

**OPTIMASI ENKRIPSI AUDIO MENGGUNAKAN ALGORITMA
PSEUDORANDOM DAN TEORI KEKACAUAN PADA PESAN SUARA**

SKRIPSI



disusun oleh

Dwitya Kurnia Widi Hastawa

16.11.0554

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019**



**OPTIMASI ENKRIPSI AUDIO MENGGUNAKAN ALGORITMA
PSEUDORANDOM DAN TEORI KEKACAUAN PADA PESAN SUARA**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Informatika



disusun oleh

Dwitya Kurnia Widi Hastawa

16.11.0554

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019**

PERSETUJUAN

SKRIPSI

OPTIMASI ENKRIPSI AUDIO MENGGUNAKAN ALGORITMA PSEUDORANDOM DAN TEORI KEKACAUAN PADA PESAN SUARA

yang dipersiapkan dan disusun oleh

Dwitya Kurnia Widi Hastawa
16.11.0554

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 5 April 2019

Dosen Pembimbing,


Dony Ariyus, M.Kom
NIK. 190302128

PENGESAHAN

SKRIPSI

OPTIMASI ENKRIPSI AUDIO MENGGUNAKAN ALGORITMA PSEUDORANDOM DAN TEORI KEKACAUAN PADA PESAN SUARA

yang dipersiapkan dan disusun oleh

Dwitya Kurnia Widi Hastawa
16.11.0554

telah dipertahankan di depan Dewan Penguji
pada tanggal 24 September 2019

Susunan Dewan Penguji

Nama Penguji

Ainul Yaqin, M.Kom
NIK. 190302255

Barka Satya, M.Kom
NIK. 190302126

Dony Ariyus, M.Kom
NIK. 190302128

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 2 Oktober 2019

DEKAN FAKULTAS ILMU KOMPUTER



Krisnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan atau diterbitkan oleh orang lain, kecuali secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka. Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Yogyakarta, 28 Agustus 2019



Dwitya Kurnia Widi H.
NIM. 16.11.0554

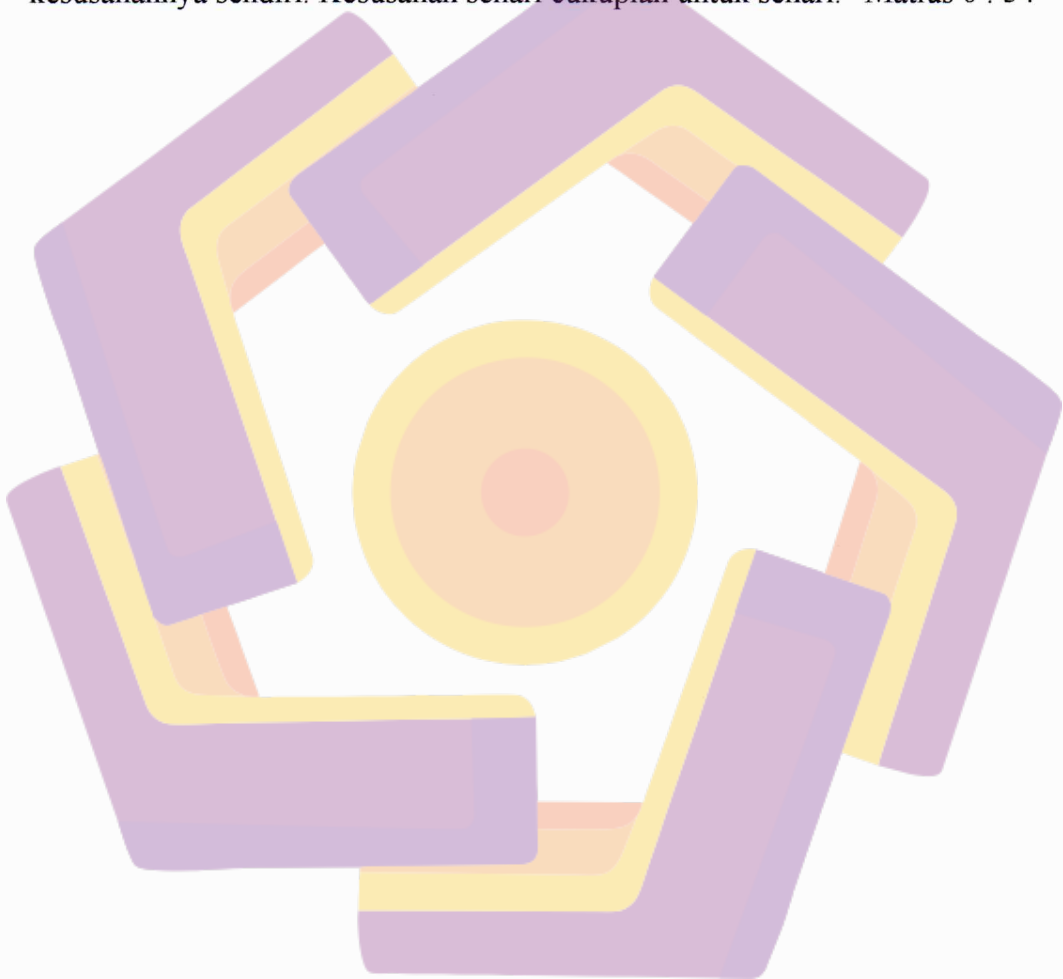
MOTTO

“Dadosa Kesaput Ratri!”

“Sarwa kadonyan wus mesthi sirna!”

“Berjalanlah waktu siang, saat hati terasa terang. Lakukanlah sebelum malam tiba.
Sebab bulan purnama tidak selalu datang menerangimu.”

“Sebab itu janganlah kamu kuatir akan hari besok, karena hari besok mempunyai kesusahannya sendiri. Kesusahan sehari cukuplah untuk sehari.” Matius 6 : 34

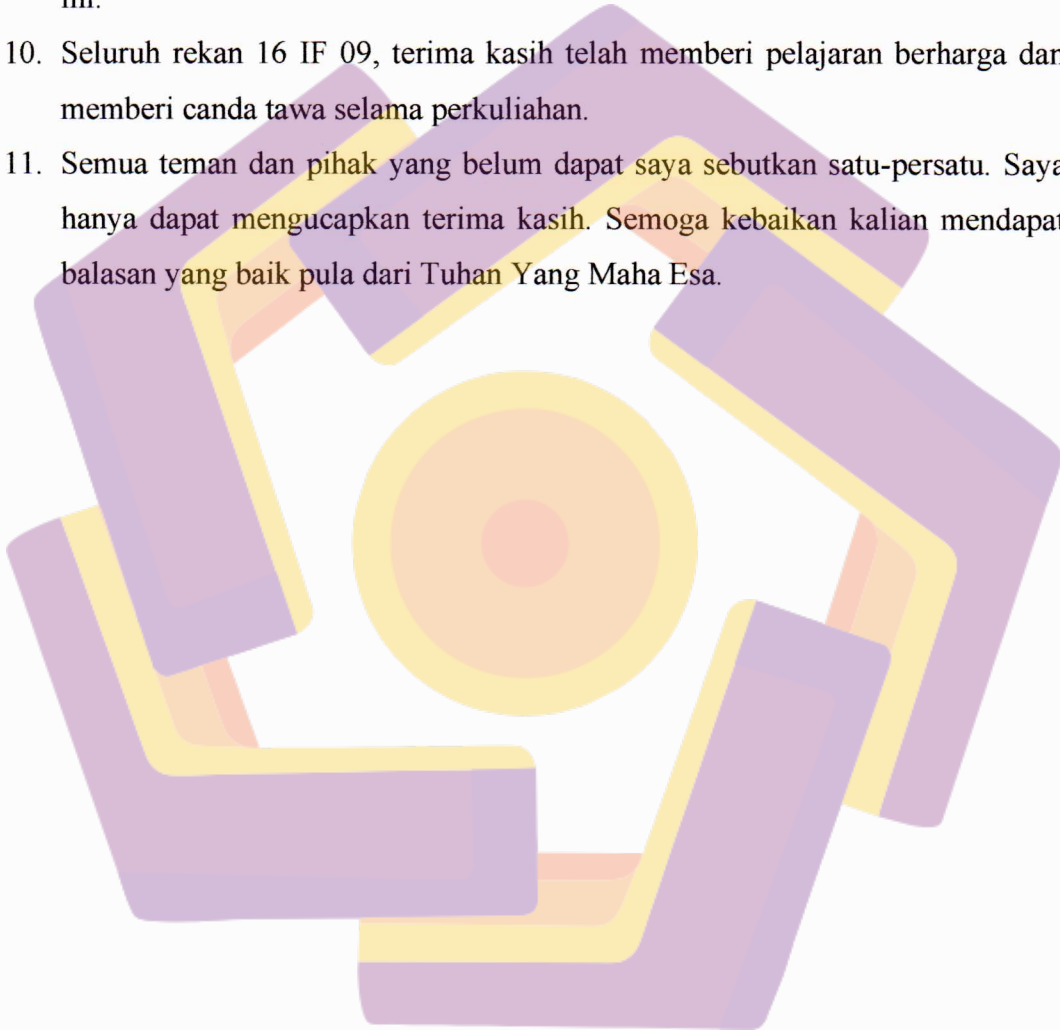


PERSEMBAHAN

Saya haturkan puji syukur kepada Tuhan Yang Maha Esa, oleh karena berkat, kasih, dan tuntunan-Nya, saya telah menyelesaikan skripsi ini dengan sebaik-baiknya. Dan pada halaman persembahan ini, saya ingin berterimakasih sebesar-besarnya kepada :

1. Kedua orang tua saya tercinta yang telah membimbing, mendidik, memberi semangat kepada saya dengan cinta kasihnya yang sangat luar biasa. Saya hanya bisa membalas dengan berusaha semaksimal mungkin untuk menyelesaikan pendidikan saya di Universitas Amikom Yogyakarta ini.
2. Kakak saya tercinta, Praditya Okta Ekanawati dan Yusmanto yang selalu memberi semangat dan mengingatkan untuk selalu menyelesaikan tugas. Hal itu yang membantu saya untuk lebih bersemangat menyelesaikan skripsi ini.
3. Sahabat saya, Faham Wicaksono, yang selalu memberi waktu luang apabila saya kesulitan dan jenuh dalam mengerjakan skripsi. Ucapan terima kasih ini mungkin tidak seberapa dengan waktu yang telah diluangkan di setiap waktu.
4. Rekan saya, Calvin Perdana Haryanto, yang telah membantu saya untuk mencari banyak literasi di Universitas Gajah Mada untuk membantu menyelesaikan skripsi ini.
5. Rekan-rekan saya di Startup Wujudkan Indonesia, yang selalu memberikan semangat dalam mengerjakan skripsi dan mengingatkan untuk tidak menyerah dalam keadaan apapun.
6. Pengurus Innovative Academy Hub UGM, karena telah menyediakan tempat bagi saya untuk mengerjakan skripsi dan berdiskusi mengenai penelitian saya. Mungkin ucapan terima kasih ini tidak sebanding karena kami sering merepotkan dan membuat masalah.
7. Bapak pembimbing Dony Ariyus, yang tmemberi masukan dan saran. Serta dengan sabar membimbing saya alam menulis dan mengerjakan penelitian yang saya angkat dalam skripsi ini.

8. Teman-teman di Institut Telkom Purwokerto dan rekan di Telkom Akses Purwokerto yang selalu mendukung saya dalam mengerjakan tugas di kampus dan skripsi.
9. Semua teman organisasi, baik BEM, SEMA, maupun rekan Asisten di Forum Asisten yang telah memberi canda tawa selama masa kuliah di kampus tercinta ini.
10. Seluruh rekan 16 IF 09, terima kasih telah memberi pelajaran berharga dan memberi canda tawa selama perkuliahan.
11. Semua teman dan pihak yang belum dapat saya sebutkan satu-persatu. Saya hanya dapat mengucapkan terima kasih. Semoga kebaikan kalian mendapat balasan yang baik pula dari Tuhan Yang Maha Esa.



KATA PENGANTAR

Salam Sejahtera!

Puji syukur kehadiran Tuhan Yang Maha Esa sehingga penulis dapat menyelesaikan Skripsi dengan judul “Optimasi Enkripsi Audio Menggunakan Algoritma Pseudorandom dan Teori Kekacauan pada Pesan Suara” dengan baik, walaupun disadari karya penulis masih ada beberapa kekurangan yang tidak lepas dari keterbatasan penulis.

Tujuan penulisan skripsi ini adalah untuk memenuhi syarat dalam menempuh ujian sarjana pada jurusan Informatika UNIVERSITAS AMIKOM YOGYAKARTA.

Dalam penulisan Skripsi ini tidak lepas dari kendala dan hambatan. Namun, berkat tekad, usaha, dan dorongan, serta bantuan dari berbagai pihak, akhirnya penulis dapat menyelesaikan Skripsi ini. Oleh karena itu, Penulis ingin mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M selaku Ketua UNIVERSITAS AMIKOM YOGYAKARTA.
2. Ibu Krisnawati, S.Si., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom.
3. Bapak Dony Ariyus, M.Kom selaku dosen pembimbing yang selalu memberikan bimbingan dan arahan kepada penulis.
4. Kedua orang tua penulis yang telah memberikan segala dukungan, dorongan, dan motivasi serta yang selalu memberikan doa.
5. Kepada Faham Wicaksono, atas dorongan semangatnya yang luar biasa.
6. Kepada semua rekan 16 IF 09 yang selalu memberikan semangat dalam mengerjakan skripsi ini.

DAFTAR ISI

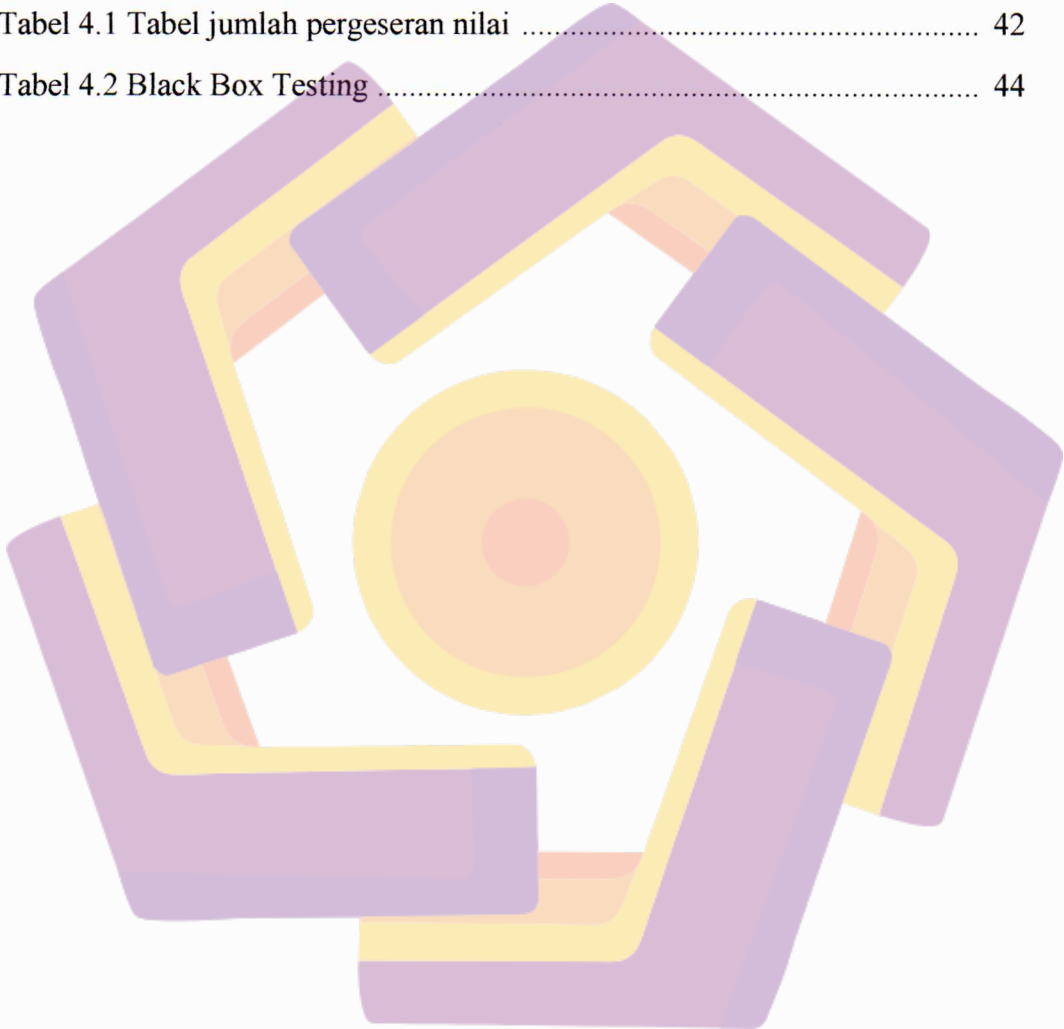
| | |
|---|----------|
| Judul | i |
| Persetujuan | ii |
| Pengesahan | iii |
| Pernyataan | iv |
| Motto | v |
| Persembahan | vii |
| Kata Pengantar | viii |
| Daftar Isi | ix |
| Daftar Tabel | xii |
| Daftar Gambar | xiii |
| BAB I. PENDAHULUAN | 1 |
| 1.1. Latar Belakang | 1 |
| 1.2. Rumusan Masalah | 2 |
| 1.3. Batasan Penelitian | 2 |
| 1.4. Maksud dan Tujuan Penelitian | 2 |
| 1.5. Metode Penelitian | 3 |
| 1.5.1. Pengumpulan Literatur | 3 |
| 1.5.2. Pengumpulan Data | 3 |
| 1.5.3. Desain | 3 |
| 1.5.4. Implementasi | 3 |
| 1.5.5. Pengujian | 3 |
| 1.6. Sistematika Penulisan | 4 |
| BAB II LANDASAN TEORI | 5 |
| 2.1. Tinjauan Pustaka | 5 |
| 2.2. Audio | 6 |
| 2.2.1. Pengertian Audio | 6 |
| 2.2.2. Bitrate | 6 |
| 2.2.3. Sample Rate | 7 |
| 2.2.4. Noise | 7 |
| 2.3. Pengenalan Kriptografi | 7 |
| 2.3.1. Pengertian Kriptografi | 7 |
| 2.3.2. Nilai Acak Dalam Kriptografi | 8 |
| 2.3.3. Komponen Kriptografi | 9 |
| 2.3.3.1. Enkripsi | 9 |
| 2.3.3.2. Dekripsi | 9 |
| 2.3.3.3. Kunci | 9 |
| 2.3.3.4. Chiphertext | 9 |
| 2.3.3.5. Plaintext | 9 |
| 2.3.3.6. Pesan | 10 |
| 2.3.3.7. Cryptanalysis | 10 |

| | |
|--|-----------|
| 2.3.4. Algoritma Kriptografi | 10 |
| 2.3.4.1. Algoritma Simetri | 10 |
| 2.3.4.2. Algoritma Asimetri | 10 |
| 2.3.4.3. Fungsi Hash | 11 |
| 2.4. Algoritma Pseudorandom | 12 |
| 2.4.1. Pengertian Algoritma Pseudorandom | 12 |
| 2.4.2. Linear Congruential | 12 |
| 2.5. Teori Kekacauan | 13 |
| 2.5.1. Pengertian Teori Kekacauan | 13 |
| 2.5.2. Logistic Map | 13 |
| 2.6. Kriptografi Pada Audio | 13 |
| 2.7. Software Yang Digunakan | 14 |
| 2.7.1. Microsoft Visual Studio 2017 | 14 |
| 2.7.2. GoldWave V6.35 | 14 |
| 2.7.3. Matlab | 14 |
| 2.8. Metode Pengujian | 14 |
| 2.8.1. Analisa Keamanan | 14 |
| 2.8.1.1. Analisa Ruang Kunci | 15 |
| 2.8.1.2. Sensitifitas Kunci | 15 |
| 2.8.2. Analisa Kemiripan Audio | 15 |
| BAB III METODE PENELITIAN | 17 |
| 3.1. Gambaran Umum Penelitian | 17 |
| 3.2. Jenis Penelitian | 17 |
| 3.3. Alur Penelitian | 18 |
| 3.4. Alat dan Bahan | 19 |
| 3.4.1. Perangkat Keras Digunakan | 19 |
| 3.4.2. Software Digunakan | 19 |
| 3.4.3. Sample yang Digunakan | 19 |
| 3.5. Analisa Sample | 20 |
| 3.6. Rancangan Implementasi | 22 |
| 3.6.1. Pembangkit Bilangan Acak | 22 |
| 3.6.1.1. Pseudorandom | 22 |
| 3.6.1.2. Teori Kekacauan | 23 |
| 3.6.2. Rancangan Enkripsi dan Dekripsi | 23 |
| 3.6.2.1. Usulan Metode | 23 |
| 3.6.2.2. Proses Enkripsi | 23 |
| 3.6.2.3. Proses Dekripsi | 30 |
| 3.7. Rancangan Aplikasi | 34 |
| 3.7.1. Gambaran Umum | 34 |
| 3.7.2. Desain | 34 |
| 3.7.3. Analisa Kebutuhan | 35 |
| 3.7.3.1. Kebutuhan Fungsional | 35 |

| | |
|--|-----------|
| 3.7.3.2. Kebutuhan Non-Fungsional | 35 |
| BAB IV HASIL DAN PEMBAHASAN | 36 |
| 4.1. Flowchart Program | 36 |
| 4.2. Implementasi | 37 |
| 4.2.1. Pengambilan Sample | 37 |
| 4.2.2. Penentuan Nilai Variabel | 37 |
| 4.2.3. Pembuatan Software | 38 |
| 4.2.3.1. Antarmuka Aplikasi | 38 |
| 4.2.3.2. Fungsi Bilangan Random | 38 |
| 4.2.3.3. Fungsi Enkripsi | 39 |
| 4.2.3.4. Fungsi Dekripsi | 40 |
| 4.2.4. Hasil Implementasi | 40 |
| 4.2.4.1. Hasil Enkripsi | 40 |
| 4.2.4.2. Hasil Dekripsi | 41 |
| 4.2.4.3. Pergeseran Nilai | 42 |
| 4.3. Pengujian | 43 |
| 4.3.1. Uji Aplikasi | 43 |
| 4.3.1.1. White Box Testing | 43 |
| 4.3.1.2. Black Box Testing | 44 |
| 4.3.2. Analisa Ruang Kunci | 44 |
| 4.3.3. Sensitifitas Kunci | 45 |
| 4.3.4. Analisa MFCC | 45 |
| BAB V KESIMPULAN DAN SARAN | 47 |
| 5.1. Kesimpulan | 47 |
| 5.2. Saran | 47 |
| DAFTAR PUSTAKA | 48 |
| DAFTAR LAMPIRAN | 49 |

DAFTAR TABEL

| | |
|---|----|
| Tabel 3.1 Sebaran amplitudo Audio 1 | 21 |
| Tabel 3.2 Sebaran amplitudo Audio 2 | 22 |
| Tabel 3.3 Nilai variabel pada proses enkripsi | 29 |
| Tabel 3.4 Rincian proses dekripsi | 33 |
| Tabel 4.1 Tabel jumlah pergeseran nilai | 42 |
| Tabel 4.2 Black Box Testing | 44 |



DAFTAR GAMBAR

| | |
|---|----|
| Gambar 2.1 Perbandingan frekuensi pada manusia | 6 |
| Gambar 2.2 Prinsip kriptografi | 8 |
| Gambar 2.3 Kriptografi simetris | 10 |
| Gambar 2.4 Kriptografi asimetris | 11 |
| Gambar 3.1 Alur penelitian | 18 |
| Gambar 3.2 Waveform audio 1 | 20 |
| Gambar 3.3 Waveform audio 2 | 21 |
| Gambar 3.4 Proses enkripsi | 30 |
| Gambar 3.5 Proses dekripsi | 33 |
| Gambar 3.6 Rancangan desain aplikasi | 34 |
| Gambar 4.1 Diagram alur pada program | 36 |
| Gambar 4.2 Penyimpanan grafik amplitudo audio 1 | 37 |
| Gambar 4.3 Penyimpanan grafik amplitudo audio 2 | 37 |
| Gambar 4.4 Tampilan antar muka aplikasi | 38 |
| Gambar 4.5 Kode program untuk operasi bilangan random | 39 |
| Gambar 4.6 Fungsi untuk enkripsi | 39 |
| Gambar 4.7 Fungsi untuk dekripsi | 40 |
| Gambar 4.8 Grafik gelombang dan spektrum pada chipper | 41 |
| Gambar 4.9 Grafik gelombang dan spektrum pada plain | 41 |
| Gambar 4.10 Perbandingan grafik amplitudo | 45 |
| Gambar 4.11 Grafik MFCC | 46 |

INTISARI

Seiring dengan perkembangan teknologi, masalah keamanan adalah salah satu aspek penting dalam berkomunikasi dan menyimpan data. Keamanan juga merupakan hal yang sangat dipertimbangkan dalam kegiatan yang terkait dengan data rahasia atau terbatas pada komunitas tertentu. Data yang mengandung informasi sensitif akan sangat berisiko jika dapat diakses oleh orang yang tidak berwenang lainnya. Untuk mengurangi risiko data jatuh ke pihak yang tidak berwenang, teknik kriptografi dapat digunakan untuk menyembunyikan informasi sehingga hanya dapat dikenali oleh mereka yang memiliki kunci.

Teori *Chaos* adalah fungsi untuk membuat serangkaian angka acak. Fungsi *Chaos* sangat sensitif terhadap nilai awal. Sensitivitas ini populer disebut efek kupu-kupu. Teori Kekacauan telah terbukti dalam proses enkripsi, karena agak salah memasukkan nilai awal sehingga hasil urutan angka akan berbeda.

Mirip dengan Teori *Chaos*, *Pseudorandom* juga menghasilkan angka acak berdasarkan angka awal sehingga seri yang berbeda angka dibentuk hingga serangkaian angka berulang. Bedanya, *pseudorandom* membutuhkan beberapa entri selain nomor awal.

Kata Kunci : Keamanan, Kriptografi, Audio, Teori Kekacauan, Logistic Map, Pseudorandom, Linear Congruential

ABSTRACT

Along with technological developments, security issues are one of the important aspects in communicating and storing data. Security is also a matter that is highly considered in activities related to confidential data or limited to certain communities. Data that contains sensitive information will be very risky if it is accessible to other unauthorized people. To reduce the risk of data falling to unauthorized parties, cryptographic techniques can be used to hide information so that it can only be recognized by those who have the key.

Chaos Theory is a function to create a series of random numbers. The chaos function is very sensitive to initial values. This sensitivity is popularly called the butterfly effect. The theory of chaos has been proven in the encryption process, because it is a bit wrong to enter the initial value so the results of the sequence of numbers will be different.

Similar to Chaos Theory, Pseudorandom also generates random numbers according to initial numbers so that different series of numbers are formed up to a series of repetitive numbers. The difference is, pseudorandom requires several entries other than the initial number.

Keywords : Security, Cryptography, Audio, Chaos Theory, Logistic Map, Pseudorandom, Linear Congruential