Penerapan Algoritma One Time PAD pada e-Mail Client Berbasis Web

Fatmasari

***Abstract*—Electronic mail (e-mail) is currently one of the internet features that are now commonly used and play a role in sending letters electronically. Fast delivery makes it easier for users, but this also increases the leakage of messages that are usually sent without security (plain text). So, some important messages can be done by applying cryptography when sending and reading e-mail. And from the many cryptographic algorithms that exist, One Time Pad can be used in this condition and this algorithm will be discussed in this paper.**

***Intisari*—Elecronic mail (e-mail) saat ini adalah salah satu dari fitur internet yang kini lazim digunakan dan berperan dalam pengiriman surat secara elektronik. Pengiriman yang cepat memang memudahkan pengguna, akan tetapi hal ini juga memperbesar kebocoran (leak) terhadap pesan yang biasanya dikirimkan tanpa adanya keamanan (plain text). Sehingga untuk beberapa pesan yang bersifat penting, maka dapat dilakukan dengan menerapkan kriptografi pada saat pengiriman dan membaca e-mail. Dan dari banyaknya algoritma kriptografi yang ada, One Time Pad adalah salah satunya yang dapat dimanfaatkan pada kondisi ini dan algoritma ini yang akan dibahas pada paper kali ini.**

***Kata Kunci*— Otp, Kriptografi, Surel,**

I. PENDAHULUAN

Dalam perkembangan teknologi saat ini, teknologi email (Electronic Mail) adalah merupakan sesuatu yang sangat penting dalam dunia komunikasi. Dikarenakan dengan adanya email manusia dapat mengirimkan pesan dan juga data melalui teknologi informasi. Pada saat sekarang ini pengiriman surat sudah sangat jarang dilakukan melalui pengiriman pos. Hal ini dikarenakan pengiriman melalui pos membutuhkan waktu yang lama dan kurang praktis. Dan ini semakin menguatkan manfaat email dalam kehidupan sehari-hari.

Pengiriman surat secara konvensional masih digunakan untuk komunikasi yang bersifat formal, seperti antar instansi pemerintah dan dunia pendidikan. Namun, terkadang banyak orang yang beralih menggunakan email untuk pengiriman surat formal karena lebih praktis dan cepat. Namun, selain berbagai macam kemudahan dan keuntungan yang ditawarkan dengan teknologi tersebut, terdapat bahaya yang mungkin timbul. Salah satunya adalah kemungkinan terjadinya kebocoran data atau informasi yang ditransmisikan. Karena pengiriman email melalui internet akan melalui proses yang cukup panjang yakni melewati beberapa server. Serta pembobolan akun email oleh seorang hacker untuk mendapatkan informasi yang penting dari sebuah email, akan sangat memungkinkan terjadinya kebocoran data.

Oleh karena itu maka perlu dilakukan sebuah penyandian (enkripsi) email untuk melakukan pengacakan pesan dan data dalam sebuah email. Agar email yang kita kirimkan tidak dapat terbaca oleh orang lain, kecuali pada orang yang berhak menerimanya.

Jurusan Sistem Informasi STMIK Antar Bangsa, Kawasan Bisnis CBD Ciledug, Jl. HOS Cokroaminoto No.29-35, RT.001/RW.001, Karang Tengah, Kec. Ciledug, Kota Tangerang, Banten, 15157 INDONESIA (telp:021 874561; e-mail: fsarie@gmail.com)

II. METODE PENGEMBANGAN

Metode pengembangan yang digunakan adalah Metode Prototyping yang merupakan metode pengembangan sistem dimana hasil analisa pembagian sistem langsung diterapkan dalam sebuah model tanpa menunggu seluruh sistem selesai dikerjakan.

Adapun tahapan dalam metode prototyping adalah :

1. Analisis
   Merupakan proses menganalisis keperluan yang terdapat pada permasalahan yang ada.
2. Desain
   Tahap ini merupakan proses dari model persentase permasalahan yang ada.
3. Pengembangan Prototype
   Proses buat prototype disini adalah pembuatan model secara keseluruhan dan rencana pemecahan masalah.
4. Evaluasi
   Merupakan evaluasi yang dilakukan pihak-pihak terhadap prototype yang telah dibuat.
5. Perbaikan protoype
   Merupakan hasil dari prototype yang dibuat dimana telah sesuai dengan yang diinginkan.

III. LANDASAN TEORI

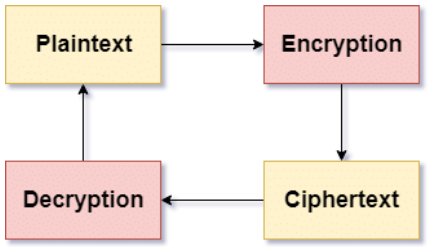
Data mempunyai peranan penting dalam melaksanakan suatu kegiatan guna mencapai suatu tujuan. Dengan pengertian ini banyak pihak yang berusaha untuk mendapatkan data untuk kepentingan masing-masing. Karena data sifatnya mudah digandakan, maka data tersebut akan menjadi mahal bila sifatnya rahasia. Keuntungan menggunakan metode enkripsi ini adalah bila pihak yang ingin mencuri data (misal data kontrol akses, file password dan lain-lain) berhasil dicuri atau dibongkar penyusup, maka ia harus mengeluarkan tenaga ekstra dan sumber daya lain untuk membaca data atau mendekripsi data tersebut.

A. Kriptografi

Kriptografi (*cryptography*) adalah studi teknik informatika yang berhubungan dengan aspek-aspek pengamanan informasi. Cryptography algorithms adalah persamaan matematika yang digunakan untuk proses enkripsi (*encryption*) dan dekripsi (*decryption*). Umumnya kedua persamaan matematika baik

untuk proses enkripsi dan dekripsi tersebut berhubungan matematis yang cukup erat.

Sedangkan Cryptographic system atau cryptosystem adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi.

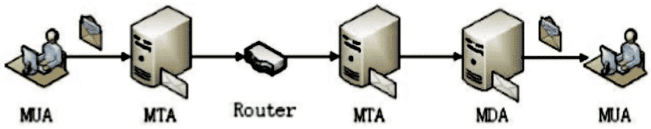


Gbr 1. Proses Kriptografi

B. E-mail

Email atau Surat Elekronik adalah sarana kirim mengirim surat melalui jalur jaringan komputer (internet). Dengan surat biasa umumnya pengirim perlu membayar per pengiriman (dengan membeli perangko), tetapi dengan email biaya yang dikeluarkan adalah biaya untuk membayar sambungan internet. Adapun langkah-langkah yang ditempuh oleh sebuah email untuk sampai di penerima adalah sebagai berikut :

1. Pengirim menulis surat elektronik melaui Mail User Agent (MUA), yang disebut Email Client.
2. Dari Email Client surat elektronik diteruskan ke Mail Transfer Agent (MTA) atau yang disebut POP3 (Post Office Protocol 3) atau IMAP (Intenet Mail Acces Protocol) server melalui SMTP (Simple Mail Transfer Protocol) milik penyedia layanan surat elektronik yang digunakan oleh pengirim.
3. Melalui jariangan internet surat elektronik tersebut diteruskan ke MTA milik penyedia layanan surat elektronik yang digunakan oleh penerima untuk kemudian dibagikan kepada MDA (Mail Delivery Agent).
4. Surat elektronik kemudian diteruskan ke komputer penerima (Email Client).



Gbr 2. Proses Pengiriman e-Mail

C. *Algoritma One Time Pad*

One Time Pad (OTP) adalah stream chiper yang melakukan enkripsi dan dekripsi setiap satu karakter. Algoritma ini ditemukan pada tahun 1918 oleh Major Joseph Mauborgne dan Gilbert Vernam sebagai perbaikan dari Vernam Chiper untuk menghasilkan keamanan yang lebih baik.

Mauborgne mengusulkan penggunaan one time pad (pad = kertas bloknot) yang berisi deretan karakter-karakter kunci yang dibangkitkan secara acak. Satu pad hanya digunakan sekali (one time) saja untuk mengenkripsi pesan, setelah itu pad yang telah digunakan dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain.

Enkripsi dapat dinyatakan sebagai penjumlahan modulo 26 dari satu karakter plaintext dengan satu karakter kunci one time pad.

$$C_i = (P_i + K_i) \bmod 26 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Jika karakter yang digunakan adalah anggota himpunan 256 karakter (seperti karakter dengan pengkodean ASCII), maka persamaan enkripsinya menjadi:

$$C_i = (P_i + K_i) \bmod 256 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2)$$

Setelah pengirim melakukan enkripsi pesan dengan kunci, maka kunci tersebut dimusnahkan. Penerima pesan menggunakan pad yang sama untuk mendekripsikan karakter-karakter chipertext menjadi karakter - karakter plaintext dengan persamaan :

$$P_i = (C_i - K_i) \bmod 26 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

Untuk alfabet 26 huruf, atau untuk ASCII 256 karakter:

$$P_i = (C_i - K_i) \bmod 256 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (4)$$

Perhatikan bahwa panjang kunci harus sama dengan panjang plaintext, sehingga tidak ada kebutuhan mengulang penggunaan kunci selama proses enkripsi.

IV. Rancangan Aplikasi

Aplikasi yang diusulkan adalah sebuah aplikasi yang menerapkan ilmu kriptografi yang berperan sebagai pengenkripsi dan pendekripsi pesan dan data dari sebuah pengiriman email. Sehingga dapat lebih mengamankan isi pesan dan data yang dikirimkan.

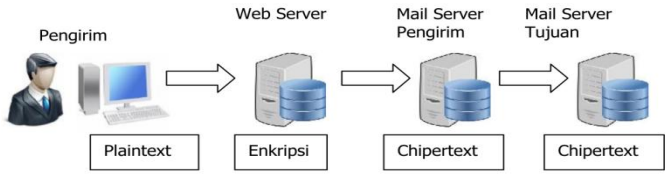
Adapun algoritma yang digunakan untuk melakukan enkripsi adalah metode one time pad, dimana metode ini terkenal aman dan bahkan sampai dengan saat ini belum ada yang bisa melakukan pemecahan kunci atas kode enkripsi yang sudah dibuat, karena satu kunci hanya digunakan untuk satu pesan atau data. Sehingga tidak terdapat kunci yang sama dalam sebuah pesan ataupun data.

Sistem aplikasi ini berbasis web dan ditanam pada sebuah komputer server sebagai pusat layanan. Setiap email yang dikirimkan melalui aplikasi ini maka user dapat melakukan enkripsi dan dekripsi pada pesan dan data attachment yang dikirimkan.

Aplikasi yang dikembngakan ini bersifat hanya sebagai pengacak pesan dan data, dan bukan sebagai mail server; sehingga bisa digunakan untuk akun email apapun asalkan mail server yang digunakan support protokol IMAP.

Berikut tahapan proses yang dilakukan aplikasi ketika seorang user mengirimkan sebuah email :

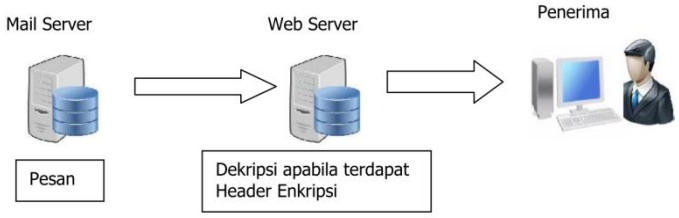
1. User mengirimkan pesan dan attachment (plaintext) dengan mengakses web server dengan mengetik alamat web server pada browser.
2. User login menggunakan username dan password email, baik itu Yahoo Mail, Gmail dan lain sebagainya yang sudah terintegrasi dengan system.
3. User mengetikkan pesan dan upload attach file untuk melakukan pengiriman pesan.
4. Pada saat proses pengiriman tersebut, aplikasi yang ada di webserver melakukan proses enkripsi pada pesan dan juga attach file yang dikirimkan.
5. Webserver menyimpan kunci yang sudah di generate oleh sistem dan disimpan ke dalam database.
6. Webserver mengirimkan pesan dan attach file yang sudah di enkripsi (chipertext) ke MailServer kepada alamat yang dituju.



Gbr 3. Skema pengiriman e-mal terenkripsi

Sedangkan proses mengakses email yang diterima dan ingin melakukan dekripsi, maka prosesnya sebagai berikut :

1. Email yang ada pada Mail Server dibaca melalui Web Server dengan protokol IMAP sebagai Incoming Connection dari Mail Server.
2. System yang ada pada Web Server akan melakukan pembacaan Header pada pesan, apabila terdapat Header yang mengindikasikan bahwa pengiriman pesan tersebut dienkripsi melalui Web Server, maka akan dilakukan proses dekripsi. Sebaliknya; apabila Header tidak mengindikasikan enkripsi dari Web Server, maka tidak perlu dilakukan proses dekripsi.



Gbr 4. Skema penerimaan e-mail terenkripsi

Dalam perkembangan teknologi saat ini, teknologi email (*Electronic Mail*) adalah merupakan sesuatu yang sangat penting dalam dunia komunikasi. Dikarenakan dengan adanya email manusia dapat mengirimkan pesan dan juga data melalui teknologi informasi.

Untuk mendukung kebutuhan aplikasi, diperlukan juga sistem basis data yang memadai dengan rancangan basis data dalam bentuk ERD (*Entity Relationship Diagarm*) adalah sebagai berikut ini:

Gbr 5. ERD (*Entity Relationship Diagarm*)

Berikut ini adalah spesifikasi basis data untuk aplikasi enkripsi dekripsi email:

Tabel : Mail
Media : Harddisk
Isi : Data Kunci
Primary : mailid

Field	Type	Length	Note
mailid	int	11	ID Mail
kunci	longblob	4.2M	Kunci Pesan
kunciattach	longblob	4.2M	Kunci Attachment
MailServerId	int	11	ID Mail Server

Tabel : MailServer
Media : Harddisk
Isi : Data Kunci
Primary : MailServerId

Field	Type	Length	Note
MailServerImap	varchar	100	IMAP Address Mail Server
MailServerSmtp	varchar	100	SMTP Address Mail Server
SmtpPort	int	11	Port SMTP
SmtpSecure	varchar	50	SMTP Secure

V. HASIL & PEMBAHASAN

A. Spesifikasi *Software*

Dibawah ini merupakan spesifikasi software (perangkat-lunak) yang dibutuhkan dalam aplikasi enkripsi email dan harus dipenuhi agar aplikasi dapat berjalan dengan baik.

1. Sistem Operasi Microsoft Windows
2. PHP 5
3. MySQL 5

B. Spesifikasi *Hardware*

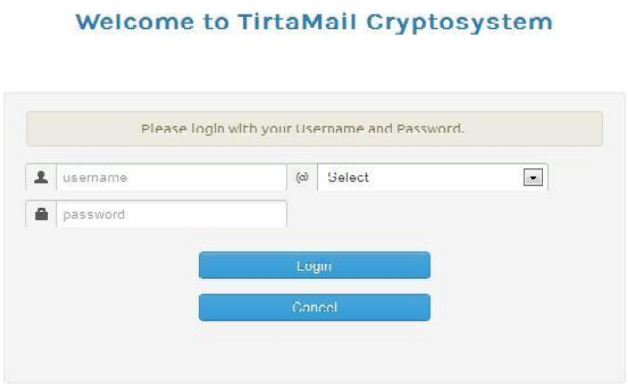
Perangkat keras yang digunakan dan telah diujicobakan dengan aplikasi ini adalah sebagai berikut :

1. Laptop Asus A43S dengan spesifikasi:
   a. Intel(R) Core (TM) i5-2450M CPU @2.50GHz
   b. RAM / Memory 4GB
   c. Hard Drive 500GB
   d. Wireless Network DW1501 Wireless-N WLAN
2. Server Hosting Rumahweb.com dengan spesifikasi :
   a. Paket Hosting Professional Hosting
   b. Disk Space 250MB
   c. Server US

d. Bandwidth 10GB
e. Virtual Memory 524.288 KB
f. Physical Memory 1.048.576 KB
g. Input Output 250KB/s

C. Tampilan Layar *Login*

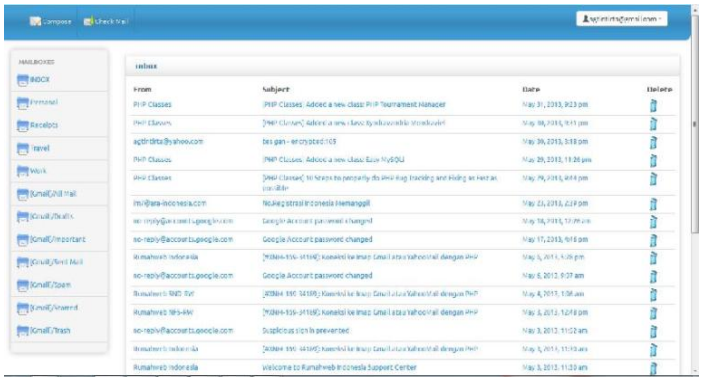
Pada halaman awal ketika aplikasi diakses, akan muncul halaman login untuk mulai menggunakan aplikasi. Untuk username dan password diisi sesuai dengan account yang dimiliki oleh user pada Mail Server yang sudah terintegrasi oleh sistem.



Gbr 6. Tampilan Layar Login

Pada tampilan halaman utama menampilkan menu untuk compose cmail, check mail serta pilihan logout apabila username diklik.

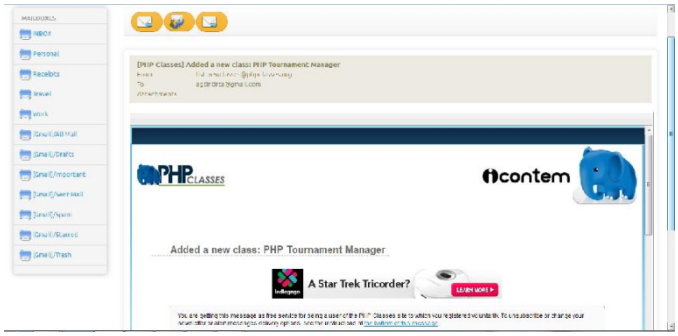
Pada bagian kiri terdapat list mailboxes yaitu daftar kotak surat yang ada pada account tersebut serta pada bagian kanannya terdapat list mail sesuai mailboxes terpillih. Pada halaman awal mailboxes secara default terpilih inbox.



Gbr 7. Tampilan Layar Halaman Utama

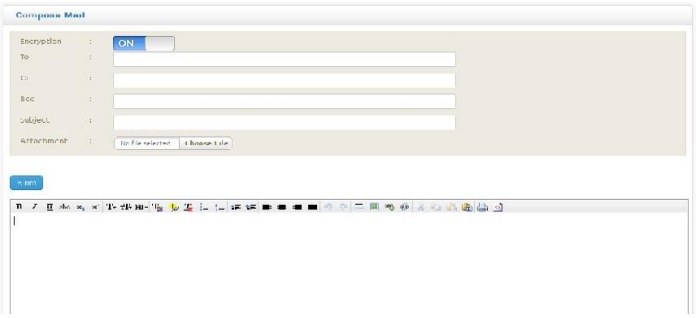
Tampilan layar read mail ini menampilkan content dari pesan yang dipilih. Terdapat pula keterangan Subject, Sender, Receiver dan juga attachment dari pesan tersebut. Pada tampilan layar Read Mail dapat mendukung pesan dalam bentuk text dan juga forrmat HTML.

Pada bagian atas terdapat menu untuk Reply, Reply All dan Forward sebagai pillihan untuk tindak lanjut dari pesan tersebut.



Gbr 8. Tampilan Layar Read Mail

Tampilan layar compose mail adalah form untuk melakukan pembuatan pesan baru, dimana pada form ini terdapat kotak isian untuk alamat yang dituju (to dan cc), subject mail serta kotak isian untuk conntent email. Pada form ini terdapat juga pilihan enkripsi; apakah akan digunakaan atau tidak (on atau off) serta terdapat tombol browse attachment untuk melampirkan file.

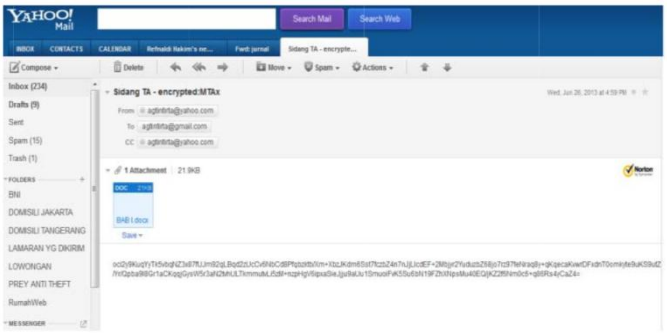


Gbr 9. Tampilan Layar Compose mail

D. Pengujian Aplikasi

Pengujian aplikkasi berguna untuk mengetahui apakah program yang telah dibuat dapat berjalan secara maksimal, maka dari itu program tersebut harus diuji dahulu mengenai kemampuannnya agar dapat berjalan sesuai dengan yang diharapkan pada saat implementasi nantinya.

Pada gambar dibawah ini, menunjukkan pesan yang terenkripsi pada Mail Server, dimana pesan tersebut tidak dapat dibaca apabila dibuka melalui WebMail penyedia layanan, namun pesan tersebut akan dapat dibaca dengan menggunakann aplikasi yang ditanam pada WebServer.



Gbr 10. Tampilan pesan terenkripsi

Gbr 11. Tampilan Pesan Terdekripsi Pada Server

Pada file attachment akan terenkripsi apabila attachment tersebut didownload melalui WebMail penyedia layanan, namun akan terdekripsi apabila di download melalui aplikasi enkripsi dekripsi email tersebut.

Berikut ini diberikan beberapa perbandingan yang digunakan untuk melakukan pengiriman dan pembacaan email yang dienkripsi.

TABELI
TABEL PENGUJIAN PROSES PADA APLIKASI

File	testing_gambar.jpg	testing_video.mp4	testing_word.docx	Text
Waktu pengiriman (detik)	32.0370	94.9136	100.6647	4.7873
Waktu enkripsi file (detik)	0.7523	2.4494	2.8164	0.0189
Waktu dekripsi file (detik)	0.4096	1.4368	1.5305	0.0108
Ukuran sebelum enkripsi	356 KB	1238 KB	1303 KB	9576 B
Ukuran sesudah enkripsi	356 KB	1238 KB	1303 KB	12768 B
Panjang kunci (karakter)	363782	1267436	1333621	9576

Dari data perbandingan tersebut, dapat diambil kesimpulan bahwa:

1. Besarnya file sebelum maupun sesudah dienkripsi tidak mengalami perubahan; yakni dengan ukuran yang sebenarnya. Hal ini merupakan keuntungan dari metode streamchiper dimana file yang di enkripsi tidak mengalami perubahan ukuran, berbeda dengan metode block chiper dimana file akan mengalami penambahan ukuran karena akan dilakukan penambahan padding sampai blok terpenuhi.
2. Panjang kunci yang dihasilkan sama dengan ukuran file yang dienkripsi.
3. Untuk pengiriman pesan, terlihat bahwa ukuran sebelum dienkripsi lebih sedikit dibandingkan dengan ukuran sesudah enkripsi. Hal ini dikarenakan output hasil enkripsi dilakukan pengkodean base64 untuk menghindari karakter-karakter ASCII yang terkonversi kedalam format HTML seperti tanda “ akan dikonversi menjadi " , tanda < akan dikonversi menjadi < dan lain sebagainya.
4. Perbandingan waktu enkripsi dan dekripsi cenderung lebih cepat waktu dekripsi. Hal ini dikarenakan dalam melakukan enkripsi dilakukan pula pembuatan kunci, sehingga membutuhkan waktu lebih lama. Sedangkan dekripsi hanya membandingkan antara kunci dengan chipertext.

E. Keunggulan Aplikasi

Setelah dilakukan analisa dari hasil implementasi aplikasi, dapat ditemukan beberapa keunggulan dan kekurangan dari aplikasi ini. Berikut ini merupakan keunggulan dari aplikasi:

1. Program dapat dengan mudah dioperasikan oleh user, karena memiliki user interface (tampilan antar muka) yang baik dan *user friendly* sesuai dengan mail server pada umumnya.
2. Bukan hanya pesan yang dapat dilakukan enkripsi melainkan attachment-nya juga, sehingga dapat mengamankan isi data yang dikirim dalam bentuk file.
3. User tidak perlu melakukan setting untuk kunci serta melakukan penyimpanan kunci, karena semua sudah diatur oleh sistem.
4. Metode enkripsi yang digunakan adalah metode one time pad yang sampai saat ini belum dapat dipecahkan (*unbreakable chiper*).
5. Enkripsi yang dilakukan cukup ringan karena one time pad termasuk enkripsi simetris.
6. Ukuran file attachment tidak mengalami penambahan ukuran file, sehingga tidak memberatkan pengiriman dan pengambilan file.
7. Kemudahan akses karena berbasis web, sehingga user tidak perlu melakukan instalasi dan dapat diakses dari PC, tablet maupun smartphone.

F. Kekurangan Aplikasi

Sedangkan kekurangan dari aplikasi; antara lain adalah:

1. Kelancaran proses terkirim dan diterimanya suatu email dari/ke server tergantung pada layanan maupun jaringan operator yang digunakan.
2. Akses email cenderung lebih lambat bila dibandingkan dengan langsung mengakses mail server yang digunakan. Hal ini karena aplikasi yang dikembangkan memang diperuntukan bukan sebagai mail server, tetapi sebagai layer dari mail server yang sudah ada dan data yang didapatkan dilakukan dengan cara berinteraksi secara system to system ke penyedia mail server tersebut.
3. Belum adanya manajemen kontak karena program saat ini hanya terfokus pada enkripsi dan dekripsi email sesuai batasan masalah.

VI. KESIMPULAN

Dari hasil perancangan dan pembuatan aplikasi enkripsi dekripsi email untuk mengamankan isi sebuah akun email dapat diambil kesimpulan sebagai berikut:

1. Aplikasi ini dapat mengamankan isi pesan dan data yang terkandung dalam akun email seseorang dengan melakukan enkripsi pada pesan dan data yang dikirimkan.

2. Dengan adanya program ini diharapkan dapat menjadi sebuah solusi dari kekhawatiran tentang keamanan sebuah email terutama para pengguna yang menggunakan layanan email gratis.
3. Dengan adanya aplikasi ini akan meminimalisasi kemungkinan kebocoran pesan dan data yang terdapat akun email apabila menjadi korban serangan hacker, karena para hacker tidak dapat membaca pesan dan data tersebut.

REFERENSI

[1] H.Barr ,Thomas 2002, Invitation to Cryptography, New Jersey, Practice Hall

[2] J.Menezes, Alfred, Paul C. Van oorschot, A. Vanstone 1997, Handbook of Applied on Chryptography, Boca Raton, CRC Press

[3] Munir ,Rinaldi 2006, Kriptografi, Bandung, Penerbit Informatika

[4] Novanto Arnowo,Ardyan 2012, Bagaimanakah Cara Kerja Surat Elektronik (email)(online), updated 05 Maret 2012, dilihat 21 April 2013, <http://www.nu.or.id/a,public-m,dinamic-s,detail- ids,14-id,36180-lang,id- c,teknologit,Bagaimanakah+Cara+Kerja+Surat+Elektronik+ +email+-.phpx>

[5] R.Stinson , Douglas 2002, Cryptography Theory and Practice, Boca Raton, CRC Press

[6] Schneier,Bruce 1996, Applied Cryptography, John Wiley & Sons Inc

[7] Sidik , Bertha 2006, Pemrograman WEB dengan PHP, Bandung, Penerbit Informatika

[8] Sjukani, Moh 2007, Struktur Data (Algoritma & Struktur Data 2), Jakarta, Mitra Wacana Media.

Fatmasari, S.Kom., M.Kom. lahir di Jakarta tahun 1978, lulus Strata Satu (S1) Jurusan Sistem Informasi Universitas Budi Luhur tahun 2006 dan pada tahun 2010 lulus program Pasca Sarjana (S2) Magister Ilmu Komputer Universitas Budi Luhur yang mana saat ini sebagai Dosen STMIK Antar Bangsa.