



UNIVERSITAS
MERCU BUANA

**APLIKASI KRIPTOGRAFI UNTUK *SHORT MESSAGE SERVICE*
MENGUNAKAN ALGORITMA EL GAMAL DENGAN PEMBANGKIT
KUNCI SECARA OTOMASI MENGGUNAKAN *TIMESTAMP* DAN
MANUAL BERBASIS ANDROID**

UNIVERSITAS
Chesa Bagus Wiraksana
41513110133
MERCU BUANA

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2017**



UNIVERSITAS
MERCU BUANA

**APLIKASI KRIPTOGRAFI UNTUK *SHORT MESSAGE SERVICE*
MENGUNAKAN ALGORITMA EL GAMAL DENGAN PEMBANGKIT
KUNCI SECARA OTOMASI MENGGUNAKAN *TIMESTAMP* DAN
MANUAL BERBASIS ANDROID**

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Persyaratan
Menyelesaikan Gelar Sarjana Komputer

Disusun oleh :

Chesa Bagus Wiraksana

41513110133

UNIVERSITAS
MERCU BUANA

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

2017

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41513110133
Nama : Chesa Bagus Wiraksana
Judul Tugas Akhir : Aplikasi Kriptografi Untuk *Short Message Service*
Menggunakan Algoritma El Gamal Dengan Pembangkit
Kunci Secara Otomasi Menggunakan *Timestamp* Dan
Manual Berbasis Android.

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.

UNIVERSITAS
MERCU BUANA

Jakarta, 29 Desember 2017



Chesa Bagus Wiraksana

LEMBAR PENGESAHAN

Nama : Chesa Bagus Wiraksana
NIM : 41513110133
Jurusan : Teknik Informatika
Fakultas : Ilmu Komputer
Judul : Aplikasi Kriptografi Untuk *Short Message Service*
Menggunakan Algoritma El Gamal Dengan Pembangkit
Kunci Secara Otomasi Menggunakan *Timestamp* Dan
Manual Berbasis Android.

Jakarta, 28 Desember 2017

Disetujui dan diterima oleh,



(Dr. Ir. Eliyani)

Dosen Pembimbing

UNIVERSITAS
MERCU BUANA



Desi Ramayanti, S.Kom., M.T.

Kaprodi Informatika



Andi Nugroho., ST., M.Kom

Koordinator Tugas Akhir

KATA PENGANTAR

Segala puji dan syukur kehadirat ALLAH SWT atas berkat dan rahmat hidayahnya Alhamdulillah diberikan kemudahan dalam menyelesaikan laporan tugas akhir yang telah saya kerjakan, dalam penyusunan laporan tugas akhir ini merupakan salah satu syarat akademik Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana dalam menempuh gelar sarjana strata 1 (S1).

Dengan terselesaikannya penyusunan laporan tugas akhir atau skripsi ini tidak terlepas peran serta pihak yang telah memberikan banyak bantuan sehingga penulis dapat menyelesaikan dengan sebaik-baiknya, dengan segala kerendahan hati penulis menyadari bahwa penulisan laporan tugas ini masih banyak kekurangan, tetapi penulis berusaha memperbaiki dan menyajikan sebuah laporan tugas akhir baik sehingga dapat berguna bagi penulis maupun orang lain yang membutuhkannya.

Dalam melakukan pembuatan aplikasi, penyusunan serta penulisan tugas akhir ini, penulis banyak sekali dibantu oleh berbagai pihak. Maka, penulis ingin sekali menyampaikan rasa banyak terima kasih kepada:

1. Kepada Ibu Dr. Ir. Eliyani selaku dosen pembimbing tugas akhir Program Studi Informatika Universitas Mercu Buana.
2. Kepada Ibu Desi Ramayanti, S.Kom,.M.T. selaku Ketua Program Studi Informatika Universitas Mercu Buana.
3. Kepada Bapak Andi Nugroho, ST,. M.Kom selaku koordinator Tugas Akhir Informatika Universitas Mercu Buana.
4. Kepada Bapak Drs. Achmad Kodar, M.T selaku dosen pembimbing akademik Program Studi Informatika Universitas Mercu Buana.
5. Kepada kedua orang tua yang selalu memberikan dukungan dan semangat.
6. Kepada teman-teman yang telah memberikan masukan, saran dalam pembuatan laporan tugas akhir ini.
7. Dan semua pihak yang tidak dapat saya sebutkan satu persatu, yang turut membantu dalam penyusunan laporan tugas akhir ini.

Jakarta, Desember 2017
Penulis

Chesa Bagus Wiraksana

Daftar Isi

ABSTRAKSI	i
ABSTRACT	ii
LEMBAR PERNYATAAN	iii
LEMBAR PERSETUJUAN SIDANG	iv
LEMBAR PENGESAHAN SIDANG	v
KATA PENGANTAR	vi
Daftar Isi	vii
Daftar Gambar	x
Daftar Tabel	x
Definisi	xi
BAB 1. PENDAHULUAN	1-1
1.1. Latar Belakang.....	1-1
1.2. Rumusan Permasalahan.....	1-2
1.3. Tujuan & Manfaat Penelitian.....	1-2
1.3.1 Tujuan Penelitian.....	1-2
1.3.2 Manfaat Penelitian.....	1-2
1.4. Ruang Lingkup & Batasan Penelitian.....	1-3
1.5. Metodologi Penelitian.....	1-3
1.5.1 Metode Pengumpulan Data.....	1-3
1.6. Sistematika Penulisan Laporan.....	1-4
1.6.1 Pendahuluan.....	1-4
1.6.2 Landasan Teori.....	1-4
1.6.3 Analisis Sistem.....	1-4
1.6.4 Perancangan Sistem.....	1-4
1.6.5 Implementasi Dan Testing.....	1-4
1.6.6 Penutup.....	1-4
BAB 2. LANDASAN TEORI	2-1
2.1. Definisi Kriptografi.....	2-1
2.2. Tujuan Kriptografi.....	2-2
2.3. Jenis Kriptografi.....	2-2
2.3.1 Kriptografi Simetris.....	2-2
2.3.2 Kriptografi Asimetris.....	2-3
2.4. Terminologi Kriptografi.....	2-4
2.4.1 Pesan, Plainteks, dan Cipherteks.....	2-4

2.5.	Keamanan Sistem Kriptografi	2-5
2.5.1	Jenis-Jenis Ancaman Keamanan	2-5
2.5.2	Serangan Pada Sistem Kriptografi	2-6
2.6.	Algoritma El Gamal.....	2-6
2.7.	Pengertian <i>Short Message Service</i> (SMS)	2-7
2.8.	Mekanisme Kerja SMS.....	2-8
2.9.	Implementasi Teknologi SMS	2-11
2.10.	Android	2-11
2.11.	Fitur dan Arsitektur Android	2-12
2.12.	Java	2-13
2.13.	Pemodelan Sistem.....	2-13
2.13.1	Unified Modelling Language (UML).....	2-13
2.13.2	Metode Pengembangan Perangkat Lunak.....	2-14
BAB 3.	ANALISA SISTEM.....	3-1
3.1.	Analisa Masalah.....	3-1
3.2.	Analisa Kebutuhan Pengguna.....	3-1
3.3.	Analisa Kebutuhan Sistem.....	3-1
3.3.1	Analisa Kebutuhan Software	3-2
3.3.2	Analisa Kebutuhan Hardware	3-2
	Perangkat keras yang digunakan dalam pembuatan aplikasi adalah sebagai berikut :.....	3-2
3.3.3	Analisa Kebutuhan Fungsional.....	3-2
3.3.4	Analisa Kebutuhan Non Fungsional.....	3-3
3.3.5	Uraian Prosedur Penggunaan Aplikasi	3-3
BAB 4.	PERANCANGAN	4-1
4.1.	Perancangan Algoritma El Gamal	4-1
4.1.1	Proses Pembentukan Kunci	4-1
4.1.2	Proses Enkripsi	4-1
4.1.3	Proses Dekripsi.....	4-5
4.2.	Perancangan Sistem	4-6
4.2.1	Gambaran Umum Sistem	4-7
4.2.2	Use Case Diagram	4-8
4.2.3	Activity Diagram	4-9
4.3.	Perancangan Antar Muka	4-11
4.3.1	Perancangan Halaman Utama (Main Menu).....	4-11
4.3.2	Perancangan Halaman Kotak Masuk (Inbox)	4-12
4.3.3	Perancangan Halaman Input Kontak Dan Tentang (Main Menu).....	4-13
4.3.4	Perancangan Halaman Buat Pesan (Create Message).....	4-14

4.3.5	Perancangan Halaman Input Kunci (Input Key).....	4-15
4.3.6	Perancangan Halaman Dekripsi Manual (Manual Decryption).....	4-15
BAB 5.	IMPLEMENTASI DAN PENGUJIAN	5-1
5.1.	Lingkungan Implementasi.....	5-1
5.1.1	Perangkat Keras	5-1
5.1.2	Perangkat Lunak Platform	5-1
5.2.	Hasil Implementasi.....	5-2
5.2.1	Hasil Implementasi Antarmuka Android.....	5-2
5.2.2	Hasil Implementasi Fungsi Algoritma El Gamal.....	5-7
5.3.	Hasil Pengujian.....	5-12
5.3.1	Metode Pengujian	5-12
5.3.2	Skenario Uji Coba.....	5-13
5.3.3	Hasil Uji Coba.....	5-15
BAB 6.	PENUTUP	6-1
6.1.	Kesimpulan.....	6-1
6.2.	Saran.....	6-1
	Daftar Pustaka.....	A
	LAMPIRAN KODE SUMBER.....	C



UNIVERSITAS
MERCU BUANA

Daftar Gambar

<i>Gambar 2-1 Skema Kriptografi</i>	2-1
<i>Gambar 2-2 Skema Kriptografi Dengan Kunci Simetris</i>	2-3
<i>Gambar 2-3 Skema Kriptografi Dengan Kunci Asimetris</i>	2-4
<i>Gambar 2-4 Mekanisme Intra-Operator SMS (Wahana Komputer, 2005)</i>	2-9
<i>Gambar 2-5 Mekanisme Inter-Operator SMS (Wahana Komputer, 2005)</i>	2-10
<i>Gambar 2-6 Jumlah Versi Android</i>	2-12
<i>Gambar 2-7 Model perancangan air terjun (Water Fall)</i>	2-15
<i>Gambar 4-1 Flowchart Proses Enkripsi Algoritma El Gamal</i>	4-2
<i>Gambar 4-2 Flowchart Proses Dekripsi Algoritma El Gamal</i>	4-5
<i>Gambar 4-3 Flowchart Gambaran Umum SMS.</i>	4-7
<i>Gambar 4-4 Use Case Diagram SMS</i>	4-8
<i>Gambar 4-5 Activity Diagram Proses Enkripsi SMS</i>	4-9
<i>Gambar 4-6 Activity Diagram Proses Dekripsi SMS</i>	4-10
<i>Gambar 4-7 Rancangan Antarmuka Halaman Utama</i>	4-11
<i>Gambar 4-8 Rancangan Antarmuka Kotak Masuk</i>	4-12
<i>Gambar 4-9 Rancangan Antarmuka Input Kontak</i>	4-13
<i>Gambar 4-10 Rancangan Antarmuka Tentang</i>	4-13
<i>Gambar 4-11 Rancangan Antarmuka Buat Pesan</i>	4-14
<i>Gambar 4-12 Rancangan Antarmuka Input Kunci</i>	4-15
<i>Gambar 4-13 Rancangan Dekripsi Pesan Secara Manual</i>	4-16
<i>Gambar 5-1 Implementasi Halaman Utama/Kotak Masuk</i>	5-2
<i>Gambar 5-2 Implementasi Halaman Pilih Kontak</i>	5-3
<i>Gambar 5-3 Implementasi Halaman Buat Pesan Baru</i>	5-4
<i>Gambar 5-4 Implementasi Halaman Kotak Masuk Pesan</i>	5-5
<i>Gambar 5-5 Implementasi Tampilan Informasi Tentang</i>	5-6
<i>Gambar 5-6 Implementasi Tampilan Fungsi Algoritma El Gamal</i>	5-7
<i>Gambar 5-7 Implementasi Hasil Fungsi El Gamal Dengan Aplikasi SMS Default</i>	5-8
<i>Gambar 5-8 Implementasi El Gamal Dengan Mengirim Pesan Secara Beruntun</i>	5-9
<i>Gambar 5-9 Implementasi Tombol Kirim Pesan Tanpa Fungsi Enkripsi</i>	5-10
<i>Gambar 5-10 Implementasi Pengiriman Plainteks 160 Karakter Pada El Gamal SMS</i>	5-10
<i>Gambar 5-11 Implementasi Halaman Menginput Kunci Untuk Manual Enkripsi</i>	5-11
<i>Gambar 5-12 Implementasi Membaca Pesan Dengan Metode Dekripsi Manual</i>	5-12

Daftar Tabel

<i>Tabel 4-1 Plainteks Di Konversi Ke Kode ASCII</i>	4-3
<i>Tabel 4-2 Proses Enkripsi Plainteks Ke Chiperteks</i>	4-4
<i>Tabel 4-3 Proses Dekripsi Chiperteks Ke Plainteks</i>	4-6
<i>Tabel 5-1 Smartphone Yang Digunakan Untuk Implementasi Aplikasi</i>	5-1
<i>Tabel 5-2 Skenario Pengujian Aplikasi</i>	5-13
<i>Tabel 5-3 Hasil Pengujian Aplikasi</i>	5-15



Definisi

Istilah	Pengertian
Kriptografi	Pengertian Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita [Bruce Schneier - Applied Cryptography].
Enkripsi	Di bidang kriptografi, enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus.
Dekripsi	Dekripsi merupakan proses kebalikan dari enkripsi dimana proses ini akan mengubah <i>ciphertext</i> menjadi <i>plaintext</i> dengan menggunakan algoritma 'pembalikan' dan key yang sama.
Plainteks	Plainteks adalah suatu teks yang memberikan suatu informasi dan tidak menggunakan proses <i>formatting</i> teks yang khusus. Dalam kriptografi plaintext adalah pesan asli yang belum diubah.
Ciphertexts.	Ciphertext adalah pesan ter-enkripsi (tersandi) yang merupakan hasil dari proses enkripsi.
<i>Short Message Service</i> (SMS)	<i>Short Message Service</i> atau lebih dikenal dengan sebutan SMS merupakan sebuah teknologi yang memungkinkan untuk menerima maupun mengirimkan pesan antar telepon bergerak/ponsel
Komunikator	Komunikator adalah pihak yang bertindak sebagai pengirim pesan kepada komunikan. komunikator merupakan seseorang atau sekelompok orang yang berinisiatif untuk menjadi sumber dalam sebuah hubungan.
Komunikan	Komunikan adalah partner atau rekan dari komunikator dalam komunikasi. Ia berperan sebagai penerima berita atau pesan.