SISTEM KEMANAN DATA MENGGUNAKAN ALGORITMA KRIPTOGRAFI BLOWFISH PADA APLIKASI CHATTING

Nur Sakti
Dosen STMIK Lamappapoleonro Soppeng
Sistem Informasi, STMIK Lamappapoleonro Soppeng
e-mail : chaktysci@gmail.com

Abstrak

cara pengiriman pesan mungkin tidak harus lagi memakai kertas sebagai media pesan, sekarang kita bias menggunakan banyak aplikasi untuk bertukar pesan seperti email, chatting, dan lain sebagainya. secara ril hubungannya jika pesan pada email atau chatting itu sangat penting dan harus dijaga kerahasiaannya maka pencegahannya adalah menerapkan system keamanan pada chatting tersebut untuk mencegah dari orang yang tidak berhak misalnya sniffing. kriptografi Blowfish yang merupakan metode enkripsi yang mirip dengan DES (Data Encryption Standard) (DES-like cipher) dan diciptakan oleh Bruce Schneier yang ditujukan untuk mikroposesor besar (32 bit ke atas dengan cache data yang besar). pada penelitian ini diangkat kriptografi klasik sebagai dasar pemahaman algoritma kriptografi dan diaplikasikan penggunaannya melalui program komputer keamanan pesan dengan metode enkripsi menggunakan algoritma kriptografi blowfish.

Kata Kunci : Sistem,*Kriptografi Blowfish, Chatting.*

Abstract

The way message delivery may no longer have to use paper as a message medium, now we can use many applications to exchange messages such as email, chat, and so forth. in real terms if the message on email or chat is very important and must be kept confidential the prevention is to apply security system on the chat to prevent from unauthorized people such as sniffing. Blowfish cryptography is an encryption method similar to DES (Data Encryption Standard) (DES-like cipher) and created by Bruce Schneier devoted to large microposesors (32 bits upwards with large data cache). in this study raised classical cryptography as the basis of understanding of cryptographic algorithms and applied its use through the computer program of message security with encryption method using blowfish cryptography algorithm.

Keywords: System, Cryptography Blowfish, Chatting.

1. PENDAHULUAN

1.1. Latar Belakang Masalah

Keamanan dalam hidup saat ini adalah hal yang sangat penting. Arti dari keamanan itu sendiri adalah menjaga suatu unsure yang sangat penting dari tindakan yang tidak diinginkan beberapa contohnya adalah informasi dan pesan. Jika kita bertukar pesan (misalnya surat), maka kita tentu ingin pesan yang kita kirim sampai kepihak yang ditujuh dengan aman. Sehingga pesan yang kita kirim tidak bisa dibaca oleh orang lain yang tidak berhak. Contoh lain dalam dunia teknologi saat ini cara pengiriman pesan mungkin tidak harus lagi memakai kertas sebagai media pesan, sekarang kita bias menggunakan banyak aplikasi untuk bertukar pesan seperti email, chatting, dan lain sebagainya. Maka secara ril

hubungannya jika pesan pada email atau chatting itu sangat penting dan harus dijaga kerahasiaannya maka pencegahannya adalah menerapkan system keamanan pada chatting tersebut untuk mencegah dari orang yang tidak berhak misalnya sniffing. Dalam masalah keamanan yang disebutkan bias diselesaikan dengan menggunakan kriptografi.

Kriptografi tidak hanya menyediakan alat untuk keamanan pesan, tetapi juga merupakan suatu kumpulan teknik dalam menyembunyikan kerahasiaan pesan. Ada beberapa algoritma kriptografi yang sudah terbuka untuk dipelajari dan digunakan untuk proses keamanan data pada jaringan komputer, seperti Blowfish, DES (Data Encryption Standard), AES, RC-4, TwoFish, RC-5, IDE, RSA, dan lain-lain. Salah satu algoritma kriptografi yang akan dibahas dalam tugas akhir ini adalah kriptografi Blowfish yang merupakan metode enkripsi yang mirip dengan DES (Data Encryption Standard) (DES-like cipher) dan diciptakan oleh Bruce Schneier yang ditujukan untuk mikroposesor besar (32 bit ke atas dengan cache data yang besar). 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 diatas, penulis merancang sebuah aplikasi untuk keamanan pesan dengan metode enkripsi menggunakan algoritma kriptografi blowfish dengan judul **"Sistem Kemanan Data Menggunakan Algoritma Kriptografi Blowfish Pada Aplikasi Chatting"**.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah diatas, rumusan masalahnya adalah:

1. Bagaimana implementasi algoritma kriptografi blowfish untuk enkripsi dan deskripsi pesan pada aplikasi chatting untuk jaringan LAN.
2. Bagaimana merancang aplikasi chatting dengan enkripsi dan deskripsi menggunakan algoritma kriptografi Blowfish untuk jaringan LAN.

1.3. Tujuan Penelitian

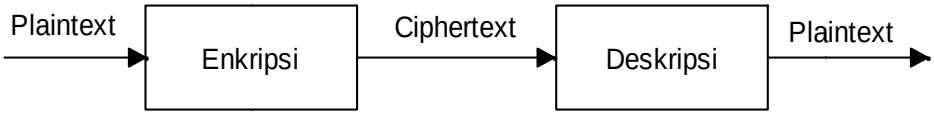
Adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Untuk mengimplementasikan algoritma kriptografi Blowfish untuk enkripsi dan deskripsi pesan pada aplikasi chatting untuk jaringan LAN.
2. Untuk merancang aplikasi chatting dengan enkripsi dan deskripsi menggunakan algoritma kriptografi Blowfish.

2. LANDASAN TEORI

2.1. Pengertian Kriptografi

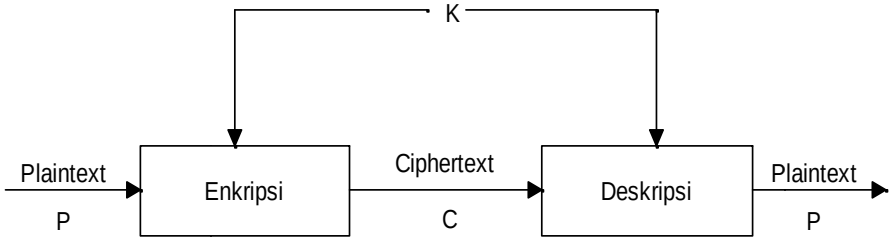
Kriptografi (cryptography) berasal dari bahasa Yunani: "Cryptos" artinya "Secret" (Rahasia) sedangkan "graphein" artinya "Writing" (Tulisan). Sedangkan kriptografi berarti "secret writing" (tulisan rahasia). Jadi kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara 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. Urutan proses kriptografi secara umum dapat dilihat pada gambar dibawah ini.



Gambar 2.1 Mekanisme Enkripsi dan Deskripsi

2.2. Algoritma Simetris

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 2.2 Algoritma Simetri.

2.3. Algoritma Asimetris

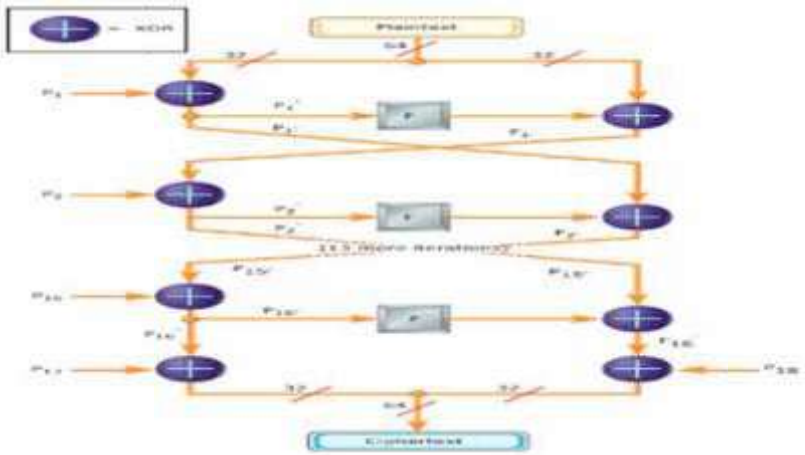
Algoritma asimetri (juga disebut algoritma kunci publik) didesain sedemikian sehingga kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk deskrisi. Enkripsi dengan kunci publik Ke dinyatakan sebagai berikut :

EKe (M) = C

DKd (C) = M

2.4. Algoritma *Blowfish*

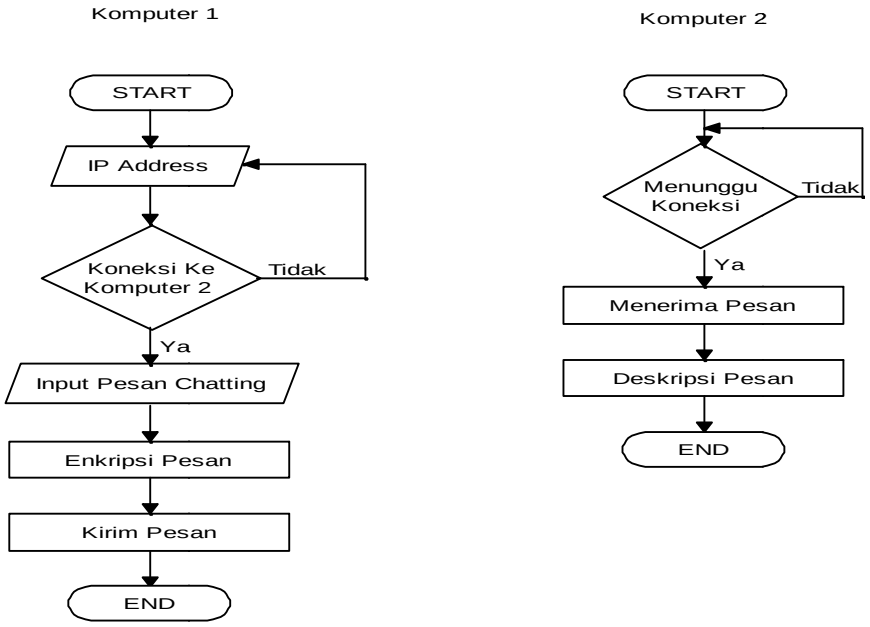
Blowfish termasuk dalam enkripsi block Cipher 64-bit dengan panjang kunci yang bervariasi antara 32-bit sampai 448-bit. Algoritma Blowfish terdiri atas dua bagian yaitu Pembangkitan sub-kunci (Key-Expansion) dan Enkripsi Data. Enkripsi Data terdiri dari iterasi fungsi sederhana (Feistel Network) sebanyak 16 kali putaran. Semua operasi adalah penambahan (addition) dan XOR pada variabel 32-bit. Pada algoritma Blowfish, digunakan banyak subkey. Kunci-kunci ini harus dihitung atau dibangkitkan terlebih dahulu sebelum dilakukan enkripsi atau dekripsi data. Pada jaringan feistel, Blowfish memiliki 16 iterasi, masukannya adalah 64-bit elemen data atau sebut saja "X".



Gambar 2.3 Algoritma Blowfish.

3. METODE PENELITIAN

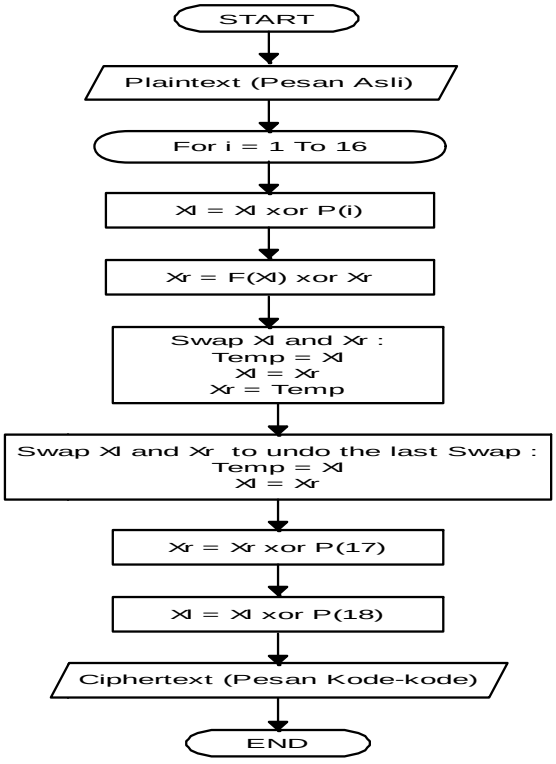
3.1. Flowchart Sistem



Gambar 3.1 Flowchart Proses Pengiriman Pesan.

Dalam melakukan pengiriman dan penerimaan pesan (*chating*) dari Server pada aplikasi yang dibuat, pertama melakukan pengaturan ip addres yang digunakan untuk mengirim dan menerima pesan (*chating*) dari Server, Kemudian mengkoneksikan pesan (*chating*) Client dengan Server. Setelah berhasil konek ke Server, maka muncul pesan (*chating*) masuk pada (*chating*) Client yang terkirim ke (*chating*) 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.

3.2. Flowchart Enkripsi



Gambar 3.1 Flowchart Enkripsi.

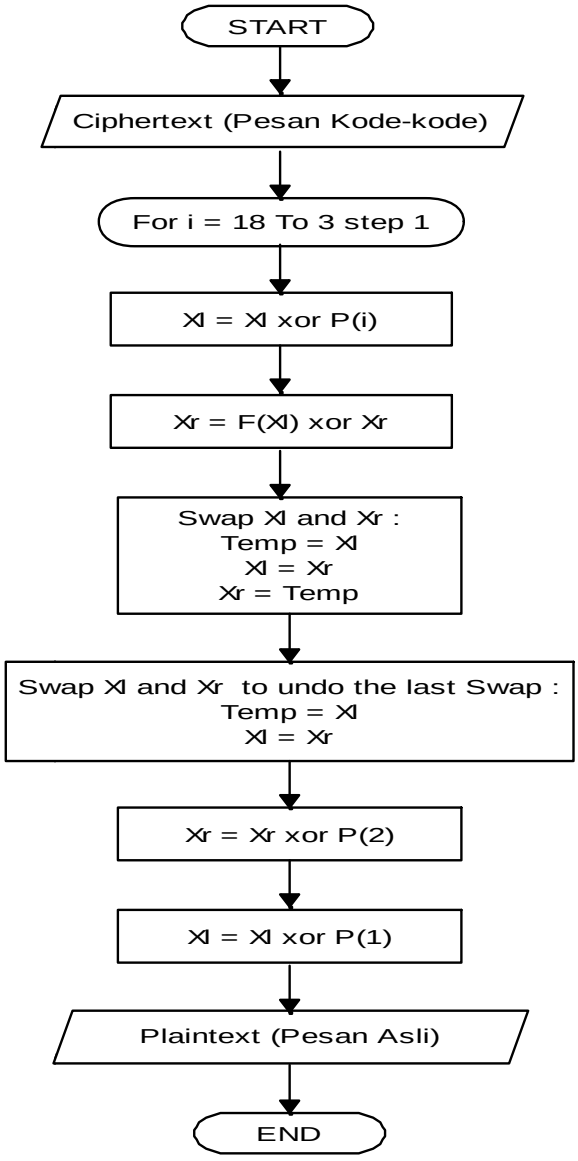
Pada gambar diatas adalah menjelaskan tentang proses enkripsi pertama masukkan palintext atau pesan asli,langkah langkah untuk melakukan proses enkripsi adalah sebagai berikut :

1. Bagi X menjadi dua bagian yang masing masing terdiri dari 32 bit yaitu Xl dan Xr
2. Untuk iterasi i = 1 sampai 16 lakukan :
   a. Xl=Xl Xor P(i)
   b. Xr=F(Xl)XorXr
   c. Tukar Xl dan Xr
3. Setelah iterasi ke-enambelas,tukar Xl dan Xr lagi untuk membatalkan proses pertukaran terakhir.
4. Lalu lakukan :
   a. Xr = Xr Xor P(17)

b. Xl = Xl Xor P(18)

5. Terakhir, Gabungkan kembali Xl dan Xr dalam 64-bit blok data untuk medapatkan ciphertext.
6. Ulangi blok diatas sampai seluruh blok dari data terenkripsi, kemudian masukkan ciphertext kedalam file tujuan.

3.3. Flowchart Dekripsi



Gambar 3.1 : Flowchart Dekripsi.

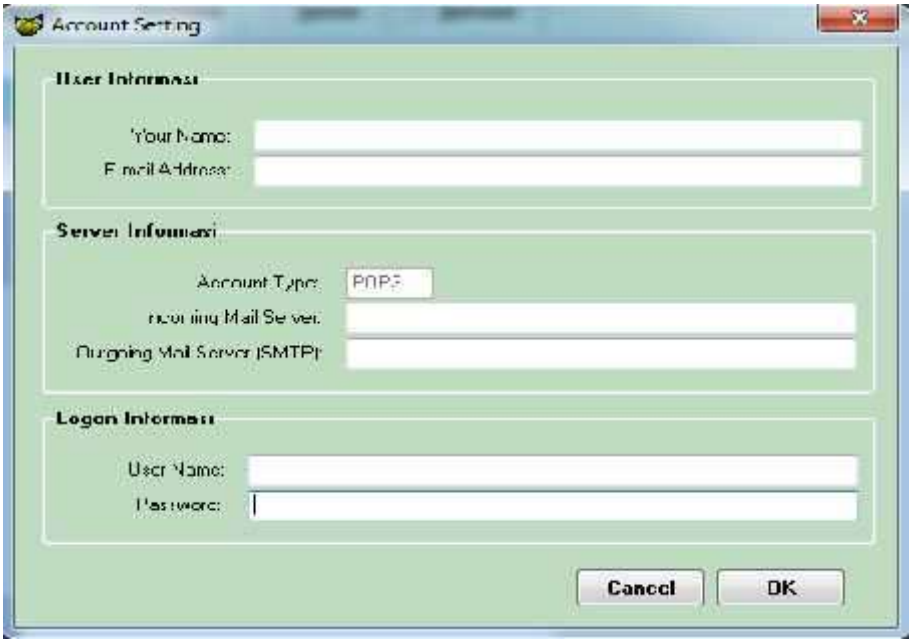
Proses deskripsi pada gambar diatas hampir sama dengan proses enkripsi hanya saja sub kunci P(1) sampai P(18) digunakan dalam urutan terbalik yaitu P(1) menjadi P(18) , P(2) menjadi P(17) dan seterusnya. Didalam proses deskripsi ciphertext diubah kembali kedalam bentuk plaintext atau kondisi semula sebelum dienkripsi.

4. HASIL DAN PEMBAHASAN

4.1. 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.

4.1.1. Form *Account*

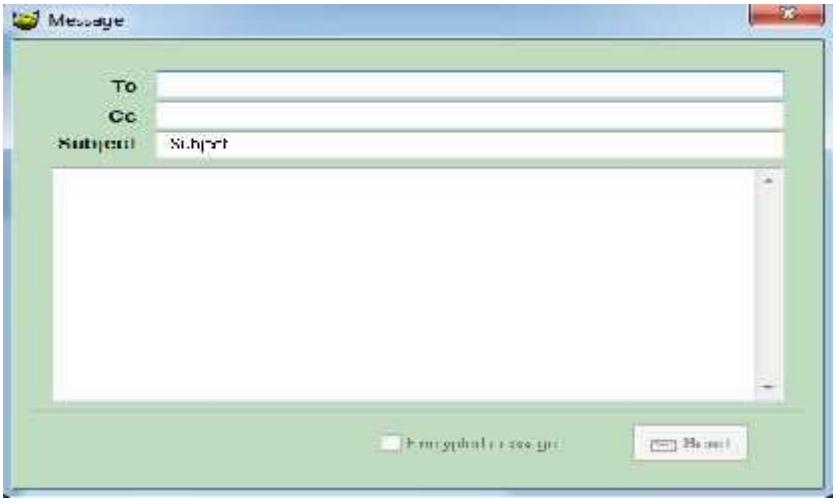


Gambar 4.1 : Form Account

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.

4.1.2. 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 4.2 : Form *Message*

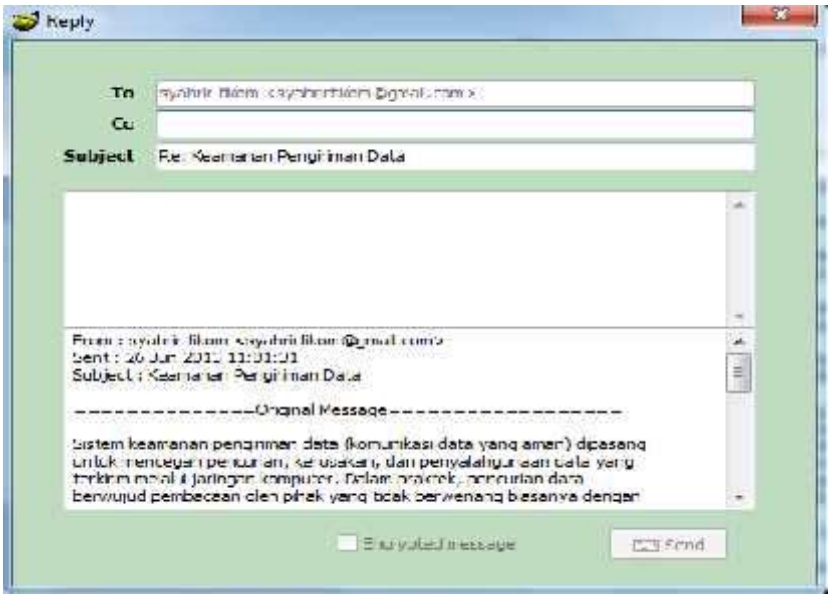
4.1.3. Form *Show*

Form show ini merupakan form yang digunakan untuk memunculkan pesan email yang dikirim oleh pengirim. Pada form ini juga terdapat fasilitas untuk mendeskripsi pesan email dengan memberi tanda centang pada "*Descrypt message*" maka secara otomatis pesan akan kembali seperti semula (pesan asli). Untuk memunculkan form show ini, klik dua kali pada email yang masuk atau bisa klik satu kali kemudian tekan enter.

Gambar 4.3 : Form *Show*

4.1.4. 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 4.4 : Form *Replay*

5. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, maka penulis mengambil 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.
5. Hasil deskripsi dengan kriptografi menggunakan algoritma klasik pada aplikasi ini lebih panjang dari plaintextnya (pesan asli) karena ada penambahan karakter, namun pesan sudah bisa terbaca.

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.