PENGEMBANGAN DAN IMPLEMENTASI ALGORITMA ONE TIME PAD DENGAN MENGGUNAKAN KUNCI GAMBAR ATAU IMAGE PADA KEAMANAN TEKS EMAIL

Muhammad Ilham Yahya[1], Ari Eko Wardoyo[2], Yeni Dwi Rahayu[3], Deni Arifianto[4], Lutfi Ali Muharrom[5]
Mahasiswa[1], Dosen[2,3,4,5]
Teknik Informatika, Universitas Muhammadiyah Jember

Abstrak

Perkembangan dunia internet sangatlah pesat dalam penggunaannya. Salah satu fasilitas atau layanan yang sangat vital dalam dunia internet adalah Email. Email pada dasarnya hanyalah sebuah pesan elektronik yang dikirimkan melalui media jaringan internet. Dengan adanya *email*, proses pengolahan, penyimpanan serta pendistribusian data dan informasi sangatlah mudah dilakukan dan digunakan oleh semua kalangan lapisan masyarakat. Namun masalah yang timbul dari kemudahan yang diberikan adalah keamanan email. Salah satu masalah yang timbul adalah penyadapan yang dilakukan oleh pihak ketiga. Dimana masalah ini menjadi sangat vital karena pesan email bukanlah hanya pesan biasa, namun juga adalah pesan pribadi atau penting. Apabila informasi dari pesan email tersadap oleh pihak ketiga sangatlah berbahaya. Dengan demikian keamanan dari suatu pesan email sangatlah penting. Sehingga diperlukan sebuah sistem yang mampu mengamankan suatu pesan email dengan suatu metode sebagai pemecah masalah. Metode yang dimaksud adalah kriptografi yang menerapkan algoritma one time pad dengan menggunakan kunci gambar diharapkan isi pesan atau informasi dari email akan aman dan tidak bocor kepada penyadap atau pihak yang tidak bertanggung jawab sehingga tetap terjaga suatu kerahasian informasinya.

Kata Kunci : email, enkripsi, deskripsi, one time pad, gambar.

Abstract

The using of cyber world are highly increasing. One of facility or service that has vital role in the cyber world is email. Email is basically an electronical message sent through internet network media. The existence of email makes data and information's processing, storaging, and also distribution are easier to do and use by every part of the society. Yet, there is a problem emerging from the easiness that has given. That problem is email security. One of the problem is tapping that has been done by the third side. This kind of problem become very vital because the email messages are not ordinary messages but it contains private message and important ones. If the information of email message are tapped by third side, it will be dangerous. So that the security of email message is very important indeed and it requires a system that has the capability to secure an email message using a methode as problem solver. The intended methode is cryptography that applying one pad algorithm by using image key. Hopefully the content of the message or information of the email will be saved and doesn't leak to the tapper or the irresponsible side so that the secrecy of information is protected.

Keyword : Email, Encryption, Description, One Time Pad, Image.

1. Pendahuluan

Dunia *internet* pada era sekarang ini sangatlah luas penggunaan dan perkembangannya, salah satu fasilitas dan layanan yang sangat vital dalam dunia *internet* adalah pesan *email*. *Email* pada dasarnya hanyalah sebuah pesan elektronik yang dikirimkan melalui media jaringan *internet*. Dengan adanya *email*, proses pengolahan, penyimpanan serta pendistribusian data dan informasi sangatlah mudah dilakukan dan digunakan oleh semua kalangan lapisan masyarakat. Aspek kemudahan yang di dapat tersebut ternyata berbanding berbalik dengan faktor *confidentiality* (kerahasiaan), *integrity* dan *availability* (ketersediaan) (Diana, 2012).

Seiring berjalannya waktu, *email* menjadi sebuah aplikasi yang sering digunakan untuk mengirim pesan. Namun, ada beberapa ancaman yang tidak diketahui oleh pengguna saat menggunakan *email* seperti penyadapan isi *email*, merubah isi *email* oleh orang yang tidak berkepentingan dan menjadikan *email* itu tidak asli lagi. Keamanan menjadi aspek yang sangat penting dalam pengiriman isi *email* untuk mencegah atau jatuhnya data kepada pihak-pihak lain yang tidak berkepentingan sehingga adanya kemungkinan kebocoran atau penyalahgunaan data dapat dihindari (Fauzi, 2014).

Salah satu upaya yang dapat dilakukan dalam pengamanan *email* adalah kriptografi. Dalam kriptografi terdapat metode yang cukup penting dalam pengamanan informasi atau pesan, salah satunya adalah enkripsi (*encryption*). Enkripsi adalah proses yang dilakukan untuk mengubah pesan asli menjadi pesan yang telah diubah supaya tidak mudah dibaca (*chipertext*). Sedangkan untuk mengubah pesan tersembunyi menjadi pesan biasa (*plaintext*) disebut deskripsi (*decryption)*.

Berdasarkan paparan serta analisa masalah tersebut, maka dapat disimpulkan bahwa sebuah keamanan pada sebuah informasi sangatlah penting terutama pada sisi *email*. Oleh karena itu penulis mengangkat sebuah judul menurut analisa diatas dengan judul **"Pengembangan dan Implementasi**

Algoritma *One Time Pad* Dengan Menggunakan Kunci Gambar Atau *Image* Pada Keamanan Teks *Email*"

.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dapat dirumuskan permasalahan sebagai berikut:

1. Apakah algoritma *One Time Pad* mampu melakukan pengamanan terhadap informasi atau pesan pada *email*sehingga dapat menjaga kerahasiaan dan keamanandengan menggunakan algoritma *One Time Pad*tetap terjaga informasinya ?
2. Apakahgambar atau *image* mampu menggantikan kunci enkripsi dan deskripsi sebagai pengganti kunci pada algoritma *One Time Pad*?
3. Apakah Algoritma *One Time Pad*mampu mengenkripsi dan mendeskripsi huruf kapital [A-Z], huruf kecil [a-z], kombinasi huruf kapital [A-Z] dan huruf kecil [a-z], tanda baca, karakter khusus, angka, dan plainteks yang panjang ?
4. Berapakah tingkat akurasi dari algoritma *One Time Pad* dalam melakukan enkripsi dan deskripsi dengan menggunakan kunci gambar ?

1.3 Batasan Masalah

Adapun yang menjadi batasan dalam penyusunan penelitian ini adalah sebagai berikut :

1. Masalah implementasi algoritma *One Time Pad*diterapkan hanya untuk keamanan dan kerahasiandalam bentuk teks.
2. Kunci enkripsi dan deskripsi hanya berupa gambar atau *image* dengan format jpg dan png.
3. Hasil enkripsi dikodekan ke kode *ASCII*.
4. Hanya menggunakan *email* dari *Gmail*.
5. Aplikasi pengamanan teks *email* dibangun menggunakan Bahasa Pemrograman *Java*.

1.4 Tujuan Penelitian

Maksud dari tujuan penelitian ini adalah sebagai berikut :

1. Membuat suatu sistem pengamanan informasi*email*berupa teksdengan menerapkan algoritma *One Time Pad* sehingga tetap terjaga kerahasiaan informasinya dari orang tidak bertanggung jawab.
2. Mengembangkan algoritma *One Time Pad* dengan mengganti pembangkit kunci bawaan dari algoritma tersebut sebagai gantinya menggunakan kunci gambar atau *image*dalam melakukan enkripsi dan deskripsi.
3. Mengetahui hasil dari algoritma *One Time Pad* dalam melakukan enkripsi dan deskripsi pada huruf kapital [A-Z], huruf kecil [a-z], kombinasi huruf kapital [A-Z] dan huruf kecil [a-z], tanda baca, karakter khusus, angka, dan plainteks yang panjang.
4. Mengetahuitingkat akurasi dari algoritma *One Time Pad* dalam melakukan enkripsi dan deskripsi dengan menggunakan kunci gambar.

1.5 Manfaat Penelitian

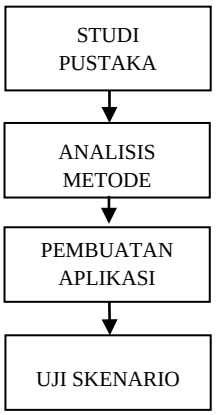
Manfaat dari Penelitian ini sebagai berikut :

1. Memberikan suatu keamanan informasi yang ada didalam *email* dari orang-orang yang tidak berhak membaca isi dari informasi yang ada di dalam *email* tersebut sehingga kerahasiaan dan keamanan dari informasinya dapat tetap terjaga.
2. Penerima dan Pengirim mampu mengingat dengan mudah kunci yang disepakati dengan menggunakan gambar atau *image* dari pembentukan kunci yang diterapkan algoritma *One Time Pad* sebelumnya.

2. Metode Penelitian

2.1 Tahapan Penelitian

Penelitian ini akan dikerjakan dalam beberapa tahap. Adapun tahapan dari penelitian ini, sebagai berikut :



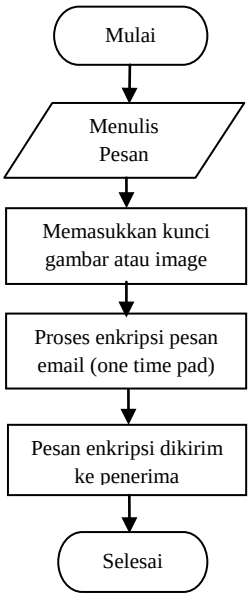
Gambar 2.1 Tahapan Penelitian

Studi pustaka dilakukan untuk mencari literatur terhadap bahan-bahan materi yang dibutuhkan yang berhubungan dengan topik yang diambil sebagai dasar pembahasan Pengamanan Teks *Email* (*Elektronik Mail*) sehingga penulisan tugas akhir tidak menyimpang dari teori-teori yang sebelumnya telah ada dan diakui kebenarannya.

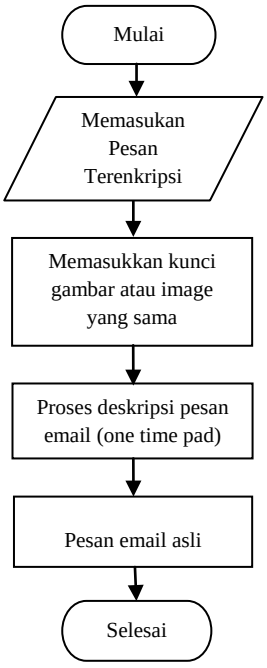
Analisis metode yaitu analisa yang dilakukan oleh penulis tentang metode yang di pakai untuk pengamanan teks *Email* (*Elektronik Mail*). Analisis metode yang dilakukan seperti alur perancangan dari sistem dan uji perhitungan manual metode.

Setelah melakukan studi pustaka dan analisis metode dilakukan pembuatan aplikasi pengamanan teks *Email* yang meliputi perancangan sistem dan dilanjutkan desain dan *coding* aplikasi.

Skenario uji yaitu pengujian yang dilakukan untuk menguji hasil penelitian. Skenario uji dilakukan dengan mengirimkan pesan *Email* ke *Email* tujuan dengan menggunakan sistem pengamanan teks *Email* yang telah dibuat.



Gambar 2.1.1 *Flowchart* Enkripsi Pengiriman *Email*



Gambar 2.1.2 *Flowchart* Deskripsi Pesan *Email*

2.3 Pembentukan Kunci

Aturan dari pembentukan kunci yang dikembangkan pada algoritma *One Time Pad* :

1. Kunci yang digunakan untuk enkripsi deskripsi adalah berupa gambar atau *image.*
2. Gambar atau *image* yang digunakan sebagai kunci harus memiliki banyak *pixel* sesuai dengan panjang *plaintext* atau lebih dari *plaintext*.

Plaintext : ONE → panjang teks 3

$\sqrt{3}=1{,}73$

= 2 → di bulatkan

Jadi,

Baris (x) = 2 → hasil akar

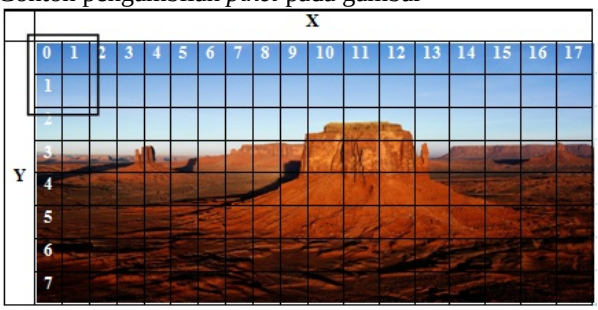
Kolom (y) = 2 → hasil akar

Total *pixel* = Baris x Kolom

= 2 x 2 = 4 *pixel*

Jika total *pixel* < panjang *plaintext* , maka Baris + 1 dan Kolom + 1 *Key Image* :

Contoh pengambilan *pixel* pada gambar



Jadi *pixel* yang diambil dengan posisi x,y yaitu (0,0), (0,1), dan (1,0) sesuai dengan panjang plainteks dan disimpan di *variable array*.

3.4 Pembahasan Enkripsi Algoritma *One Time Pad*

Enkripsi dapat digambarkan hasil *XOR* antara *bit* karakter *plaintext* dan *bit* karakter *key* :

Ci = (Pi *XOR* Ki) Mod 256

Keterangan :

Ci = karakter *ciphertext*

Pi = karakter *plaintext*

Ki = karakter kunci

Ubah setiap karakter plainteks menjadi kode *ASCII* dan *biner* 24 *bit* sebagai berikut :

Plainteks		
Karakter	**Kode ASCII**	**Biner 24 bit**
B	66	000000000000000001000010
e	101	000000000000000001100101
s	115	000000000000000001110011
o	111	000000000000000001101111
k	107	000000000000000001101011

Ubah setiap warna *pixel* gambar menjadi *hexa*, *hexa* ke desimal, dan desimal ke *biner* 24 *bit* :

Color Hexa Code	**Desimal**	**Biner 24 bit**
14396E	1325422	000101000011100101101110
14396E	1325422	000101000011100101101110
14396E	1325422	000101000011100101101110
14396E	1325422	000101000011100101101110
14396E	1325422	000101000011100101101110

Setelah dilakukan langkah diatas, kemudian *biner* plainteks dan *biner* kunci di *XOR*-kan :

Cipherteks			
Ci = Pi *XOR* Ki	Desimal Ci	Ci Mod 256	Karakter ASCII
000101000011100100101100	1325356	44	,
000101000011100100001011	1325323	11	
000101000011100100011101	1325341	29	
000101000011100100000001	1325313	1	
000101000011100100000101	1325317	5	

Pada hasil enkripsi di atas ada karakter ascii yang tidak tampil karena kode ascii 0 sampai 31 adalah *Control Characters* dan 127 sampai 256 adalah *Special Characters*.

4.5 Pembahasan Deskripsi Algoritma *One Time Pad*

Enkripsi dapat digambarkan hasil *XOR* antara *bit* karakter cipher*text* dan *bit* karakter *key* :

Pi = (Ci *XOR* Ki) Mod 256

Berikut adalah proses deskripsi *One Time Pad* :

Plainteks			
Pi = Ci *XOR* Ki	Desimal Pi	Pi Mod 256	Karakter ASCII
000101000011100101000010	1325378	66	B
000101000011100101100101	1325413	101	e
000101000011100101110011	1325427	115	s
000101000011100101101111	1325423	111	o
000101000011100101101011	1325419	107	k

4.6 Model Pengujian

Untuk mengetahui tingkat keberhasilan dari aplikasi yang dibuat maka dilakukan beberapa uji coba dengan menggunakan sejumlah karakter yang berbeda. Berikut tujuh model pengujian yang dilakukan :

1. Penggunaan huruf kapital A-Z.
2. Penggunaan huruf kecil a-z.
3. Penggunaan kombinasi huruf kapital A-Z dan huruf kecil a-z.
4. Penggunaan tanda baca.
5. Penggunaan karakter khusus.
6. Penggunaan angka.
7. Penggunaan plainteks yang panjang.

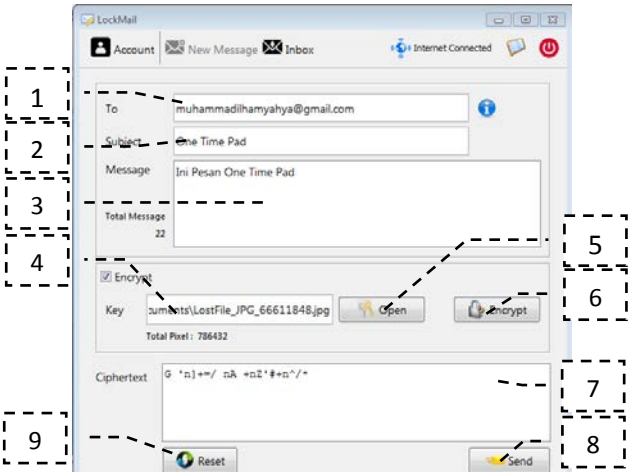
3. Implementasi dan Pengujian

Implementasi sistem ini adalah tahap dimana setiap sistem siap untuk dioperasikan pada aktivitas yang sebenarnya, sehingga diketahui apakah sistem telah dibuat sesuai dengan apa yang direncanakan. Pada implementasi perangkat lunak ini akan dijelaskan bagaimana program sistem ini bekerja dengan memberikan tampilan aplikasi yang dibuat.

3.1 Proses Penggunaan Aplikasi LockMail

3.1.1 Tampilan *Menu New Message*

Pada tampilan *menu new message* ini menampilkan *form* untuk mengirim pesan baru *email* - dan terdapat *form* untuk enkripsi pesan *email.*



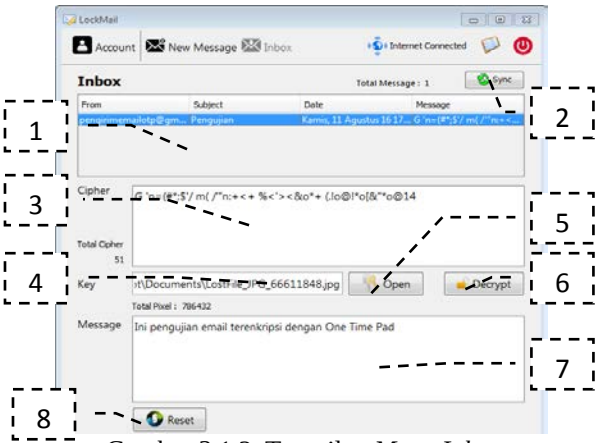
Gambar 3.1.3 Tampilan *Menu New Message*

Penjelasan Tampilan *New Message* sebagai berikut :

1. Inputan alamat *email* tujuan sesuai format (Contoh: xxx@gmail.com).
2. Inputan *subject* pesan *email*.
3. Inputan pesan atau teks *email*.
4. Inputan *url* atau alamat lokasi dari gambar.
5. *Button Open* berfungsi untuk menampilkan *window* untuk memilih gambar.
6. *Button Encrypt* berfungsi untuk melakukan proses enkripsi pesan teks *email*.
7. *Textarea* atau wadah untuk menampung hasil dari proses enkripsi.
8. *Button Send* berfungsi untuk mengirim pesan *email*.
9. *Button Reset* berfungsi untuk me-*reset* semua inputan.

3.1.2 Tampilan *Menu Inbox*

Pada tampilan *menu inbox* ini menampilkan pesan *email* yang masuk dan terdapat *form* deskripsi pesan *email* yang terenkripsi.



Gambar 3.1.2 Tampilan *Menu Inbox*

Penjelasan Tampilan *Menu Inbox* sebagai berikut :

1. *Table Inbox* berfungsi menampung pesan *email*.
2. *Button Sync* berfungsi untuk mengambil *inbox* dari pesan *email* untuk di tampung di tabel *inbox*.

3. *Textarea* atau wadah untuk menampung dari pesan teks *email* yang dipilih dari tabel *inbox*.
4. Inputan *url* atau alamat lokasi dari gambar.
5. *Button Open* untuk menampilkan window yang berfungsi untuk memilih gambar.
6. *Button Decrypt* berfungsi untuk melakukan proses dekripsi pesan teks *email.*
7. *Textarea* atau wadah berfungsi untuk menampung hasil dari proses dekripsi.
8. *Button Reset* berfungsi untuk me-*reset* semua inputan.

3.2 Pengujian

Pada tahap pengujian ini dilakukan uji hasil dari aplikasi yang dibangun menggunakan algoritma *One Time Pad* dengan menggunakan gambar yang memilki resolusi dan size yang sama sebagai kuncinya dengan beberapa proses pengujian yang dilakukan sehingga dapat diketahui hasil dari proses pengujian tersebut dalam melakukan pengamanan sebuah teks.

$$\text{Akurasi} = \frac{\Sigma\text{Berhasil} - \Sigma\text{Gagal}}{\Sigma\text{Total Data}} \text{x } 100\%$$

$$\text{Akurasi Rata} - \text{rata} =$$

$$= \frac{\sum_{n=1} \text{Akurasi Pengujian}_n}{\Sigma\text{Pengujian}} \text{x } 100\%$$

3.2.1 Pengujian penggunaan huruf besar A-Z

Berhasil = 25 data
Gagal = 0 data

$$\text{Akiurasi} = \frac{25 - 0}{25} \text{x } 100\% = 100\%$$

Jadi, pada pengujian penggunaan huruf kapital A-Z dari 25 data uji diperoleh tingkat akurasinya adalah 100%.

3.2.2 Pengujian penggunaan huruf kecil a-z

Berhasil = 25 data
Gagal = 0 data

$$\text{Akurasi} = \frac{25 - 0}{25} \text{x } 100\% = 100\%$$

Jadi, pada pengujian penggunaan huruf kecil a-z dari 25 data uji diperoleh tingkat akurasinya adalah 100%.

3.2.3 Pengujian penggunaan huruf besar A-Z dan huruf kecil a-z

Berhasil = 25 data
Gagal = 0 data

$$\text{Akurasi} = \frac{25 - 0}{25} \text{x } 100\% = 100\%$$

Jadi, pada pengujian penggunaan kombinasi huruf kapital A-Z dan huruf kecil a-z dari 25 data uji diperoleh tingkat akurasinya adalah 100%

3.2.4 Pengujian penggunaan tanda baca

Berhasil = 25 data
Gagal = 0 data

$$\text{Akurasi} = \frac{25 - 0}{25} \text{x } 100\% = 100\%$$

Jadi, pada pengujian penggunaan tanda baca dari 25 data uji diperoleh tingkat akurasinya adalah 100%.

3.2.5 Pengujian penggunaan karakter khusus

Berhasil = 23 data
Gagal = 2 data

$$\text{Akurasi} = \frac{25 - 0}{25} \text{x } 100\% = 100\%$$

Jadi, pada pengujian penggunaan tanda baca dari 25 data uji diperoleh tingkat akurasinya adalah 100%.

3.2.6 Pengujian penggunaan angka

Berhasil = 25 data
Gagal = 0 data

$$\text{Akurasi} = \frac{25 - 0}{25} \text{x } 100\% = 100\%$$

Jadi, pada pengujian penggunaan angka dari 25 data uji diperoleh tingkat akurasinya adalah 100%.

3.2.7 Pengujian penggunaan plainteks yang panjang

Berhasil = 25 data
Gagal = 0 data

$$\text{Akurasi} = \frac{25 - 0}{25} \text{x } 100\% = 100\%$$

Jadi, pada pengujian penggunaan plainteks yang panjang dari 25 data uji diperoleh tingkat akurasinya adalah 100%.

3.3 Kesimpulan Hasil Pengujian

Berdasarkan hasil dari 7 pengujian yang dilakukan, ditemukan hasil dari pengujian tersebut sebagai berikut :

Akurasi pengujian 1 : 100%
Akurasi pengujian 2 : 100%
Akurasi pengujian 3 : 100%
Akurasi pengujian 4 : 100%
Akurasi pengujian 5 : 100%
Akurasi pengujian 6 : 100%
Akurasi pengujian 7 : 100%

$$\text{Akurasi Rata} - \text{rata} = \frac{700}{7} \text{x } 100\% = 100\%$$

Dapat ditarik sebuah kesimpulan dalam pengujian yang dilakukan bahwa algoritma *One Time Pad* dengan menggunakan gambar sebagai kuncinya dalam melakukan enkripsi dan deskripsi harus menggunakan gambar yang memiliki resolusi dan *size*

yang sama karena telah terbukti dengan melakukan pengujian diatas akurasi rata-ratanya adalah 100% dalam melakukan proses enkripsi dan deskripsi.

4. Penutup

4.1 Kesimpulan

Dari hasil penelitian, analisis, perancangan sistem, pembuatan program sampai tahap penyelesaian program, maka penulis dapat mengambil kesimpulan sebagai berikut :

1. Algoritma *One Time Pad* terbukti mampu menjamin kerahasiaan informasi dari *email* dalam bentuk teks.
2. Gambar atau *Image* terbukti mampu menggantikan pembentukan atau pembangkitan kunci yang diterapkan dalam algoritma *One Time Pad* untuk melakukan enkripsi dan deskipsi.
3. Algoritma *One Time Pad* terbukti mampu mengenkripsi dan mendeskripsi huruf kapital [A-Z], huruf kecil [a-z], kombinasi huruf kapital [A-Z] dan huruf kecil [a-z], tanda baca, karakter khusus, angka, dan plainteks yang panjang dari pengujian yang dilakukan dengan syarat gambar memiliki resolusi dan *size* yang sama.
4. Tingkat akurasi dari algoritma *One Time Pad* ini rata-rata adalah 100% dari pengujian yang dilakukan dengan menggunakan kunci gambar yang memiliki resolusi dan *size* yang sama dalam melakukan proses enkripsi dan deskripsi.

4.2 Saran

Adapun yang menjadi saran dalam penulisan skripsi ini adalah sebagai berikut:

1. Penambahan fungsi *attachment* agar aplikasi ini mampu mengamankan pesan atau informasi dari jenis file apapun tidak hanya berupa text.
2. Aplikasi ini masih banyak kekurangan dari segi fitur-fitur yang ada seperti *menu outbox*, penyisipan *attachment* dan lain sebagainya. Sehingga masih diperlukan pengembangan selanjutnya.

Daftar Pustaka

Ariyanto, E., Pravitasari, T.I & Setyorini. 2008. *"Analisa Implementasi Algoritma Stream Cipher Sosemanuk Dan Dicing Dalam Proses Enkripsi Data"*. Seminar Nasional Informatika 2008 (semnasIF 2008) ISSN: 1979-2328.

Dafiyanto, Dedik. 2013. "Penerapan Algoritma Kriptografi Asimetris RSA untuk Keamanan Isi Text Email". Jember: Unviersitas Muhammadiyah Jember.

Diana, *April 2012:1-12*, "Studi dan Implementasi Algoritma Caesar Cipher untuk Keamanan Pesan Email yang Bersifat Rahasia". Universitas Bina Darma. Vol. x, No. x, *http://eprints.binadarma.ac.id/153/1/STUDIDANIMPLEMENTASIALGORITMACAESARCIPHERUNTUKKEAMANANPESANEMAILYANGBERSIFATRAHASIA.pdf*, 6 Mei 2016.

Fauzi. 2014. Penerapan TRIPEL DES (DATA ENCRYTION STANDARD) Pada Sistem Keamanan Teks E-Mail. Jember : Universitas Muhammadiyah Jember.

Muhammad TP, Fazil. 2014. "Penerapan Kriptografi RC 6 Pada Pengiriman dan Penerimaan Pesan Email di Android". Medan: Universitas Sumatera Utara.

Rickson Saragih, Firman. 2008, "Penggunaan Kriptografi One Time Pad (Algoritma Vernam) dalam Pengamanan Informasi". Sekolah Teknik Elektro dan Informatika (STEI) ITB. *http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2007-2008/Makalah/MakalahIF2153-0708-014.pdf.* 5 Mei 2016.

Sholeh. M & J.V. Hamokwarong. 2011. "Aplikasi Kritografi Dengan Metode Vernam Cipher Dan Metode Permutasi Biner". Momentum, Vol.7, No.2, *http://www.unwahas.ac.id/publikasiilmiah/index.php/MOMENTUM/article/view/105/100* . 12 Mei 2016.

Suprayogi, *Mei 2014: 75-83*, "APLIKASI ENKRIPSI EMAIL DENGAN MENGGUNAKAN METODE BLOWFISH BERBASIS J2SE". Techno.COM. Vol. 13, No. 2, *http://download.portalgaruda.org/article.php?article=174803&val=5192&title=APLIKASI%20ENKRIPSI%20EMAIL%20DENGAN%20MENGGUNAKAN%20METODE%20BLOWFISH%20BERBASIS%20J2SE*, 5 Mei 2016.

Wahana Komputer, 2010."The Best Encryption Tools". PT Elex Media Komputindo: Jakarta.

Wibowo, Ivan. *April 2009.* "*Penerapan Algoritma Kriptografi Asimetris RSA untuk Keamanan Data di Oracle,* Jurnal Informatika. Vol. 5, No. 1, *ti.ukdw.ac.id/ojs/index.php/informatika/article/download/68/32*, 11 Mei 2016.

Yasin Muttaqin, Fitra. 2014. "Algoritma Kriptografi New Rot Sebagai Aplikasi Instant Messaging Pada Yahoo Messenger. Jember: Universitas Muhammadiyah Jember.

Zaki, A. 2009."*Trik Mengamankan Komputer untuk Pemula*". PT Elex Media Komputindo: Jakarta.