



UNIVERSITAS
MERCU BUANA

PENGAMANAN PESAN MENGGUNAKAN APLIKASI ENKRIPSI
DENGAN METODA ALGORITMA CAESAR CIPHER



UNIVERSITAS
AGUS RIYADI
41510120014
MERCU BUANA

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2015



UNIVERSITAS
MERCU BUANA

PENGAMANAN PESAN MENGGUNAKAN APLIKASI ENKRIPSI
DENGAN METODA ALGORITMA CAESAR CIPHER

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

UNIVERSITAS
MERCU BUANA

AGUS RIYADI

41510120014

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2015

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41510120014

Nama : AGUS RIYADI

Judul Tugas Akhir : Pengamanan Pesan Menggunakan Aplikasi Enkripsi
Dengan Metoda Algoritma Caesar Cipher

Menyatakan bahwa Tugas Akhir dengan judul yang tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat kecuali kutipan-kutipan dan teori-teori yang digunakan dalam skripsi ini. Apabila ternyata ditemukan didalam Laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 23 Juni 2015





LEMBAR PENGESAHAN


Nama : AGUS RIYADI
NIM : 41510120014
Jurusan : Teknik Informatika
Fakultas : Ilmu Komputer
Judul : Pengamanan Pesan Menggunakan Aplikasi Enkripsi Dengan
Metoda Algoritma Caesar Cipher

Jakarta, 23 Juni 2015

Disetujui dan diterima oleh,


UNIVERSITAS
Sabar Rudiarto, M.Kom.
MERCUBUANA
Kaprodi Teknik Informatika


Sabar Rudiarto, M.Kom.
Kaprodi Teknik Informatika


Umniy Salamah, ST, MMSI
Koordinator Tugas Akhir

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas karunia yang telah diberikan kepada penulis sehingga penulis dapat menyelesaikan Laporan Tugas Akhir tepat pada waktunya, dimana Laporan Tugas Akhir tersebut merupakan salah satu persyaratan untuk dapat menyelesaikan Program Studi Strata Satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

Penulis menyadari bahwa Laporan Tugas Akhir ini masih belum dapat dikatakan sempurna. Karena itu, kritik dan saran akan diterima dengan senang hati. Penulis juga menyadari bahwa Laporan Tugas Akhir ini takkan dapat selesai tepat pada waktunya tanpa bantuan, bimbingan, dan motivasi dari berbagai pihak. Maka dari itu, dengan segala kerendahan hati, Penulis ingin menyampaikan ucapan terima kasih kepada :

1. Sabar Rudiarto M.kom, selaku Pembimbing Tugas Akhir dan Kaprodi Teknik Informatika Universitas Mercu Buana yang telah membimbing penulis dengan semua nasihat, semangat dan ilmunya dalam menyusun laporan tugas akhir ini.
2. Umniy Salamah, ST, MMSI, selaku Koordinator Tugas Akhir Teknik Informatika Universitas Mercu Buana
3. Ibu saya yang selama ini telah memberikan nasihat dan kasih sayangnya.
4. Beserta semua pihak yang telah memotivasi dan ikut memberikan bantuannya kepada penulis yang namanya tidak dapat penulis sebutkan satu per satu.

Semoga Tuhan Yang Maha Esa membalas kebaikan yang telah diberikan kepada penulis dan penulis berharap semoga laporan tugas akhir ini bermanfaat bagi kita semua. Amin

Jakarta, Juni 2015

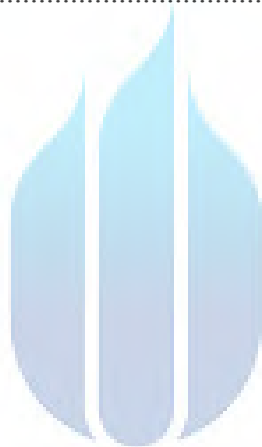
Agus Riyadi

DAFTAR ISI

Lembar pernyataan.....	iii
Lembar pengesahan.....	iv
Kata pengantar	v
Abstract	vi
Abstrak	vii
Daftar isi	viii
Daftar gambar	xi
Daftar tabel	xii
Bab I Pendahuluan	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat	3
1.5 Metode Penelitian	4
1.5.1 Metode Pengumpulan Data	4
1.5.2 Metode Pengembangan Perangkat Lunak	5
1.6 Metoda Pengujian	6
1.7 Sistematika Penulisan	7
Bab II Landasan Teori	9
2.1 Definisi Kriptografi	9
2.2 Perkembangan Kriptografi	9
2.3 Tujuan Kriptografi	11
2.4 Jenis Kriptografi	12

2.4.1 Sistem Kriptografi Simetri	13
2.4.1.1 Sistem Transposisi	14
2.4.1.2 Sistem Substitusi	16
2.4.2 Sistem Kriptografi Asimetri	18
2.4.3 Fungsi Hash	20
2.5 Kriptanalisis	21
2.5.1 kriptanalisis sistem Caesar Cipher	22
2.6 Bahasa Pemrograman Java	26
2.6.1 Pengertian Class dan Object	26
2.6.2 Konsep Dasar Pemrograman Java	27
Bab III Analisa dan Perancangan Sistem	28
3.1 Analisa Masalah	28
3.2 Analisa Sistem	29
3.3 Perancangan sistem	30
3.3.1 Model Pengembangan Sistem	31
3.4 Perancangan Proses	32
3.4.1 Use Case Diagram.....	33
3.4.1.1 Skenario Use Case	34
3.4.2 Activity Diagram	36
3.4.3 Sequence Diagram	40
3.4.3.1 Sequence Diagram Enkripsi Pesan	40
3.4.3.2 Sequence Diagram Dekripsi Pesan	41
3.5 Perancangan Interface	42
Bab IV Implementasi dan Pngujian	46
4.1 Implementasi Aplikasi	46
4.1.1 Lingkungan Perangkat Lunak	46
4.1.2 Spesifikasi Perangkat Keras yang Digunakan	48
4.1.3 Sistem Interface	48

4.2 Pengujian Aplikasi	51
4.2.1 Pengetesan Program	51
4.2.1 Data Hasil Pengujian	52
4.2.2 Analisa Hasil	63
4.3 Analisa Pengguna Aplikasi	66
Bab V Penutup	68
5.1 Kesimpulan	68
5.2 Saran	68
Daftar Pustaka	70



UNIVERSITAS
MERCU BUANA

DAFTAR GAMBAR

Gambar 2.1 Leon Battista Alberti 's cipher	10
Gambar 2.2 Thomas Jefferson Whell.....	11
Gambar 2.3 Algoritma simetri	14
Gambar 2.4 Algoritma asimetri	19
Gambar 3.1 Arsitektur proses	31
Gambar 3.2 Blok diagram aplikasi	32
Gambar 3.3 Use Case Diagram Enkripsi	33
Gambar 3.3 Use Case Diagram Dekripsi	34
Gambar 3.4 Activity diagram enkripsi	37
Gambar 3.5 Activity diagram dekripsi	39
Gambar 3.6 Sequence diagram enkripsi	41
Gambar 3.7 Sequence diagram dekripsi	42
Gambar 3.8 Rancangan User Interface aplikasi Caesar Cipher	43
Gambar 3.9 Objek antar muka aplikasi	44
Gambar 4.1 Aplikasi Caesar Cipher	49
Gambar 4.2 Aplikasi Caesar Cipher Input pesan	50
Gambar 4.2 Aplikasi Caesar Cipher Dekripsi pesan	50
Gambar 4.3 Pengujian kesalahan sistem	63

DAFTAR TABEL

Tabel 2.1 Contoh sistem transposisi 1	14
Tabel 2.2 Contoh sistem transposisi 2	15
Tabel 2.3 Contoh sistem transposisi 3	15
Tabel 2.4 Pergeseran caesar cipher	16
Tabel 2.5 Jenis serangan terhadap pesan terenkripsi	21
Tabel 2.6 Distribusi Frekuensi Standart (DFS) Bahasa Indonesia	23
Tabel 2.7 DFS contoh sandi Caesar Cipher	23
Tabel 3.1 Skenario Use Case Enkripsi Pesan	35
Tabel 3.2 Skenario Use Case Dekripsi Pesan	35
Tabel 3.3 Fungsi Objek antar muka	44
Tabel 4.1 Spesifikasi lingkungan pengujian	48
Tabel 4.2 Hasil pengujian black box	52
Tabel 4.3 Hasil pengujian 1	56
Tabel 4.4 Hasil pengujian 2	57
Tabel 4.5 Hasil pengujian 3	58
Tabel 4.6 Hasil pengujian 4	59
Tabel 4.7 Hasil pengujian 5	60
Tabel 4.8 Hasil pengujian 6	61