LAPORAN TUGAS AKHIR

PENYEMBUNYIAN PESAN *TEXT* TERENKRIPSI MENGGUNAKAN METODE KRIPTOGRAFI *STREAM CIPHER* DAN STEGANOGRAFI *END OF FILE (EOF)* DENGAN *FILE* INDUK PDF

Laporan ini disusun guna memenuhi salah satu syarat untuk menyelesaikan program studi Teknik Informatika S-1 pada Fakultas Ilmu Komputer Universitas Dian Nuswantoro

Disusun oleh:

Nama : Bely Arifpriyanto

NIM : A11. 2008. 03998

Program Studi : Teknik Informatika (S-1)

FAKULTAS ILMU KOMPUTER

UNIVERSITAS DIAN NUSWANTORO

SEMARANG

2013

PERSETUJUAN LAPORAN TUGAS AKHIR

Nama Pelaksana	:	Bely Arifpriyanto
NIM	:	A11. 2008. 03998
Program Studi	:	Teknik Informatika
Fakultas	:	Ilmu Komputer
Judul Tugas Akhir	:	Penyembunyian Pesan *Text* Terenkripsi Menggunakan Metode Kriptografi *Stream Cipher* Dan Steganografi *End Of File* (EOF) Dengan *File* Induk PDF

Tugas Akhir ini telah diperiksa dan disetujui,

Semarang, 11 Juni 2013

Menyetujui :	Mengetahui :
Pembimbing	Dekan Fakultas Ilmu Komputer
L. Budi Handoko, M. Kom	Dr. Abdul Syukur

PENGESAHAN DEWAN PENGUJI

Nama Pelaksana	:	Bely Arifpriyanto
NIM	:	A11. 2008. 03998
Program Studi	:	Teknik Informatika
Fakultas	:	Ilmu Komputer
Judul Tugas Akhir	:	Penyembunyian Pesan *Text* Terenkripsi Menggunakan Metode Kriptografi *Stream Cipher* Dan Steganografi *End Of File* (EOF) Dengan *File* Induk PDF

Tugas akhir ini telah diujikan dan dipertahankan dihadapan Dewan Penguji pada Sidang Tugas Akhir bulan Juli 2013. Menurut pandangan kami, tugas akhir ini memadai dari segi kualitas maupun kuantitas untuk tujuan penganugrahan gelar Sarjana Komputer (S. Kom)

Semarang, 11 Juli 2013

Dewan Penguji

Nova Rijati, S.Si, M.Kom
Anggota Penguji 1

Elkaf Rahmawan P, M. Kom
Anggota Penguji 2

Sendi Novianto, S.Kom, M.T
Ketua Penguji

PERNYATAAN KEASLIAN TUGAS AKHIR

Sebagai mahasiswa Universitas Dian Nuswantoro, yang bertanda tangan di bawah ini, saya :

Nama Pelaksana : Bely Arifpriyanto

NIM : A11. 2008. 03998

Menyatakan bahwa karya ilmiah saya yang berjudul :

PENYEMBUNYIAN PESAN *TEXT* TERENKRIPSI MENGGUNAKAN METODE KRIPTOGRAFI *STREAM CIPHER* DAN STEGANOGRAFI *END OF FILE* (EOF) DENGAN *FILE* INDUK PDF

Merupakan karya asli saya (kecuali cuplikan dan ringkasan yang masing-masing telah saya jelaskan sumbernya). Apabila di kemudian hari, karya disinyalir bukan merupakan karya asli saya, yang disertai dengan bukti-bukti yang cukup, maka saya bersedia untuk dibatalkan gelar saya beserta hak dan kewajiban yang melekat pada gelar tersebut. Demikian surat pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Semarang

Pada tanggal : 11 Juli 2013

Yang menyatakan

(Bely Arifpriyanto)

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai mahasiswa Universitas Dian Nuswantoro, yang bertanda tangan dibawah ini, saya :

Nama : Bely Arifpriyanto

NIM : A11. 2008. 03998

Demi mengembangkan Ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Dian Nuswantoro Hak Bebas Royalti Non-Ekskusif (*non-exclusif Royalti-Free Right*) atas karya ilmiah saya yang berjudul :

PENYEMBUNYIAN PESAN *TEXT* TERENKRIPSI MENGGUNAKAN METODE KRIPTOGRAFI *STREAM CIPHER* DAN STEGANOGRAFI *END OF FILE* (EOF) DENGAN *FILE* INDUK PDF

beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Ekseklusif ini Universitas Dian Nuswantoro berhak untuk menyimpan, mengsalin ulang (memperbanyak), menggunakan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya dan menampilkan/mempublikasikannya di internet atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Universitas Dian Nuswantoro, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian surat pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Semarang

Pada tanggal : 11 Juli 2013

Yang menyatakan

(Bely Arifpriyanto)

UCAPAN TERIMA KASIH

Dengan memanjatkan puji syukur kehadirat Allah, Tuhan yang Maha Pengasih dan Maha Penyayang yang telah melimpahkan segala rahmat-Nya kepada penulis sehingga laporan Tugas Akhir dengan judul "Penyembunyian Pesan *Text* Terenkripsi Menggunakan Metode Kriptografi *Stream Cipher* Dan Steganografi *End Of File* (EOF) Dengan *File* Induk PDF" dapat penulis selesaikan sesuai dengan rencana karena dukungan dari berbagai pihak yang tidak ternilai besarnya. Oleh karena itu penulis menyampaikan terima kasih kepada :

1. Dr. Ir. Edi Noersasongko, M. Kom, selaku Rektor Universitas Dian Nuswantoro Semarang.
2. Dr. Abdul Syukur, selaku Dekan Fakultas Ilmu Komputer Universitas Dian Nuswantoro Semarang.
3. Dr. Heru Agus Santoso, selaku Ka. Progdi Teknik Informatika.
4. L. Budi Handoko, M. Kom, selaku pembimbing tugas akhir yang memberikan semangat, dukungan, membantu pemunculan ide penelitian, memberikan informasi referensi yang penulis butuhkan dan bimbingan yang berkaitan dengan penelitian penulis.
5. Dosen-dosen pengampu pada Fakultas Ilmu Komputer Teknik Informatika Universitas Dian Nuswantoro Semarang yang telah memberikan ilmu dan pengalamannya masing-masing, sehingga penulis dapat mengimplementasikan ilmu yang telah disampaikan.
6. Teman-teman seperjuangan angkatan 2008, yang telah memberikan semangat dan dukungan dalam penyelesaian Tugas Akhir ini.

Semoga Tuhan Yang Maha Esa memberikan balasan yang lebih besar kepada beliau-beliau, dan pada akhirnya penulis berharap bahwa penulisan laporan tugas akhir ini dapat bermanfaat dan berguna sebagaimana fungsinya.

Semarang, Juni 2013

Penulis

ABSTRAK

Pada jaman sekarang ini, internet sudah menjamur di semua kalangan baik kalangan muda maupun kalangan bisnis. Kita sebagai orang umum juga harus dipaksa untuk menggunakan internet, baik itu untuk keperluan pengiriman data maupun hanya sekedar berkirim pesan pendek berbentuk *chatting* menggunakan *handphone*. Akan tetapi, dalam pengiriman data tersebut banyak pihak yang tidak berkepentingan ingin mendapatkan data yang dikirimkan tersebut.

Oleh karena itu, dalam penelitian ini penulis mempunyai pemikiran untuk membuat aplikasi untuk mengamankan data yang penting. Dalam hal ini, hanya berfokus pada teks. Untuk metode yang diterapkan dalam sistem keamanan ini, penulis menggunakan gabungan dua buah metode yaitu kriptografi dan steganografi. Hal ini dilakukan untuk menjaga keamanan data setelah di kriptografi selanjutnya dilakukan penyimpanan ke *file* lain yang sering kita sebut steganografi.

Dalam kriptografi ini, pesan akan dienkripsi atau diacak sedemikian rupa sehingga orang lain tidak dapat mengetahui apa yang ada dalam pesan tersebut. Pada metode kriptografi ini, penulis menggunakan algoritma *stream cipher* sebagai algoritma yang paling cocok digunakan untuk mengacak pesan atau menyandikan pesan tersebut.

Setelah pesan dapat tersandikan dengan baik, langkah selanjutnya adalah melakukan steganografi. Dalam steganografi, pesan yang tadi sudah terenkripsi dengan baik kemudian disembunyikan pada *file* lain yang dirasa tidak terlalu penting apabila dilihat oleh orang lain menggunakan teknik *End Of File* (EOF). Hal ini dilakukan untuk mengaburkan pandangan manusia supaya pesan yang ada di dalamnya masih tetap terjaga. Setelah semua langkah tersebut selesai, baru pesan dapat dikirimkan kepada pihak penerima tanpa diketahui oleh orang lain.

Kata kunci : kriptografi, *stream cipher*, steganografi, *End of File* (EOF).

Xi + 63 halaman + 9 tabel + 44 gambar

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

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.