



UNIVERSITAS  
**MERCU BUANA**

**Pengembangan Algoritma Caesar Cipher  
Dengan Teknik Kriptografi Untuk Keamanan Data**



UNIVERSITAS  
SAIFUDIN  
41511120085  
**MERCU BUANA**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS MERCU BUANA  
JAKARTA  
2016**



UNIVERSITAS  
**MERCU BUANA**

**Pengembangan Algoritma Caesar Cipher  
Dengan Teknik Kriptografi Untuk Keamanan Data**

*Laporan Tugas Akhir*

Diajukan Untuk Melengkapi Persyaratan  
Menyelesaikan Gelar Sarjana Komputer



UNIVERSITAS  
Disusun oleh :  
**SAIFUDIN**  
**41511120085**  
MERCU BUANA

**PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS MERCU BUANA  
JAKARTA  
2016**

## LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41511120085

Nama : Saifudin

Judul Tugas Akhir : Pengembangan Algoritma Caesar Cipher Dengan Teknik  
Kriptografi Untuk Keamanan Data

Menyatakan bahwa skripsi tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 28 Agustus 2016



( SAIFUDIN )

## LEMBAR PENGESAHAN

**Nama** : Saifudin  
**NIM** : 41511120085  
**Program Studi** : Informatika  
**Fakultas** : Ilmu Komputer  
**Judul** : Pengembangan Algoritma Caesar Cipher  
Dengan Teknik Kriptografi Untuk Keamanan Data



Jakarta, Agustus 2016

Disetujui dan diterima oleh

UNIVERSITAS  
MERCU BUANA

Drs. Achmad Kodar, MT.

Pembimbing

Dr. Yaya Sudarya Triana, M.Kom.

Kaprodi Informatika

Desi Ramayanti, S.Kom, MT.

Koordinator Tugas Akhir Informatika

## Kata Pengantar

Syukur Alhamdulillah penulis panjatkan kepada Allah SWT, karena atas limpahan rahmat, taufik, dan hidayah-Nya sehingga penulis mampu menyelesaikan tugas akhir dengan judul “Pengembangan Algoritma Caesar Cipher Dengan Teknik Kriptografi Dalam Keamanan Data”.

Tugas akhir ini diselesaikan sebagai salah satu syarat untuk menyelesaikan Program Studi Strata Satu (S1) pada Program Studi Informatika Universitas Mercu Buana. Selesaiannya tugas akhir ini tentunya tidak lepas dari berbagai pihak yang memberikan dorongan, uluran tangan dan bantuan dalam menyelesaikan tugas akhir ini. Oleh karena itu, dengan segala kerendahan hati penulis mengucapkan terima kasih kepada :

1. Bapak Drs, Achmad Kodar, MT., selaku Pembimbing Tugas Akhir yang telah membimbing penulis dengan sabar dalam menyelesaikan laporan tugas akhir ini.
2. Ibu Desi Ramayanti, S.Kom, MT., selaku Koordinator Tugas Akhir Informatika Universitas Mercu Buana yang telah dengan sabar memberi tenggang waktu sampai batas akhir semester untuk penulis mengajukan sidang tugas akhir ini.
3. Bapak Muhammad Rifqi, dosen Universitas Mercu Buana selaku Pemberi ide dan judul sehingga penulis dapat menyelesaikan tugas akhir ini.
4. Bapak DR. Yaya Sudarya Triana, M.Kom., selaku Kepala Program Studi Informatika Universitas Mercu Buana.
5. Ibu, Bapak serta keluarga tercinta yang selalu mendoakan dan mendukung penulis dalam menyelesaikan kuliah di Universitas Mercu Buana.
6. Teman satu angkatan program studi Informatika Yunita Anggraeni, yang telah membantu menyelesaikan aplikasi sehingga laporan tugas akhir ini bisa diselesaikan.
7. Teman-teman program studi Informatika angkatan XX yang telah memberikan banyak dukungan, semangat, pengalaman dalam perkuliahan dan pencerahan pada skripsi ini.
8. Saudara, teman dan sahabat-sahabat yang telah memberikan dukungan moral untuk terus menyelesaikan perkuliahan dan tugas akhir ini.

Penulis berharap semoga semoga Allah SWT membalas kebaikan dan ketulusan semua pihak yang sudah banyak membantu penulis dalam tugas akhir ini dengan melimpahkan rahmat dan karunia-Nya, aamiin. Semoga dari tugas akhir ini dapat memberikan manfaat dan kebaikan bagi banyak pihak demi kemajuan bersama, Aamiin,

Jakarta ,18 Agustus 2016

SAIFUDIN



## Daftar Isi

Kata Pengantar .....	i
ABSTRAKSI .....	iii
<i>ABSTRACT</i> .....	iv
Daftar Isi .....	v
Daftar Gambar .....	viii
Daftar Tabel .....	ix
BAB 1. PENDAHULUAN .....	1-1
1.1. Latar Belakang .....	1-1
1.2. Rumusan Permasalahan .....	1-2
1.3. Tujuan Dan Manfaat Penelitian .....	1-3
<b>1.3.1 Tujuan Penelitian</b> .....	1-3
<b>1.3.2 Manfaat Penelitian</b> .....	1-3
1.4. Ruang Lingkup & Batasan Penelitian .....	1-3
1.5. Metodologi Penelitian .....	1-4
1.6. Sistematika Penulisan .....	1-6
<b>1.6.1 Pendahuluan</b> .....	1-6
<b>1.6.2 Landasan Teori</b> .....	1-6
<b>1.6.3 Analisis Sistem</b> .....	1-6
<b>1.6.4 Perancangan Sistem</b> .....	1-6
<b>1.6.5 Implementasi Dan Testing</b> .....	1-6
<b>1.6.6 Penutup</b> .....	1-6
BAB 2. LANDASAN TEORI .....	2-1
2.1. Data dan Informasi .....	2-1
2.2. Keamanan Data dan Informasi .....	2-1
2.3. Layanan Keamanan Jaringan Dalam Komunikasi Data .....	2-2
2.4. Mekanisme Keamanan Jaringan .....	2-3
2.5. Kriptografi .....	2-4
<b>2.5.1 Pengertian Kriptografi</b> .....	2-4
<b>2.5.2 Sejarah Kriptografi</b> .....	2-7
<b>2.5.3 Sistem Kriptografi</b> .....	2-10
<b>2.5.4 Kriptografi Klasik</b> .....	2-11
<b>2.5.5 Sistem Kriptografi Klasik berbasis Substitusi</b> .....	2-15
<b>2.5.6 Serangan Terhadap Kriptografi</b> .....	2-20
2.6. Tinjauan Matematis .....	2-23
<b>2.6.1 Konsep Dasar Kriptografi</b> .....	2-23

2.6.2	<b>Aritmatika Modular</b> .....	2-24
2.7.	<i>Java</i> .....	2-24
2.7.1	<b>Pengertian Java</b> .....	2-24
2.7.2	<b>Sejarah Java</b> .....	2-25
2.7.3	<b>Fitur-fitur Java</b> .....	2-26
2.7.4	<b>Kelebihan Java</b> .....	2-28
2.8.	NetBeans .....	2-30
2.8.1	<b>Pengertian NetBeans</b> .....	2-30
2.8.2	<b>Sejarah NetBeans</b> .....	2-31
2.9.	UML (Unified Modeling Language) .....	2-31
2.9.1	<b>Class Diagram</b> .....	2-32
2.9.2	<b>Use Case Diagram</b> .....	2-32
2.9.3	<b>Activity Diagram</b> .....	2-33
2.9.4	<b>Sequence Diagram</b> .....	2-33
2.10.	Metode Pengujian <i>Black Box</i> .....	2-34
BAB 3.	<b>ANALISA DAN PERANCANGAN SISTEM</b> .....	3-1
3.1.	Analisa Sistem .....	3-1
3.1.1	Analisa Sistem .....	3-1
3.1.2	Analisa Masalah .....	3-1
3.1.3	Analisa Pemecahan Masalah .....	3-2
3.1.4	Analisa Pembuatan Sistem .....	3-3
3.2.	Perancangan Sistem .....	3-5
3.2.1	Use Case Diagram .....	3-5
3.2.2	Activity Diagram .....	3-7
3.2.3	Diagram Sequence .....	3-9
3.3.	Perancangan Algoritma .....	3-11
3.4.	Perancangan Antar Muka Kriptografi .....	3-13
3.4.1	Tampilan Menu Awal .....	3-13
3.4.2	Tampilan Menu Enkripsi .....	3-13
3.4.3	Tampilan Menu Dekripsi .....	3-14
	Gambar 3.10. <i>Kode ASCII</i> .....	3-17
BAB 4.	<b>IMPLEMENTASI DAN PENGUJIAN</b> .....	4-1
4.1.	Implementasi .....	4-1
4.1.1	<b>Perangkat Keras</b> .....	4-1
4.1.2	<b>Perangkat Lunak Platform</b> .....	4-1
4.2.	Hasil Implementasi .....	4-1
4.2.1	Implementasi Antar Muka (Interface) .....	4-1



4.2.2	Implementasi Algoritma .....	4-6
4.3.	Pengujian Sistem .....	4-11
4.3.1	Metode Pengujian .....	4-11
4.3.2	Skenario Pengujian .....	4-11
4.3.3	Hasil Pengujian .....	4-15
4.3.4	Kesimpulan Hasil Pengujian.....	4-23
BAB 5.	PENUTUP .....	5-1
	Kesimpulan .....	5-1
5.1.	Saran.....	5-1
<b>Daftar Pustaka</b>	.....	<b>A</b>
<b>LAMPIRAN</b>	.....	<b>B</b>



## Daftar Gambar

Gambar 1.1	Ilustrasi Model Waterfall .....	1-4
Gambar 2.1	Skema proses enkripsi dan dekripsi .....	2-7
Gambar 2.2	Hieroglyphics .....	2-8
Gambar 2.3	Scytale .....	2-8
Gambar 2.4	Risalah fi Istikhraj al-Mu'amma .....	2-9
Gambar 2.7	Simulasi penyandian Caesar Cipher .....	2-16
Gambar 2.8	Ilustrasi Sandi Affine .....	2-18
Gambar 3.1	Proses Enkripsi kombinasi Caesar Affine Cipher .....	3-5
Gambar 3.2	Use Case enkripsi deskripsi .....	3-6
Gambar 3.3	Activity Diagram proses Enkripsi .....	3-7
Gambar 3.4	Activity Diagram proses Dekripsi .....	3-8
Gambar 3.5	Sequence Diagram Proses Enkripsi .....	3-9
Gambar 3.6	Diagram Sequence Proses Dekripsi .....	3-10
Gambar 3.7	Tampilan Menu awal .....	3-13
Gambar 3.8	Tampilan Form Enkripsi .....	3-13
Gambar 3.9	Tampilan Form Dekripsi .....	3-14
Gambar 3.10	Kode ASCII .....	3-17
Gambar 4.1	Tampilan awal menu .....	4-2
Gambar 4.2	Tampilan Menu Login .....	4-2
Gambar 4.3	Tampilan menu enkripsi .....	4-3
Gambar 4.4	Form Dekripsi .....	4-4
Gambar 4.5	Tampilan popup salah login .....	4-18
Gambar 4.6	Fungsi Enkripsi .....	4-19
Gambar 4.7	Tampilan Simpan Hasil .....	4-20
Gambar 4.8	Tampilan popup salah login .....	4-21
Gambar 4.9	Hasil uji Dekripsi .....	4-21

## Daftar Tabel

Tabel 2.1	<i>Cipher Substitusi</i> .....	2-12
Tabel 2.2	Tabel nilai operasi XOR.....	2-24
Tabel 3.1	Proses Enkripsi .....	3-6
Tabel 3.2	Proses Dekripsi.....	3-6
Tabel 4.1	Skenario Pengujian Menu Awal.....	4-12
Tabel 4.2	Skenario Pengujian Halaman Login.....	4-12
Tabel 4.3	Skenario Pengujian Halaman Form Enkripsi .....	4-12
Tabel 4.4	Skenario Pengujian Halaman Form Dekripsi .....	4-14
Tabel 4.5	Hasil Pengujian Menu Awal.....	4-15
Tabel 4.6	Hasil Pengujian Halaman Login.....	4-15
Tabel 4.7	Hasil Pengujian Halaman Form Enkripsi .....	4-16
Tabel 4.8	Hasil Pengujian Halaman Form Dekripsi.....	4-17

