BAB I
PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi yang semakin cepat, membawa dampak yang luar biasa terhadap perkembangan layanan informasi. Segala informasi menjadi semakin cepat dan mudah untuk diakses oleh siapa saja, kapan saja dan dimana saja. Seiring dengan perkembangan tersebut dunia penunjang penyebaran informasi tersebut juga turut berkembang dengan pesat. Dunia fotografi yang dulu dikenal hanya untuk kalangan eksklusif, saat ini telah menjadi hal yang biasa dan menjadi tren dalam kehidupan masyarakat di perkotaan maupun masyarakat di pedesaan. Semua produsen perangkat elektronik seakan-akan berlomba-lomba untuk membuat jenis kamera baru yang mudah digunakan dan dengan tambahan berbagai fungsi yang menarik. Peningkatan teknologi dalam kamera juga semakin maju dengan munculnya kamera digital. Setiap tahun perkembangan kualitas foto juga meningkat seiring meningkatnya jumlah *pixel* yang terdapat pada kamera. Hal ini juga menyebabkan berbagai jenis peralatan elektronik maupun komunikasi mengalami konvergensi dengan dicangkokkannya kamera pada peralatan tersebut.

Dengan adanya perkembangan peralatan fotografi yang semakin maju, serta perkembangan layanan informasi yang tersedia di internet, membuat setiap orang bebas dan mudah untuk bertukar foto maupun gambar dengan siapa saja. Namun bagi beberapa orang tidak setiap foto atau gambar tersebut diijinkan untuk diambil secara bebas, karena adanya alasan kerahasiaan dan alasan khusus lainnya. Maka dalam hal ini diperlukan sistem keamanan yang andal serta dapat menjamin *privacy* gambar yang dikirim. Selama proses pemindahan gambar, keamanan dari gambar tersebut menjadi hal yang krusial, terutama bila pemindahannya dilakukan dengan mentransmisi melalui suatu jaringan. Untuk menjaga kerahasiaan gambar-gambar tersebut selama ditransmisi dapat dilakukan proses kriptografi.

Kriptografi adalah ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan ditransfer dari suatu tempat ke tempat lain, isi dari pesan tersebut kemungkinan dapat diambil oleh pihak lain. Untuk menjaga keamanan pesan,

maka pesan tersebut dapat diacak atau diubah menjadi kode yang tidak dapat dimengerti oleh orang lain menggunakan suatu kunci tertentu. Bila pesan telah sampai, penerima pesan dapat melakukan proses untuk mengembalikan pesan yang teracak menjadi pesan awal. Salah satu algoritma kriptografi adalah algoritma MMB (Modular Multiplication-based Block cipher). Untuk merealisasikan algoritma tersebut menjadi suatu program enkripsi-dekripsi, maka digunakan bahasa pemrograman Visual basic 6.0.

I.2 Identifikasi Masalah

1. Bagaimana cara merealisasikan suatu program yang dapat melakukan proses enkripsi dan deskripsi menggunakan algoritma MMB (Modular Multiplication-based Block cipher) untuk meningkatkan keamanan dan kerahasiaan dalam pengiriman file gambar?
2. Bagaimana kinerja teknik enkripsi dan deskripsi menggunakan kunci simetrik dan algoritma MMB (Modular Multiplication-based Block cipher) secara teori dan implementasi?

I.3 Tujuan

Memahami algoritma MMB (Modular Multiplication-based Block cipher) dan merealisasikan suatu program enkripsi dan deskripsi file gambar dengan menggunakan algoritma MMB untuk meningkatkan keamanan dan kerahasiaan data informasi dalam proses pengiriman.

I.4 Pembatasan Masalah

1. Program enkripsi dan deskripsi dirancang menggunakan algoritma MMB (Modular Multiplication-based Block cipher).
2. Bahasa pemrograman yang dirancang untuk melakukan enkripsi dan dekripsi terhadap file gambar adalah Visual Basic 6.0.

I.5 Sistematika Penulisan

Laporan tugas akhir ini disusun dengan sistematika sebagai berikut:

- **Bab I**

  Membahas latar belakang masalah, identifikasi masalah, tujuan dibuatnya makalah ini, batasan-batasan masalah, serta sistematika penulisan laporan ini.

- **Bab II**

  Menjelaskan teori-teori yang berkaitan dengan kriptografi, serta metode dan algoritma MMB (Modular Multiplication-based Block cipher).

- **Bab III**

  Membahas mengenai perancangan program dan cara kerja program enkripsi dan deskripsi menggunakan algoritma MMB (Modular Multiplication-based Block cipher). Selain itu juga dibahas mengenai *digital signature* menggunakan algoritma ElGamal.

- **Bab IV**

  Membahas hasil pengujian beserta analisis dari proses enkripsi dan dekripsi menggunakan beberapa file gambar dengan format jpg, bmp, dan gif.

- **Bab V**

  Merumuskan kesimpulan dan saran.