

TUGAS AKHIR

**TEKNIK KRIPTOGRAFI UNTUK MENJAGA KEAMANAN INFORMASI
DENGAN MEMANFAATKAN CITRA DIGITAL SEBAGAI KUNCI**



Disusun Oleh:

Muhamad Arfiq Khoiron (1110651034)

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

2015

HALAMAN PENGESAHAN

**TEKNIK KRIPTOGRAFI UNTUK MENJAGA KEAMANAN INFORMASI DENGAN
MEMANFAATKAN CITRA DIGITAL SEBAGAI KUNCI**

Disusun Oleh:
Muhamad Arfiq Khoiron
1110651034

Telah dipertahankan di depan dosen penguji
pada tanggal 29 Mei 2015
dan dinyatakan telah memenuhi syarat

Disahkan oleh:

Dosen Penguji 1

Dosen Pembimbing

Lutfi Ali Muharom, S.Si
NPK. 10 09 550

Ari Eko Wardoyo, S.T., M.Kom
NIP. 197502214 200501 1 001

Dosen Penguji 2

Dosen Pembimbing 2

Yulio Rahmadi, S.Kom
NPK. 10 03 545

Bakhtiyar Hadi Prakoso, S.Kom
NPK. 12 03 716

Jember, 29 Mei 2015

Mengetahui,

Dekan
Fakultas Teknik

Ketua Program Studi
Teknik Informatika

Ir. Rusgianto, M.M
NIP. 131 863867

Agung Nilogiri, S.T., M.Kom
NIP. 19770330 2005001 1 002

MOTTO

“Jaga Hati dan Mulut Tetap Senada”

PERSEMBAHAN

Karya tulis ini penulis persembahkan untuk:

Buk'e dan Pak'e yang saya patuhi

Seluruh Guru Ngaji di Musholla yang saya patuhi

Almamater Universitas Muhammadiyah Jember

Dosen Pembimbing dan Penguji yang saya hormati

Seluruh dosen mata kuliah yang saya hormati

Teman-teman yang memberikan dorongan semangat untuk saya

KATA PENGANTAR

Syukur Alhamdulillah penulis ucapkan atas segala kenikmatan yang Allah SWT berikan selama ini sehingga penulis dapat menyelesaikan penelitian ini, tak lupa sholawat dan salam semoga tetap terlimpahkan kepada Rosulullah Muhammad SAW.

Tak lupa penulis haturkan terimakasih kepada seluruh pihak yang telah membantu dalam pengerjaan laporan penelitian ini dengan judul “*Teknik Kriptografi untuk Mengamankan Informasi dengan Memanfaatkan Citra Digital Sebagai Kunci*”

1. Buk’e dan Pak’e yang saya patuhi
2. Bapak Ir. Rusgianto, MM selaku Dekan Fakultas Teknik
3. Bapak Agung Nilogiri, ST., M.Kom selaku Kaprodi Teknik Informatika
4. Bapak Daryanto, S.Kom., M.Kom selaku Dosen Wali
5. Bapak Ari Eko Wardoyo, ST., M.Kom selaku Dosen Pembimbing Tugas Akhir
6. Bapak Lutfi Ali Muharom, S.Si dan Bapak Yulio Rahmadi, S.Kom selaku Dosen Penguji Tugas Akhir
7. Seluruh Dosen Mata Kuliah yang saya hormati
8. Fina Rohmatul Uma yang saya sayangi
9. Teman-teman yang memberikan dorongan semangat

Dalam laporan ini, tentunya masih terdapat kekurangan baik secara teknis maupun non teknis, oleh karenanya penulis tetap mengharapkan kritik dan saran yang membangun agar laporan ini dapat mendekati titik sempurna.

Jember, 29 Mei 2015

Muhamad Arfiq Khoiron
NIM. 1110651034

TEKNIK KRIPTOGRAFI UNTUK MENJAGA KEAMANAN INFORMASI DENGAN MEMANFAATKAN CITRA DIGITAL SEBAGAI KUNCI

¹Muhamad Arfiq Khoiron (1110651034),

²Ari Eko Wardoyo, S.T., M.Kom, ³Bakhtiyar Hadi Prakoso, S.Kom

Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember

Email : mu.apieq@gmail.com

Abstrak

Keamanan sebuah informasi kini menjadi hal yang sangat mutlak untuk menjaga agar informasi tersampaikan pada pihak yang tepat. Kriptografi merupakan ilmu untuk menyamarkan suatu pesan demi menjaga kerahasiaannya. Suatu pesan (*plaintext*) harus melalui proses enkripsi terlebih dulu menjadi bentuk yang tidak berarti (*ciphertext*) sebelum dikirimkan ke penerima yang berhak. Hanya pihak yang berhak lah yang dapat melakukan proses dekripsi, yaitu mengubah kembali *ciphertext* menjadi *plaintext* memakai suatu kunci rahasia.

Desain sebuah algoritma untuk kriptografi telah banyak dibuat oleh kriptografer, dari algoritma yang bersifat klasik maupun modern. Pada umumnya algoritma yang dibuat terkuncikan oleh sebuah teks rahasia. Pada kesempatan ini penulis akan mengembangkan algoritma *caesar cipher* yang mana kunci untuk proses enkripsi dan dekripsi adalah sebuah gambar yang sama dengan memanfaatkan citra digital. Dalam sebuah citra berwarna, setiap piksel memiliki nilai intensitas warna *red*, *green*, *blue* yang dapat diubah dalam sebuah data teks. Nilai intensitas warna inilah yang akan menentukan banyaknya pergeseran huruf untuk proses enkripsi dan deskripsi yang berbeda pada tiap karakter.

Hasil yang didapatkan adalah sebuah pengembangan dari algoritma *caesar cipher* yang menggunakan citra digital sebagai kunci untuk proses enkripsi dan deskripsi. Dengan demikian informasi dalam bentuk *chiphertext* akan lebih sulit dipecahkan oleh penerima yang tidak berhak.

Kata kunci : *Kriptografi, Citra Digital, Caesar Cipher*

CRYPTOGRAPHY TECHNIQUE TO MAINTAIN SECURITY OF INFORMATION BY USING DIGITAL IMAGE AS A KEY

¹*Muhamad Arfiq Khoiron (1110651034),*

²*Ari Eko Wardoyo, S.T., M.Kom,* ³*Bakhtiyar Hadi Prakoso, S.Kom*

*Informatics Engineering Study Program Faculty of Engineering Muhammadiyah University
of Jember*

Email : mu.apieq@gmail.com

Abstract

An information security has now become very essential to keep the information passed on to the appropriate parties. Cryptography is the science of disguising a message in order to maintain confidentiality. A message (plaintext) must go through the encryption process first into a form that does not mean (ciphertext) before being sent to recipients who qualify. Only the party entitled to the one who can perform the decryption process, namely changing the ciphertext back into plaintext using a secret key.

Design an algorithm for cryptography has been widely made by cryptographers of algorithm that is both classic and modern. In general algorithm devised locked by a secret text. On this occasion the author will develop algorithms which caesar cipher keys for encryption and decryption is a similar picture by using digital image. In a color image, each pixel has a color intensity value of red, green, blue which can be converted into a text data. Color intensity values is what will determine the number of shifts letter for encryption and a different description for each character.

The results obtained are a development of caesar cipher algorithm that uses a digital image as a key for encryption and description. Thus the information in the form of ciphertext will be more difficult to resolve by an unauthorized recipient.

Keyword : *Kriptography, Digital Image, Caesar Cipher*

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
MOTTO	iii
PERSEMBAHAN	iv
KATA PENGANTAR	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah/Ruang Lingkup	2
1.4 Tujuan	3
1.5 Manfaat	3
BAB II TINJAUAN PUSTAKA	4
2.1 Kriptografi	4
2.2 Enkripsi dan Dekripsi	5
2.3 Algoritma Kriptografi Klasik	5
2.4 Metode Kriptografi Caesar Cipher atau Sift Cipher	6
2.5 Citra Digital	7
2.6 Bahasa Pemrograman JAVA	8
BAB III METODE PENELITIAN	10
3.1 Studi literatur	10
3.2 Perancangan sistem	10
3.2.1 Diagram Blok	11
3.2.2 Diagram Alur Algoritma	12

3.2.3 Rancangan Antar Muka.....	16
3.3 Metode Pengujian.....	18
BAB IV IMPLEMENTASI DAN PENGUJIAN.....	19
4.1 Implementasi.....	19
4.1.1 Perangkat Keras	19
4.1.2 Perangkat Lunak.....	19
4.1.3 Implementasi Antar Muka	19
4.2 Pengujian.....	21
4.2.1 Lingkungan Pengujian.....	22
4.2.2 Metode Pengujian.....	22
4.2.3 Pelaksanaan Pengujian	22
4.3 Hasil Pengujian.....	22
4.3.1 Pengujian konversi data integer dalam bentuk char	22
4.3.2 Pengujian enkripsi dan dekripsi seluruh karakter input keyboard	24
4.3.3 Pengujian enkripsi dan dekripsi dengan jumlah karakter < 30000	27
4.3.4 Pengujian enkripsi dan dekripsi dengan jumlah karakter = 30000	28
4.3.5 Pengujian enkripsi dan dekripsi dengan jumlah karakter > 30000	34
BAB V KESIMPULAN DAN SARAN	36
5.1 Kesimpulan	36
5.2 Saran.....	36
DAFTAR PUSTAKA	37
BIODATA PENULIS	38
LAMPIRAN	39
Lampiran 1.....	39
Lampiran 2.....	92
Lampiran 3.....	148

DAFTAR TABEL

Tabel 2.1 Contoh-contoh warna dalam hexadesimal.....	8
Tabel 4.1 Konversi data Integer ke dalam bentuk char pada Java	22
Tabel 4.2 Proses Enkripsi	25
Tabel 4.3 Proses Dekripsi.....	26
Tabel 4.4 Pengujian enkripsi seluruh karakter input keyboard	26
Tabel 4.5 Pengujian dekripsi seluruh karakter input keyboard	28
Tabel 4.6 Pengujian enkripsi dengan jumlah karakter < 30000	29
Tabel 4.7 Pengujian dekripsi dengan jumlah karakter < 30000	30
Tabel 4.8 Pengujian enkripsi dengan jumlah karakter = 30000	32
Tabel 4.9 Pengujian dekripsi dengan jumlah karakter =30000	33
Tabel 4.10 Pengujian enkripsi dengan jumlah karakter > 30000	34
Tabel 4.11 Pengujian enkripsi dengan jumlah karakter > 30000	35

DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi/Dekripsi Sederhana.....	5
Gambar 2.2 Ilustrasi metode kriptografi Shift Chiper atau Caesar Cipher	6
Gambar 2.3 Komposisi warna RGB	8
Gambar 3.1 Diagram Blok Aplikasi Kriptografi	11
Gambar 3.2 Diagram Alur Proses Enkripsi	12
Gambar 3.3 Diagram Alur Proses Dekripsi.....	14
Gambar 3.4 Desain Antar Muka Enkripsi dan Dekripsi.....	16
Gambar 3.5 Desain Antar Muka Impor File Teks (Plainteks).....	16
Gambar 3.6 Desain Antar Muka Impor File Teks (Cipherteks).....	17
Gambar 3.7 Desain Antar Muka Input Lokasi dan Nama Citra Berwarna.....	17
Gambar 3.8 Desain Antar Muka Input Indek yang dipakai.....	17
Gambar 3.9 Desain Antar Muka Ekspor Cipherteks dalam File Teks	17
Gambar 4.1 Antar Muka Enkripsi dan Dekripsi.....	19
Gambar 4.2 Antar Muka Impor File Teks (Plainteks).....	20
Gambar 4.3 Antar Muka Impor File Teks (Cipherteks)	20
Gambar 4.4 Antar Muka Input Lokasi dan Nama Citra Berwarna.....	21
Gambar 4.5 Antar Muka Input Indek yang dipakai.....	21
Gambar 4.6 Antar Muka Ekspor Cipherteks dalam File Teks	21