ENKRIPSI DAN DEKRIPSI SUARA MENGGUNAKAN METODE AES 128 BIT DENGAN *SECRET KEY*

SKRIPSI

ANGELIKA

1710511032

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2021

ENKRIPSI DAN DEKRIPSI SUARA MENGGUNAKAN METODE AES 128 BIT DENGAN SECRET KEY

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh
Gelar Sarjana Komputer

ANGELIKA

1710511032

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2021

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Angelika
NIM : 1710511032
Tanggal : 20 Juni 2021

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 20 Juni 2021
Yang Menyatakan,

(Angelika)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Angelika

NIM : 1710511032

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

ENKRIPSI DAN DEKRIPSI SUARA MENGGUNAKAN METODE AES 128 BIT DENGAN *SECRET KEY*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilih Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 20 Juni 2021

Yang Menyatakan,

(Angelika)

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Tugas Akhir berikut:

Nama : Angelika

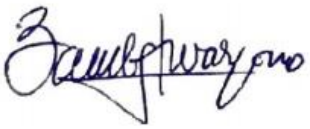
NIM : 1710511032

Program Studi : Informatika

Judul : Enkripsi dan Dekripsi Suara Menggunakan Metode AES 128 Bit Dengan *Secret Key*

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Henki Bayu Seta, S.Kom., MTI
Ketua Penguji



Bambang Tri Wahyono, S.Kom, M.Si.
Anggota Penguji

Jayanta, S.Kom., M.Si.
Pembimbing 1

Mayanda Mega Santoni, S.Kom., M.Kom.
Pembimbing 2

Dr. Ermatita, M.Kom.
Dekan

Yuni Widiastiwi, S.Kom., Msi.
Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Persetujuan : 23 Juli 2021

ENKRIPSI DAN DEKRIPSI SUARA MENGGUNAKAN METODE AES 128 BIT DENGAN *SECRET KEY*

Angelika

ABSTRAK

Pengiriman atau pertukaran data adalah hal yang sering terjadi dalam dunia teknologi informasi. Salah satu data yang biasa dilakukan pertukaran adalah suara. Suara biasanya digunakan untuk berkomunikasi. Data yang dikirim kadang seringkali berisi data yang penting bahkan sangat rahasia dan harus dijaga keamanannya. Untuk menjaga keamanan data, dapat dilakukan dengan menggunakan kriptografi. Salah satu teknik kriptografi adalah *Advanced Encryption Standard* atau biasa disebut AES. Terdapat 3 jenis AES yaitu: AES-128, AES-192 dan AES-256. Pengiriman data melalui wireless kadang terdapat *noise*, sehingga data yang dikirimkan tidak sama dengan yang diterima. Untuk mengatasi hal tersebut dapat dilakukan dengan *Forward Error Correction*(FEC) yaitu metode yang mampu mengoreksi error dari informasi yang ditransmisikan. Untuk mengenkripsi informasi dari audio pada penelitian ini ditambahkan dan di*control* oleh *Secret key* Controller dan Interleaver lain harus ditambahkan ke *output* dikendalikan oleh *Secret key* Controller. Penelitian ini bertujuan untuk melakukan kriptografi pada suara guna menjaga keamanan data dengan menggunakan teknik kriptografi *Advanced Encryption Standard* (AES) dengan dengan parameter uji yaitu waktu, ukuran file dan nilai SNRnya. Hasil pada penelitian ini didapatkan enkripsi yang baik dengan rata-rata filter sebesar 400Hz.

Kata Kunci : AES, Enkripsi Suara, Dekripsi Suara

VOICE ENCRYPTION AND DECRYPTION USING AES 128 BIT WITH SECRET KEY METHODS

Angelika

ABSTRACT

Sending or exchanging data is something that often happens in the world of information technology. One of the data that is usually exchanged is voice. Voice is usually used to communicate. The data sent sometimes often contains data that is important and even very confidential and must be kept safe. To maintain data security, it can be done using cryptography. One of the cryptographic techniques is the Advanced Encryption Standard or commonly called AES. There are 3 types of AES, namely: AES-128, AES-192 and AES-256. Sending data via wireless sometimes there is noise, so the data sent is not the same as what is received. To overcome this, it can be done with Forward Error Correction (FEC), which is a method that is able to correct errors from the transmitted information. To encrypt the information from the audio in this study added and controlled by the Secret key Controller and another Interleaver must be added to the output controlled by the Secret key Controller. This study aims to perform cryptography on voice in order to maintain data security by using the Advanced Encryption Standard (AES) cryptographic technique with test parameters namely time, file size and SNR value. The results in this study obtained good encryption with an average filter of 400Hz.

Keywords: AES, Voice Encryption, Voice Decryption.

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadirat Tuhan Yang Mahakuasa atas limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini. Skripsi ini disusun sebagai syarat Tugas Akhir Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.

Dalam penyelesaian tugas akhir ini tidak lepas dari bantuan banyak pihak yang telah memberikan masukan kepada penulis. Untuk itu penulis mengucapkan terima kasih kepada:

1. Ibu Dr. Ermatita, M.Kom., selalu dekan Fakultas Ilmu Komputer.
2. Ibu Yuni Widiastiwi, S.Kom, M.Si selaku Kepala Program Studi Sarjana Jurusan Informatika.
3. Bapak Jayanta, S.Kom., M.Si dan Ibu Mayanda Mega Santoni, S.Kom., M.Kom selaku dosen pembimbing dari pihak jurusan.
4. Orang tua penulis, Cucu Setiawati yang telah memberikan banyak dukungan melalui doa yang tidak putus-putusnya, dan pengertian atas hal-hal yang dialami oleh penulis saat proses pembuatan skripsi ini.
5. Kedua teman penulis tercinta, Tesa Lonika Siahaan dan Muhammad Rafii Deimas yang memberikan dukungan.
6. Seluruh pihak yang terlibat dalam kelancaran pembuatan skripsi ini dan yang belum disebutkan di atas, penulis ucapkan terima kasih.

Akhir kata penulis berharap agar skripsi ini dapat bermanfaat bagi semua pembaca.

Jakarta, 20 Juni 2021

Penulis

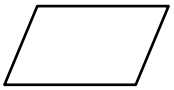
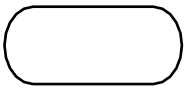
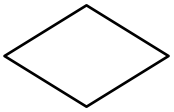
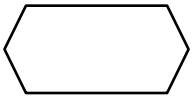
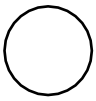
DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SIMBOL

Diagram *Flowchart*

No	Gambar	Nama	Keterangan
1		*Input / Output*	Sebagai elemen paling penting yang berhubungan dengan tujuan yaitu elemen *inputan* dan keluaran
2		*Garis Alir (Flow Line)*	Untuk menyatakan arah dalam alur program
3		*Proses*	Untuk menunjukkan proses pengolahan data pada program
4		*Terminator*	Digunakan biasanya dalam memulai proses atau program dan dapat pula mengakhirinya
5		*Decision*	Biasanya digunakan dalam kondisi percabangan atau kondisi yang membutuhkan tindak lanjut dua opsi atau keputusan.
6		*Preparation*	Berhubungan dengan penyimpanan atau data storage
7		*On Page Connector*	Untuk menyatakan penghubung antara beberapa diagram alir dalam satu halaman yang sama