

TUGAS AKHIR

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



MUHAMMAD ILHAM YAHYA

1210651206

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2016**

TUGAS AKHIR

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

Disusun Untuk Melengkapi dan Memenuhi Syarat Kelulusan

Guna Meraih Gelar Sarjana Komputer

Program Studi Teknik Informatika Universitas Muhammadiyah Jember



MUHAMMAD ILHAM YAHYA

1210651206

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2016**

HALAMAN PENGESAHAN

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

MUHAMMAD ILHAM YAHYA

1210651206

Telah Mempertanggung Jawabkan Laporan Tugas Akhirnya Pada Sidang
Tugas Akhir Tanggal 29 Oktober 2016 Sebagai Salah Satu Syarat Kelulusan
Guna Meraih Gelar Sarjana Komputer
Program Studi Teknik Informatika Universitas Muhammadiyah Jember

Disetujui Oleh :

**Dosen Pembimbing :
Pembimbing I**

**Dosen Penguji :
Penguji I**

**Ari Eko Wardoyo, S.Kom., M.Kom
NIP. 19750214 200501 1 001**

**Lutfi Ali Muharrom, M.Si
NPK. 10 09 550**

Pembimbing II

Penguji II

**Yeni Dwi Rahayu, S.ST., M.Kom
NPK. 11 03 590**

**Deni Arifianto, S.Kom., M.Kom
NPK. 11 03 588**

**Mengesahkan,
Dekan Fakultas Teknik**

**Mengetahui,
Ketua Program Studi Teknik
Informatika**

**Ir. Suhartinah, MT.
NPK. 95 05 246**

**Yeni Dwi Rahayu, S. ST., M.Kom
NPK. 11 03 590**

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang Maha Pengasih lagi Maha Penyayang, Yang hanya kepadaNya-lah segala sesuatu bergantung. Alhamdulillah tak lupa senantiasa saya panjatkan karena hanya dengan ridho, kemurahan dan kekuasaanNya-lah proyek akhir yang berjudul :

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

dapat diselesaikan dengan segala kelebihan dan tak lepas dari kekurangan yang terdapat di dalamnya.

Proyek akhir ini menjelaskan tentang bagaimana melakukan pengamanan terhadap pesan teks *email* menggunakan algoritma *One Time Pad* dengan kunci gambar atau *image* dalam melakukan enkripsi dan deskripsi.

Dengan segala kerendahan hati, penulis memohon maaf jika ternyata di kemudian hari diketahui bahwa hasil dari proyek akhir ini masih jauh dari kesempurnaan. Semoga bermanfaat bagi setiap insan yang mempergunakannya untuk kebaikan di jalan Allah SWT.

Jember, 7 Oktober 2016

Penulis

DAFTAR ISI

Halaman Sampul	i
Halaman Judul	ii
Halaman Pengesahan	iii
Halaman Pernyataan	iv
Abstrak	v
Abstract	vi
Halaman Persembahan Dan Terima Kasih	vii
Kata Pengantar	viii
Daftar Isi	ix
Daftar Gambar	xii
Daftar Tabel	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
BAB II KAJIAN PUSTAKA	4
2.1 Keamanan Data.....	4
2.2 Kriptografi	5
2.3 <i>Email</i>	6
2.3.1 <i>Gmail</i>	6
2.4 <i>Java</i>	7
2.5 <i>One Time Pad (Vernam)</i>	8
2.6 Bilangan <i>Biner</i>	8
2.7 Operasi <i>Biner</i>	9
2.7.1 Operasi <i>Biner AND</i>	9
2.7.2 Operasi <i>Biner OR</i>	10

2.7.3 Operasi <i>Biner XOR</i>	10
2.8 Gambar atau <i>Image</i>	11
2.9 ASCII (<i>American Standard Code for Information Interchange</i>)	12
BAB III METODE PENELITIAN	17
3.1 Tahapan Penelitian	17
3.1.1 Studi Pustaka	17
3.1.2 Analisis Metode	18
3.1.3 Pembuatan Aplikasi.....	18
3.1.4 Skenario Uji	21
3.2 Analisis Sistem	21
3.2.1 Analisis Masalah.....	21
3.2.2 Analisis Persyaratan	22
3.3 Pembentukan Kunci.....	22
3.4 Pembahasan Enkripsi Algoritma <i>One Time Pad</i>	24
3.5 Pembahasan Deskripsi Algoritma <i>One Time Pad</i>	28
BAB IV IMPLEMENTASI DAN PENGUJIAN	29
4.1 Hasil Implementasi	29
4.1.1 Proses Penggunaan Aplikasi LockMail	29
4.1.1.1 Tampilan <i>Menu Utama</i>	29
4.1.1.2 Tampilan <i>Menu Account</i>	30
4.1.1.3 Tampilan <i>Menu New Message</i>	31
4.1.1.4 Tampilan <i>Menu Inbox</i>	32
4.2 Pengujian	33
4.2.1 Pengujian menggunakan kunci gambar dengan resolusi dan <i>size</i> yang sama pada kunci gambar yang digunakan dalam melakukan proses enkripsi dan deskripsi	33
4.2.1.1 Pengujian penggunaan huruf kapital A-Z	34
4.2.1.2 Pengujian penggunaan huruf kecil a-z	36
4.2.1.3 Pengujian penggunaan kombinasi huruf kapital A-Z dan huruf kecil a-z.....	39
4.2.1.4 Pengujian penggunaan tanda baca	41

4.2.1.5 Pengujian penggunaan karakter khusus	44
4.2.1.6 Pengujian penggunaan angka	46
4.2.1.7 Pengujian penggunaan plainteks yang panjang	48
4.2.2 Pengujian menggunakan kunci gambar yang di resize pada proses deskripsi	63
4.2.2.1 Pengujian penggunaan huruf kapital A-Z	63
4.2.2.2 Pengujian penggunaan huruf kecil a-z	65
4.2.2.3 Pengujian penggunaan kombinasi huruf kapital A-Z dan huruf kecil a-z.....	68
4.2.2.4 Pengujian penggunaan tanda baca	70
4.2.2.5 Pengujian penggunaan karakter khusus	73
4.2.2.6 Pengujian penggunaan angka	75
4.2.2.7 Pengujian penggunaan plainteks yang panjang	77
4.3 Kesimpulan Hasil Pengujian	95
BAB V PENUTUP	97
5.1 Kesimpulan	97
5.2 Saran	97
Daftar Pustaka	98
Identitas Penulis	101

DAFTAR PUSTAKA

- Diana. April 2012. *Studi dan Implementasi Algoritma Caesar Cipher untuk Keamanan Pesan Email yang Bersifat Rahasia.*
<http://eprints.binadarma.ac.id/153/1/STUDIDANIMPLEMENTASIALGORITMACAESARCIPHERUNTUKKEAMANANPESANEMAILYANGBERSIFATRAHASIA.pdf>. Diakses 6 Mei 2016.
- Edukasi Indonesia. 2015. *Sejarah Singkat Gmail.*
<http://www.edukasinesia.com/2016/05/gmail-apa-itu-gmail-dan-bagaimana-sejarah-terbentuknya-gmail.html>. Diakses 3 Mei 2016.
- Emka, Ifhtul. Juni 2010. Operasi logika dasar AND, OR dan NOT.
<http://emka.web.id/special/electro/2010/operasi-logika-dasar-and-or-dan-not/>. Diakses 10 Juni 2016.
- Jlw Ansori. 2010. *Setting POP dan SMTP Yahoo dan Gmail.*
<http://jlw-saran.blogspot.co.id/2012/04/setting-pop-dan-smtp-yahoo-dan-gmail.html>. Diakses 2 Mei 2016.
- Fauzi. 2014. *Penerapan TRIPEL DES (DATA ENCRYPTION STANDARD) Pada Sistem Keamanan Teks E-Mail.* Jember : Universitas Muhammadiyah Jember.
- Gamatika Zone. Maret 2011. Operasi Biner.
<https://gamatika.wordpress.com/2011/03/08/operasi-biner-2/>. Diakses 6 Mei 2016.
- Injosoft. 2015. *ASCII Code - The extended ASCII table.*
<http://www.ascii-code.com/>. Diakses 11 Juni 2016.
- Manggala Budiasa, Rheno. 2010. *Analisis Kriptografi dalam penentuan Cipherteks kode ASCII melalui metode Aljabar Boolean.*
http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2009-2010/Makalah1/Makalah1_IF3058_2010_062.pdf. Diakses 5 Mei 2016.

Poerwanta, Rendi. Oktober 2013. *PERANCANGAN SISTEM INVENTORY SPARE PARTS MOBIL PADA CV.AUTO PARTS TOYOTA BERBASIS APLIKASI JAVA.*

<http://ejournal.unsri.ac.id/index.php/jsi/article/viewFile/739/280>. Diakses 5 Mei 2016.

Riyadi, Deffri. *STUDI ANALISIS PENGGUNAAN GNU PRIVACY GUARD (GPG) SEBAGAI ENKRIPSI KEAMANAN EMAIL BERBASIS WINDOWS.*

http://digilib.esaunggul.ac.id/public/UEU-Undergraduate-5364-2005-81-143_Deffri_Riyadi.pdf. Diakses 5 Mei 2016.

Rickson Saragih, Firman. 2008, *Penggunaan Kriptografi One Time Pad (Algoritma Vernam) dalam Pengamanan Informasi*”.

<http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2007-2008/Makalah/MakalahIF2153-0708-014.pdf>. Diakses 5 Mei 2016.

Sholeh. M & J.V. Hamokwarong. 2011. *Aplikasi Kriptografi Dengan Metode Vernam Cipher Dan Metode Permutasi Biner.*

<http://www.unwahas.ac.id/publikasiilmiah/index.php/MOMENTUM/article/view/105/100>. Diakses 12 Mei 2016.

Teknik Elektronika. 2015. *Pengertian Gerbang Logika Dasar dan Jenis-jenisnya.*

<http://teknikelektronika.com/pengertian-gerbang-logika-dasar-simbol/>.

Diakses 10 Juni 2016.

Wahana Komputer. 2010. *The Best Encryption Tools*. PT Elex Medi Komputindo: Jakarta.

Wibowo, Ivan. April 2009. *Penerapan Algoritma Kriptografi Asimetris RSA untuk Keamanan Data di Oracle.*

<http://ti.ukdw.ac.id/ojs/index.php/informatika/article/download/68/32>.

Diakses 11 Mei 2016.

Wikipedia. Oktober 2016. *Citra*. <https://id.wikipedia.org/wiki/Citra>. Diakses 12 Juni.

Yunanda, Martha. 2016. *Sistem Bilangan Biner.*

[http://sejarahmatematika1.blogspot.co.id/2015/04/sistem-bilangan-binер_24.html](http://sejarahmatematika1.blogspot.co.id/2015/04/sistem-bilangan-biner_24.html). Diakses 2 Mei 2016.