Implementasi Kriptografi menggunakan Algoritma Double X3 sebagai Add on pada Mozilla Firefox

Ramdani
STMIK Bani Saleh, ramdaniabenk2013@gmail.com

Amat Suroso
STMIK Bani Saleh, ahmad_suroso04@yahoo.com

ABSTRAK

Perkembangan teknologi internet saat ini telah mengalami kemajuan yang sangat pesat dan salah satunya adalah pengiriman pesan secara elektronik yang disebut *e-mail*. Seiring dengan perkembangan zaman, pengiriman pesan melalui *e-mail* semakin meningkat sehingga diperlukan sistem keamanan yang mampu menjaga kerahasiaan pesan yang dikirim melalui *e-mail*. Sering terjadinya penyadapan pesan oleh pihak-pihak yang tidak bertanggung jawab membuat penulis melakukan analisis dan membuat aplikasi *add-ons* yang mampu menjaga keamanan *e-mail*. Aplikasi tersebut dibuat dengan penggabungan tiga jenis algoritma cipher yaitu *subtitusi cipher, transposisi cipher* dan *XOR cipher*.

Untuk mempersingkat algoritma yang dipakai, penulis memberi nama menjadi algoritma Double X3 untuk mengenkripsi dan mendekripsi pesan yang akan dikirim pada *Mozilla Firefox*. *Mozilla Firefox* dipilih karena disamping merupakan web browser yang cukup banyak digunakan oleh para pengguna internet, juga terdapat fitur yang bernama *Add-on* yang telah secara luas bebas untuk dikembangkan oleh siapa saja serta aplikasi yang *open source* yang selalu melakukan perkembangan terhadap pengguna aplikasi ini.

Semoga dengan adanya *Add-on* ini dapat membantu mengamankan informasi pengguna pada saat mengirim pesan melalui media internet.

Kata Kunci : Kriptografi, Enkripsi, Email, Mozilla Firefox, Add-on

PENDAHULUAN

Latar Belakang Masalah

Sebagai kebutuhan utama dalam bidang komunikasi dan informasi saat ini, teknologi internet mampu menghadirkan informasi dengan cepat dan efisien. Salah satu layanan yang disediakan dengan adanya jaringan internet adalah surat elektronik. Surat elektronik (email) adalah pesan, umumnya berupa teks, yang dikirim dari pengirim kepada penerima melalui jalur internet. Namun dengan cepatnya perkembangan email juga menyebabkan adanya kebutuhan akan keamanan data yang dikirim. Karena keamanan data di surat elektronik tidaklah terjamin dan selalu ada resiko terbuka untuk umum, dalam artian semua isinya dapat dibaca oleh orang lain. Hal ini disebabkan karena surat elektronik itu akan melewati banyak server sebelum sampai di tujuan. Tidak tertutup kemungkinan ada orang yang menyadap surat elektronik yang dikirimkan tersebut . Salah satu media untuk menggunakan layanan email adalah dengan menggunakan Aplikasi web browser.

Web Browser merupakan software yang digunakan untuk menampilkan dan melakukan interaksi dengan dokumen-dokumen yang disediakan oleh server web. Oleh karena itu dari sisi penguna sendiri perlu adanya suatu cara untuk dapat mengurangi resiko terjadinya penyadapan suatu informasi. Salah satu cara untuk melindungi data yang terkirim dalam jaringan internet adalah dengan menggunakan kriptografi sehingga kerahasiaan data yang dikirim dapat terjamin. Kriptografi adalah metode untuk menjaga kerahasiaan pesan dengan cara mengubahnya dari satu bentuk ke bentuk lainnya yang tidak dapat dimengerti lagi artinya. Pada saat ini kriptografi memiliki beberapa jenis, dari kriptografi klasik sampai kriptografi modern. Penggunaan satu algoritma kriptografi untuk pengamanan teknologi informasi masih dianggap kurang aman, karena semakin kompleks algoritma yang digunakan untuk pengamanan data, maka

semakin sulit untuk memecahkan keamanan yang dibentuk oleh gabungan dari beberapa algoritma yang berbeda.

Berangkat dari permasalahan tersebut, penulis tertarik untuk menggabungkan tiga algoritma cipher untuk mengamankan suatu data yang ingin dikirim yaitu Shift cipher, Columnar transposition, dan XOR cipher. Untuk mempersingkat algoritma yang dipakai, penulis memberi nama ' Double X3'. Karena pada prosesnya terdapat dua cipher XOR dari tiga jenis algoritma cipher yang berbeda dalam proses enkripsi maupun dekripsi. Dalam mengimplementasikan algoritma ini penulis menggunakan web browser mozilla firefox, karena disamping merupakan web browser yang cukup banyak digunakan oleh para pengguna internet pada web browser ini juga terdapat fitur yang bernama Add-on yang berfungsi sebagai repositori untuk menginstal perangkat tambahan pada aplikasi Mozilla. Juga telah secara luas bebas untuk dikembangkan oleh siapa saja serta aplikasi yang open source yang selalu melakukan perkembangan terhadap pengguna aplikasi ini.

Dengan adanya Add-on ini, memungkinkan pengguna untuk mengembangkan fitur enkripsi surat elektronik pada Mozilla Firefox. Maka judul yang diambil pada penelitian ini adalah "Implementasi Kriptografi menggunakan Algoritma Double X3 sebagai Add on pada Mozilla Firefox ".

TINJAUAN PUSTAKA

Pengertian Kriptografi

Kriptografi (cryptography) berasal dari bahasa Yunani yang terdiri atas kata "cryptos" yang artinya rahasia, dan "graphein" yang artinya tulisan. Berdasarkan terminologi, kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara mengubahnya dari satu bentuk ke bentuk lainnya yang tidak dapat dimengerti lagi artinya. Kriptografi disebut ilmu, karena didalamnya menggunakan berbagai metode (rumusan), dan sebagai seni, karena didalamnya membutuhkan teknik khusus dalam mendesainnya. (Rinaldi Munir, 2006).

Kriptografi merupakan cabang ilmu dari kriptologi. Pelaku kriptografi ialah kriptografer (cryptographer), yang bertugas untuk mengubah plainteks menjadi cipherteks dengan algoritma dan kunci tertentu. Sedangkan lawan dari kriptografi adalah kriptanalisis (cryptanalysis), merupakan ilmu yang memecahkan cipherteks menjadi plainteks kembali tanpa mengatahui kunci, dan pelakunya ialah kriptanalis (criptanalys).

Setiap algoritma kriptografi terdiri dari algoritma enkripsi (E) dan algoritma dekripsi (D). Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu himpunan yang berisi elemen plaintext dan himpunan yang berisi elemen ciphertext. Secara umum dapat digambarkan secara matematis sebagai berikut:

$$Ek(P) = C \ (proses\ enkripsi)$$

$$Dk(C) = P \ (proses\ dekripsi)$$

$$Dk(E(P)) = P \ (proses\ enkripsi)$$

Dalam proses enkripsi, plaintext disandikan dengan P dengan suatu kunci K lalu dihasilkan pesan C. Pada proses dekripsi, C diuraikan dengan menggunakan kunci K sehingga menghasilkan P yang sama dengan sebelumnya.

Tujuan mendasar dari kriptografi itu sendiri adalah sebagai berikut :

a. Kerahasiaan (confindentiality)
Memastikan bahwa tidak ada yang dapat membaca pesan selain orang yang dituju.

b. Integritas data (data integrity)
Suatu layanan yang menjamin bahwa pesan yang asli tidak mengalami perubahan.

c. Otentikasi (authentication)
Mengidentifikasi pihak-pihak yang berkomunikasi maupun mengidentifikasi kebenaran pesan.

d. Ketiadaan penyangkalan (non-repudiation)
Layanan yang mencegah terjadinya penyangkalan oleh pengirim pesan atau penyangkalan oleh penerima pesan sudah menerima pesan.

Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu:

a. Enkripsi
Merupakan proses pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan asli disebut plaintext, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan cipher atau kode.

b. Dekripsi
Merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks asli), disebut dengan dekripsi pesan.

c. Kunci

Yang dimaksud di sini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia (private key) dan kunci umum (public key).

METODE PENELITIAN

Pada bab ini akan dijelaskan tentang analisis terhadap masalah yang ada berdasarkan teori yang ada pada bab sebelumnya. Analisis ini bertujuan untuk menemukan solusi dari permasalahan dalam melakukan implementasi algoritma Doube X3 pada browser Firefox serta perancangan perangkat perangkat lunak yang dibangun.

a. Proses Enkripsi Shift Cipher

Tahap pertama dalam mengenkripsi pesan dengan *Shift Cipher* pada algoritma Double X3 yaitu mengambil seluruh pesan yang akan dienkripsi beserta kuncinya dan memeriksa setiap karakter yang ada. Apakah karakter-karakter yang ada telah didukung atau belum. Bila seluruh karakter telah didukung, selanjutnya adalah membandingkan banyaknya karakter pada pesan dan kunci. Bila karakter pada kunci lebih sedikit dari pesan maka sistem akan otomatis menambahkan beberapa karakter yang telah ditentukan sebelumnya pada kunci dengan hasil akhirnya yaitu jumlah karakter pada pesan sama dengan jumlah karakter pada kunci. Sedangkan karakter yang telah ditentukan oleh sistem dapat dilihat pada Tabel 2.1. Dan bila sebaliknya, maka beberapa karakter pada kunci akan dihapus dan disesuaikan dengan jumlah karakter pada pesan. Dan sebagai tambahan bila pada pesan terdapat perintah enter maka secara otomatis akan dikonversi menjadi karakter titik. Kemudian seluruh karakter pada kunci akan dijumlahkan dengan cara mengkonversikannya menjadi bilangan Desimal. Lalu hasilnya di-mod-kan dengan 94. Hasil inilah yang nantinya menjadi nilai pergeseran pada karakter.

b. Proses Enkripsi XOR Cipher pertama

Pada proses enkripsi XOR Cipher dalam algoritma Double X3 ini sedikit berbeda dengan teori pada bab 2. Proses awal yang dilakukan pada enkripsi ini adalah mengambil hasil dari *Shift Cipher* kemudian membandingkan jumlah karakter pada pesan dengan kunci. Bila karakter pada kunci lebih sedikit dari pesan maka maka sistem akan otomatis menambahkan beberapa karakter yang telah ditentukan sebelumnya oleh sistem pada kunci dengan hasil akhirnya yaitu jumlah karakter pada pesan sama dengan jumlah karakter pada kunci. Sedangkan karakter yang telah ditentukan oleh sistem dapat dilihat pada Tabel 3.1. Dan bila sebaliknya, maka beberapa karakter pada kunci akan dihapus dan disesuaikan dengan jumlah karakter pada pesan.

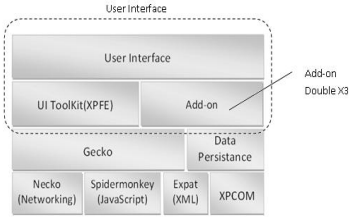
c. Proses Enkripsi Columnar Transposition

Untuk mengenkripsi *file* dengan algoritma *Columnar Transposition*, sistem mengambil seluruh karakter dari hasil *XOR Cipher* yang pertama secara berurutan. Kemudian karakter-karakter tersebut disusun ke dalam matriks dua dimensi dengan jumlah kolom yang sudah ditentukan yakni 6 sesuai dengan teori pada bab 2 dan jumlah baris yang dinamis sesuai dengan kebutuhan dari *file* atau sama dengan panjang file dibagi 6. Penyusunan karakter ini dimulai dengan baris pertama sampai kolom ke enam, kemudian kebaris berikutnya. Akan tetapi, karakter spasi dimasukkan pada proses ini. Sedangkan penambahan karakter di akhir plainteks hanya satu jenis karakter yaitu ‘ ‘ (spasi) dengan maksimum 5 *byte*. Karena panjang karakter modulo 6 adalah maksimum 5. Apabila karakter-karakter tersebut telah tersusun yang dimulai dari baris pertama sampai baris selanjutnya. Maka hasil penyusunan ulang karakter-karakter berdasarkan urutan kolom akan menghasilkan Cipherteks.

PEMBAHASAN

Analisa

Kinerja Perangkat Lunak



Gambar 1. Add-on Double X3 pada Arsitektur Mozilla Firefox

Pada arsitektur Mozilla Firefox, add-on Double X3 ini terdapat pada sub sistem dari User Interface. User Interface adalah satu lapisan utama antara pengguna dan mesin browser / render (Gecko). UI menyediakan berbagai fitur seperti sebagai halaman

web bookmark, pengaturan preferensi internet, visualisasi halaman web, download file, dan lain-lain. UI dapat di integrasikan dengan lingkungan desktop untuk menyediakan manajemen sesi peramban atau komunikasi dengan aplikasi desktop lainnya. Add-on sendiri memiliki beberapa jenis dalam kegunaannya.

Pada add-on Double X3 ini termasuk dalam jenis *extension. Extension* sendiri berfungsi untuk menambahkan fitur baru pada firefox atau mengubah fungsionalitas yang sudah ada. Dalam pembangunan add-on Double X3 ini yaitu berfungsi sebagai fitur pada Mozilla Firefox untuk mengamankan data yang ingin dikirim menggunakan keamanan kriptografi. Dengan adanya add-on ini pengguna dapat mengamankan suatu informasi sebelum mengirimnya melalui internet.

a. XPI Packaging Scheme

File xpi merupakan sebuah arsip yang telah terkompresi yang digunakan oleh berbagai aplikasi Mozilla, termasuk Firefox, Thunderbird, dan SeaMonkey. File ini nantinya digunakan untuk menambahkan fungsionalitas pada aplikasi yang akan dijalankan yaitu Browser Mozilla Firefox.

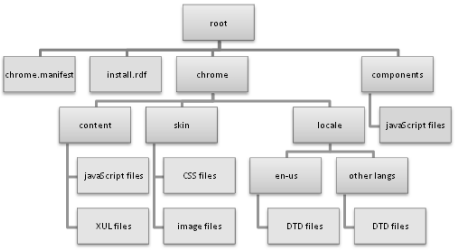
Pada pembuatan *add*-on Double X3 ini file xpi merupakan file instalasi *add*-on pada Mozilla Firefox. Untuk menghasilkan sebuah file berekstensi xpi, perlu melakukan beberapa tahapan yang dilakukan dalam melakukan *Packaging.* Untuk lebih jelasnya proses pembentukan xpi bisa dilihat pada Gambar 4.2.

Gambar 2 Tahapan penciptaan xpi

Pada penciptaan *xpi* terdapat 4 file yang penting untuk diketahui yaitu :

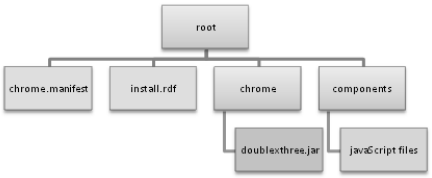
- install.rdf
  File ini Ini berisi metadata yang mengidentifikasi add-on, memberikan informasi tentang siapa yang menciptakannya, dengan versi berapa saja add-on ini kompatibel, bagaimana harus diperbarui, dan sebagainya. Untuk lebih jelasnya dapat dilihat script yang dibangun dalam pembuatan add-on Double X3.
- chrome.manifest
  File ini merupakan file untuk meregitrasikan extension yang dibuat ke dalam Mozilla Firefox dan menampilkan file yang dibuat pada tampilan Mozilla Firefox. Untuk lebih lengkapnya dapat dilihat script yang dibangun dalam pembuatan add-on Double X3.
- nama_file.js
  nama_file.js merupakan file Javascript yang berisi fungsi dari extension yang dibuat. Pada pembuatan add-on Double X3 yang peneliti buat di antaranya file ini berfungsi untuk mengenkripsi dan mendekripsi pesan menggunakan Algoritma Double X3.
- nama_file.xul
  File ini merupakan file yang berisi tampilan extension yang dibuat di dalam Mozilla Firefox.

Pada Gambar 3 menunjukkan struktur yang ideal dalam pembuatan sebuah *Firefox Extension*. Folder *components*, *skin* dan *locale* merupakan *optional*. Dalam pembuatan add-on Double X3 folder *components* dan *locale* tidak digunakan.



Gambar 3 Struktur Awal dari sebuah Firefox Extension

Setelah selesai pembuatan Struktur Awal dari *Firefox Extension*, kemudian selanjutnya proses yang akan dilakukan adalah pembuatan *file jar*. File *.jar* merupakan gabungan dari semua folder maupun file yang terdapat di folder chrome. Sedangkan cara untuk pembuatan sebuah file *.jar* pada penelitian ini yaitu dengan cara mengkompresi seluruh folder dan file yang terdapat di folder chrome menjadi file zip, lalu extension *.zip* tersebut diubah menjadi file *.jar*. Struktur yang baru setelah melakukan pembuatan file *.jar* akan menjadi seperti pada Gambar 4.



Gambar 4 Penciptaan file jar di dalam folder chrome

Setelah terciptanya file *jar*, proses akhir selanjutnya adalah menciptakan file *xpi.* File xpi merupakan gabungan dari keseluruhan file yang terdapat pada folder root termasuk file *jar*. Sedangkan proses untuk membuat file *xpi* sendiri yaitu sama dengan pembuatan file *jar* yaitu dengan cara mengkompresi seluruh folder dan file yang terdapat pada folder root menjadi file zip, lalu extension *.zip* tersebut diubah menjadi file *.xpi* Sehingga struktur yang baru akan menjadi seperti pada Gambar 5.

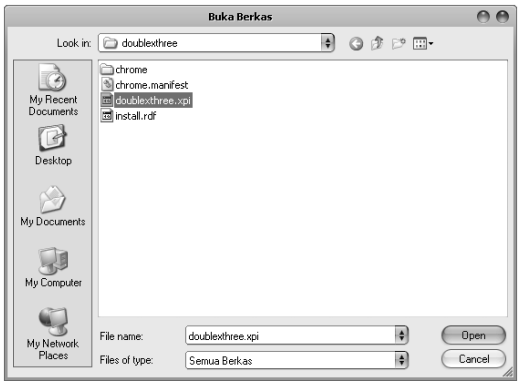
Gambar 5. Penciptaan file xpi

b. Instalasi Add-on

Untuk melakukan proses instalasi add-on *Double X3*, file yang dibutuhkan adalah file xpi yang telah dibahas pada bab sebelumnya. Adapun langkah-langkah instalasi yang harus dilakukan adalah dengan melakukan hal-hal berikut :

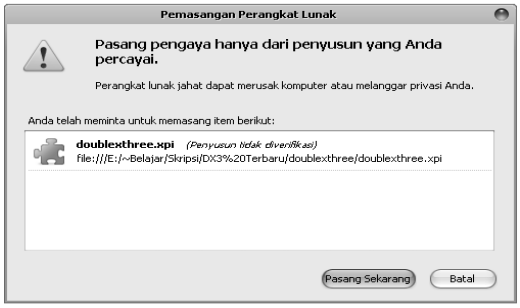
1. Membuka file xpi dengan *Mozilla Firefox* seperti pada gambar 6 dan gambar 7.

Gambar 6 Open File di Browser Firefox



Gambar 7 Seleksi File doublexthree.xpi

2. *Firefox* telah mengunduh file *doublexthree.xpi* secara sempurna. Klik *Pasang sekarang* seperti pada gambar 8.

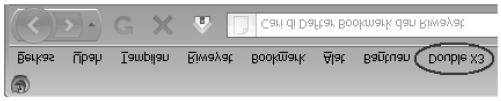


Gambar 8 Instalasi Add-on Double X3

3. Restart *Firefox* untuk menyelesaikan instalasi.
4. Jika berhasil maka pada jendela *Firefox* akan tampil informasi sebuah *Add-on* baru telah tepasang yang ditunjukkan oleh gambar 4.9.

Gambar 9 Informasi Add-on Double X3

5. Apabila muncul *toolbar* baru seperti yang ditunjukkan oleh gambar 4.10, maka add-on *Double X3* telah terpasang secara sempurna.



Gambar 10 Double X3 Extension

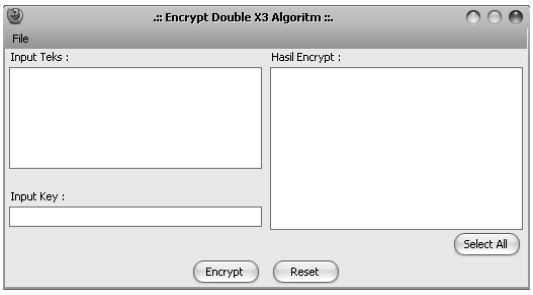
c. Tampilan Menu Utama

Tampilan dari menu utama terdiri dari beberapa sub menu yaitu *Encrypt Text*, *Decrypt Text*, *Help*, dan *About*. Apabila di klik pada beberapa sub menu tersebut maka akan menampilkan *form* baru sesuai dengan fungsinya masing-masing. Tampilan menu utama dapat ditunjukkan oleh gambar 11.

Gambar 11 Tampilan Menu Utama

d. Tampilan Sub Menu Encrypt Text

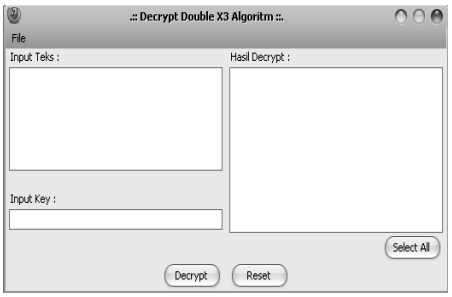
Pada sub menu Encrypt Text, terdapat menu *File* dimana di dalamnya terdapat sub menu *Open File,Save File*, dan *Exit.* Beberapa sub menu tersebut bila di klik maka akan menampilkan *form* baru sesuai dengan fungsinya masing-masing. Selain itu, juga terdapat tombol *Encrypt* yang berfungsi untuk mengenkripsi sebuah pesan. Tombol *Select All* berfungsi untuk menseleksi seluruh hasil dari pesan yang telah di enkripsi. Sedangkan tombol *Reset* berfungsi untuk menghapus seluruh teks yang terdapat pada form *Input text*, *input key*, dan *hasil encrypt*. Tampilan sub menu Encrypt Text dapat ditunjukkan oleh gambar 12.



Gambar 12 Tampilan Sub Menu Encrypt Text

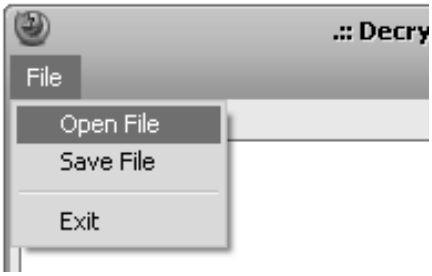
e. Tampilan Sub Menu Decrypt Text

Pada sub menu Decrypt Text, terdapat menu *File* dimana di dalamnya terdapat sub menu *Open File,Save File*, dan *Exit.* Beberapa sub menu tersebut bila di klik maka akan menampilkan *form* baru sesuai dengan fungsinya masing-masing. Selain itu, juga terdapat tombol *Decrypt* yang berfungsi untuk mendekripsi sebuah pesan. Tombol *Select All* berfungsi untuk menseleksi seluruh hasil dari pesan yang telah di dekripsi. Sedangkan tombol *Reset* berfungsi untuk menghapus seluruh teks yang terdapat pada form *Input text*, *input key*, dan *hasil decrypt*. Tampilan sub menu Decrypt Text dapat ditunjukkan oleh gambar 13.

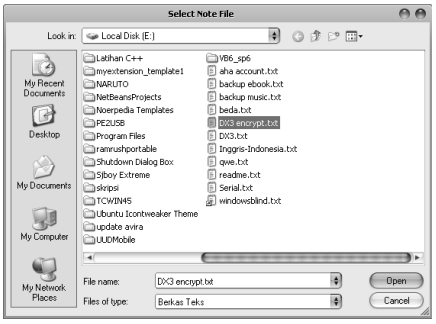


Gambar 13 Tampilan Sub Menu Decrypt Text

Untuk menjelaskan bagaimana langkah dari proses dekripsi, penulis akan memberikan contoh untuk dekripsi DX3 encrypt.txt yang berada pada direktori E, dapat dilihat pada gambar 14 dan gambar 15.



Gambar 14. Open File Decrypt Text



Gambar 15. Seleksi File DX3 encrypt.txt

KESIMPULAN DAN SARAN

Kesimpulan

Setelah melakukan penelitian dan pengujian, maka penulis mendapatkan suatu kesimpulan yang dapat digunakan sebagai garis besar dari keseluruhan

rangkuman dari skripsi ini. Adapun kesimpulan dari penelitian ini adalah sebagai berikut :

1. Sistem pengamanan data dapat dibuat dengan menggabungkan tiga algoritma kriptografi, seperti pada penelitian ini yang menggabungkan algoritma Cipher Subtitusi, Cipher Transposisi, dan XOR Cipher.
2. Add-on Double X3 ini telah mendukung Mozilla Firefox versi 3.0.* sampai 7.0.*.
3. Add-on Double X3 ini telah mendukung file teks (.txt) pada saat membaca maupun menyimpan hasil dari enkripsi dan dekripsi.

Saran

Berdasarkan penelitian dan implementasi sistem yang telah dilakukan, maka diberikan saran sebagai berikut :

1. Karakter yang didukung hanya pada ASCII 7-bit saja sehingga karakter diluar dari ASCII 7-bit tidak didukung, untuk pengembangan selanjutnya perlu adanya perluasan karakter yang didukung sehingga mempersulit kripanalis untuk membacanya.
2. File yang telah didukung hanya berupa file teks (.txt) saja, untuk pengembangan selanjutnya perlu adanya dukungan dari file teks lainnya seperti *.rtf, *.doc, *.docx, dan sebagainya.

DAFTAR PUSTAKA

Kurniawan, Yusuf. 2004. Kriptografi: Keamanan Internet dan Jaringan Komunikasi. Informatika, Bandung.

Stallings, William. 2003. Cryptography and Network Security, Pearson Education, New Jersey.

Feldt, Kenneth C. 2007. Programming Firefox: Building Application in the Browser. O'Reilly Media, USA.

Edwards, James. 2009. Build your own Firefox Extension. SitePoint, Australia.

Goodman, Danny. 2003. Javascript & DHTML Cookbook. O'Reilly & Associates, USA.

Wicaksono, Rizki. 2009. MITM Attack on Mandiri Internet Banking using SSLStrip. http://www.ilmuhacking.com.

Wicaksono, Rizki. 2009. Sniffing SSL Traffic using oSpy. http://www.ilmuhacking.com.

Deakin, Neil. XUL Tutorial.

Raharjo, Budi. 2005. Keamanan Sistem Informasi Berbasis Internet.

Hasan, Ahmed. 2007. Conceptual Architecture of Mozilla Firefox