KRIPTOGRAFI FILE BERTIPE *EXECUTABLE* DENGAN METODE ENKRIPSI *VIGENERE CIPHER* GUNA MELINDUNGI DARI *CRACKING SOFTWARE*

Fitri Suryani[1], Dr. Ir. Dwi Eko Waluyo[2]

Mahasiswa Jurusan Sistem Informasi[1], Dosen Pembimbing[2]

Universitas Dian Nuswantoro Semarang

Abstrak

Perangkat lunak merupakan suatu perangkat yang memudahkan pekerjaan manusia. Penggunaan perangkat lunak atau software akan mengefisiesikan waktu dan meringankan pekerjaan pengguna. Ada beberapa *software* komerisal yang aktifasinya menggunakan serial *key*. Beberapa pembajak *software* mampu membongkar algoritma pengecekan serial *key software* komersial tersebut, sehingga beberapa *software* komersial tersebut bisa dibajak dan bisa menyebabkan kerugian finansial bagi pengembang *software* tersebut. Dari permasalahan tersebut maka penulis mencoba membuat Kriptografi File Bertipe *Executable* Dengan Metode Enkripsi *Vigenere Chiper* Guna Melindungi Dari *Cracking Software.* File *executable* itu sendiri merupakan sebuah file yang bisa dieksekusi secara langsung tanpa membutuhkan program lain. Sedangkan kriptografi dijadikan solusi permasalahan ini karena kriptografi merupakan ilmu yang telah diaplikasikan untuk pengamanan data. Kriptografi dapat digunakan untuk mengamankan data-data penting pada sebuah file. Data yang terkandung dalam file disandikan atau dienkripsiuntuk diubah menjadi simbol tertentu sehingga hanya orang tertentu saja yang dapat mengetahui isi dari data tersebut. Pembuatan kriptografi ini bertujuan untuk melindungi *software* dari pembajakan sehingga tidak akan meminimalisir kerugian finansial bagi pengembang s*oftware.* Banyak teknik cracking yang dapat digunakan para pembajak software untuk menjebol algoritma software. Dalam pembuatan kriptografi ini penulis menggunakan metode enkripsi *vigenere chiper*. Untuk menyandikan sebuah pesan digunakan sebuah tabel alfabet yang disebut tabel *vigenere*. Aplikasi yang akan dibuat nantinya tidak akan menyandikan 26 karakter alfabetis namun akan menyandikan 256 karakter key ASCII. Laporan tugas akhir akan meguraikan salah satu cara mengamankan *software* komersial dengan teknik kriptografi. Hal-hal apa yang menjadi kendala dalam

pembuatan sistem dan apa yang menjadi kelebihan sistem akan diulas pada bagian akhir tugas akhir ini.

Kata kunci : Kriptografi, file executable, *software*, *cracking*, Metode *Vigenere Cipher*.

1. LATAR BELAKANG

Perangkat lunak merupakan suatu perangkat atau alat yang digunakan oleh pengguna atau instansi perusahaan untuk meringankan pekerjaaan mereka. Penggunaan perangkat lunak akan mengefisiensikan waktu dan meringankan pekerjaan pengguna. Tidak sedikit instansi perusahaan yang memakai.

Ada beberapa perangkat lunak atau *software* komersial yang aktifasinya menggunakan serial *key*. Beberapa pembajak *software* menggunakan celah keamanan tersebut untuk membajak *software*. Pembajak *software* yang mengetahui algoritma pengecekan serial *key software* komersial tersebut akan membongkar algoritmanya.

Berdasar pada analisis dari masalah tersebut maka penulis mengusulkan judul penelitian "Kriptografi File Bertipe *Executable* Dengan Metode Enkripsi *Vigenere Chiper* Guna Melindungi Dari *Cracking Software "* sebagai bahan pertimbangan dalam proses pengamanan *software* komersial sehingga diharapkan mampu mengamankan suatu *software* komersial dari para pembajak *software* dan juga mampu meminimalisir kerugian finansial para pengembang *software* komersial.

2. RUMUSAN MASALAH

1) Bagaimana meminimalisir pembajakan *software* komersial sehingga mampu meminimalisir kerugian finansial bagi pengembang *software* komersial?
2) Bagaimana cara mengamankan *software* komersial dengan *kriptografi* menggunakan metode *Vigenere Chiper*?

3. TUJUAN PENELITIAN

Tujuan dari penelitian ini adalah untuk mengamankan *software* komersial dari pembajakan dengan enkripsi *Vigenere Chiper* sehingga menghasilkan file *executable* yang telah dikombinasikan dengan algoritma *Vigenere Chiper.*

4. LANDASAN TEORI

a) 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.

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.

b) File *executable* adalah sebuah file yang bisa dieksekusi secara langsung tanpa membutuhkan program lain. File executable hanya terdapat dalam sistem operasi DOS dan Windows. Pada umumnya file executable berekstensi .exe tetapi ada juga yang berekstensi .bat atau .com. Pada sistem operasi windows. Pada sistem operasi windows terdapat portable executable. Portable executable adalah format file untuk executable yang digunakan dalam versi 32-bit maupun 64-bit dari sistem operasi windows. Istilah "portable" mengacu pada fleksibilitas format dalam berbagai lingkungan arsitektur sistem operasi perangkat lunak. Format PE adalah struktur data yang merangkum informasi yang diperlukan untuk Windows OS loader untuk mengelola kode dieksekusi dibungkus. Ini termasuk referensi perpustakaan dinamis untuk menghubungkan ekspor, API dan tabel impor, data sumber daya manajemen dan thread-lokal (TLS) penyimpanan data. Pada sistem operasi NT, format PE digunakan untuk EXE, DLL, SYS (device driver), dan jenis file lainnya. Extensible Firmware Interface (EFI) spesifikasi menyatakan bahwa PE adalah format executable standar dalam lingkungan EFI.

c) Beberapa aplikasi menggunakan data yang bukan hanya bilangan

tetapi juga huruf dari alfabet dan karakter khusus lainnya. Data semacam ini disebut dengan data alfanumerik dan mungkin dapat ditunjukkan dengan kode numerik. Jika bilangan-bilangan dimasukkan dalam data, maka bilangan-bilangan tersebut juga dapat ditunjukkan dengan kode khusus.

Set karakter alfanumerik secara khusus mencakup 26 huruf alfabet (termasuk huruf besar dan huruf kecil), angka dalam digit sepuluh desimal, dan sejumlah simbol seperti +, =, *, $, …, dan !. Dua kode alfabet yang paling umum dipakai adalah ASCII (American Standard Code for Information Interchange) dan EBCDIC (Extended Binary Coded Decimal Interchange Code). ASCII merupakan kode 7-bit dan EBCDIC berupa kode 8- bit. Jika suatu komputer menangani 8-bit (1-byte) kode lebih efisien, versi 8-bit, disebut dengan ASCII-8 juga telah dikembangkan.

Sistem American Standard Code for Information Interchange (ASCII): ASCII dan EBCDIC merupakan cikal bakal dari set karakter lainnya. ASCII merupakan set karakter yang paling umum digunakan hingga sekarang. Set karakter ASCII terdiri dari 128 – (27) buah karakter yang masing-masing memiliki lebar 7-bit atau gabungan tujuh angka 0 dan 1, dari 0000000 sampai dengan 1111111. Mengapa 7-bit? Karena komputer pada awalnya memiliki ukuran memori yang sangat terbatas, dan 128 karakter dianggap memadai untuk menampung semua huruf Latin dengan tanda bacanya, dan beberapa karakter kontrol. ASCII telah dibakukan oleh ANSI (American National Standards Institute) menjadi standar ANSI X3.4-1986. (Kode-kode ASCII dapat dilihat pada lampiran.)

d) Pengertian Kriptografi

Kriptografi merupakan sebuah ilmu yang digunakan untuk penyandian data. Kriptografi telah dikenal dan dipakai cukup lama sejak kurang lebih tahun 1900 sebelum masehi pada prasasti-prasasti kuburan.

Ilmu Kriptografi sebenarnya sudah mulai dipelajari manusia sejak tahun 400 SM, yaitu pada zaman Yunani kuno. Dari catatan bahwa “Penyandian Transposisi” merupakan sistem kriptografi pertama yang digunakan atau dimanfaatkan. Bidang ilmu ini terus berkembang seiring dengan kemajuan peradaban manusia, dan memegang peranan penting dalam strategi peperangan yang terjadi dalam sejarah manusia, mulai dari sistem kriptografi “Caesar Chiper” ang terkenal pada zaman Romawi kuno, “Playfair Cipher” yang digunakan Inggris dan “ADFVGX Cipher” yang digunakan Jerman pada Perang Dunia I hingga algoritma-algoritma kriptografi rotor yang populer pada Perang Dunia II , seperti Sigaba / M-134 (Amerika

Serikat), Typex (Inggris), Purple (Jepang), dan mesin kriptografi legendaris Enigma (Jerman). Sejarah telah dipenuhi oleh contoh-contoh orang yang berusaha merahasiakan informasi rahasia mereka dari orang lain.

Seiring dengan perkembangan zaman, kebutuhan akan metode yang lebih canggih tidak dapat dihindari. Sekarang, dengan adanya era informasi, kebutuhan itu menjadi lebih penting lagi. Dengan adanya fasilitas internet, maka permintaan akan pelayanan informasi semakin meningkat dengan seiringnya perkembangan teknologi. Pertukaran data yang sensitif seperti nomor account kartu kredit, sudah sering dilakukan dan menjadi hal yang biasa di dalam dunia internet. Karena itu, melindungi data sudah menjadi hal penting yang sangat kruisal di dalam hidup.

Ada tiga istilah yang berkaitan dengan proteksi data yaitu kriptografi, kriptologi, dan kriptanalisis. Arti ketiganya kurang lebih sama. Secara teknis, kriptologi adalah ilmu yang mempelajari tentang komunikasi pada jalur yang tidak aman beserta masalah-masalah yang berhubungan dengan itu.

Kriptografi berasal dari kata "Crypto" yang berarti rahasia dan "graphy" yang berarti tulisan. Jadi, dapat dikatakan bahwa kriptografi adalah tulisan yang tersembunyi. Dengan adanya tulisan yang tersembunyi ini, orang-orang tidak mengetahui bagaimana tulisan tersebut disembunyikan dan tidak mengetahui bagaimana cara membaca maupun menerjemahkan tulisan tersebut. William Stallings mendefinisikan kriptografi sebagai "the art and science of keeping messages secure.

Kriptografi berbasis pada algoritma pengkodean data informasi yang mendukung kebutuhan dari dua aspek keamanan informasi, yaitu *secrecy* (perlindungan terhadap kerahasiaan data informasi) dan *authenticity* (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan.

Kriptografi menjadi dasar bagi keamanan komputer dan jaringan karena merupakan sarana bagi distribusi data dan informasi. Sehingga data dan informasi tersebut harus diamankan agar hanya orang-orang yang berhak mengaksesnya yang dapat mengetahui maupun menggunakan data tersebut. Salah satu cara yang paling banyak digunakan dalam mengamankan data adalah dengan kriptografi. Data-data tersebut diamankan dengan sedemikian rupa oleh pengirim sehingga orang lain tidak dapat mengenali data tersebut.

Pembakuan penulisan pada kriptografi dapat ditulis dalam bahasa matematika. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan asli (*plaintext*)

menjadi suatu pesan dalam bahasa sandi (*ciphertext*).

$C = E(M)$, dimana :

M=pesan asli

E = proses enkripsi

C = pesan dalam bahasa sandi

(untuk ringkasnya disebut sandi)

Sedangkan dekripsi adalah proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali.

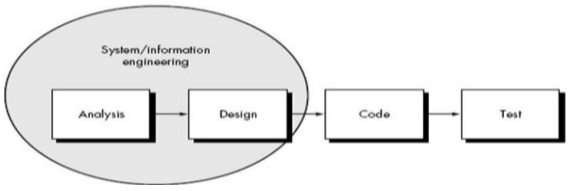
$M=D(C)$

D = proses dekripsi

Umumnya, selain menggunakan fungsi tertentu dalam melakukan enkripsi dan dekripsi, seringkali fungsi itu diberi parameter tambahan yang disebut dengan istilah kunci.

5. METODE PENELITIAN

Tahap pengembangan dimulai dengan analisa sampai dengan pengujian. Dimana setiap tahap harus diselesaikan terlebih dahulu secara penuh diteruskan ke tahap berikutnya untuk menghindari terjadinya sebuah pengulangan tahapan.



Gambar : Pengembangan Sistem Dengan Model Squential Liniear

6. HASIL PENELITIAN

a. Tampilan Aplikasi Kriptografi File Executable

Gambar. Tampilan Aplikasi Kriptografi File Executable

b. Tampilan Aplikasi Kriptografi File Executable setelah memasukkan program file *.exe yang akan dienkripsi

Gambar : Tampilan Aplikasi Kriptografi File Executable setelah memasukkan program file *.exe yang akan dienkripsi.

c. Tampilan messagebox yang menunjukkan aplikasi kriptografi ini berhasil mengenkrip program *.exe

Gambar : Tampilan Messagebox aplikasi Kriptografi yang menunjukkan bahwa aplikasi berhasil mengenkrip sebuah software *.exe

7. KESIMPULAN

1) Aplikasi ini membantu para pembuat software komersial dalam mengamankan software yang mereka komerisialkan dari tangan para pembajak software. Banyaknya teknik-teknik yang digunakan para pembajak software dalam membobol software komersial membuat penulis berinisiatif membuat aplikasi ini untuk melindungi software para pembuat software dari tangan para pembajak software.

2) Aplikasi ini dibuat dengan menggunakan algoritma Vigenere cipher. Pada penjelasan dari laporan program diatas telah dijelaskan jalannya sebuah aplikasi enkripsi EXE V3Lock dalam mengenkripsi sebuah file EXE.

8. SARAN

1) Aplikasi ini telah dirancang sedemikian rupa dan sampai saat ini aplikasi enkripsi EXE V3Lock aman dari tangan para pembajak software. Belum ada yang mampu membongkar algoritma kunci dari aplikasi ini sehingga sampai saat aplikasi ini masih aman. Apabila kelak terdapat bug-bug atau cela untuk membongkar aplikasi ini disarankan bug-bug tersebut ditutup atau dibenahi sebagai tahap pengembangan berikutnya dari program atau aplikasi ini.

2) Untuk tahap pengembangan selanjutnya juga disarankan pula untuk memakai algoritms enkripsi bertingkat sebagai pengembangan dari enkripsi Vigenere Cipher dalam kriptografi file EXE.

DAFTAR PUSTAKA

Munir, Rinaldi. (2006). *Kriptografi*. Bandung : Informatika

Ariyus, Dony. (2008). *Pengantar Ilmu Kriptografi : Teori, Analisis dan Implementasi.* Yogyakarta : Andi Offset

Hermawan, Julius. (2004). *Analisa Desain & Pemrograman Berorientasi Obyek dengan UML dan Visual Basic.net.* Jakarta : Andi

Ariyus, Dony. (2005). *Kamus Hacker*. Yogyakarta : Andi Offset

Anonimous, *ASCII table and Extended ASCII Table*, www.asciitable.com, 10 Agustus 2009

Prastowo, Andi. *Metode Penelitian Kualitatif dalam Perspektif Rancangan Penelitian.* Yogyakarta : Ar-Ruzz Media. 2012.

Eko Hari Rachmawanto (2010). *Teknik Keamanan Data Menggunakan Kriptografi dengan Algoritma Vernam Cipher dan Steganografi dengan Metode End Of File (EOF).* Laporan Tugas Akhir. Universitas Dian Nuswantoro.