BAB I
PENDAHULUAN

1.1 Latar Belakang

Identity-Based Encryption merupakan teknik enkripsi dengan menggunakan kunci asimetris yang mempunyai keistimewaan, yaitu kunci publik yang digunakan dapat berupa sembarang string. Biasanya, enkripsi menggunakan kunci publik yang rumit dan sulit diingat. *Identity-Based Encryption* menggunakan kunci yang lebih "user-friendly". Kunci publik pada *Identity-Based Encryption* ini dapat berupa alamat email, nomor telepon, ataupun suatu kalimat. Kelebihan lain dari teknik enkripsi ini yaitu tidak diperlukannya penentuan pasangan kunci sebelum melakukan enkripsi. Dengan menggunakan *Identity-Based Encryption*, seseorang dapat mengirimkan pesan yang telah dienkripsi dengan kunci publik walaupun penerima belum mempunyai bahkan belum pernah mendengar kunci privat sekalipun.

1.2 Perumusan Masalah

Adapun permasalahan yang ingin diangkat dalam penelitian tugas akhir ini adalah:

1. Bagaimana kemudahan penggunaan *Identity-Based Encryption* untuk pengamanan pengiriman informasi.
2. Bagaimana *Identity-Based Encryption* menghasilkan kunci yang dibutuhkan.
3. Bagaimana *Identity-Based Encryption* dapat menghilangkan kebutuhan sertifikat untuk kunci publik.

1.3 Tujuan Penelitian

Tujuan penelitian dari tugas akhir ini adalah:

1. Mempelajari kemudahan yang di hasilkan dengan menggunakan string identitas sebagai kunci publik dan mengimplementasikan sistem *Identity-Based Encryption Boneh-Franklin.*

2. Analisis kecepatan proses-proses pada sistem Identity Based Encryption Boneh Franklin dengan menggunakan perhitungan kecepatan proses berdasarkan waktu pada sistem operasi yang di gunakan serta analisis file hasil encode dan decode pesan text dengan menggunakan AES.

1.4 Batasan Masalah

Pembahasan masalah pada tugas akhir ini akan dibatasi pada ruang lingkup :

1. Tidak menganalisis secara matematis teknik *Identity-Based Encryption Boneh-Franklin*.
2. File yang digunakan untuk enkripsi adalah berupa file pesan text.
3. Fungsi hash, fungsi AES dan fungsi pairing yang digunakan pada kurva elips diambil dari implementasi yang telah ada dari MIRACL 5.0.
4. Implementasi perangkat lunak digunakan bahasa pemrograman Microsoft Visual C++ 6.0.

1.5 Metodologi Pemecahan Masalah

Metode yang digunakan dalam penyelesaian Tugas Akhir ini yaitu:

1. Studi Literatur

   Diperlukan untuk memecahkan rumusan permasalahan berdasarkan referensi dan mengumpulkan data yang berkaitan dengan perumusan masalah.
2. Analisis masalah dan kebutuhan perangkat lunak yang akan dibangun.
3. Merancang pemecahan masalah berdasarkan hasil analisis yang didokumentasikan dalam suatu spesifikasi.
4. Implementasi

   Tahap pembuatan perangkat lunak *Identity-Based Encryption Boneh-Franklin*.
5. Penyusunan laporan tugas akhir dan kesimpulan akhir.

1.6 Sistematika Penulisan

Tugas Akhir ini akan disusun dengan sistematika sebagai berikut :

Bab I Pendahuluan.

Bab ini memberikan gambaran secara garis besar tentang Tugas Akhir yang dilakukan penulis. Mencakup latar belakang pembuatan Tugas Akhir, perumusan masalah, pembatasan masalah, tujuan, metodologi pemecahan masalah dan sistematika penulisan.

Bab II Dasar Teori.

Bab ini menjelaskan seluruh teori yang menjadi landasan konseptual dan pendukung penyelesaian Tugas Akhir ini yaitu teori tentang mekanisme *Identity-Based Encryption Boneh-Franklin*.

Bab III Perancangan dan Implementasi Sistem *Identity Based Encryption*.

Menjelaskan tentang proses analisis masalah dan kebutuhan perangkat lunak. Berisi rancangan yang meliputi proses enkripsi dan dekripsi suatu pesan dengan menggunakan *Identity-Based Encryption Boneh-Franklin.*

Bab IV Pengujian dan Analisis.

Mengimplementasikan dan analisis dari proses enkripsi suatu pesan dengan menggunakan *Identity-Based Encryption Boneh-Franklin*.

Bab V Kesimpulan.

Bab ini berisi kesimpuan dari keseluruhan sistem yang dibuat serta saran yang berkaitan dengan aplikasi Tugas Akhir ini dan kemungkinan pengembangan selanjutnya.