* dan *one time pad* akan dilakukan dengan cara mengenkripsi *plaintext* awal menggunakan *Vigenere cipher* yang akan menghasilkan *ciphertext* sementara. Selanjutnya dari *ciphertext* sementara tersebut kemudian akan dienkripsi lagi menggunkan *one time pad* untuk menghasilkan *ciphertext* yang akan digunakan. Sedangkan untuk dekripsi *ciphertext* maka akan didekripsikan menggunakan *one time pad* terlebih dahulu yang menghasilkan *plaintext* sementara. Kemudian dari *plaintext* sementara akan di dekripsikan kembali menggunakan *Vigenere cipher* yang menghasilkan *plaintext* awal (*plaintext* sebelum proses enkripsi). Adapun proses enkripsi dan dekripsi menggunakan *Vigenere cipher* dan *one time pad* bisa dilihat pada gambar 3.1.



Gambar 3.1 Proses Enkripsi Dekripsi Vigenere cipher dan One-Time Pad

Dalam pembuatan aplikasi Pesan ini akan dibuat dengan menggunakan bahasa pemrograman PHP.

3.2 Desain Sistem

3.3 Metode yang diusulkan

1. Autentikasi Pengguna

Bagian autentikasi ini dibuat sebagai tampilan awal pada aplikasi Pesan yang akan dibuat. Pada tampilan ini akan digunakan untuk proses validasi pengguna. Pengguna akan dimintai mengisi *form login* berupa *E-mail* dan *password* untuk membuktikan bahwa pengguna itu berhak memasuki aplikasi Pesan atau tidak. Tujuan dari dibuatnya bagian autentikasi ini adalah untuk membatasi pengguna, yang mana agar pengguna yang memiliki *E-mail* dan *password* yang *valid* saja yang dapat menggunakan aplikasi Pesan. Adapun rancangan desain dari halaman *autentikasi* pengguna adalah sebagai berikut :

Gambar 3.2 Desain Halaman Autentikasi Pengguna

Pada gambar 3.2 menunjukkan bahwa terdapat 2 bagian utama dalam tampilan yaitu bagian *Header,* form *Login* dan bagian buat *account.* Pejelasan dari masing-masing bagian adalah sebagai berikut :

- Bagian *Header*

  Pada bagian ini bertuliskan *header* dari sistem Pesan yang dibuat. Didalamnya hanya tedapat nama sistem yang dibuat yaitu "Pesan Enkrip".

- Bagian *form Login*

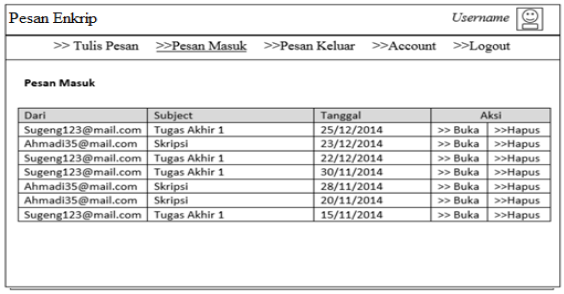
  Bagian ini berisikan dua *form* yang harus diisi apabila pengguna hendak memasuki sistem Pesan, yaitu *form E-mail* dan *form password*

- *Buat Account* Baru

  Pada bagaian ini merupakan fungsi yang digunakan untuk pengguna yang belum terdaftar atau belum memiliki *account E-mail*.

2. Pesan Masuk

Tampilan pesan masuk digunakan untuk menampilkan pesan yang diterima dari pengirim, baik itu pesan yang sifatnya Pesan asli atau Pesan yang sudah dienkripsi. Tampilan Pesan masuk akan langsung keluar setelah proses *Autentikasi* pengguna dilakukan, dengan kata lain tampilan Pesan masuk inilah yang merupakan tampilan yang pertamakali dimunculkan ketika pengguna memasuki sistem. Pada bagian ini dapat diperoleh informasi berupa Pesan pengirim, subject pesan dan juga tanggal pengiriman. Adapun untuk lebih jelasnya dapat dilihat pada gambar dibawah:



Gambar 3.3 Desain Halaman Pesan Masuk

Pada gambar 3.3 memperlihatkan beerapa bagian pada tampilan kotak masuk yaitu bagian *header*, bagian menu dan bagian informasi Pesan masuk. Adapun penjelasan dari masing-masing bagaian adalah sebagai berikut :

- Bagian *Header*

  Pada bagian *header* selain ditampilkan nama sistem aplikasi Pesan juga ditampilkan foto dan *username* dari pengguna.

- Bagian Menu

  Pada bagian ini terdapat *form menu* yang terdiri dari Tulis Pesan, Pesan Masuk, Pesan Keluar, *Account* dan *Logout*.

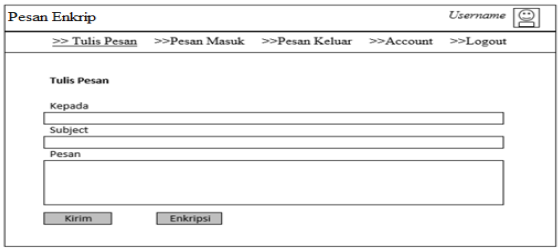
- Pesan Masuk

  Pesan masuk ini berisi pesan yang dikirim oleh pengirim dimana Pesan tersebut berupa informasi yang disampaikan oleh pengirim kepada pembaca atau penerima.

3. Tulis Pesan

Pada bagian ini terdapat tampilan *form* yang bisa digunakan oleh pengguna untuk

menuliskan sebuah pesan baru. Adapun desain tampilan sebagai berikut :



Gambar 3.4 Desain Halaman Tulis Pesan

Pada gambar 3.4 memperlihatkan beberapa bagian pada tampilan tulis Pesan yaitu bagian *header,* bagian menu dan formtulis Pesan. Adapun penjelasan dari masing-masing bagian adalah sebagai berikut :

- Bagian *Header*

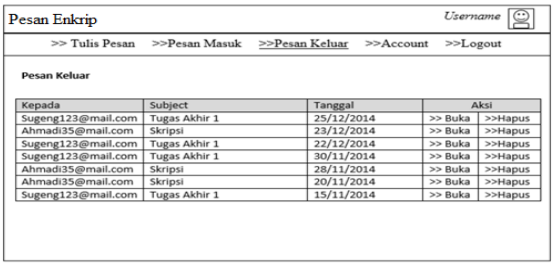
  Pada bagian *header* selain ditampilkan nama sistem Pesan juga ditampilkan foto dan *username* dari pengguna.
- Bagian Menu

  Pada bagian ini terdapat *form menu* yang terdiri dari Tulis Pesan, Pesan Masuk, Pesan Keluar, *Account* dan *Logout.*
- Tulis Pesan

  Pada bagian *form* ini penulisan Pesan dapat membuat Pesan baru dimana pengguna dapat mengisi beberapa *form* yang telah disediakan yaitu *form* alamat *E-mail* yang dituju, subject dan isi Pesan.

4. Pesan Keluar

Tampilan pesan keluar digunakan untuk menampilkan Pesan yang telah terkirim, baik itu pesan yang sifatnya Pesan asli atau Pesan yang sudah dienkripsi. Pada bagian ini dapat diperoleh informasi berupa alamat *E-mail* yang dituju, subject pesan dan juga tanggal pengiriman. Adapun untuk lebih jelasnya dapat dilihat pada gambar dibawah



Gambar 3.5 Desain Halaman Pesan Keluar

Pada gambar 3.5 memperlihatkan beberapa bagian pada tampilan kotak keluar yaitu bagian *header,* bagian menu dan bagian informasi Pesan keluar. Adapun penjelasan dari masing-masing bagaian adalah sebagai berikut :

- Bagian *Header*

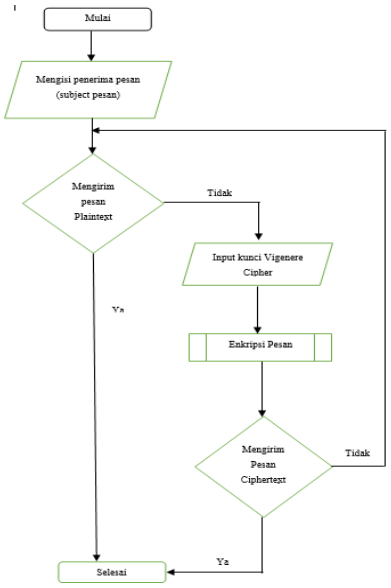
  Pada bagian *header* selain ditampilkan nama sistem Pesan juga ditampilkan foto dan *username* dari pengguna.
- Bagian Menu

  Pada bagian ini terdapat *form menu* yang terdiri dari Tulis Pesan, Pesan Masuk, Pesan Keluar, *Account* dan *Logout.*
- Pesan keluar

Pesan keluar ini berisi pesan yang sudah pernah dikirimkan. Dalam tampilan Pesan masuk ini ditampilkan alamat email yang dituju, subject, tanggal pengiriman dan juga pilihan untuk membuka pesan atau menghapus pesan.

3.4 Desain Sistem

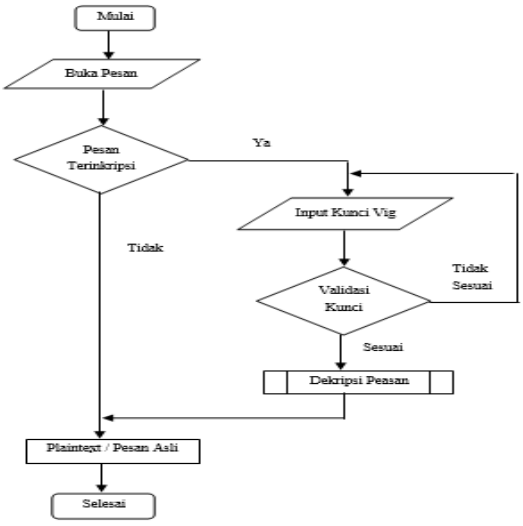
Penggunaan ekripsi Pesan dengan menggunakan algoritma *Vigenere Cipher* dan *OTP* dapat dilihat melalui diagram alur pengiriman Pesan baru pada sistem enkripsi Pesan sebagai berikut:



Gambar 4.2 Flowchart pengiriman pesan baru pada Sistem Enkripsi Pesan

Pada gambar 4.2 memperlihatkan alur pengiriman Pesan baru yaitu untuk mengirimkan Pesan dapat dilakukan dengan mengisi terlebih dahulu *form* penerima, *form subject*, *form* pesan dilanjutkan dengan menekan tombol kirim. Apabila Pesan yang dikirimkan tanpa megisi *form* kunci *Vigenere Cipher* maka Pesan yang dikrimkan adalah Pesan *plaintext* (pesan asli). Sedangkan untuk mengirim Pesan *Ciphertext* (pesan rahasia) dibutuhkan mengisi *form* kunci *Vigenere Cipher* yang kemudian dengan kunci tersebut sistem akan melakukan proses enkripsi yang mana hasil enkripsi tersebut dapat dikirimkan sebagai Pesan *Ciphertext* (pesan rahasia).

Sedangkan pada penggunaan dekripsi dapat dilihat pada diagram alur membuka pesan masuk sebagai berikut:



Gambar 4.3 Flowchart Dekripsi Pesan Masuk

Pada gambar 4.3 menunjukkan bahwa untuk melakukukan proses dekripsi dapat dimulai dengan membuka pesan yang diterima. Apabila Pesan yang diterima tidak terenkripsi maka tidak perlu dilakukan proses dekripsi. Sedangkan apabila Pesan yang diterima terenkripsi maka di perlukan mengisi *form* kunci *Vigenere Cipher* kemudian menekan tombol dekripsi. Bila kunci *Vigenere Cipher* dimasukkan tidak sesuai maka proses dekripsi tidak dapat dilakukan. Sedangkan bila kunci yang dimasukkan sesuai maka dilakukan proses dekripsi, sehingga diperoleh pesan *plaintext* (pesan asli).

4. Pembahasan

4.1 Langkah Pengujian

Pengujian yang akan dilakukan haruslah mengikuti langkah-langkah pengujian yang sudah direncanakan. Adapun langkah-langkah yang akan dilakukan dalam menguji keamanan pesan mengggunakan *Vigenere Cipher* dan *One Time Pad* (*OTP*) pada sistem enkripsi Pesan adalah:

1. Memasuki sistem enkripsi Pesan
2. Membuka kotak masuk Pesan
3. Membuka *search engine*
4. Ketikkan pada *form* pencarian dengan kata kunci "*Vigenere Cipher* dan *One Time Pad"*.
5. Ketikkan pada *form* pencarian dengan kata kunci "Vigenere Cipher *and One Time Pad decrypt tool"*
6. Ketikkan pada *form* pencarian dengan kata kunci "*Vigenere Cipher decrypt tool"*
7. Pilih alamat yang akan digunakan. Misalkan dipilih dari salah satu hasil pencarian diatas dengan alamat "http://www.dcode.fr/vigenere-cipher" maka akan masuk dalam sistem kriptanalis yang ditunjukkan pada gambar 4.14.
8. Masukkan pesan yang telah di enkripsi dengan *Vigenere Cipher* dan *OTP* yang sudah disalin dari tahap ke-3 pada *form decryption* (dekripsi) dan masukkan kunci kemudian tekan tombol dekripsi yang tersedia.
9. Ketikkan pada *form* pencarian dengan kata kunci "*One Time Pad decrypt tool"*
10. Pilih alamat yang akan digunakan. Misalkan dipilih dari salah satu hasil pencarian diatas dengan alamat "http://rumkin.com/tools/cipher/otp.php" maka akan masuk dalam sistem

kriptanalis yang ditunjukkan pada gambar 4.16

11. Masukkan pesan yang telah di enkripsi dengan *Vigenere Cipher* dan *OTP* yang sudah disalin dari tahap ke-3 pada *form decryption* (dekripsi) dan masukkan kunci kemudian tekan tombol dekripsi yang tersedia.

4.2 Analiais Hasil Pengujian

Berdasarkan pengujian keamanan algoritma *Vigenere Cipher* dan *One Time Pad* (*OTP*) untuk keamanan Pesan yang telah dilakukan menghasilkan :

a) Pencarian sistem kriptanalis untuk *Vigenere Cipher* dan *One Time Pad* menggunakan *search engine* tidak dapat ditemukan. Hanya dapat menemukan sistem kriptanalis untuk *Vigenere Cipher* saja atau *One Time Pad* saja.
b) Untuk mendekripsikan *ciphertext Vigenere Cipher* dan *One Time Pad* membutuhkan 2 kunci.
c) Mendekripsi *ciphertext Vigenere Cipher* dan *One Time Pad* menggunakan sistem kriptanalis *Vigenere Cipher* tidak dapat memperoleh *plaintext.*
d) Mendekripsi *ciphertext Vigenere Cipher* dan *One Time Pad* menggunakan sistem kriptanalis *One Time Pad* tidak dapat memperoleh *plaintext.*

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan pembahasan dan hasil pengujian yang sudah dilakukan pada bab-bab sebelumnya, maka dapat diambil kesimpulan bahwa penggunaan algoritma *Vigenere Cipher* dan *One Time Pad* (OTP) pada sistem enkripsi Pesan menjadikan Pesan yang dikirimkan menjadi lebih aman. Supaya dapat membuka pesan maka pengguna memerlukan kunci enkripsi yang mana kunci enkripsi hanya akan diberikan kepada pengguna yang berhak menerima pesan saja.

5.2 Saran

Dalam penerapan enkripsi Pesan menggunakan algoritma *Vigenere Cipher* dan *One Time Pad* pada sistem enkripsi Pesan *Vigenere Cipher* dan *One Time Pad*, terdapat beberapa hal yang sekiranya perlu diperhatikan agar lebih baik kedepannya, diantaranya yaitu:

1. Penerapan algoritma *Vigenere Cipher* dan *One Time Pad* untuk keamanan Pesan ini dapat dijadikan sebagai referensi untuk

dikembangkan menjadi keamanan Pesan yang lebih baik.

2. Penerpan algoritma *Vigenere Cipher* dan *One Time Pad* ini dapat di modifikasi atau dikembangkan dengan menambahkan algoritma enkripsi yang lain.
3. Penerapan algoritma *Vigenere Cipher* dan *One Time Pad* tidak hanya untuk keamanan Pesan saja tetapi juga bias diterapkan pada sistem yang lain.

DAFTAR PUSTAKA

[1] A. Zelvina, S. Efendi and D. Arisandi, "Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa," *JURNAL DUNIA TEKNOLOGI INFORMASI* , pp. 56-62, 2012.

[2] C. Nakasoshie, Diana and V. Sahfitri, "STUDI DAN IMPLEMENTASI ALGORITMA CAESAR CIPHER UNTUK KEAMANAN PESAN EMAIL YANG BERSIFAT RAHASIA," *Jurnal Ilmiah Studi dan Implementasi Algoritma Caesar Cipher untuk Keamanan Pesan Email yang Bersifat Rahasia,* pp. 1-20, 2012.

[3] M. FAIRUZABADI, "IMPLEMENTASI KRIPTOGRAFI KLASIK MENGGUNAKAN BORLAND DELPHI," *Jurnal Dinamika Informatika,* pp. 65-78, 2010.

[4] M. F. E. Purnomo, W. A. Priyono, S. S. N, R. Ambarwati and A. Wulandari, "Implementasi Algoritma Kriptografi RC4 Pada DSP TMS320C6713 Sebagai Pendukung Sekuritas Jaringan Komunikasi Voice over Internet Protocol (VoIP)," *Jurnal EECCIS,* Desember 2012.

[5] A. K. Dwi P, "Penerapan Algoritma Vigenere Cipher pada Aplikasi SMS Android," *Makalah IF3058 Kriptografi,* 2012.

[6] S. P. Agustanti, "PENERAPAN ALGORITMA ONE-TIME-PAD (OTP) UNTUK KEAMANAN LAYANAN PESAN SINGKAT (SHORT MESSAGES SERVICES, SMS)," *Jurnal Informatika Global,* pp. 47-51, 2010.