BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi internet memberikan banyak kemudahan untuk mengakses informasi dan melakukan komunikasi. Namun, lalu lintas informasi yang beredar tidaklah terjamin keamanannya. media komunikasi umum yang dapat digunakan oleh siapapun, sehingga sangat rawan terhadap serangan seperti hacker, virus, penipuan elektronik, penyadapan informasi oleh pihak-pihak yang tidak berhak, dan lain sebagainya. Oleh karena penggunaan internet yang sangat luas seperti pada bisnis, perdagangan, bank, industri dan pemerintahan yang umumnya mengandung informasi yang bersifat rahasia maka keamanan informasi menjadi faktor utama yang harus dipenuhi.

Salah satu teknik pengamanan data adalah dengan menggunakan kriptografi. Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Suatu pesan teks dapat dienkripsi menggunakan algoritma kriptografi tertentu sehingga menghasilkan teks lain yang dinamakan ciphertext yaitu suatu teks yang berisi karakter-karakter yang akan sulit dimengerti atau tidak bermakna apabila dibaca oleh pihak yang tidak berkepentingan.

Tugas akhir ini akan memperlihatkan contoh penerapan algoritma kriptografi Elgamal pada suatu teks. Teks akan dienkripsi sehingga menghasilkan suatu ciphertext, ciphertext ini kemudian dapat didekripsi kembali menjadi file teks seperti semula. Penggunaan tanda tangan digital (Digital Signature) bertujuan untuk untuk memastikan integritas dan keaslian berita/data berikut pengirimnya.

1.2 Rumusan Masalah

1. Bagaimana cara kerja algoritma kriptografi Elgamal?
2. Bagaimana penerapan enkripsi dan dekripsi menggunakan algoritma Elgamal?
3. Bagaimana penerapan digital signature pada pesan

1.3 Tujuan

1. Mempelajari cara kerja algoritma elgamal
2. Membuat aplikasi enkripsi dan dekripsi teks menggunakan algoritma Elgamal
3. Menambahkan digital signature pada pesan teks

1.4 Pembatasan Masalah

1. Hanya menerima input Alphanumerik (A-Z, a-z, 0-9)
2. Tidak menangani masalah pengiriman data seperti email, SMS, atau lainnya.
3. Bahasa pemrograman menggunakan JAVA.
4. *Compiler* menggunakan NetBeans IDE.

1.5 Sistematika Pembahasan

Bab I Pendahuluan: Membahas latar belakang, rumusan masalah, tujuan, dan batasan masalah

Bab II Dasar Teori: Membahas teori-teori yang berhubungan dengan Kriptografi, Enkripsi dan Dekripsi, dan Algoritma Elgamal

Bab III Perancangan Aplikasi: membahas tentang perancangan aplikasi enkripsi dan dekripsi kriptografi Elgamal

Bab IV Pengujian: Membahas hasil pengujian terhadap aplikasi yang dihasilkan

Bab V Kesimpulan dan Saran: Membahas tentang kesimpulan yang diperoleh selama melakukan penelitian dan saran untuk penelitian selanjutnya.