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

Mengetahui,
Ketua Jurusan Ilmu Komputer/ Informatika
FSM UNDIP

Nurdin Bahtiar, S.Si, MT
NIP. 19790720 200312 1 002

Semarang, September 2014
Panitia Penguji Tugas Akhir
Ketua,

Dra. Indriyati, M.Kom
NIP. 19520610 198303 2 001

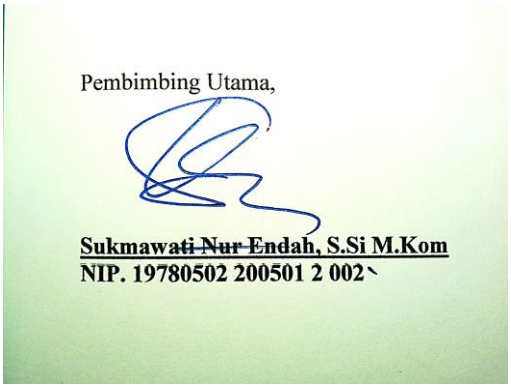
HALAMAN PENGESAHAN

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



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 meyelesaikan 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 Jurusa 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

DAFTAR GAMBAR

DAFTAR TABEL

LAMPIRAN

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 ukuran *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 Encyption 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 *mod*e 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. *Mod*e operasi yang digunakan adalah *mod*e *Cipher Block Chaining* (CBC)
5. Sistem ini akan diimplementasikan berbasis *dekstop*, 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.