

**KEAMANAN PESAN SUARA DENGAN METODE LEAST SIGNIFICANT
BIT DAN ADVANCED ENCRYPTION STANDARD**

SKRIPSI

ZAINUL FAHRUDIN BERUTU

081402005



**DEPARTEMEN STUDI TEKNOLOGI INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS SUMATERA UTARA**

MEDAN

2015

KEAMANAN PESAN SUARA DENGAN METODE LEAST SIGNIFICANT BIT
DAN ADVANCED ENCRYPTION STANDARD

SKRIPSI

Diajukan untuk melengkapi tugas dan memenuhi syarat untuk memperoleh ijazah
Sarjana Teknologi Informasi



PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS SUMATERA UTARA

MEDAN

2015

UCAPAN TERIMA KASIH

Puji dan Syukur penulis panjatkan kehadiran Tuhan Yang Maha Esa atas berkat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini sebagai syarat untuk dapat memperoleh ijazah Sarjana Teknologi Informasi, Program Studi S1 Teknologi Informasi Universitas Sumatera Utara. Ucapan terimakasih penulis sampaikan kepada:

1. Kedua orang tua dan keluarga penulis yang telah memberikan dukungan dan motivasi baik materil dan spiritual, Ayahanda Muhammad Daud Berutu dan Ibunda Juhairani Sitinjak yang selalu sabar mendidik dan membesarkan penulis.
2. Ibu Sarah Purnamawati, ST., M.Sc selaku pembimbing satu dan Bapak Baihaqi Siregar, S.Si.,M.T selaku pembimbing dua yang telah banyak meluangkan waktu dan pikirannya, memotivasi dan memberikan kritikan dan saran kepada penulis dengan sabar.
3. Ucapan terima kasih juga penulis sampaikan kepada Bapak Dr. Sawaluddin, M.IT dan Bapak Dr. Syahril Efendi, S.Si.,M.IT selaku penguji yang telah bersedia menjadi dosen pembeding penulis.
4. Ucapan terimakasih juga ditujukan kepada Ketua dan Sekretaris Program Studi Teknologi Informasi, Bapak M. Anggia Muchtar, S.T.,MM.IT. dan Bapak M. Fadly Syahputra B.Sc.,M.Sc.IT.
5. Dekan dan Wakil Dekan Fakultas Ilmu Komputer dan teknologi Informasi Universitas Sumatera Utara, semua dosen dan pegawai di Program Studi Teknologi Informasi.

6. Terima kasih kepada staf pegawai administrasi tata usaha Program Studi Teknologi Informasi, Ibu Delima Harahap dan terutama Abangda Faisal Hamid, yang telah banyak membantu penulis dalam menyelesaikan semua urusan administrasi di Program Studi Teknologi Informasi, serta telah banyak meluangkan waktu untuk bertukar pikiran.
7. Terima kasih kepada staf pegawai administrasi tata usaha Fakultas Ilmu Komputer dan Teknologi Informasi Ibu Bamelia dan Kakak Nasriatul Naumi Nasution yang telah banyak meluangkan waktu untuk bertukar pikiran dan membantu saya dalam menyelesaikan administrasi.
8. Terima kasih kepada Kakak Zubaidah Berutu. S.Pd, Abangda Muhammad Syah Berutu. ST. dan Adinda Amir Mahmud Berutu. SH, serta seseorang yang spesial Indry Waty Puspita S.Sos yang selalu memberikan dukungan dan motivasi kepada penulis.
9. Terima kasih kepada seluruh sahabat-sahabat terbaik penulis di angkatan 2008 Teknologi Informasi Universitas Sumatera Utara, yang tidak dapat saya sebutkan satu persatu.
10. Terima kasih kepada rekan dan junior penulis yang terus mendukung dan membantu penulis tanpa henti, Dimas Aditya Septian, Mirwan Hanafi, Fernando Abelta Kaban, Alex Winner Pasaribu, Sintong Tolhas Marulitua Siregar, Reza Taqyuddin, Afifudin, Wisnu Wardhana Sitorus, Patricia Margaretha, Nana Nerina Nasution, Fernando Ginting, Andre Sep Medio Sitepu, Teddy Vandia, Aser Heber Ginting, Syarief Husein Hasibuan, Muhammad Rinaldi, Ikram Hadi Muhammad Simatupang, Andrian Junaidi, Aldo Refangga Sembiring, Samuel Agusta Emri Surbakti, Yohanes Bedi Ginting, Josef Karansa, serta teman-teman lainnya yang tidak dapat saya sebutkan satu persatu.

Akhir kata, saya ucapkan terima kasih kepada semua pihak yang terkait dalam menyelesaikan skripsi ini yang tidak bisa penulis sebut satu persatu. Semoga Tuhan Yang Maha Esa memberikan berkah dan karunia kepada kita semua.

ABSTRAK

Pesan Suara terlebih termasuk dalam pesan pribadi diharapkan hanya pengirim dan penerima yang dapat mendengarkan pesan suara tersebut. Hal tersebut dimaksudkan untuk menjaga kerahasiaan pesan suara tersebut. Dalam penelitian ini, dilakukan pengaplikasian konsep dari enkripsi dan steganografi dalam pengamanan pesan suara. Digunakan Advanced Encryption Standard sebagai metode enkripsi, dan menggunakan Least Bit Significant sebagai metode steganografi. Yang mana pesan suara disisipkan ke dalam file cover WAV.

Kata Kunci : Enkripsi, Steganografi, AES, LSB, Pesan suara.

ABSTRACT

The voicemail especially included in the private message is expected that only the sender and the receiver who can listen to the voicemail. It is intended for keeping the secrecy of the message. In this research, has been done the application of the concept of encryption and steganography in the security of the voicemail. Used the Advanced Encryption Standard as the method of encryption, and using the Least Bit Significant as the method of Steganography. Which the voicemail is inserted into the file cover, WAV.

Keywords: Encryption, Steganography, AES, LBS, The Voicemail.

DAFTAR ISI

	Halaman
Persetujuan	ii
Pernyataan	iii
Ucapan Terima Kasih	iv
Abstrak	vi
Abstract	vii
Daftar Isi	viii
Daftar Tabel	xi
Daftar Gambar	xii
Bab 1 Pendahuluan	
1.1. Latar Belakang	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	3
1.7. Sistematika Penelitian	4
Bab 2 Landasan Teori	5

2.1.	Kriptografi	5
2.1.1.	Klasifikasi Kriptografi	5
2.2.	Steganografi	7
2.2.1.	Pengertian Steganografi	7
2.2.2.	Metode Steganografi	7
2.3.	Perbedaan Steganografi dengan Kriptografi	9
2.4.	Advanced Encryption Standard	9
2.4.1.	Proses Enkripsi dan Dekripsi	10
2.5.	Least Bit Significant	12
2.6.	WAV	13
2.7.	Penelitian Terdahulu	14
Bab 3	Analisis dan Perancangan Sistem	15
3.1.	Analisis Sistem	15
3.1.1.	Flowchart Enkripsi AES	15
3.1.2.	Flowchart Dekripsi AES	16
3.1.3.	Flowchart Penyisipan Pesan Audio	18
3.1.4.	Flowchart Ekstraksi Pesan Audio	19
3.2.	Analisis AES	20
3.2.1.	Enkripsi AES	20
3.2.2.	Dekripsi AES	24
3.3.	Analisis LSB	24
3.4.	Perancangan Antarmuka	25
3.4.1.	Perancangan Antarmuka Halaman Utama	25

	3.4.2. Perancangan Antarmuka Halaman Tentang	26
	3.4.3. Perancangan Antarmuka Halaman Help	27
Bab 4	Implementasi dan Pengujian Sistem	28
	4.1. Implementasi Aplikasi	28
	4.1.1. Spesifikasi Kebutuhan Perangkat Keras	28
	4.1.2. Spesifikasi Kebutuhan Perangkat Lunak	28
	4.2. Tampilan Antarmuka Aplikasi	28
	4.2.1. Tampilan Menu Utama	29
	4.3. Pengujian Aplikasi	29
	4.3.1. Pengujian Tampilan Menu Utama	29
	4.3.2. Pengujian Enkripsi dan Penyisipan	31
	4.3.3. Pengujian Dekripsi dan Ekstraksi	35
Bab 5	Kesimpulan dan Saran	39
	5.1. Kesimpulan	39
	5.2. Saran	39
	Daftar Pustaka	40
	Lampiran	41

DAFTAR TABEL

	Halaman
Tabel 2.1 Tabel Perbandingan Jumlah Putaran pada AES	10
Tabel 2.2 Tabel Penelitian Terdahulu	14
Tabel 3.1 Tabel SBox	20
Tabel 4.1 Hasil Perekaman Suara	32
Tabel 4.2 Perbandingan Setelah Enkripsi AES	32
Tabel 4.3 Hasil Proses Ekstraksi	38

DAFTAR GAMBAR

		Halaman
Gambar 2.1	Ilustrasi Enkripsi Pada AES	11
Gambar 2.2	Ilustrasi Dekripsi Pada AES	11
Gambar 2.3	Struktur Chunk Dari Format WAV	13
Gambar 3.1	Flowchart Enkripsi AES	16
Gambar 3.2	Flowchart Dekripsi AES	17
Gambar 3.3	Proses Penyisipan Pesan Audio Kedalam File Cover	18
Gambar 3.4	Flowchart Proses Ekstraksi Pesan Audio	19
Gambar 3.5	Matriks 4x4 Dari State Dan Chipper Key	21
Gambar 3.6	Visualisasi Dari Pemilihan Subbyte Dengan Nilai Pada State Adalah 32	22
Gambar 3.7	Hasil Dari State Yang Telah Disubstitusi	22
Gambar 3.8	Proses Dan Hasil Dari Proses Shiftrows	23
Gambar 3.9	Hasil Dari Proses Kedua Hingga Keenam	23
Gambar 3.10	Hasil Dari Ketujuh Hingga Kesembilan	24
Gambar 3.11	Tampilan Rancangan Halaman Utama	26
Gambar 3.12	Rancangan Antarmuka Halaman Utama	27
Gambar 3.13	Rancangan Antarmuka Halaman Help	27
Gambar 4.1	Tampilan Menu Utama Aplikasi Pengamanan Pesan Suara	29
Gambar 4.2	Tampilan Tombol	30
Gambar 4.3	Tampilan Tombol Ketika Sedang Merekam	30
Gambar 4.4	Tampilan Tombol Setelah Merekam	31
Gambar 4.5	Jendela Pemberitahuan	31
Gambar 4.6	Gambar Bentuk Gelombang Hasil Perekaman Pesan Suara	

	Dari Pengujian Empat Dan Lima	33
Gambar 4.7	Gambar Bentuk Gelombang Hasil Proses Penyisipan Pesan Suara Dari Pengujian Empat Dan Lima	34
Gambar 4.8	Gambar Dari Gabungan Bentuk Gelombang Dari Pesan Suara Pada Pengujian Empat Dan Pengujian Lima	34
Gambar 4.9	Gambar Dari Gabungan Bentuk Gelombang Dari Hasil Penyisipan Pada Pengujian Empat Dan Pengujian Lima	35
Gambar 4.10	Gambar Dari Gabungan Bentuk Gelombang Dari Hasil Penyisipan Pada Pengujian Empat Dan Pengujian Lima Dengan Bentuk Gelombang File Cover	35
Gambar 4.11	Jendela Dalam Memilih Pesan Suara Yang Akan Di Decode	36
Gambar 4.12	Tampilan Setelah Melakukan Pemilihan File Pesan	36
Gambar 4.13	Jendela Pemberitahuan Proses Ekstraksi Berhasil	37
Gambar 4.14	Hasil Cetak Bentuk Gelombang Dari Hasil Proses Ekstraksi Pada Pengujian Empat Dan Pengujian Lima	37