DAFTAR ISI

ABSTRAK iv

ABSTRACT v

KATA PENGANTAR vi

UCAPAN TERIMA KASIH vii

DAFTAR ISI viii

DAFTAR GAMBAR xi

DAFTAR TABEL xiii

DAFTAR ISTILAH xiv

DAFTAR SINGKATAN xv

BAB I Pendahuluan 1

1.1 Latar Belakang 1

1.2 Rumusan Masalah 3

1.3 Tujuan Penelitan 3

1.4 Batasan Masalah 3

1.5 Metode Penelitian 4

1.6 Sistematika Penelitian 5

BAB II Landasan Teori 6

2.1 Algoritma AES 8

2.2 Kriptosistem Kurva Elips 13

2.2.1 Kurva Eliptik pada F_p 13

2.2.2 Operasi Matematika pada Kurva Eliptik F_p 14

2.2.3 Aturan Penjumlahan Dua Titik pada Kurva Eliptik F_p 15

2.2.4 Point Compress dan Decompress 16

2.3 Algoritma Pertukaran Kunci Diffie-Hellman 16

2.4 Algoritma Kurva Eliptik Diffie-Hellman 18
2.5 Perbedaan Diffie-Hellman dengan ECDH 19
2.6 Pengolahan Suara 20
2.6.1 ADC (*Analog to Digital Converter*).....20
2.6.2 Format Suara WAV.....22
2.7 Parameter Performansi 23
2.7.1 Waktu performansi 23
2.7.2 Koefisien korelasi 23
2.7.3 *Avalanche Effect*.....24
2.7.4 SNR (*Signal Noise Ratio*) 24

BAB III Perancangan Sistem 25

3.1 Identifikasi Kebutuhan Sistem.....25
3.1.1 Spesifikasi Perangkat Keras (*Hardware*).....25
3.1.2 Spesifikasi Perangkat Lunak (*Software*).....25
3.2 Perencanaan Sistem.....25
3.2.1 Konversi Data Suara .wav ke Hexadecimal.....26
3.2.2 Proses Enkripsi dengan Algoritma AES 27
3.2.1 Proses Enkripsi dan Dekripsi Kunci Rahasia AES dengan Algoritma ECDH 29
3.3 Tampilan antar muka.....31

BAB IV Pengujian Sistem Dan Analisis Hasil.....33

4.1 Lingkungan Pengujian 33
4.2 Skenario Pengujian Sistem.....33
4.2.1 Pengujian fungsionalitas sistem menjalankan proses kriptografi 33
4.2.2 Pengujian pengaruh parameter pada ECDH terhadap koefisien korelasi dan waktu komputasi 33
4.2.3 Pengujian waktu komputasi dan koefisien korelasi algoritma ECDH.....34
4.2.4 Pengujian *avalanche effect* algoritma ECDH 34

4.2.5 Pengujian perhitungan kesukaran pemecahan kunci ECDH dan DH 34
4.2.6 Pengujian perbandingan waktu komputasi algoritma DH dan ECDH 35
4.2.7 Pengujian performansi enkripsi dan dekripsi suara 35
4.2.8 Pengujian subyektif 35
4.3 Analisis hasil pengujian sistem 36
4.3.1 Pengujian fungsionalitas sistem menjalankan proses kriptografi 36
4.3.2 Pengujian pengaruh parameter pada ECDH terhadap koefisien korelasi dan waktu komputasi 38
4.3.3 Pengujian waktu komputasi dan koefisien korelasi algoritma ECDH 40
4.3.4 Pengujian avalanche effect algoritma ECDH 42
4.3.5 Pengujian perhitungan kesukaran pemecahan kunci ECDH dan DH 43
4.3.6 Pengujian perbandingan total waktu komputasi DH dan ECDH 44
4.3.7 Pengujian performansi enkripsi dan dekripsi suara 44
4.2.7 Pengujian subyektif 46

BAB V PENUTUP 47

5.1 Kesimpulan 47
5.2 Saran 48

Daftar Pustaka 49

Lampiran