SISTEM KEAMANAN PESAN EMAIL MENGGUNAKAN ALGORITMA KRIPTOGRAFI KLASIK

Ismail[1] , Muh. Syahrir[2]
Sistem Informasi[1], Teknik Informatika[2]
STMIK Lamappapoleonro Soppeng[1], Universitas Indonesia Timur[2]
e-mail : ismail@stmik.ypls.ac.id[1] , syahrirfikom@gmail.com[2]

Abstrak

Penelitian ini bertujuan untuk merancangan aplikasi keamanan pesan email dengan enkripsi menggunakan algoritma kriptografi klasik dan juga mengimplementasikan hasil enkripsi algoritma kriptografi klasik untuk keamanan pesan email. Algoritma yang digunakan untuk enkripsi adalah algoritma kriptografi klasik. Algoritma ini merupakan algoritma sederhana atau dasar dari algoritma kriptografi. Bahasa pemrograman yang digunakan untuk merancang aplikasinya adalah Delphi 2009 dengan menggunakan metode pengujian Black Box. Hasil penelitian ini menunjukan bahwa sistem atau aplikasi yang dibuat sudah mampu memenuhi kebutuhan aplikasi email client yang menerapkan enkripsi dengan algoritma kriptografi klasik.

Kata Kunci : Pesan Email, Algoritma Kriptografi Klasik.

Abstract

This study aims to merancangan application security by encrypting email messages using classical cryptographic algorithms and also implements the results of classical cryptographic algorithms for encryption security to email messages. The algorithm used for encryption is classical cryptography algorithms. This algorithm is a simple algorithm or the basis of cryptographic algorithms. Programming language is used to design applications using Delphi 2009 with Black Box testing method. These results indicate that the system or application has been made to meet the needs of client email applications that implement encryption with classical cryptography algorithms.

Keywords: Messaging Email, Classical Cryptography Algorithms.

PENDAHULUAN

1. Latar Belakang

Dalam melakukan pengiriman dan penerimaan informasi atau pesan menggunakan email perlu dijaga keamanannya, karena email menggunakan jaringan internet yang merupakan media komunikasi umum (Publik), maka siapapun bisa mengakses informasi atau pesan pada jaringan tersebut. Sehingga memudahkan seseorang atau pihak lain yang tidak bertanggung jawab menyadap informasi atau pesan yang dikirim dengan email tersebut. Dengan demikian, proses pengiriman dan penerimaan informasi atau pesan menjadi tidak aman. Maka dibutuhkan sebuah sistem yang dapat mengamankan informasi atau pesan email yang dikirim melalui jaringan internet.

Salah satu cara untuk menjaga keamanan informasi atau pesan yaitu penyandian pesan atau enkripsi. Enkripsi merupakan suatu cara pengkodean atau penyandian pesan menjadi pesan yang

tidak bisa dimengerti oleh pihak yang tidak diinginkan. Sehingga pesan rahasia yang dikirim hanya dapat dimengerti oleh pihak-pihak tertentu yang dapat mendeskripsi pesan hasil enkripsi menjadi pesan sebenarnya. Ilmu tentang enkripsi dan deskripsi pesan ini disebut dengan kriptografi.

Pada zaman dahulu, algoritma kriptografi dilakukan dalam basis karakter (huruf). Karena kriptografi hanya digunakan pada pesan-pesan berbentuk tulisan. Algoritma kriptografi inilah yang disebut algoritma kriptografi klasik atau sering disebut kriptografi klasik. Tidak seperti pada zaman sekarang ini, dimana komputer adalah sarana utama melakukan pertukaran data, pesan dan informasi, sehingga pengguna algoritma kriptografipun dilakukan pada data-data komputer dalam mode bit-bit atau byte-byte data. Akibatnya kriptografi klasik telah jarang, bahkan sudah tidak digunakan lagi. Karena itulah penulis pada tugas akhir ini mengangkat kembali kriptografi klasik sebagai dasar pemahaman algoritma kriptografi dan diaplikasikan penggunaannya melalui program komputer. Dari hal tersebut, dibuat sebuah aplikasi untuk keamanan pesan email dengan metode enkripsi menggunakan algoritma kriptografi klasik.

2. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

a) Untuk merancang aplikasi yang digunakan untuk keamanan pesan email dengan enkripsi menggunakan algoritma kriptografi klasik.
b) Untuk mengimplementasikan enkripsi dan deskripsi algoritma kriptografi klasik untuk keamanan pesan email

TINJAUAN PUSTAKA

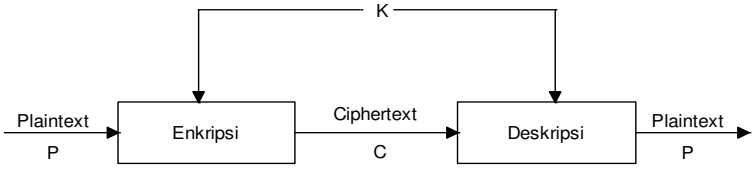
1. Pengertian Kriptografi

Kriptografi (cryptography) berasal dari bahasa Yunani: "Cryptos" artinya "Secret" (Rahasia) sedangkan "graphein" artinya "Writing" (Tulisan). Sedangkan kriptografi berarti "secret writing" (tulisan rahasia). Jadi kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke bentuk yang tidak dapat dimengerti. *(Firtin Fia. dkk, 2011).*

Secara umum kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plaintext) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan informasi baru (ciphertext) yang tidak dapat dibaca seecara langsung. Ciphertext tersebut dapat dikembalikan menjadi informasi awal (plaintext) melalui proses deskripsi.

2. Algoritma Simetri

Algoritma simetri disebut juga sebagai algoritma konvensional adalah algoritma yang menggunakan kunci enkripsi yang sama dengan kunci deskripsinya. Yang termasuk algoritma kunci simetri adalah DES, RC2, RC4, RC5, RC6, IDEA, Twofish, Magenta, FEAL, SAFER, LOKI, CAST, Rijndael (AES), Blowfish, GOST, A5, Kasumi dan lain-lain.



Gambar 1. Alur Algoritma Simetri

3. Algoritma Kriptografi Klasik

Algoritma kriptografi klasik adalah algoritma yang berbasi karakter, yaitu enkripsi dan deskripsi dilakukan pada setiap karakter pesan. *(Nathasia Novi D. dkk, 2011).* Kriptografi mempunyai sejarah yang panjang, mulai dari kriptografi Caesar yang berkembang pada zaman sebelum Masehi sampai kriptografi modern yang digunakan dalam komunikasi antar komputer di abad 20. Ada 2 teknik yang paling dasar, yaitu teknik subsitusi dan teknik transposisi. *(Fairuzabadi Muhammad. 2010).*

4. Email

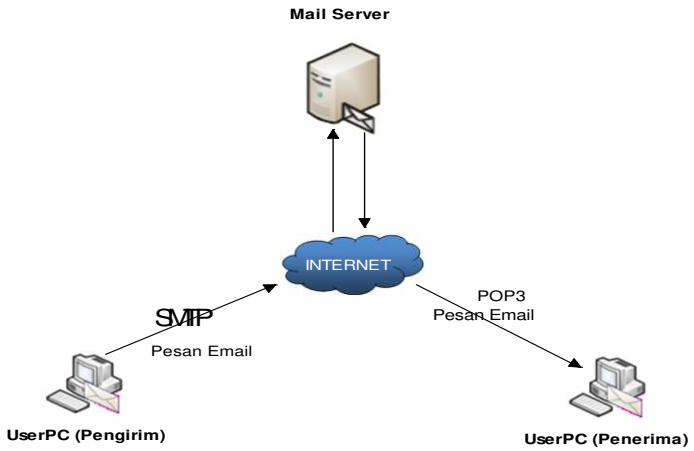
Email atau kalau dalam istilah Indonesia adalah surat elektronik yaitu aplikasi yang memungkinkan para pengguna internet untuk saling berkirim pesan melalui alamat elektronik di internet dimanapun mereka berada. Para pengguna email memiliki sebuah mailbox (kotak surat) elektronik yang tersimpan dalam suatu mailserver. Suatu mailbox memiliki sebuah alamat sebagai pengenal agar dapat berhubungan dengan mailbox lainnya, baik dalam bentuk peerimaan maupun pegiriman pesan. System Nama Domain (DNS) memastikan bahwa semua pengguna (user) memiliki alamat yang unik, tidak ada alamat yang sama diantara sekian juta pemakai internet *(Ghafur Abdul. 2011).*

Layanan email biasanya dikelompokkan dalam dua basis yaitu email berbasis client dan email berbasis web. Bagi pengguna email berbasis client, aktifitas peremailan dilakukan dengan menggunakan perangkat lunak email client, misalnya Eudora atau Outlook Express. Perangkat lunak ini menyediakan fungsi-fungsi penyuntingan dan pembacaan email secara offline (tidak tersambung ke internet). koneksi hanya diperlukan untuk melakukan pengiriman (send) atau penerima (recieve) email dari mailbox.

METODE PENELITIAN

1. Analisis Sistem Lama

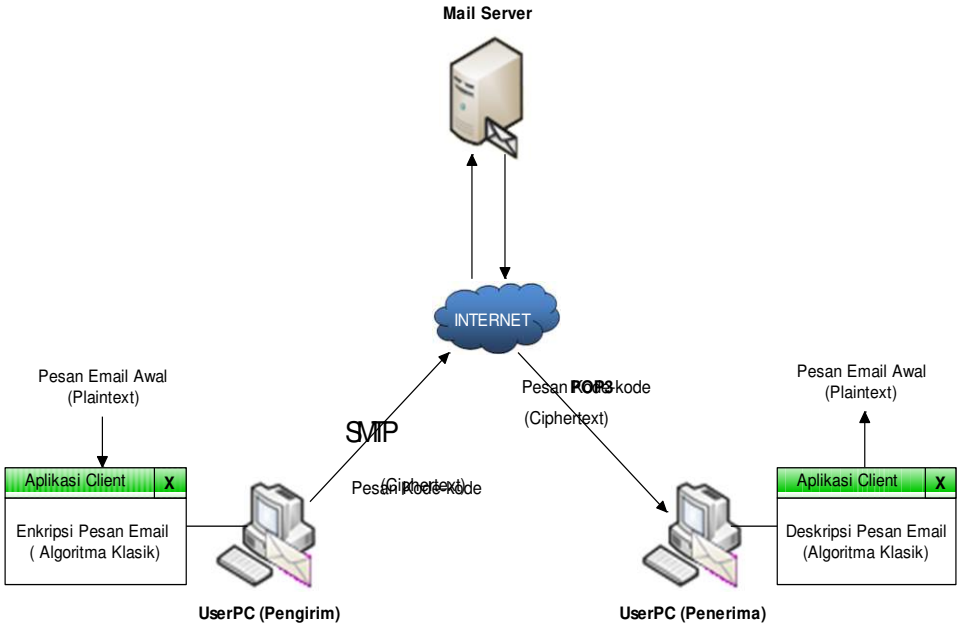
Proses pengiriman pesan email yang dilakukan adalah dimana pengirim mengirim pesan email dengan menggunakan port protokol SMTP *(Simple Mail Transfer Protocol)* ke Mail Server melalui jaringan internet dan penerima menerima pesan email yang dikirim ke Mail Server dengan menggunakan port protokol POP3 *(Post Office Protocol Version 3)* melalui jaringan internet. Proses pengiriman email dapat di gambarkan sesuai pada Gambar berikut :



Gambar 2. Sistem Lama

2. Analisis Sistem Baru

Proses pengiriman pesan email dengan aplikasi yang akan dibuat adalah dimana pengirim melakukan enkripsi terhadap pesan email *(plaintext)* dengan algoritma kriptografi klasik menjadi pesan kode-kode *(Ciphertext)* agar tidak bisa dibuka atau dibaca oleh pihak lain yang tidak berhak yang akan dikirim dengan menggunakan port protokol SMTP *(Simple Mail Transfer Protocol)* ke Mail Server melalui jaringan internet. Dan penerima menerima pesan email yang berupa kode-kode *(Ciphertext)* yang terkirim ke Mail Server dengan menggunakan port protokol POP3 *(Post Office Protocol Version 3)* melalui jaringan internet, kemudian melakukan deskripsi pesan kode-kode *(Ciphertext)* dengan algoritma kriptografi klasik menjadi pesan email *(Plaintext)* seperti semula atau sebelum dienkripsi agar pesan dapat dibuka atau dibaca. Proses pengiriman email yang diusulkan dapat dilihat pada Gambar berikut;



Gambar 3. Struktur Alur Sistem Baru

3. Metode Pengumpulan Data

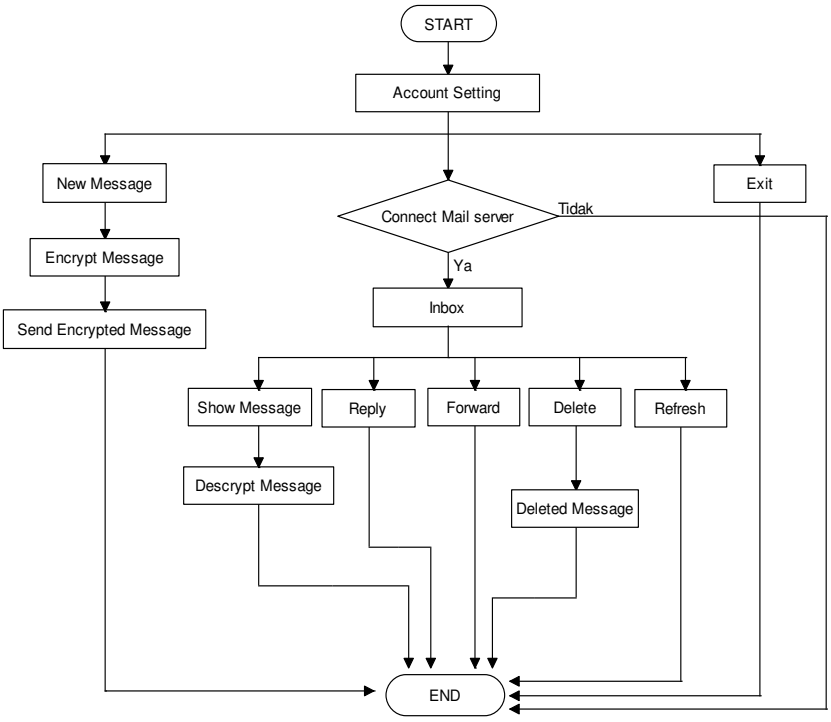
Teknik pengumpulan data yang digunakan pada penelitian ini adalah sebagai berikut:

a) Observasi
   Melakukan pengamatan langsung untuk mencari informasi yang berkaitan dengan informasi sistem keamanan pesan email.

b) Literatur Studi
   Pengumpulan data yang dilakukan penulis dengan cara mencari bahan yang mendukung dalam pendefinisian masalah melalui buku, internet yang erat kaitannya dengan permasalahan yang menjadi objek penelitian. Teknik ini dilakukan untuk memperoleh informasi bagaimana gambaran sistem dan memperoleh informasi yang dibutuhkan.

4. Perancangan Sistem Secara Umum

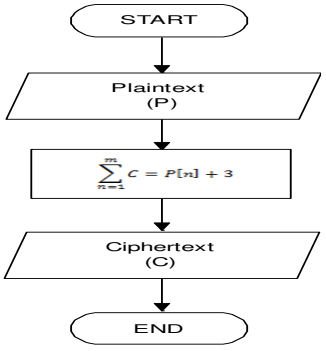
Berikut adalah perancangan aplikasi secara umum yang digambarkan melalui flow map DFD:



Gambar 4. Sistem Secara Umum

Dalam melakukan pengiriman dan penerimaan pesan email dari Mail Server pada aplikasi yang dibuat, pertama melakukan pengaturan akun email yang digunakan untuk mengirim dan menerima email dari Mail Server, Kemudian mengkoneksikan Email Client dengan Mail Server. Setelah berhasil konek ke Mail Server, maka muncul pesan email masuk pada Email Client yang terkirim ke Mail Server. Jika pesan email yang terkirim dari Mail Server terenkripsi, maka pesan di deskripsi agar pesan dapat terbaca. Untuk melakukan pengiriman pesan, buat pesan baru kemudian melakukan enkripsi terhadap pesan yang akan dikirim kemudian kirim pesan yang telah dienkripsi.

5. Flowchart Enkripsi Pesan Email



Gambar 4. Flowchart Enkripsi Pesan Email

Proses enkripsi pesan email dengan algoritma kriptografi klasik sesuai dengan flowchart pada Gambar diatas adalah :

a) Masukan plaintext (P) yaitu sembarang karakter.
b) Hitung posisi karakter (n) ditambah 3
c) Maka akan di peroleh ciphertext (C)

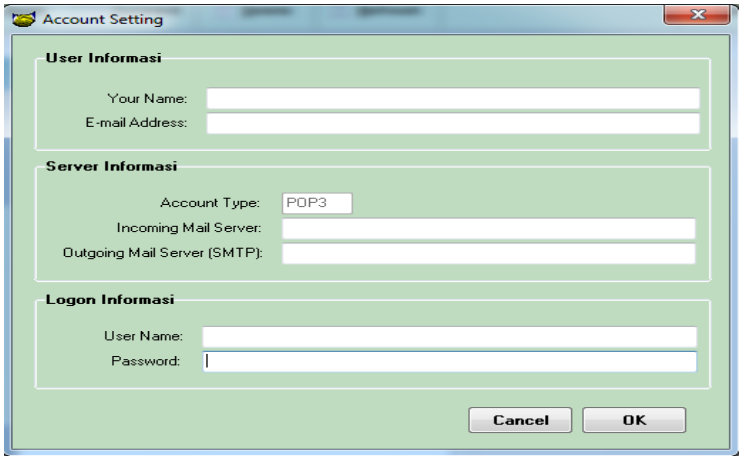
HASIL PENELITIAN

1. Implementasi Program

Pada bagian ini akan dijelaskan mengenai struktur dan perancangan antarmuka dari email client. Antarmuka merupakan bagian yang sangat penting dalam penggunaan perangkat lunak. Antarmuka yang friendly dan yang baik akan memudahkan pengguna (*user*) untuk berinteraksi dengan sistem yang terdapat dalam sebuah perangkat lunak. Aplikasi keamanan pesan email dengan enkripsi menggunakan algoritma kriptografi klasik mempunyai struktur antarmuka untuk memudahkan pengguna dalam berinteraksi:

a) *Form Account*

Form ini merupakan form account yang digunakan untuk pengaturan akun email pengguna untuk bisa menggunakan aplikasi ini. Pengguna pada aplikasi ini hanya dibatasi satu pengguna saja. Pada form account pengguna menginputkan account emailnya yaitu Your Name, Email Address, Username, Password dan menginputkan protokol POP3 dan SMTP-nya untuk bisa mengkoneksikan ke Mail Server. Untuk mengakses form account ini bisa melalui tombol Account Setting dan juga bisa melalui menu Tools kemudian Account Setting.



Gambar 5. Form Account

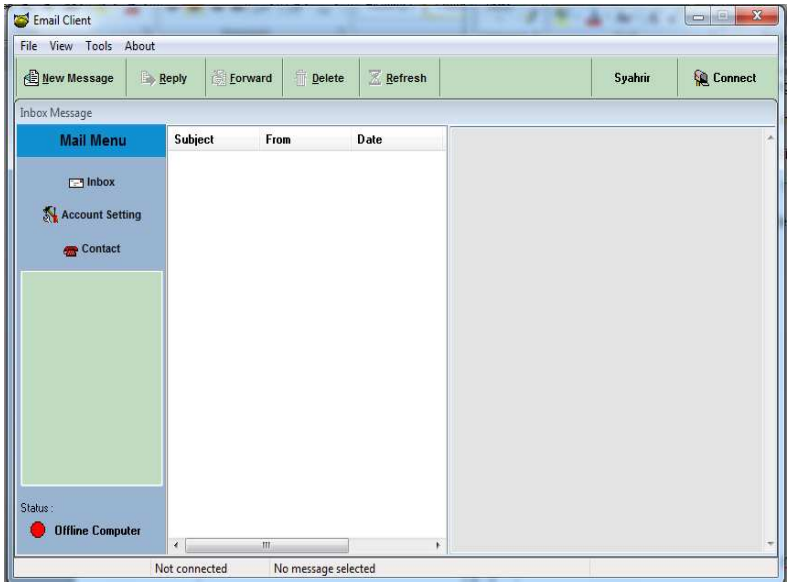
b) *Form Message*

Form message ini merupakan form yang digunakan untuk mengirim pesan email ke pengguna yang lainnya. Pada form ini juga terdapat fasilitas enkripsi pesan email dengan memberi tanda centang pada "*Encrypted message*" maka secara otomatis pesan email akan terenkripsi. Untuk mengakses form message ini bisa melalui tombol *New Message* dan juga bisa melalui menu File kemudian *New Message.*

Gambar 6. Form Message

c) Form Utama

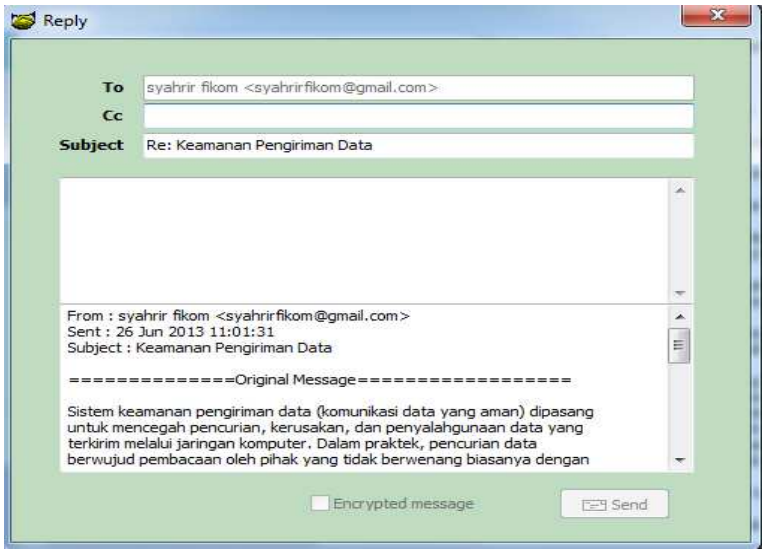
Form utama ini merupakan tampilan utama dari keseluruhan sistem aplikasi email client yang dilengkapi enkripsi menggunakan algoritma kriptografi klasik. Pada form utama ini terdapat beberapa menu dan tombol untuk membuka form yang lainnya yang juga menjadi bagian sistem seperti menu *File, View, Tools, About* dan tombol *New Message, Reply, Forward, Delete, Refresh, Connect*



Gambar 7. Tampilan Form Utama

d) *Form Replay*

Form reply ini merupakan form yang digunakan untuk membalas pesan email yang masuk. Form ini hampir sama dengan form message yang juga terdapat fasilitas untuk mengenkripsi pesan email yang akan dikirim ke pengguna lainnya, namun pada form ini bisa melihat pesan email yang masuk atau pesan email yang akan dibalas. Untuk mengakses form ini caranya klik pada email yang masuk kemudian klik tombol Reply.



Gambar 8. Tampilan Form Replay

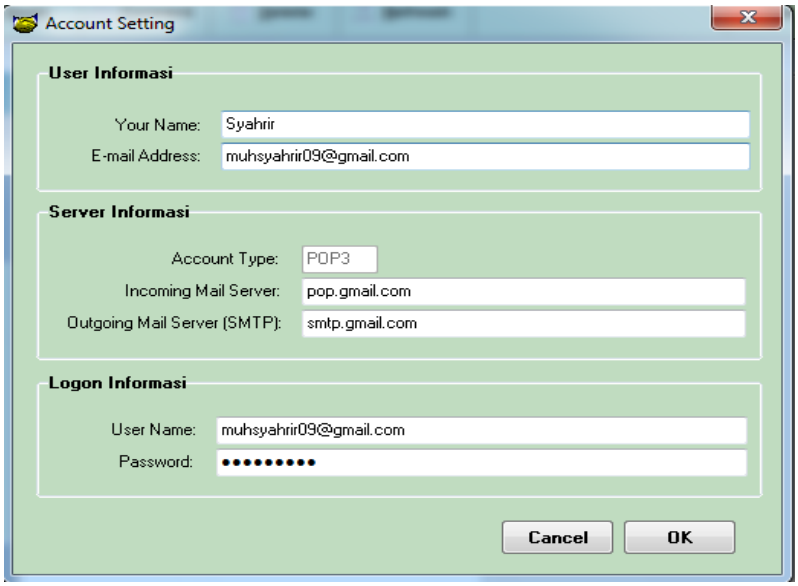
2. Pengujian Sistem

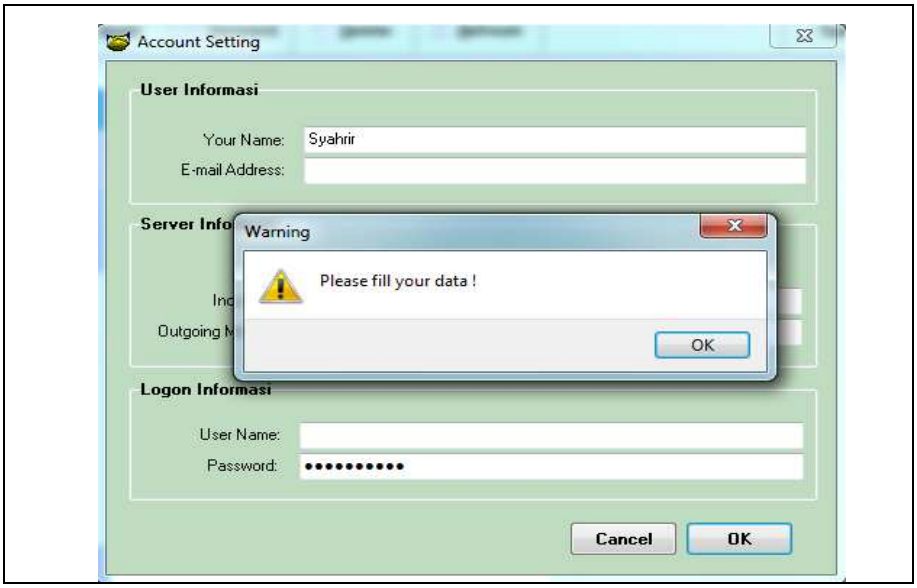
Untuk mencoba keberhasilan perangkat lunak atau aplikasi yang telah dibuat, apakah perangkat lunak atau aplikasi itu berjalan dengan baik, maka harus dilakukan pengujian terhadap perangkat lunak atau aplikasi tersebut. Pengujian ini dilakukan dengan menggunakan metode pengujian Black Box yang berfokus pada persyaratan fungsional perangkat lunak untuk mendapatkan serangkaian kondisi input yang sesuai dengan persyaratan fungsional program.

a. Pengujian Koneksi Email Client Dengan Mail Server

Pengujian proses koneksi email client ke mail srver atau proses pengambilan pesan email dari mail server dimana proses pengujiannya adalah pertama melakukan pengaturan akun email yang akan digunakan di account setting. Kemudian melakukan koneksi ke mail server.

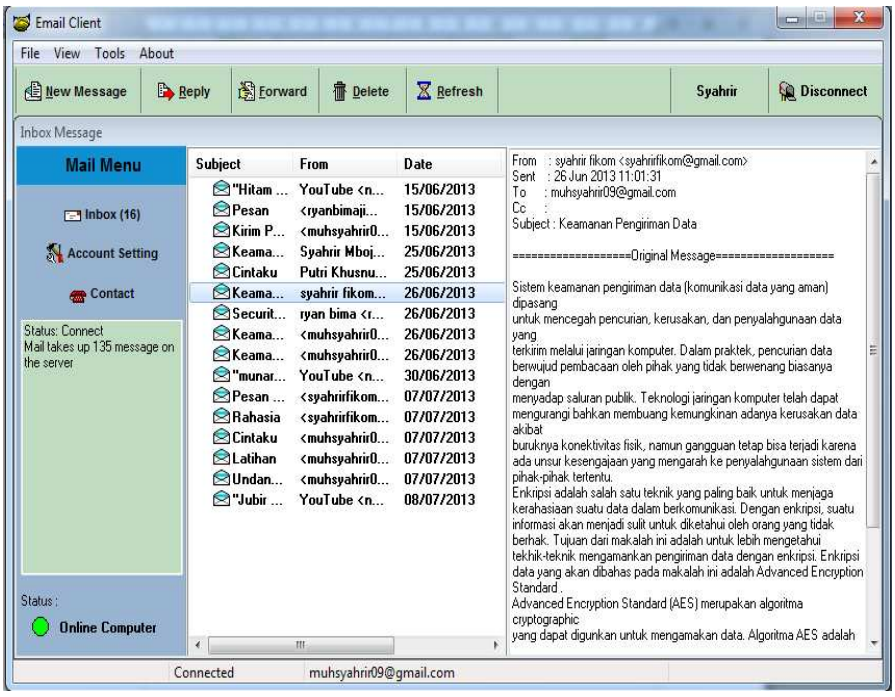
Tabel 1. Pengujian Pengaturan Akun Email

Kasus Dan Hasil Uji (Data Normal)			
Data	**Yang Diharapkan**	**Pengamatan**	**Kesimpulan**
OK	Menyimpan data yang sudah diinput pada Notepad	Data tersimpan di notepad	Diterima
Screen Shoot			
			
Kasus dan Hasil Uji (Data Salah)			
Data	**Yang Diharapkan**	**Pengamatan**	**Kesimpulan**
OK	Menampilka pesan peringatan	Pesan peringatan muncul	Diterima
Screen Shoot			



Tabel 2. Pengujian Koneksi Email Client Dengan Mail Server

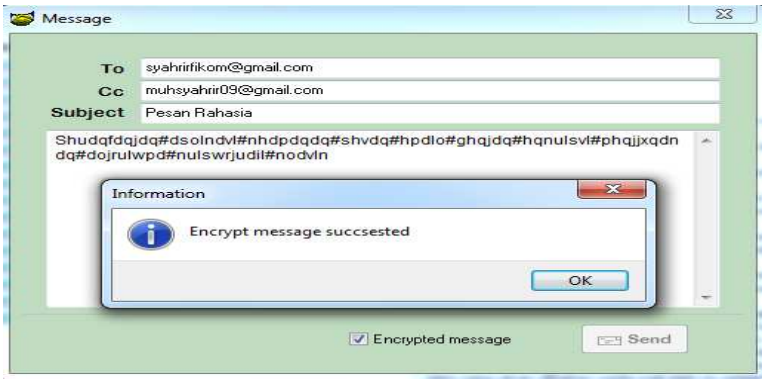
Kasus Dan Hasil Uji			
Data	**Yang Diharapkan**	**Pengamatan**	**Kesimpulan**
Connect	Menampilkan email yang ada pada mail server	Email yang ada pada mail server tampil	Diterima
Screen Shoot			



b. Pengujian Enkripsi Pesan Email

Untuk melakukan enkripsi pesan email pada aplikasi yang dibuat, dilakukan pada saat melakukan pengiriman pesan email ke pengguna lainnya dengan tujuan untuk mengamankan pesan email yang akan dikirim.

Tabel 3. Pengujian Enkripsi Pesan Email

Kasus Dan Hasil Uji			
Data	**Yang Diharapkan**	**Pengamatan**	**Kesimpulan**
Encrypted message	Pesan email yang diinput terenkripsi dan muncul informasi kesuksesan proses enkripsi.	Pesan berubah menjadi pesan yang tidak bisa dimengerti.	Diterima
Screen Shoot			
			

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, maka diambil beberapa kesimpulan sebagai berikut:

1. Sistem yang dibuat sudah mampu memenuhi kebutuhan aplikasi email client yang menerapkan enkripsi dengan algoritma kriptografi klasik.
2. Perangkat lunak atau aplikasi ini hanya mengamankan isi pesan email bukan mengamankan jalur transfer email.
3. Pada aplikasi yang dibuat ini, hanya penerima yang dituju atau orang yang memiliki kunci yang sama yang bisa membaca isi pesan email yang dikirim oleh pengirim.
4. Semua karakter pada body email bisa di enkripsi dan di deskripsi dengan sempurna menggunakan algoritma kriptografi klasik.

DAFTAR PUSTAKA

Fairuzabadi Muhammad. 2010, ***Implementasi Kriptografi Klasik Menggunakan Borland Delphi,*** Jurnal Dinamika Informatika: Volume 4, Nomor 2, September 2010: 65-78.

Firtin Fia. dkk, 2011, ***Rancang Bangun Sistem Enkripsi Pengiriman Informasi Menggunakan Algoritma Kriptografi Klasik*****,** Proyek Akhir PENS-ITS Keputih Sukolilo Surabaya.

Fiva, Rosalana. 2009, ***Langkah Mudah Administrasi Jaringan Menggunakan Linux Ubuntu 9***, Semarang.

Ghafur Abdul. 2011, *Rancang Bangun Aplikasi Pengamanam Email Menggunakan Algoritma Elgamal (Skripsi S1 Tidak Diterbitkan)*, Jurusan Teknik Informatika Fakultas Sains Dan Teknologi UIN Maulana Malik Ibrahim Malang.

Hermawan Widyo. 2009, *Panduan Praktis Delphi 2009*, Andi: Yogyakarta; Wahana Komputer: Semarang.

Kurniawan W. 2007, *Computer Starter Guide: Jaringan Komputer*, Andi: Yogyakarta.

Lusiana Veranica. 2010, *Perancangan Perangkat Lunak Untuk Keamanan Informasi Pada E-mail Menggunakan Algoritma AES Dan RSA (Tesis Tidak Dipublikasikan)*, Magister Sistem Informasi UNDIP Semarang.

Madcoms. 2009. *Panduan Lengkap Membangun Sistem Jaringan Komputer*, Andi: Yogyakarta.

Nathasia Novi D. dkk, 2011. *Penerapan Teknik Kriptografi Stream Cipher Untuk Keamanan Basis Data*, Jurnal Basis Data, ICT Reseaarch Center UNAS: Vol.6, No.1, Mei 2011.

Sukmaaji A.dkk, 2008. *Jaringan Komputer Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan*, Andi: Yogyakarta