BAB I
PENDAHULUAN

1.1 Latar Belakang

Penggunaan komputer dalam berbagai bidang kehidupan membawa perkembangan yang sangat pesat pada perangkat keras maupun perangkat lunak komputer. Sebelum adanya kemajuan di bidang telekomunikasi dan komputer, manusia menggunakan uang secara nyata untuk bertransakasi secara tatap muka. Pada dua dekade ini, kemajuan telekomunikasi dan komputer memungkinkan manusia untuk menyimpan data secara digital.

Aktivitas penyimpanan data secata digital tentu saja mempunyai banyak resiko. Hal ini jelas terlihat apabila dalam aktivitas tersebut terdapat informasi yang penting dapat diakses oleh orang lain yang tidak berkepentingan (*unauthorized person*), misalnya informasi mengenai *password* atau PIN (Nathasia & Wicaksono, 2011). Saat ini masalah keamanan pada komputer menjadi isu penting pada era teknologi informasi.

Komputer laptop dan media penyimpan (*drives*) *portabel* yang sering dibawa-bawa menjadi rentan terhadap kemungkinan hilang atau dicuri. Bila terjadi, data-data yang tersimpan didalamnya tentu saja turut terbawa oleh pencuri atau jatuh ke tangan pihak lain. Datanya itu sendiri mungkin sudah di *back-up*, namun nilai dari informasinya tentu menjadi pertimbangan tersendiri terlebih lagi bila data tersebut bersifat pribadi, penting atau sensitif, yang mungkin saja dapat memberikan berdampak buruk bagi pemiliknya. Perlindungan terhadap informasi yang berharga dapat dilakukan dengan menggunakan metode/algoritma tertentu, diantaranya yang popular adalah kriptografi dan steganografi. Kedua metode ini mempunyai keunggulan masing-masing dalam mengamankan data dan telah digunakan dalam semua bidang kehidupan.

Kriptografi yang berasal dari kata yunani "*cryptos*" yang artinya rahasia dan "*graphein*" yang artinya tulisan, sehingga kriptografi adalah ilmu untuk menjaga kerahasiaan pesan dengan cara menyandikan ke bentuk yang tidak dimengerti. Keungulan dari kriptografi adalah kemampuan penyandian pesan

sehingga pesan terlihat seperti diacak. Kriptografi tidak sekedar berupa kerahasiaan data (*privacy*) saja, tapi juga bertujuan untuk menjaga integritas data (*data integrity*), keaslian data (*authentication*) dan anti penyangkalan (*non-repudiation*) (Nathasia & Wicaksono, 2011; Sukrisno & Utami, 2007). Di dalam kriptografi terdapat 5 hal utama yaitu enkripsi, dekripsi, dan kunci (*key*), pengirim, dan penerima. Enkripsi merupakan proses penyandian *plainteks* (pesan awal) menjadi *cipherteks* (pesan yang tersandikan), sedangkan dekripsi merupakan kebalikan dari proses enkripsi. Baik proses enkripsi dan dekripsi, keduanya menggunakan kunci untuk menjaga kerahasiaan data. Penggunaan kriptografi mulai dari penggunaan kartu ATM, penggunaan *password* untuk *file-file* dokumen kantor, transaksi dengan kartu kredit, transaksi di bank, percakapan dengan handphone, dan akses internet telah membuktikan pentingnya kriptografi dalam pengamanan informasi.

Salah satu algoritma dalam kriptografi modern berbasis bit yang sering digunakan yaitu *stream cipher* (cipher aliran). Algoritma ini beroperasi pada *plainteks/cipherteks* dalam bentuk bit tunggal sehingga pesan dienkripsikan/didekripsikan bit per bit. Dengan demikian algoritma ini lebih valid untuk digunakan mengamankan data.

Sedangkan steganografi berasal dari kata "*steganos*" berarti rahasia dan "*graphein*" yang berarti tulisan. Dalam proses pelaksanaannya steganografi hampir sama dengan kriptografi, yaitu adanya kunci dan pesan. Sedangakan proses yang terjadi dalam steganografi adalah *embedding* (menanamkan pesan ke dalam data) dan *extracting* (membaca pesan yang tertanam pada data). Salah satu algoritma yang digunakan dalam steganografi yaitu *End Of File* (EOF), dimana pesan disisipkan di bagian akhir data asli. Dengan menggunkaan teknik ini, orang lain tidak akan mengetahui adanya data tambahan/pesan dalam *file* asli. *File* tambahan ini hanya dapat dibuka oleh penerimanya saja. Hal ini merupakan keunggulan steganografi dalam hal *invisibility* (ketidaktampakan secara kasat mata). Metode ini sangat bermanfaat untuk pengamanan data digital. Fungsi dari steganografi sendiri yaitu membuat data yang disisipkan menjadi tidak tampak secara kasat mata sehingga seolah-olah sama dengan data aslinya.

Pada penelitian yang dilakukan oleh Irfianti (Irfianti, 2007), di paparkan bahwa *Stream Cipher* merupakan teknik yang efektif dan sulit untuk dipecahkan oleh Kriptanalis. Hal ini dikarenakan penggunaan fungsi XOR dalam proses enkripsinya. Namun, kelemahan dari algoritma *Stream Cipher* ini adalah hasil enkripsi yang masih tampak oleh mata manusia, sehingga mudah dikenali sebagai data yang telah mengalami proses enkripsi. Sedangkan menurut Natashia (Nathasia & Wicaksono, 2011), dijelaskan bahwa *stream cipher* merupakan salah satu algoritma kunci simetris modern yang menggunakan pembangkit aliran kunci (*keystream generator*). Pembangkit aliran kunci ini kemudian di XORkan dan apabila kunci yang digunakan adalah acak maka algoritma ini berada pada tingkat keamanan tinggi.

Penelitian lainnya yaitu mengenai EOF pada steganografi yang dilakukan oleh Sikrisno (Sukrisno & Utami, 2007), Iswahyudi (Iswahyudi, Setyaningsih, & Widyastuti, 2012), Nani Paskalis (Nani, 2011), Aditya (Aditya, Pratama, & Nurlifa, 2010), dan Wandani (Wandani, Budiman, & Sharif, 2012) menjelaskan bahwa EOF merupakan algoritma steganografi yang mempunyai tingkat keamanan yang cukup baik. Algoritma EOF digunakan untuk meyembunyikan pesan rahasia dengan cara manambahkan bit-bit pesan yang akan disembunyikan ke akhir *file* citra penampung. Algoritma ini tidak mengganggu kualitas data awal yang akan disisipkan pesan dan juga tidak kasat mata.

Menurut penelitian yang telah dilakukan di atas, dapat dilihat bahwa algoritma *Stream Cipher* dan EOF mempunyai kemampuan yang baik dalam menyembunyikan data. Dalam algoritma *Stream Chiper* yang merupakan salah satu algoritma dari kriptografi mempunyai kelebihan yaitu tidak mudah untuk didekripsi oleh orang awam. Akan tetapi mempunyai sedikit kelemahan yaitu secara kasat mata masih tampak bahwa *file* tersebut adalah hasil dari kriptografi.

Oleh karena itu, penulis menambahkan sebuah metode yaitu steganografi untuk menyembunyikan *file* yang telah dienkripsi tersebut. Dengan demikian perlu dibuat aplikasi yang mampu mengamankan data digital dalam sebuah komputer, sehingga penulis membuat "PENYEMBUNYIAN PESAN *TEXT* TERENKRIPSI MENGGUNAKAN METODE KRIPTOGRAFI *STREAM CIPHER* DAN STEGANOGRAFI *END OF FILE (EOF)* DENGAN *FILE*

INDUK PDF" sebagai judul untuk menyusun laporan Tugas Akhir guna menyelesaikan Program Studi Strata I di Universitas Dian Nuswantoro Semarang.

1.2 Rumusan Masalah

Berdasarkan penjelasan dari latar belakang telah dijelaskan bahwa algoritma *Stream Cipher* dan EOF mempunyai kelebihan masing-masing, sedangkan untuk menutupi kekurangannya maka pada penelitian ini akan melakukan penggabungan antara algoritma *Stream Cipher* dan EOF, maka permasalahan yang akan dianalisa oleh penulis dalam pembuatan laporan Tugas Akhir ini dapat dirumuskan :

"Bagaimana menggabungkan algoritma *Stream Cipher* dan EOF menjadi algoritma yang aman dalam penyembunyian pesan melalui proses enkripsi dan dekripsi *file* supaya tidak mudah untuk dideteksi oleh orang awam dan menyembunyikan *file* tersebut pada *file* lain yang disebut *file* induk supaya *file* asli tidak dapat dilihat secara kasat mata atau mengaburkan pandangan dari mata manusia sehingga *file* tersebut selain aman juga tidak terlihat secara kasat mata".

1.3 Batasan Masalah

Untuk membatasi ruang lingkup permasalahan dalam penelitian dan agar tidak menyimpang dari pokok permasalahan, maka penulis memberikan batasan-batasan dalam penulisan penyembunyian pesan menggunakan *stream cipher* dan *EOF*, diantaranya hanya akan dibahas :

a. *File* yang akan di enkripsi adalah *file* teks, antara lain *file* . *txt*, . *doc*, dan . *docx*.
b. Metode yang digunakan untuk hiding file yaitu EOF *(End of File)* karena EOF mempunyai kemampuan untuk di implementasikan dalam bentuk *file* apapun.
c. *File* yang akan di hiding, mula-mula akan dienkripsi terlebih dahulu dengan menggunakan *stream cipher*.
d. Aplikasi enkripsi pesan ini akan diimplementasikan menggunakan bahasa pemrograman Visual Basic 6. 0.

1.4 Tujuan Penelitian

Tujuan dari penelitian yang dilakukan penulis adalah :

a. Menerapkan metode *stream cipher* untuk diterapkan pada proses enkripsi *file* dan dekripsinya.
b. Menyembunyikan *file* yang telah terenkripsi tersebut ke dalam *file* lain menggunakan metode EOF *(End Of File)* sehingga tidak terlihat secara kasat mata.

1.5 Manfaat Penelitian

Hasil laporan tugas akhir ini diharapkan akan memberika manfaat bagi penulis, akademik, para pembaca antara lain:

a. Bagi Akademik

Sebagai acuan dan tolak ukur sejauh mana pemahaman dan penguasaan mahasiswa terhadap materi perkuliahan yang diberikan sehingga dapat dijadikan sebagai bahan evaluasi akademik untuk meningkatkan mutu pendidikan pada Universitas Dian Nuswantoro.

b. Bagi Penulis

- Dengan penelitian ini diharapkan perancangan basis data tersebut menjadi sarana menerapkan materi-materi yang telah didapat selama ini dan mengembangkan ilmu yang diperoleh selama di perkuliahan, dan juga dapat digunakan untuk mengetahui sejauh mana penguasaan terhadap materi-materi tersebut.
- Melatih penulis dalam memahami permasalahan yang ada tentang bagaimana prosedur pengolahan data yang baik dan benar berdasarkan kaedah dan aturan sistem yang ada.

c. Bagi Pembaca

- Diharapkan dapat digunakan sebagai sumber informasi untuk penelitian lebih lanjut.
- Agar pembaca dapat mengetahui sistem yang sedang berkembang saat ini.