BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam sebuah instansi atau perusahaan ada data rahasia dalam bentuk *file* yang harus dimiliki oleh sekelompok orang, karena jika data rahasia milik bersama dipegang dan dikuasai oleh satu orang, maka orang tersebut dapat dengan mudah membuka dan menggunakan data tersebut tanpa perlu meminta persetujuan dari pihak yang lain, misalnya pada laporan keuangan sebuah instansi atau perusahaan. Apabila hanya satu orang saja yang memegang laporan keuangan tersebut bisa saja mengganti dan menyalahgunakan laporan tersebut. Masalah yang muncul adalah bagaimana membagi data rahasia menjadi beberapa bagian.

Masalah ini dapat diselesaikan dengan menggunakan protokol *Secret Sharing*. Dengan menggunakan protokol *secret sharing*, data rahasia dapat dibagi menjadi *n* bagian dan dibutuhkan *n* bagian untuk merekonstruksi kembali data. *Secret sharing* telah diimplementasikan pada *software symantec*, dimana *software* tersebut memungkinkan pengguna untuk memecah kunci menjadi beberapa bagian, dan pecahan kunci dapat disatukan kembali menjadi kunci yang utuh untuk digunakan pada proses enkripsi dan proses dekripsi *file* menggunakan metode *Pretty Good Privacy* (PGP). (Symantec Corporation, 2015)

Pemecahan *file* juga dapat dilakukan dengan menggunakan aplikasi *HJSplit*. Aplikasi ini membagi (*split*) suatu *file* dengan ukuran besar menjadi beberapa bagian, dan dapat menyatukan (*join*) kembali pecahan-pecahan *file* menjadi *file* awal. Beberapa alasan *file* dengan ukuran besar dipecah menjadi *file* dengan ukuran kecil menggunakan *HJSplit*, adalah terbatasnya kapasitas media penyimpanan dan efisiensi waktu untuk meng-*upload* dan men-*download file* ke *server*. Namun, sayangnya *HJSplit* tidak memiliki proteksi, sehingga siapapun yang memperoleh pecahan *file* dapat melakukan rekonstruksi dan memperoleh *file* awal. (HJSplit.org, 2014)

Beberapa penelitian terdahulu mengenai *secret sharing* adalah jurnal penelitian "Penerapan Metode *Shamir Secret Sharing Schemes* pada Aplikasi Kriptografi *File*" yang disusun oleh Tsuwaibatul Aslamiyah pada tahun 2011, jurnal penelitian "Analisis Keamanan Pada Kombinasi Protokol *Secret Sharing* Dan *Three-Pass*" yang disusun oleh Satria Prayudi yang ditulis pada tahun 2016, dan jurnal penelitian "*Verifiable Multi-Secret Sharing Based on LSFR*", yang ditulis oleh Hu, C., Liao, X., & Cheng pada tahun 2012.

Permasalahan lain yang muncul adalah bagaimana jika salah satu atau beberapa bagian hilang, sehingga *file* tidak dapat direkonstruksi kembali. Permasalahan ini dapat diselesaikan dengan menggunakan *Visual Cryptography*. Keuntungan dari *Visual Cryptography* terletak pada proses dekripsinya yang tidak menggunakan komputasi kriptografi yang terlalu kompleks. Walaupun demikian skema tersebut masih memiliki kelemahan juga, yaitu proses pendekripsian *file* mudah dilakukan oleh siapa saja jika pihak tersebut memiliki sedikitnya jumlah *k* pecahan yang tersedia. Skema tersebut dapat dibuat menjadi lebih aman dengan menambahkan sebuah kunci simetrik dalam proses enkripsi dan dekripsinya. Dengan demikian, jika pihak penyeludup ingin merekonstruksi *file* asli dengan hanya menggunakan jumlah *k pecahan* yang dimilikinya, namun tidak mengetahui kunci yang digunakan, maka proses tersebut akan gagal. Proses rekonstruksi *file* awal akan berhasil jika memiliki sedikitnya jumlah *k* pecahan *file* dan mengetahui kunci simetrik yang digunakan. Untuk menambah pengamanan *file*, maka *file* akan dienkripsi terlebih dahulu dengan menggunakan metode *Tiny Encryption Algorithm* (TEA), sebelum dipecah menjadi beberapa bagian dengan skema k-n *Visual Cryptography*.

Berdasarkan persoalan yang dipaparkan di atas, maka dibuatlah sebuah perangkat lunak untuk mengimplementasikan skema tersebut. Oleh karena itu, penulis mengambil skripsi yang berjudul "Implementasi Metode *Tiny Encryption* dan Skema *k-n Visual Cryptography* untuk Pengamanan dan Pemecahan *File* Rahasia".

1.2 Rumusan Masalah

Masalah yang muncul adalah bagaimana membagi data rahasia menjadi beberapa bagian apabila ada *file* rahasia yang harus dipegang oleh beberapa orang. Masalah ini dapat diselesaikan dengan menggunakan protokol *Secret Sharing dan Visual Cryptography*, dimana pemecahan *file* dengan skema *k-n Visual Cryptography* tidak memperkecil ukuran *file* awal, karena proses yang terjadi bukanlah proses pemenggalan (*split*) isi *file*, tetapi proses yang dilakukan adalah membagikan bit 1 dari *file* awal secara acak ke semua bagian (*share*) *file*. Bagian atau pecahan yang tidak memperoleh bit 1, akan diberikan bit 0, sehingga ukuran *file* pecahan (*share*) tetap sama dengan ukuran *file* awal.

1.3 Batasan Masalah

Permasalahan yang akan diteliti memiliki ruang lingkup yang cukup luas, sehingga penulis membatasi masalah tersebut sebagai berikut:

1. *File* yang dapat diproses adalah semua tipe *file*.
2. Nilai *n* (jumlah pecahan *file*) dibatasi minimum 6 dan maksimum 10.
3. Nilai *k* (jumlah pecahan minimum untuk rekonstruksi *file*) dibatasi minimum 2 dan maksimum sama dengan nilai *n*.
4. Pada saat penggabungan, pecahan *file* yang dipilih harus memiliki ukuran data yang sama.

1.4 Tujuan Penelitian

Tujuan dari penelitian adalah menghasilkan suatu aplikasi yang dapat mengenkripsi *file* menggunakan metode TEA dan menggunakan skema *k-n* kriptografi visual untuk memecah suatu *file* digital menjadi *n* bagian, akan tetapi dibutuhkan hanya *k* bagian untuk merekonstruksi kembali *file*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. Aplikasi dapat digunakan untuk mengamankan *file* digital dengan menggunakan metode TEA dan memecah *file* menjadi beberapa bagian, tetapi hanya dibutuhkan sebagian pecahan untuk merekonstruksi atau mengembalikan *file* awal.
2. Laporan hasil penelitian dapat digunakan untuk memahami cara kerja metode TEA dan *visual cryptography*.

1.6 Metode Penelitian

Tahapan-tahapan yang akan dilakukan dalam penelitian ini adalah sebagai berikut :

1. Studi Literatur

   Tahap studi literatur ini dilaksanakan untuk mengumpulkan dan mempelajari informasi yang diperoleh dari buku, jurnal, skripsi dam berbagai sumber referensi lain yang berkaitan dan mendukung penelitian mengenai *Visual Cryptography* ini.
2. Analisis Permasalahan

   Pada tahap ini dilakukan analisis terhadap berbagai informasi yang telah diperoleh dari berbagai sumber yang terkait dengan penelitian agar didapatkan metode yang tepat untuk menyelesaikan masalah dalam penelitian ini.
3. Perancangan Sistem

   Pada tahap ini dilakukan perancangan sistem untuk menyelesaikan permasalahan yang terdapat di dalam tahap analisis.

   Dalam program yang akan dibangun terdiri atas dua bagian, yaitu proses pemecahan *file* dan proses penggabungan *file*:

   1. Proses pemecahan *file*, yaitu proses yang dilakukan untuk mengamankan *file* dengan metode TEA dan memecah *file* menjadi *n* bagian dengan *Visual Cryptography*.

2. Proses penggabungan *file*, yaitu proses yang dilakukan untuk mengembalikan *file* rahasia, dengan menggabung sebanyak *k* pecahan *file* rahasia (dimana $k < n$) dan hasil penggabungan didekripsi dengan menggunakan metode TEA.