

**APLIKASI KRIPTOGRAFI SUARA MENGGUNAKAN
ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES)**



SKRIPSI

**Disusun Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer
Pada Jurusan Ilmu Komputer/ Informatika**

**Disusun Oleh:
RISWAN SAPUTRA
J2F009073**

**JURUSAN ILMU KOMPUTER/ INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO**

2014

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Riswan Saputra

NIM : J2F009073

Judul : Aplikasi Kriptografi Suara Menggunakan Algoritma *Advanced Encryption Standard* (AES)

Dengan ini saya menyatakan bahwa dalam tugas akhir/ skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Semarang, September 2014



Riswan Saputra
J2F009073

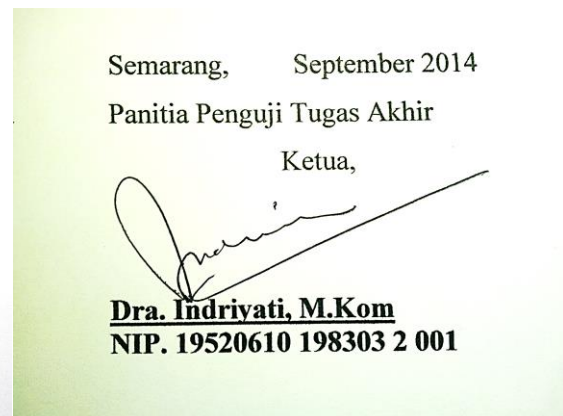
HALAMAN PENGESAHAN

Judul : Aplikasi Kriptografi Suara menggunakan Algoritma *Advanced Encryption Standard* (AES)

Nama : Riswan Saputra

NIM : J2F009073

Telah diujikan pada sidang tugas akhir pada tanggal 12 September 2014 dan dinyatakan lulus pada tanggal 19 September 2014




HALAMAN PENGESAHAN


Judul : Aplikasi Kriptografi Suara menggunakan Algoritma *Advanced Encryption Standard* (AES)

Nama : Riswan Saputra

NIM : J2F009073

Telah diujikan pada sidang tugas akhir pada tanggal 12 September 2014

Pembimbing Utama,

Sukmawati Nur Endah, S.Si M.Kom
NIP. 19780502 200501 2 002

Semarang, September 2014
Pembimbing Anggota,

Ragil Saputra, S.Si, M.Cs
NIP. 19801021 200501 1 003

ABSTRAK

Komunikasi berupa pesan suara menjadi salah satu cara alternatif untuk saling berbagi informasi. Masalah yang dihadapi saat melakukan pengiriman informasi adalah integritas data pesan suara mungkin berubah pada penerima. Salah satu solusi untuk meningkatkan keamanan pesan suara adalah dengan melakukan enkripsi. Enkripsi merupakan teknik kriptografi untuk mengubah pesan suara asli menjadi pesan suara terenkripsi untuk menyembunyikan informasi di dalam pesan tersebut. Aplikasi kriptografi suara yang dikembangkan menggunakan algoritma *Advanced Encryption Standard* (AES). Algoritma AES merupakan algoritma enkripsi yang memiliki variasi panjang kunci yang beragam yaitu 128 Bit, 192 Bit dan 256 Bit. Pesan suara yang dienkripsi dalam algoritma AES melewati empat tahap dalam satu putarannya yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey*. Aplikasi kriptografi suara menggunakan algoritma AES menghasilkan pesan suara terenkripsi sehingga menghasilkan pesan suara yang "tidak bernilai" informasi apapun. Pesan suara terenkripsi didekripsi untuk mendapatkan pesan asli kembali.

Kata Kunci : Teknik Kriptografi, *Advanced Encryption Standard* (AES), Enkripsi, Dekripsi

ABSTRACT

Communication in the form of voice message became one of the alternative ways to share information. The problem faced when sending information was voice message data integrity might change at receiver. One of the solutions to improve the security of voice messages was by using encryption. Encryption was a cryptographic technique to change the original voice message into encrypted voice message to hide information in the message. The application was developed using Advanced Encryption Standard (AES) was an encryption algorithm which had key length variations diverse: 128 Bit, 192Bit and 256 Bit. Voice message encrypted in AES algorithm passed through four stages in a single rotation, namely SubBytes, ShiftRows, MixColumns and AddRoundKey. AES cryptographic applications produced voice message which had encrypted, produced voice message which was "not worth" any information. Encrypted voice message was decrypted to get the original message back.

Keywords : Cryptographic Technique, Advanced Encryption Standard (AES), Encrypted, Decrypted

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah S.W.T yang telah melimpahkan rezeki, nikmat dan karunia-Nya sehingga penulis dapat menyelesaikan laporan Tugas akhir yang berjudul “Aplikasi Kriptografi Suara Menggunakan Algoritma *Advanced Encryption Standard* (AES)” dengan baik dan lancar. Laporan Tugas Akhir ini disusun untuk memenuhi syarat gelar Sarjana Strata 1 (S1) pada Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro Semarang.

Sebagai pelaksanaan penyusunan Laporan Tugas Akhir ini, penulis banyak mendapat bimbingan, arahan, dan bantuan dari berbagai pihak. Oleh karena itu dengan segala kerendahan hati, penulis ingin mengucapkan terima kasih dengan tulus kepada :

1. Dr. Muhammad Nur, DEA, selaku Dekan FSM UNDIP
2. Nurdin Bahtiar, S.Si, M. T, selaku Ketua Jurusan Ilmu Komputer / Informatika
3. Indra Waspada, S. T, M.TI, selaku Koordinator Tugas Akhir
4. Sukmawati Nur Endah, S.Si, M.Kom, selaku dosen pembimbing I
5. Ragil Saputra, S.Si, M.Cs, selaku dosen pembimbing II

Penulis menyadari bahwa masih banyak kekurangan dalam penyusunan laporan tugas akhir ini, baik dalam segi materi maupun penyampaian materi. Hal ini dikarenakan keterbatasan pengetahuan dan kemampuan penulis. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun demi kesempurnaan Tugas Akhir ini. Semoga laporan Tugas Akhir ini bermanfaat bagi penulis dan juga pembaca.

Semarang, September 2014

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PENGESAHAN	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xiii
LAMPIRAN	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan dan Manfaat	3
1.4 Ruang Lingkup.....	3
1.5 Sistematika Penulisan	4
BAB II LANDASAN TEORI	5
2.1 Suara Digital/ Audio	5
2.2 Definisi Kriptografi.....	7
2.3 <i>Mode Operasi Chaining Block Cipher</i>	9
2.4 <i>Algoritma Advanced Encryption Standard</i>	11
2.5 <i>Transformasi Advanced Encryption Standard</i>	12
2.5.1 <i>Proses Enkripsi Advanced Encryption Standard</i>	12

2.5.2	Proses Dekripsi <i>Advanced Encryption Standard</i>	17
2.6	Penjadwalan Kunci (<i>Key Schedule</i>)	19
2.7	<i>Unified Modeling Language</i>	21
2.7.1	<i>Use Case Diagram</i>	22
2.7.2	<i>Class diagram</i>	23
2.7.3	<i>Sequence diagram</i>	26
2.7.4	<i>Activity Diagram</i>	27
2.8	Model Proses <i>Unified Process</i>	28
2.9	Bahasa Pemrograman <i>C Sharp/ C#</i>	30
BAB III <i>INCEPTION DAN ELABORATION</i>		32
3.1	Fase <i>Inception</i>	32
3.1.1	Deskripsi Sistem	32
3.1.2	Kebutuhan Non-fungsional	38
3.1.3	Model <i>Use Case</i>	38
3.2	Fase <i>Elaboration</i>	43
3.2.1	Perancangan Arsitektur Sistem	43
3.2.2	Perancangan Alur Proses Enkripsi dan Dekripsi	48
3.2.3	Perancangan Antarmuka dan Pengujian.....	69
BAB IV <i>CONSTRUCTION DAN TRANSITION</i>		75
4.1	Fase <i>Construction</i>	75
4.1.1.	Implementasi Sistem	75
4.1.2.	Implementasi Objek	75
4.1.3.	Implementasi Antarmuka	84
4.2	Fase <i>Transition</i>	87
4.2.1.	Pengujian Perekaman Suara	87
4.2.2.	Pengujian Enkripsi dan Dekripsi.....	89
BAB V PENUTUP		92

5.1 Kesimpulan	92
5.2 Saran	92
DAFTAR PUSTAKA.....	93
LAMPIRAN	95

DAFTAR GAMBAR

Gambar 2. 1	Struktur format <i>Waveform</i>	6
Gambar 2. 2	Proses Enkripsi.....	8
Gambar 2. 3	Proses Dekripsi	8
Gambar 2. 4	Proses Mode Operasi CBC.	11
Gambar 2. 5	Proses <i>SubBytes</i>	13
Gambar 2. 6	Proses <i>ShiftRows</i>	15
Gambar 2. 7	Proses <i>MixColumns</i>	16
Gambar 2. 8	Operasi perkalian dan penjumlahan.....	16
Gambar 2. 9	Proses <i>AddRoundKey</i>	17
Gambar 2. 10	Matriks Pengali pada tahap <i>InvMixColumns</i>	19
Gambar 2. 11	Contoh <i>Use Case Diagram</i>	22
Gambar 2. 12	Contoh Sebuah <i>Class</i>	24
Gambar 2. 13	Contoh Sebuah Objek	24
Gambar 2. 14	Contoh <i>Class diagram</i>	25
Gambar 2. 15	Contoh <i>Sequence diagram</i>	27
Gambar 2. 16	Contoh <i>Activity Diagram</i>	28
Gambar 2. 17	Fase-fase dalam <i>Unified Process</i>	30
Gambar 3. 1	Alur Proses Kriptografi Suara.....	32
Gambar 3. 2	Alur Kerja Proses Enkripsi	34
Gambar 3. 3	Alur Kerja Proses Dekripsi	36
Gambar 3. 4	<i>Use Case Diagram</i>	40
Gambar 3. 5	<i>Class diagram</i> Aplikasi Kriptografi Suara	44
Gambar 3. 6	<i>Sequence diagram</i> Merekam Suara	45
Gambar 3. 7	<i>Sequence diagram</i> Melakukan Enkripsi	45
Gambar 3. 8	<i>Sequence diagram</i> Mengambil <i>File</i> Suara.....	46
Gambar 3. 9	<i>Sequence diagram</i> Melakukan Dekripsi	46
Gambar 3. 10	<i>Activity Diagram</i> Enkripsi	47
Gambar 3. 11	<i>Activity Diagram</i> Dekripsi	47
Gambar 3. 12	<i>Flowchart</i> Proses Enkripsi AES	48
Gambar 3. 13	<i>Flowchart</i> Proses Dekripsi.....	49

Gambar 3. 14	<i>Flowchart</i> Proses Perekaman Suara.....	50
Gambar 3. 15	<i>Flowchart</i> Pengambilan Data Suara	51
Gambar 3. 16	<i>Flowchart</i> Proses Penjadwalan Kunci	52
Gambar 3. 17	<i>Flowchart</i> Enkripsi AES menggunakan Mode operasi CBC	56
Gambar 3. 18	Proses Pergeseran pada tahap <i>ShiftRows</i>	59
Gambar 3. 19	Perkalian <i>State Plaintext</i> dengan <i>State</i> Polinomial Tetap.....	60
Gambar 3. 20	Proses Perkalian <i>MixColumns</i>	60
Gambar 3. 21	Proses XOR <i>AddRoundKey</i>	61
Gambar 3. 22	<i>Flowchart</i> Dekripsi AES menggunakan Mode operasi CBC	63
Gambar 3. 23	Perkalian <i>state</i> data suara dengan <i>state</i> polinomial tetap.....	65
Gambar 3. 24	Proses Perkalian <i>InvMixColumns</i>	65
Gambar 3. 25	Proses XOR <i>AddRoundKey</i>	66
Gambar 3. 26	Proses <i>Shift Right</i> pada tahap <i>InvShiftRows</i>	68
Gambar 3. 27	Desain Antarmuka Pada Layar Pengirim.....	70
Gambar 3.28	Desain Antarmuka Pada Layar Penerima	70
Gambar 3. 29	Desain Antarmuka Menu Bantuan Melakukan Perekaman	70
Gambar 3. 30	Desain Antarmuka Menu Bantuan Melakukan Enkripsi	71
Gambar 3. 31	Desain Antarmuka Menu Bantuan Melakukan Dekripsi	71
Gambar 3. 32	Desain Antarmuka Menu Bantuan Tentang Aplikasi	72
Gambar 4. 1	Implementasi Antarmuka Pada Layar Pengirim.....	85
Gambar 4. 2	Implementasi Antarmuka Pada Layar Penerima.....	85
Gambar 4. 3	Menu Bantuan Langkah Perekaman Suara	85
Gambar 4. 4	Menu Bantuan Langkah Enkripsi	86
Gambar 4. 5	Menu Bantuan Langkah Dekripsi	86
Gambar 4. 6	Menu Tentang Aplikasi.....	87
Gambar 4. 7	Implementasi Perekam Suara.....	88
Gambar 4. 8	Implementasi Proses Perekaman Suara	88
Gambar 4. 9	Implementasi Proses Penyelesaian Perekaman.....	89

DAFTAR TABEL

Tabel 2. 1	Jumlah Proses Berdasarkan Bit Blok dan Kunci.....	11
Tabel 2. 2	Tabel Substitusi Box	13
Tabel 2. 3	Tabel Invers Substitusi Box	18
Tabel 2. 4	Tabel Nilai Konstan RC dalam Heksadesimal	20
Tabel 2. 5	Tabel Komponen <i>Class diagram</i>	24
Tabel 2. 6	Representasi Angka pada Multiplicity	25
Tabel 3. 1	Tabel Daftar Aktor	39
Tabel 3. 2	Tabel Daftar <i>Use Case</i> Pengirim.....	39
Tabel 3. 3	Tabel Daftar <i>Use Case</i> Penerima	39
Tabel 3. 4	Tabel Detail <i>Use Case</i> Merekam Suara	41
Tabel 3. 5	Tabel Detail <i>Use Case</i> Melakukan Enkripsi	42
Tabel 3. 6	Tabel Detail <i>Use Case</i> Mengambil <i>File</i> Suara.....	42
Tabel 3. 7	Tabel Detail <i>Use Case</i> Melakukan Dekripsi	43
Tabel 3. 8	Tabel Operasi Penjadwalan Kunci	55
Tabel 3. 9	Tabel Substitusi <i>SubBytes</i>	58
Tabel 3. 10	Tabel Proses Substitusi <i>InvSubBytes</i>	67
Tabel 3. 11	Rencana Pengujian Aplikasi Kriptografi Suara	73
Tabel 4. 1	Tabel Implementasi <i>Class</i> Aplikasi Kriptografi Suara	76
Tabel 4. 2	Tabel Implementasi Atribut <i>Class</i> FormUtama	76
Tabel 4. 3	Tabel Implementasi Operasi <i>Class</i> FormUtama	77
Tabel 4. 4	Tabel Implementasi Atribut <i>Class</i> AESLib	78
Tabel 4. 5	Tabel Implementasi Operasi <i>Class</i> AESLib.....	79
Tabel 4. 6	Tabel Implementasi Atribut <i>Class</i> Enkripsi	80
Tabel 4. 7	Tabel Implementasi Operasi <i>Class</i> Enkripsi	81
Tabel 4. 8	Tabel Implementasi Atribut <i>Class</i> Dekripsi.....	82
Tabel 4. 9	Tabel Implementasi Operasi <i>Class</i> Dekripsi.....	83
Tabel 4. 10	Tabel Implementasi Atribut <i>Class</i> Suara	83
Tabel 4. 11	Tabel Implementasi Operasi <i>Class</i> Suara.....	83
Tabel 4. 12	Tabel <i>File</i> Suara dengan Kata Kunci dan <i>initial vector</i>	90

Tabel 4. 13	Paduan Kata Kunci dan <i>initial vector</i> Untuk Skenario Abnormal	90
Tabel 4. 14	Pengujian Berdasarkan Skenario Normal Dengan Sampel A	96
Tabel 4. 15	Pengujian Berdasarkan Skenario Normal Dengan Sampel B	97
Tabel 4. 16	Pengujian Berdasarkan Skenario Abnormal Dengan Sampel A	98
Tabel 4. 17	Pengujian Berdasarkan Skenario Abnormal Dengan Sampel B	99
Tabel 4. 18	Pengujian Berdasarkan Ukuran <i>File</i> Suara Dengan Sampel A	100
Tabel 4. 19	Pengujian Berdasarkan Ukuran <i>File</i> Suara Dengan Sampel B	101

LAMPIRAN

Lampiran 1 : Dokumentasi Pengujian Black Box	96
Lampiran 2 : Implementasi Kode Aplikasi Kriptografi Suara	102

BAB I

PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup dan sistematika penulisan penelitian tugas akhir mengenai Aplikasi Kriptografi Suara Menggunakan Algoritma AES.

1.1 Latar Belakang

Pemakaian teknologi komputer sebagai salah satu aplikasi dari teknologi informasi sudah menjadi suatu kebutuhan. Informasi yang tersedia di internet semakin berkembang dan semakin beragam jenisnya. Banyaknya informasi yang tersedia memudahkan seseorang dalam menyelesaikan pekerjaan. Informasi dapat disampaikan melalui teks, citra, suara, dan lain-lain (Gadanayak, et al., 2011a). Informasi suara bisa terdapat di *voice blog*, percakapan telepon, dan lain-lain.

Suara adalah fenomena fisik yang dihasilkan oleh getaran benda. Getaran suatu benda tersebut berupa sinyal analog dengan amplitudo yang berubah secara kontinu terhadap waktu. Untuk melakukan manipulasi suara, suara dalam bentuk sinyal analog terlebih dahulu diubah menjadi sinyal digital. Komputer hanya mampu mengenal sinyal dalam bentuk digital yang merupakan tegangan yang diterjemahkan dalam angka nol dan satu bit. (Vaughan, 2011)

Secara umum, pengguna lebih suka memanipulasi suara digital/audio dengan berbagai cara seperti dikompresi untuk mengurangi *file* ataupun mengubah format audio. Namun, dalam proses manipulasi suara tersebut tidak dapat mengamankan pesan yang terdapat dalam suara.

Di bidang telekomunikasi, percakapan *user* satu dengan yang lainnya merupakan hal yang rahasia. Saat seseorang melakukan percakapan melalui telepon, dapat dimungkinkan terjadi penyadapan oleh orang lain atau pihak ketiga yang menginginkan informasi dari apa yang orang tersebut bicarakan. Jika percakapan tersebut merupakan hal yang penting, misal dalam bidang militer maupun pemerintahan, maka informasi tersebut tidak boleh diketahui oleh publik (Yuniati, et al., 2009). Oleh karena itu, diperlukan adanya pengamanan saat terjadinya percakapan. Pengamanan pada

percakapan tersebut merupakan penjagaan informasi agar nilai atau integritas informasi tetap terjaga. Salah satu teknik keamanan data suara adalah dengan kriptografi.

Kriptografi (*cryptography*) berasal dari bahasa Yunani : “*cryptos*” artinya “*secret*” (rahasia) dan “*graphein*” artinya “*writing*” (tulisan). Jadi, kriptografi berarti “*secret writing*” (tulisan rahasia). Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat di mengerti lagi maknanya. Namun saat ini kriptografi lebih dari sekedar *privacy*, tetapi juga untuk tujuan data *integrity*, *authentication*, dan *non-repudiation* (Munir, 2006). Menurut Menezes dalam bukunya yang berjudul “*Handbook of Applied Cryptography*”, Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (Menezes, et al., 1996).

Berdasarkan jenis kunci yang digunakan, kriptografi dibagi menjadi dua, yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi. Sedangkan algoritma asimetris, menggunakan kunci publik (*public key*) untuk enkripsi dan kunci privat (*private key*) untuk dekripsi. Ada beberapa jenis algoritma simetris antara lain, *Data Encryption Standard* (DES), RC2, RC4, RC5, RC6, *Advanced Encryption Standard* (AES), *One Time pad* (OTP) dan lain-lain.

Algoritma *Advanced Encryption Standard* (AES) atau Rijndael merupakan algoritma simetri yang sangat cocok dipakai untuk berbagai keperluan yang berkaitan dengan kriptografi saat ini (Sadikin, 2012). AES memiliki 4 proses dasar dalam melakukan enkripsi maupun dekripsi, yaitu melakukan substitusi, pergeseran baris, mengacak data dan melakukan operasi XOR. Algoritma AES memiliki kelebihan pada panjang blok dan struktur *round* (putaran) yang sangat rumit (Yudistira, 2011). Selain untuk mengenkripsi citra, algoritma AES juga dapat diimplementasikan pada suara. Gadanayak menjelaskan pada jurnalnya yang berjudul *Comparative Study of Different Encryption Techniques on MP3 Compression*, teknik enkripsi AES yang diimplementasi pada *file* audio memerlukan waktu yang sedikit pada saat pemrosesan, dengan mendegradasi sinyal yang tidak dapat didengar oleh pengguna yang tidak sah (Gadanayak, et al., 2011b). Proses algoritma AES yang terjadi pada objek suara tidak jauh berbeda dengan citra. Berdasarkan penelitian, perbedaan terjadi pada objek suara

yang berbentuk *stream* diubah ke dalam bentuk *byte*, kemudian memasukkannya ke blok-blok untuk dienkripsi (Shirley, 2011).

Pada Tugas Akhir ini diteliti tentang bagaimana teknik kriptografi suara diimplementasikan menggunakan algoritma AES.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dapat dirumuskan permasalahan yang dihadapi adalah bagaimana membuat suatu aplikasi kriptografi suara menggunakan algoritma AES.

1.3 Tujuan dan Manfaat

Tujuan yang ingin dicapai dalam penelitian tugas akhir ini adalah menghasilkan aplikasi kriptografi suara menggunakan algoritma AES.

Manfaat dari penelitian tugas akhir ini adalah :

1. Meningkatkan keamanan dan mempertahankan integritas data suara agar tetap terjaga.
2. Membantu dalam mengembangkan aplikasi kriptografi yang berkaitan dengan bidang keamanan data, khususnya berbasis *file* suara.

1.4 Ruang Lingkup

Ruang lingkup aplikasi kriptografi suara menggunakan algoritma AES adalah :

1. *Input* proses enkripsi berupa *file* suara digital/audio (*.wav) dan *output* berupa *file* suara digital/audio (*.wav) secara *offline*
2. Panjang *Initial Vector* (IV) pada *mode* operasi adalah 128 bit
3. Panjang suara dibagi menjadi beberapa blok, setiap blok memiliki panjang 128 bit. Panjang blok tersebut yang dimasukkan ke dalam algoritma AES
4. *Mode* operasi yang digunakan adalah *mode Cipher Block Chaining* (CBC)
5. Sistem ini akan diimplementasikan berbasis *desktop*, dengan bahasa pemrograman C# IDE Visual Studio 2010

1.5 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi menjadi beberapa pokok bahasan, yaitu :

BAB I PENDAHULUAN

Bab ini menjelaskan tentang latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup dan sistematika penulisan penelitian tugas akhir mengenai Aplikasi Kriptografi Suara Menggunakan Algoritma *Advanced Encryption Standard*.

BAB II LANDASAN TEORI

Bab ini menjelaskan konsep-konsep yang mendukung pengembangan sistem, meliputi suara *digital*/Audio, definisi kriptografi, mode operasi, algoritma *Advanced Encryption Standard*, transformasi AES, penjadwalan kunci, model proses UML, model proses *Unified Process* dan bahasa C#.

BAB III INCEPTION DAN ELABORATION

Bab ini menyajikan tahapan proses pembangunan sistem perangkat lunak menggunakan model proses *Unified Process*. Bab ini menyajikan fase *inception* dan fase *elaboration*.

BAB IV CONSTRUCTION DAN TRANSITION

Bab ini menyajikan tahapan proses pembangunan sistem perangkat lunak menggunakan model proses *Unified Process*. Bab ini menyajikan fase *construction* dan fase *transition*.

BAB V PENUTUP

Bab ini berisi kesimpulan dari pengerjaan penelitian tugas akhir ini dan saran-saran penulis untuk pengembangan lebih lanjut dari penelitian serupa.