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

Bely Arifpriyanto
Fakultas Ilmu Komputer, Universitas Dian Nuswantoro, Semarang 50131
E-mail : bely.lock@gmail.com

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).

1. PENDAHULUAN

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.

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.

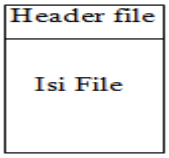
2. TINJAUAN PUSTAKA

2.1 *File*

File atau Berkas adalah sekumpulan data (informasi) yang berhubungan yang diberi nama dan tersimpan di dalam media penyimpanan sekunder (*secondary storage*). *File* memiliki ekstensi. Ekstensi berkas merupakan penandaan jenis berkas lewat nama berkas. Ekstensi biasanya ditulis setelah nama berkas dipisahkan dengan sebuah tanda titik. Pada sistem yang lama (MS-DOS) ekstensi hanya diperbolehkan maksimal 3 huruf, contohnya : *exe, bat, com, txt*. Batasan itu dihilangkan pada sistem yang lebih baru (Windows), contohnya : *mpeg,* java. Pada UNIX bahkan dikenal ada *file* yang memiliki lebih dari satu ekstensi, contohnya : *tar. z, tar. gz* (Sukrisno & Utami, 2007).

Struktur pada *file* terdiri dari 2 bagian yaitu *header file* dan isi *file*. Pada *header file* terdapat kode *biner* maupun kode ASCII yang berisikan tentang fungsi utama

pada *file*. Pada isi *file* terdapat isi dari *file* yang telah terbentuk baik berupa *text*, lagu, *video*, dll. Di bawah ini merupakan gambar struktur *file* yang ada pada semua *file*.



Gambar : Struktur *File*

2.1.2 Operator Logika

Operator logika adalah simbol-simbol yang digunakan untuk melakukan ekspresi terhadap data-data logika. Proses operasi tersebut akan menghasilkan salah satu dari dua jenis nilai kebenaran yaitu *TRUE* dan *FALSE* atau 1 dan 0. Simbol-simbol operator logika tersebut dapat dilihat pada tabel yang ada di bawah ini :

Tabel : Tabel Operator Logika

Operator	Keterangan
Not	Tidak
And	Dan
Or	Atau
Xor	*Exclusive Or*

berkurang sehingga sukar untuk menentukan posisi yang tepat bahkan tidak dapat menentukan posisi.

2.1.3 XOR

Operator biner XOR banyak digunakan dalam perhitungan biner untuk algoritma kriptografi tertentu. Notasi matematis untuk operator XOR adalah . Operator XOR merupakan operator yang digunakan untuk dua buah ekspresi. Operator XOR akan menghasilkan nilai *true* atau 1 jika kedua ekpresi memiliki nilai yang berbeda. Operator xor akan menghasilkan nilai 0 atau 0 jika kedua espresi bernilai sama.

Tabel : Aturan Nilai Kebenaran pada Operator XOR (Nathasia & Wicaksono, 2011)

Ekspresi1	Ekspresi2	Ekspresi 1 XOr Ekspresi2
0	0	0
0	1	1
1	0	1
1	1	0

2.2 Kriptografi

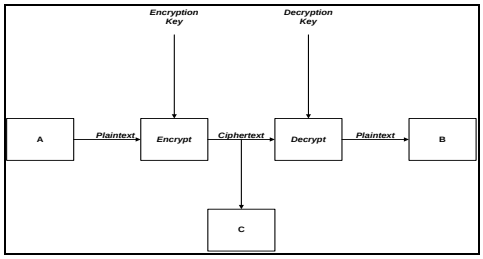
Kriptografi merupakan sebuah ilmu yang digunakan untuk penyandian data. Ada tiga istilah yang berkaitan dengan proteksi data yaitu kriptografi, kriptologi, dan kriptanalisis. Ada 4 syarat yang perlu dipenuhi, yaitu:

1.Kerahasiaan. Pesan (plaintext) hanya dapat dibaca oleh pihak yang memliki kewenangan.

2.*Autentikasi*. Pengirim pesan harus dapat diidentifikasi dengan pasti, penyusup harus dipastikan tidak bisa berpura-pura menjadi orang lain.

3.*Integritas*. Penerima pesan harus dapat memastikan bahwa pesan yang dia terima tidak dimodifikasi saat dalam proses transmisi data.

4.*Non-Repudiation*. Pengirim pesan harus tidak bisa menyangkal pesan yang dia kirimkan.



Gambar : Skenario Komunikasi Dasar Kriptografi

Enkripsi adalah istilah dalam kriptografi yang berarti proses menyandikan suatu data atau informasi berbentuk teks menjadi bentuk lain yang tidak dapat dipahami (Nathasia & Wicaksono, 2011).

2.2.1. Gambaran Umum dalam *Stream Cipher*

Stream cipher merupakan algoritma kriptografi yang ditemukan oleh Mayor J. Maugborne dan G. Vernam. Algoritma ini merupakan algoritma berjenis symetric key yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara stream cipher dimana cipher berasal dari hasil XOR antara bit plaintext dan bit key (Nathasia & Wicaksono, 2011). Algoritma stream cipher diadopsi dari one-time pad cipher, dimana dalam hal ini karakter diganti dengan bit (0 atau 1). Dengan kata lain, stream cipher merupakan versi lain dari one-time pad cipher.

2.3. Steganografi

Secara umum steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia dengan segala cara sehingga selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut (Nani, 2011).

2.3.1 Metode *End of File* (EOF)

Teknik ini menggunakan cara dengan menyisipkan data pada akhir file. Sehingga, tidak akan mengganggu kualitas data awal yang akan disisipkan pesan. Namun, ukuran file setelah disisipkan pesan rahasia akan bertambah (Sukrisno & Utami, 2007; Wandani et al. , 2012). Sebab, ukuran file yang telah disisipkan pesan rahasia sama dengan ukuran file sebelum disisipkan pesan rahasia ditambah dengan ukuran pesan rahasia yang disisipkan. Untuk mengenal data yang disisipkan pada akhir file, diperlukan suatu tanda pengenal atau simbol pada awal dan akhir data yang akan disisipkan.

3. METODE PENELITIAN

3.1 Obyek Penelitian

Di dalam tugas akhir ini penulis melakukan obyek penelitian menggunakan file induk berformat *.pdf yang akan disisipkan dengan pesan text berformat *.txt dimana file text tersebut merupakan inti isi pesan yang akan dituju kepada si penerima.

3.2 Fokus Penelitian

Pada fokus penelitian ini penulis mencoba membuat sebuah program atau aplikasi yang dapat menyembunyikan dan menyisipkan pesan text ke dalam file induk sehingga tidak tampak secara kasat mata.

3.3 Ruang Lingkup Penelitian

Dalam penelitian ini, penulis mempunyai ruang lingkup penelitian. Ruang lingkup penelitian merupakan batasan-batasan yang menyebabkan penelitian ini terbentuk. Adapun ruang lingkup dalam penelitian ini antara lain adalah :

a.Untuk file induk menggunakan format *.pdf dengan kapasitas 2 MB.

b.Untuk file pesan yang akan disisipkan bertipe *.txt dengan kapasitas 30 KB.

3.4 Metode Pengumpulan Data

Data yang dikumpulkan dalam penelitian ini merupakan data sekunder. Data diperoleh dari telaah pustaka dan dokumen yang didapat penulis dari pustaka yang mendukung, informasi dari internet, buku-buku dan artikel dari jurnal.

3.5 Metode Pengembangan Sistem

Langkah-langkah yang dilakukan adalah sebagai berikut :

a. Mengidentifikasi Kebutuhan Sistem

Adapun kebutuhan identifikasi sistem yang diperlukan dalam pembuatan aplikasi ini yaitu :

1. Identifikasi data

Data yang dibuat terdiri dari file induk, file pesan dan key password.

2. Identifikasi informasi

Informasi yang dihasilkan pada pembuatan aplikasi ini yaitu file pesan berhasil disembunyikan dan disisipkan ke dalam file induk.

b. Mengidentifikasi Kebutuhan Hardware / Software

Untuk mendukung dalam pengembangan aplikasi Penyembunyian Pesan Text Terenkripsi Menggunakan Metode Kriptografi Stream Cipher Dan Steganografi *End Of File* (EOF) Dengan File Induk PDF ini perlu diadakannya dukungan dari hardware / software yang memadahi, agar dalam pengembangannya yang akan dilakukan dapat menghasilkan sistem yang sesuai dengan kebutuhan yang ada.

c. Input

Input-an yang diperlukan dalam Aplikasi Penyembunyian Pesan Text Terenkripsi Menggunakan Metode Kriptografi Stream Cipher Dan Steganografi End Of File (EOF) Dengan File Induk PDF, untuk menyembunyikan dan menyisipkan pesan text ke file induk hanya melakukan pengoperasian dengan mengklik menu pilihan yang ada serta mengisi password sesuai kesepakatan antara pengirim dan penerima.

d. Output

Output yang dihasilkan adalah file pesan text dapat dibaca dengan mengisi key password yang telah disepakati dan membuang file induk yang tidak dibutuhkan.

3.6 Pengujian Program (Testing)

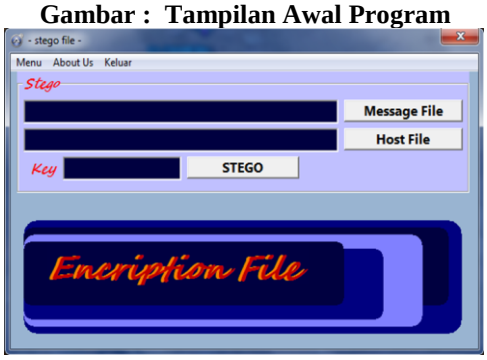
Untuk menguji aplikasi yang telah dibuat, penulis menggunakan 5 buah unit testing yaitu verifikasi, validasi, deteksi error, pengubahan format file induk *.pdf yang sudah terenkripsi menjadi file *.docx dan hasil apabila kapasitas file pesan melebihi kapasitas file induk. Sedangkan untuk verifikasi dan validasi dilakukan melalui

kuisioner, dimana penulis dapat mengetahui tanggapan dari responden terhadap aplikasi yang telah dibuat dan bagian ini akan dibahas pada pokok bahasan selanjutnya. Sedangkan deteksi error dilakukan melalui pengujian *Graphical User Interface* (GUI) dengan bentuk pengujian *black box* dan white box.

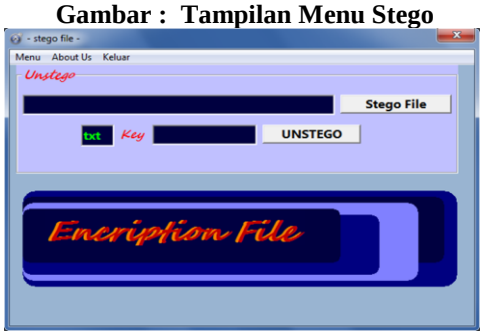
4. PERANCANGAN DAN HASIL IMPLEMENTASI

Pada tahap ini diuraikan hasil pengembangan aplikasi

Gambar : Tampilan Awal Program



Gambar : Tampilan Menu Stego



Gambar : Tampilan Menu Unstego

5. Kesimpulan

Berdasarkan hasil pengujian, maka penulis menarik kesimpulan bahwa :

1.Berdasarkan implementasi aplikasi yang telah dibuat, membuktikan bahwa *Stream Cipher* dan EOF merupakan 2 (dua) buah metode yang cocok untuk diimplementasikan pada aplikasi penyembunyian pesan.

2.Berdasarkan hasil implementasi dan kuesioner dari responden, hasil implementasi aplikasi dapat dikategorikan bahwa aplikasi ini aman dan tidak menimbulkan kecurigaan pada pihak lain, dilihat dari file hasil penyisipan pesan.

3.Proses ekstraksi berjalan lancar, dimana file hasil dipisah menjadi file pesan dan file induk, dimana pada proses ini tidak terjadi kerusakan file.

4.Hasil implementasi aplikasi menunjukkan bahwa ukuran file hasil merupakan gabungan dari file induk dan file pesan.

DAFTAR PUSTAKA

Aditya, Y. , Pratama, A. , & Nurlifa, A. (2010). Studi pustaka untuk steganografi dengan beberapa metode. Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010), 2010, 32-35.

Irfianti, A. D. (2007). METODE PENGAMANAN ENSKRIPSI RC4 STREAM CIPHER UNTUK APLIKASI. Seminar Nasional Aplikasi Teknologi Informasi 2007 (SNATI 2007), 2007(Snati), 4.

Iswahyudi, C. , Setyaningsih, E. , & Widyastuti, N. (2012). Pengamanan kunci enkripsi citra pada algoritma super enkripsi menggunakan metode end of file. Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) Periode III, (November), 278-285.

Nani, P. A. (2011). PENERAPAN ENKRIPSI ALGORITMA BLOWFISH PADA PROSES STEGANOGRAFI METODE EOF. Penerapan Enkripsi Algoritma Blowfish Pada Proses Steganografi Metode Eof, 1-6.

Nathasia, N. D. , & Wicaksono, A. E. (2011). Penggunaan Teknik Kriptografi Stream Cipher untuk Pengamanan Basis Data. Jurnal Basis Data, ICT Research Center UNAS, 6(1), 1-22.

Setiawan, A. , Endrawan, D. , Fathoni, R. , & P, S. B. (2011). Rapid Application Development, 1-12.

Sukrisno, & Utami, E. (2007). IMPLEMENTASI STEGANOGRAFI

TEKNIK EOF DENGAN GABUNGAN ENKRIPSI RIJNDAEL , SHIFT CIPHER DAN FUNGSI HASH MD5. Seminar Nasional Teknologi 2007 (SNT 2007), (November), 1-16.

Wandani, H. , Budiman, M. , & Sharif, A. (2012). Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem. Alkhawarizmi. Retrieved from http: //jurnal. usu. ac. id/index. php/alkhawarizmi/article/view/500