

**RANCANG BANGUN APLIKASI STEGANOGRAFI AUDIO PADA  
FILE MP3 DENGAN METODE LOW BIT CODING  
DAN ADVANCED ENCRYPTION STANDARD**

**TUGAS AKHIR**

untuk memenuhi sebagian persyaratan mencapai gelar Ahli Madya  
pada jenjang Diploma III jurusan Teknik Informatika



disusun oleh

**Bram Pratowo**  
**10.01.2775**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM  
YOGYAKARTA  
2012**

**PERSETUJUAN**

**TUGAS AKHIR**

**RANCANG BANGUN APLIKASI STEGANOGRAFI AUDIO PADA  
FILE MP3 DENGAN METODE LOW BIT CODING  
DAN ADVANCED ENCRYPTION STANDARD**

yang dipersiapkan dan disusun oleh

**Bram Pratowo  
10.01.2775**

telah disetujui oleh Dosen Pembimbing Tugas Akhir  
pada tanggal 27 September 2012

**Dosen Pembimbing**



**Bayu Setiaji, M.Kom  
19000003**

**PENGESAHAN**

**TUGAS AKHIR**

**RANCANG BANGUN APLIKASI STEGANOGRAFI AUDIO PADA  
FILE MP3 DENGAN METODE LOW BIT CODING  
DAN ADVANCED ENCRYPTION STANDARD**

yang dipersiapkan dan disusun oleh

**Bram Pratowo**  
**10.01.2775**

telah dipertahankan di Depan Penguji  
pada tanggal 15 Desember 2012

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

**Akhmad Dahlan, S.Kom.**  
**NIK. 190302174**

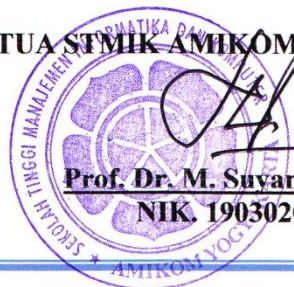


**Yuli Astuti, M.Kom.**  
**NIK. 190302146**



Tugas Akhir ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Ahli Madya Komputer  
Tanggal 2 Januari 2013

**KETUA STMK AMIKOM YOGYAKARTA**



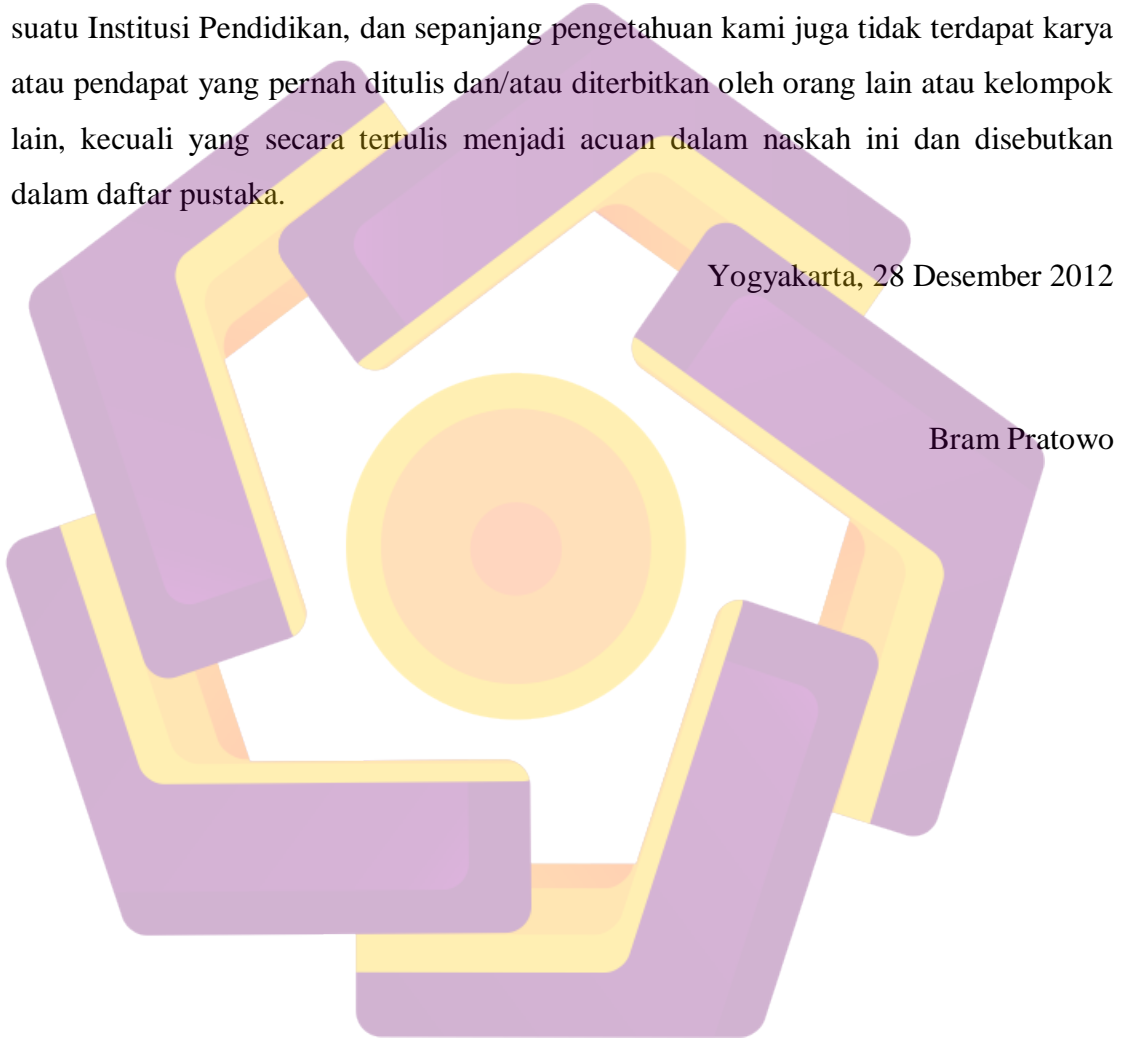
**Prof. Dr. M. Suyanto, M.M.**  
**NIK. 190302001**

## **PERNYATAAN**

Saya yang bertandatangan di bawah menyatakan bahwa Tugas Akhir ini merupakan karya sendiri (ASLI) dan isi dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan oleh orang lain atau kelompok lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan kami juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain atau kelompok lain, kecuali yang secara tertulis menjadi acuan dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 28 Desember 2012

Bram Pratowo



## MOTTO DAN PERSEMBAHAN

### Motto

Karena sesungguhnya sesudah kesulitan itu ada kemudahan.  
Sesungguhnya sesudah kesulitan itu ada kemudahan.  
Maka apabila kamu telah selesai (dari suatu urusan), kerjakanlah dengan  
sungguh-sungguh (urusan) yang lain.  
Dan hanya kepada Tuhanmulah hendaknya kamu berharap  
(Al-Insyirah 5-8)

### Persembahan

Setiap goresan tinta ini adalah bentuk keagungan dan kasih sayang yang  
diberikan oleh Allah SWT kepada umatnya.

Setiap detik, setiap waktu untuk menyelesaikan Tugas Akhir ini merupakan  
hasil getaran doa kedua orang tua, kakak, keluarga, dan orang-orang terkasih  
yang mengalir tiada henti.

Setiap pancaran dan semangat dalam penulisan Tugas Akhir ini merupakan  
dorongan dan dukungan dari sahabat-sahabatku tercinta.

Setiap materi dan pembahasan dalam Tugas Akhir ini adalah hampasan  
saran dan kritik dari kawan-kawan almamaterku.

Terima kasih kepada seluruh teman-teman di Innovation Center Amikom  
yang telah berbagi ilmu dan pengalaman

Terima kasih kepada seluruh programmer Innovation Center Amikom atas  
doa dan dukungannya

Terima kasih kepada teman-teman spesial 10-D3TI-02

Terima kasih kepada teman-teman kontrakan: Aris, Bolon, Iponk, Bambang

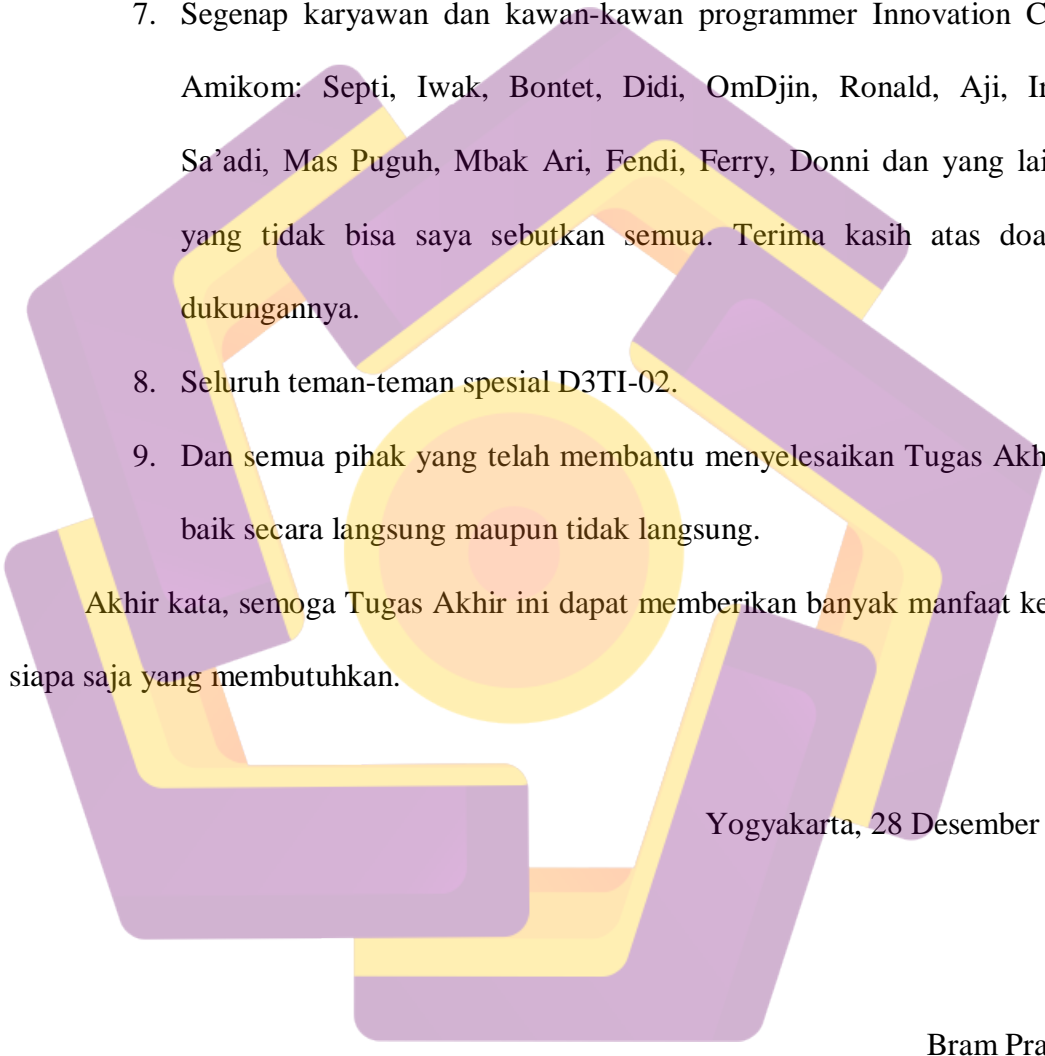
## KATA PENGANTAR

Alhamdulillah, segala puji bagi Allah SWT, karena atas berkat rahmat dan karunianya penulis dapat menyelesaikan Tugas Akhir yang berjudul **“Rancang Bangun Aplikasi Steganografi Audio pada File MP3 dengan Metode Low Bit Coding dan Advanced Encryption Standard”**.

Tugas Akhir ini disusun sebagai salah satu persyaratan akademis untuk menyelesaikan pendidikan Diploma III (D3) Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta. Penulis menyadari bahwa Tugas Akhir ini masih memiliki banyak kekurangan dan jauh dari kesempurnaan karena keterbatasan pengetahuan dan minimnya pengalaman penulis.

Pada kesempatan ini, penulis menyampaikan terima kasih kepada:

1. Bapak Prof. Dr. M. Suyanto, MM sebagai Ketua STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan M.T selaku Ketua Jurusan Diploma III Teknik Informatika.
3. Bapak Bayu Setiaji, M.Kom selaku Dosen Pembimbing yang telah banyak membantu menyelesaikan Tugas Akhir ini.
4. Bapak dan Ibu serta keluarga tercinta yang telah memberikan semangat dan dukungan sehingga Tugas Akhir ini dapat diselesaikan.
5. Bapak Ratno Kustiawan S.Kom dan Bapak Kamarudin S.Kom yang telah banyak mengajari dan memberikan pengalaman pemrograman.

- 
6. Bapak Andi Sunyoto, M.Kom dan Bapak Drs. Asro Nasiri M.Kom yang telah memberikan kesempatan belajar dan menimba pengalaman di Innovation Center Amikom.
  7. Segenap karyawan dan kawan-kawan programmer Innovation Center Amikom: Septi, Iwak, Bontet, Didi, OmDjin, Ronald, Aji, Irwan, Sa'adi, Mas Puguh, Mbak Ari, Fendi, Ferry, Donni dan yang lainnya yang tidak bisa saya sebutkan semua. Terima kasih atas doa dan dukungannya.
  8. Seluruh teman-teman spesial D3TI-02.
  9. Dan semua pihak yang telah membantu menyelesaikan Tugas Akhir ini baik secara langsung maupun tidak langsung.

Akhir kata, semoga Tugas Akhir ini dapat memberikan banyak manfaat kepada siapa saja yang membutuhkan.

Yogyakarta, 28 Desember 2012

Bram Pratowo

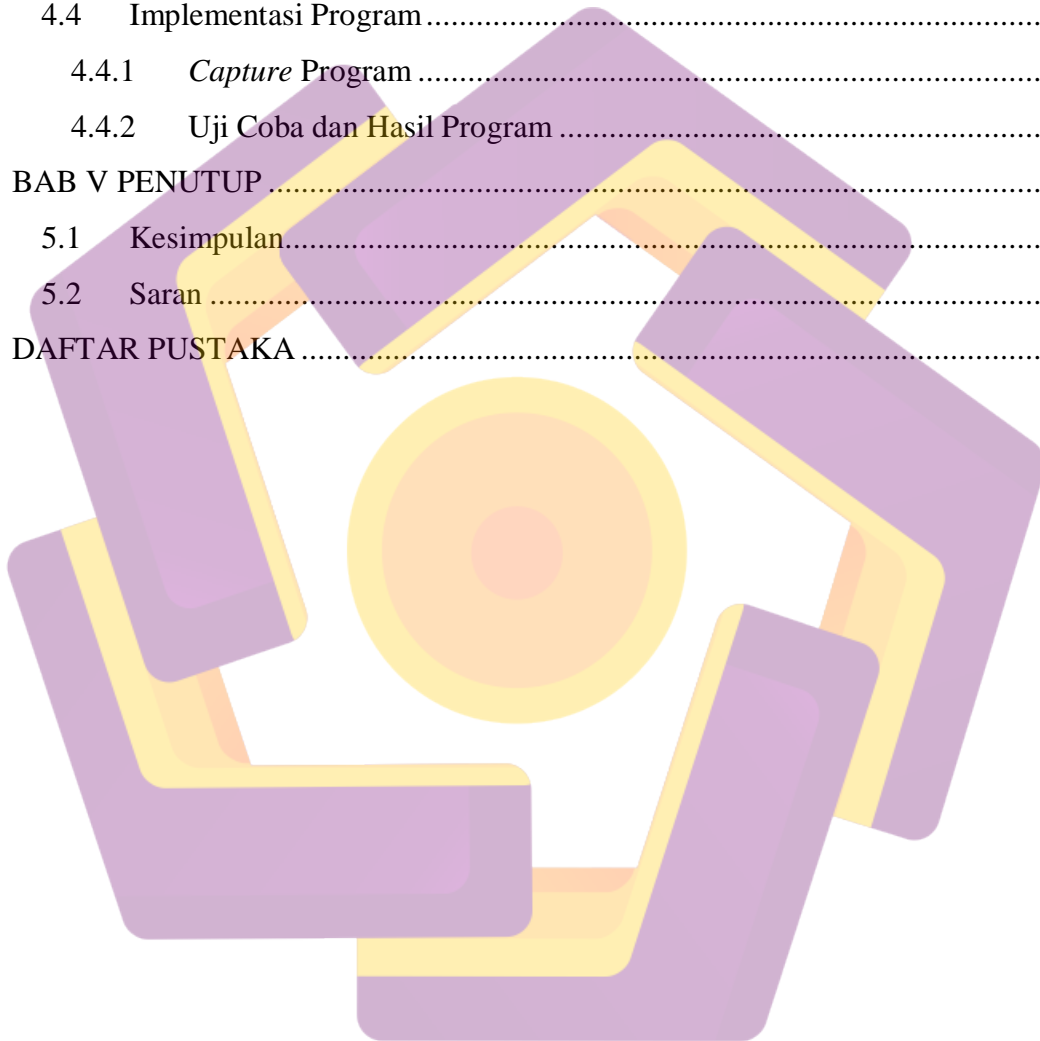
## DAFTAR ISI

JUDUL .....	i
LEMBAR PERSETUJUAN.....	ii
LEMBAR PENGESAHAN.....	iii
PERNYATAAN .....	iv
MOTTO DAN PERSEMBAHAN.....	v
KATA PENGANTAR .....	vi
DAFTAR ISI .....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL .....	xiii
INTISARI.....	xiv
ABSTRACT .....	xv
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	3
1.6 Metode Penelitian .....	4
1.7 Sistematika Penulisan .....	5
1.8 Rencana Kegiatan .....	7
BAB II LANDASAN TEORI .....	8
2.1 Kriptografi.....	8
2.1.1 Terminologi Kriptografi.....	8
2.1.2 Sejarah Kriptografi .....	8
2.1.3 Algoritma kriptografi.....	9
2.1.4 <i>Advanced Encryption Standard</i> .....	11
2.2 Steganografi.....	16



2.2.1	Terminologi Steganografi .....	16
2.2.2	Sejarah Steganografi .....	16
2.2.3	Teknik Steganografi.....	17
2.2.4	<i>Low Bit Coding</i> .....	21
2.3	Lingkungan Bahasa Pemrograman Microsoft Visual C# .....	22
2.3.1	Arsitektur .Net dan .Net <i>Framework</i> .....	23
2.4	<i>Unified Modelling Language</i> .....	27
2.4.1	<i>Use Case Diagram</i> .....	28
2.4.2	<i>Activity Diagram</i> .....	29
2.4.3	<i>Class Diagram</i> .....	29
2.4.4	<i>Sequence Diagram</i> .....	30
<b>BAB III GAMBARAN UMUM</b> .....		31
3.1	Gambaran Umum Perangkat Lunak .....	31
3.2	Alur Kerja Sistem .....	32
3.2.1	Proses <i>Embedding</i> .....	32
3.2.2	Proses <i>Extraction</i> .....	33
3.3	Fitur Perangkat Lunak.....	33
<b>BAB IV PEMBAHASAN</b> .....		36
4.1	Perancangan Sistem .....	36
4.1.1	Perancangan <i>Flowchart Program</i> .....	36
4.1.2	Perancangan <i>Unified Modelling Language</i> .....	39
4.2	Perancangan Desain Antarmuka.....	51
4.2.1	Desain Form <i>Option</i> .....	51
4.2.2	Desain Form Proses <i>Embedding</i> .....	51
4.2.3	Desain Form Proses <i>Extraction</i> .....	52
4.2.4	Desain Form Pengaturan Algoritma AES .....	53
4.3	Perancangan Kode Program .....	53
4.3.1	Algoritma Fungsi Enkripsi AES.....	53

4.3.2	Algoritma Fungsi Dekripsi AES .....	55
4.3.3	Algoritma Fungsi <i>Embedding</i> .....	56
4.3.4	Algoritma Fungsi <i>Extraction</i> .....	61
4.3.5	Angka Toleransi dan Basis Kelipatan.....	65
4.4	Implementasi Program .....	67
4.4.1	<i>Capture</i> Program .....	68
4.4.2	Uji Coba dan Hasil Program .....	71
BAB V PENUTUP .....		79
5.1	Kesimpulan.....	79
5.2	Saran .....	80
DAFTAR PUSTAKA .....		81



## DAFTAR GAMBAR

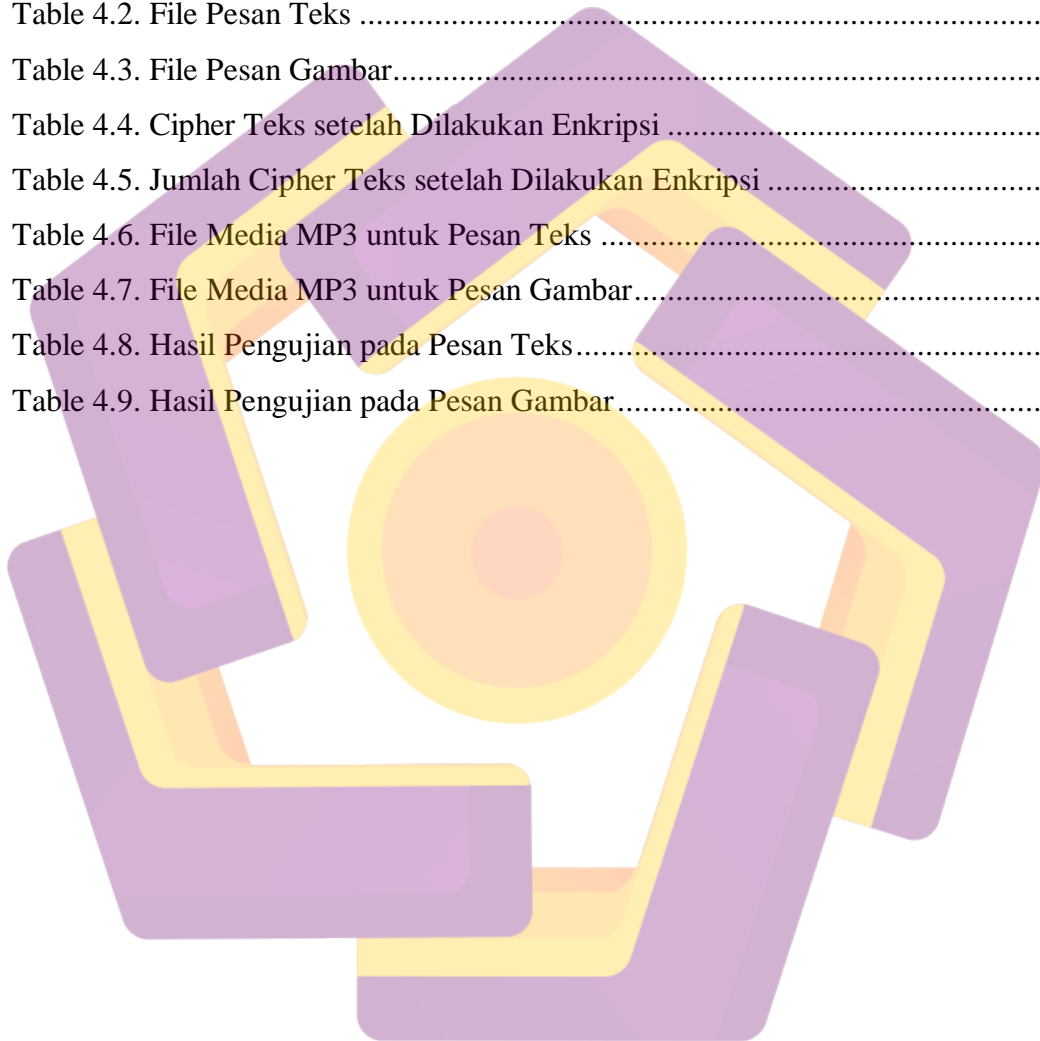
Gambar 2.1. S-Box .....	13
Gambar 2.2. Fungsi ShiftRows() .....	14
Gambar 2.3. MixColumn() .....	14
Gambar 2.4. AddRoundKey() .....	15
Gambar 2.5. Satu putaran algoritma AES .....	15
Gambar 2.6. Proses <i>Embedding</i> .....	20
Gambar 2.7. Proses Ekstraksi .....	20
Gambar 2.8. Representasi bit .....	21
Gambar 2.9. Common Language Runtime .....	23
Gambar 2.10. MSIL .....	24
Gambar 2.11. .Net Framework .....	27
Gambar 2.12. Use Case Diagram .....	28
Gambar 2.13. Activity Diagram .....	29
Gambar 2.14. Class Diagram .....	30
Gambar 2.15. Sequence Diagram .....	30
Gambar 3.1. Alur proses <i>embedding</i> .....	32
Gambar 3.2. Alur proses <i>extraction</i> .....	33
Gambar 4.1. Flowchart Embedding Data .....	37
Gambar 4.2. Flowchart Extraction Data .....	39
Gambar 4.3. Usecase Embedding Data .....	41
Gambar 4.4. Usecase Extraction Data .....	41
Gambar 4.5. Activity Diagram Pengaturan Algoritma AES .....	42
Gambar 4.6. Activity Diagram Embedding Data .....	43
Gambar 4.7. Activity Diagram Extraction Data .....	44
Gambar 4.8. Class Diagram .....	45
Gambar 4.9. Sequence Diagram Pengaturan Algoritma AES .....	48
Gambar 4.10. Sequence Diagram Embedding Data .....	49

Gambar 4.11. Sequence Diagram Extraction Data.....	50
Gambar 4.12. Desain Form Option.....	51
Gambar 4.13. Desain Form Embedding Data .....	52
Gambar 4.14. Desain Form Extraction .....	52
Gambar 4.15. Form Pengaturan Algoritma AES.....	53
Gambar 4.16. Form Option .....	68
Gambar 4.17. Proses Embedding .....	68
Gambar 4.18. Proses Embedding Berhasil.....	69
Gambar 4.19. Proses Extraction .....	69
Gambar 4.20. Proses Extraction Berhasil .....	70
Gambar 4.21. Form Pengaturan Algoritma AES.....	70



## DAFTAR TABEL

Table 1.1. Rencana Kegiatan.....	7
Table 2.1. Parameter AES .....	12
Table 4.1. Data Pengujian Enkripsi File Pesan .....	66
Table 4.2. File Pesan Teks .....	71
Table 4.3. File Pesan Gambar.....	72
Table 4.4. Cipher Teks setelah Dilakukan Enkripsi .....	73
Table 4.5. Jumlah Cipher Teks setelah Dilakukan Enkripsi .....	74
Table 4.6. File Media MP3 untuk Pesan Teks .....	75
Table 4.7. File Media MP3 untuk Pesan Gambar.....	76
Table 4.8. Hasil Pengujian pada Pesan Teks.....	76
Table 4.9. Hasil Pengujian pada Pesan Gambar.....	77



## INTISARI

Terdapat dua teknik yang biasanya digunakan untuk mengamankan pesan, yaitu kriptografi dan steganografi. Kriptografi digunakan untuk mengacak pesan (enkripsi), sehingga pihak lain yang tidak memiliki kepentingan tidak bisa membaca pesan tersebut tanpa kata kunci. Sementara steganografi digunakan untuk menyembunyikan pesan pada sebuah media lain.

Kriptografi pada aplikasi ini menggunakan metode Advanced Encryption Standard (AES) dengan variasi panjang kunci sebesar 128 bit, 192 bit, dan 256 bit. Kemudian untuk steganografi menggunakan metode Low Bit Coding yaitu penyisipan bit-bit pesan ke dalam bit-bit paling tidak signifikan dari media penampung.

Pembuatan aplikasi ini menggabungkan metode kriptografi dan steganografi, dengan cara pesan dilakukan pengacakan menggunakan algoritma AES, dan kemudian bit-bit pesan yang telah terenkripsi tersebut disisipkan ke dalam bit-bit media penampung.

**Kata Kunci:** kriptografi, steganografi, advanced encryption standard, low-bit coding



## ABSTRACT

There are two techniques that are commonly used to secure messages, the cryptography and steganography. Cryptography is used to scramble the message (encryption), so that the other party that has no interest in it, they can not read the message without the password. While steganography is used to hide a message in a different medium.

Cryptography in this application using the Advanced Encryption Standard (AES) with a key length variation at 128 bits, 192 bits, and 256 bits. Then for steganography use Low Bit Coding method, that insert of bits message into the bits of least significant of the media reservoir.

Making this application combines cryptography and steganography method, by way of a message encryption using AES algorithm, and then the bits that have been encrypted message is inserted into the receptacle media bits.

**Keywords:** cryptography, steganography, advanced encryption standard, low-bit coding

