PEMBUATAN APLIKASI SECURE E-BOOK UNTUK KARYA ILMIAH PENS-ITS

Muhammad Hamsah
Jurusan Teknik Informatika, Idris Winarno, Edi Satriyanto
Politeknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember Surabaya
Kampus PENS-ITS Keputih Sukolilo Surabaya 60111
Telp (+62)31-5947280, 5946114, Fax. (+62)31-5946114
Email: hamsah.it07@gmail.com

Abstrak

Aplikasi E-book dalam hal ini adalah sebuah aplikasi yang dapat mengkonversi bentuk file teks dengan ekstensi .doc atau .docx menjadi sebuah file dengan ekstensi baru. File baru tersebut akan berfungsi sama dengan ebook pada umumnya dan diperlukan sebuah reader untuk membaca format file tersebut. Untuk mengkonversinya dilakukan proses encoding dan enkripsi pada file masukkan yang selanjutnya akan disimpan dengan ekstensi baru. Metode enkripsi dan dekripsi yang akan digunakan adalah metode matrix hill chipper.

Hill Cippher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi.

Kata kunci : *E-book, Reader, Encoding Matrix Hill Chipper***.**

1. Latar Belakang

Kemajuan dan perkembangan teknologi informasi telah berpengaruh dalam segala aspek kehidupan terutama dalam bidang pendidikan. PENS-ITS adalah salah satu lembaga pendidikan tinggi yang selalu mengedepankan pengaplikasian teknologi informasi.

Salah satu dari teknologi yang saat ini makin banyak digunakan dan dibutuhkan adalah penggunaan ebook sebagai media pengetahuan dan pembelajaran yang sedikit banyak telah menggeser buku konvensional.

Kebutuhan akan adanya ebook yang berisi tentang karya ilmiah baik itu berupa penelitian, tugas akhir dan sebagainya semakin besar. Oleh karena itu dalam tugas akhir ini kami ingin membuat aplikasi ebook yang nantinya diharapkan dapat digunakan di PENS-ITS.

Dalam aplikasi ebook ini akan dapat mengkonversi file yang berekstensi *.doc* dan docx menjadi file dangan ekstensi baru. Untuk mengkonversinya dilakukan proses enkripsi pada file masukkan yang selanjutnya akan disimpan dengan ekstensi baru. Metode enkripsi dan dekripsi yang akan digunakan adalah metode *matrix hill chipper.*

Adapun dasar digunakannya enkripsi dalam pembuatan aplikasi ini adalah untuk menciptakan ebook yang aman. Karena file ebook yang telah dikonversi hanya dapat dibuka dengan aplikasi reader khusus yang bisa mendeskripsikan file tersebut sehingga bisa dibaca.

2. Tinjauan Pustaka

a. Base64 Encoding/Decoding

Base64 adalah sebuah skema encoding yang merepresentasikan data biner ke dalam format ASCII. Umumnya digunakan pada berbagai aplikasi, seperti e-mail via MIME, data XML, atau untuk keperluan encoding URL. Prinsip encodingnya adalah dengan memilih kumpulan dari 64 karakter yang dapat di-print (printable). dengan demikian, data dapat disimpan dan ditransfer melewati media yang didesain untuk menangani data tekstual. penggunaan lain encoding Base64 adalah untuk melakukan obfuscation atau pengacakan data.

b. Kriptografi

Kriptografi adalah sebuah cara untuk mengamankan sebuah informasi. Informasi yang harus dijaga kerahasiaannya haruslah diubah menjadi sebuah Informasi yang tidak bisa dibaca oleh orang selain yang berhak membacanya.

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita [bruce Schneier - Applied Cryptography] Dalam kriptografi, pesan atau informasi yang dapat dibaca disebut sebagai plaintext atau clear text. Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext disebut enkripsi. Pesan yang tidak dapat terbaca tersebut disebut ciphertext. Proses yang merupakan kebalikan dari enkripsi disebut sebagai dekripsi. Proses ekripsi dapat digunakan untuk membuat ciphertext kembali menjadi plaintext.

Ahli di bidang kriptografi disebut sebagai cryptographer. Cryptanalyst merupakan orang yang melakukan cryptanalysis, yaitu seni dan ilmu untuk memecahkan ciphertext menjadi plaintext tanpa melalui cara yang seharusnya (dekripsi). Jadi, cryptanalysis merupakan kebalikan dari kriptografi. Cabang matematika yang mencakup kriptografi dan cryptanalysis disebut cryptology dan pelakunya disebut cryptologist.

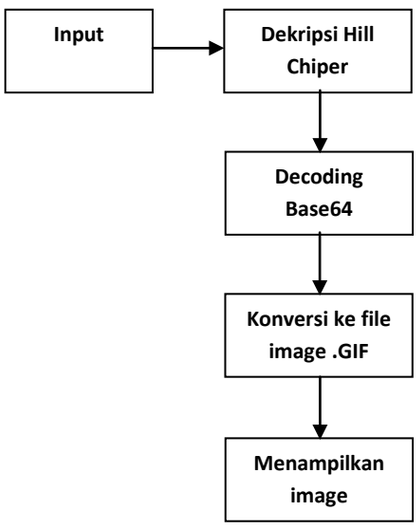
c. Hill Chipper

Hill Cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi.

Hill Cipher diciptakan oleh Lester S. Hill ada tahun 1929 [2]. Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. *Hill Cipher* tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya.

3. Perancangan dan Pembuatan Sistem

a. Proses Konversi

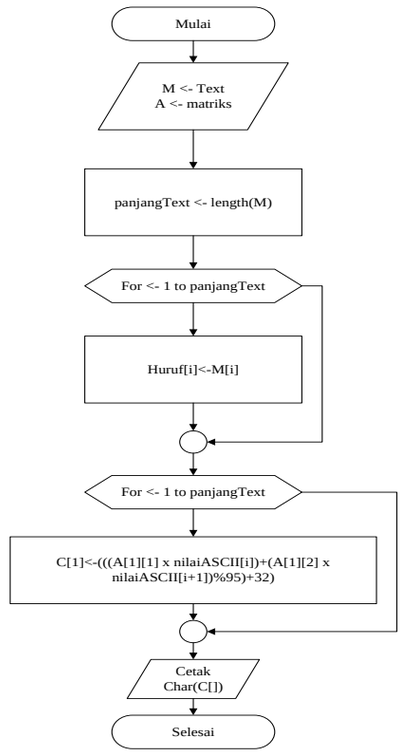


Gambar 1. Proses Konversi File

-

Pada tahap konversi dilakukan beberapa proses untuk mendapatkan file dengan ekstensi .eff diantaranya:

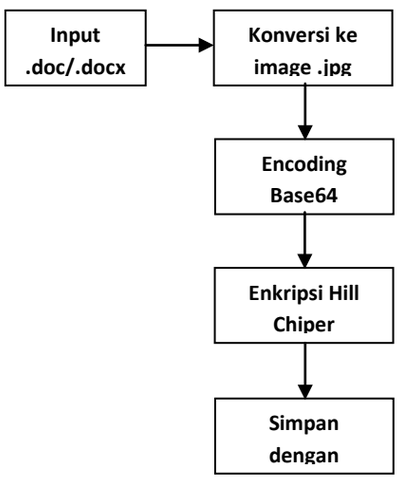
- Input Masukan File
  Pada tahap ini user memasukkan file input berupa file Microsoft word dengan tipe file .doc maupun .docx
- Konversi Image
  File *document* yang sudah dimasukkan kemudian di konversi menjadi gambar
- Encoding Base64
  Pada tahap ini gambar kemudian di konversi ke dalam bentuk string dengan metode Base64 yakni dengan merubah data biner ke dalam bentuk ASCII
- Enkripsi dengan Metode Hill Chipper
  Selanjutnya dilakukan enkripsi tehadap data yang diperoleh dari proses encoding base64 dengan mengunakan metode *hill chipper*. proses dari enkripsi menggunakan metode hill chipper dapat dilihat dalam flowchart berikut



Gambar 2. Flowchart Enkripsi Hill Chipper

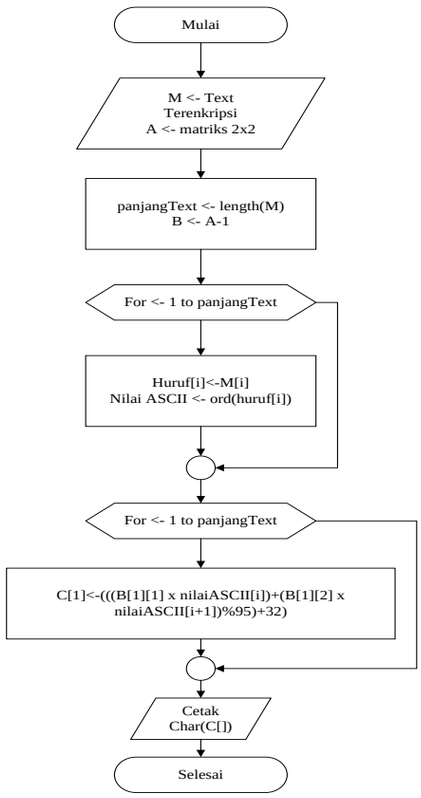
- Penyimpanan
  Pada proses ini dilakukan penyimpanan file kedalam direktori yang diinginkan dengan ekstensi file .eff

b. Proses Reading



Gambar 3. Proses Konversi File

- Input Masukan File
  Pada tahap ini user memasukkan file input berupa file ebook yang dengan ekstensi .eff
- Dekripsi Hill Chipper
  Pada tahap ini file .eff di dekripsi menggunakan metode hill chipper (proses algoritma hill chipper dijelaskan dalam gambar 4)

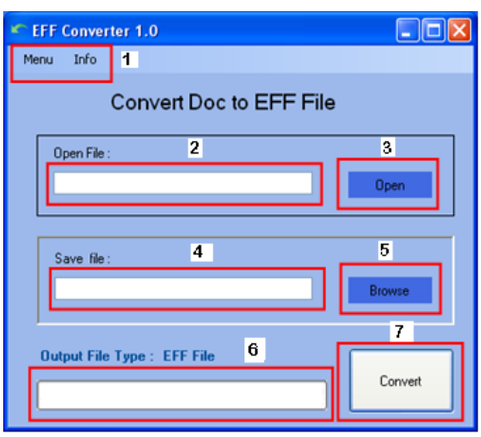


Gambar 4. Flowchart Dekripsi Hill Chipper

- Decoding Base64
  Pada tahap ini hasil dari proses dekripsi hill chipper didecode dengan metode base64 untuk mengembalikan dalam bentuk biner.
- Konversi ke image
  Dari proses decode base64 akan dihasilkan file biner dalam bentuk gambar
- Menampilkan image
  Dalam tahap ini dihasilkan ebook berupa gambar yang ditampilkan dalam form utama dari aplikasi *reader*

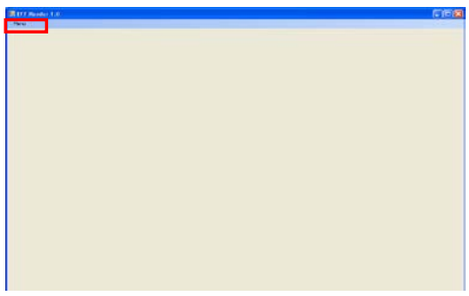
Desain Antar muka program

- Program Converter



Gambar 5. Desain Antar Muka Aplikasi Converter

- Program Reading



Gambar 6. Desain Antar Muka Aplikasi Reader

4. Uji Coba dan Analisa

4.1 Hasil Running Program

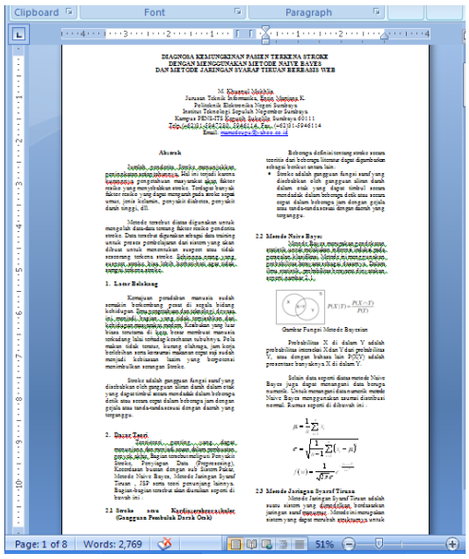
Dalam tahap ini akan dilakukan pengujian dan analisa terhadap jalannya aplikasi dengan input berbagai file dokumen dengan spesifikasi tertentu.

Tabel.1 menunjukkan spesifikasi file dokumen input yang digunakan pada percobaan 1

Tabel 1. Spesifikasi Dokumen Input Percobaan

Spesifikasi	Keterangan
Ekstensi file input	.doc
Ukuran kertas	F4 (13 inch x 8,5 inch)
Header/footer	Tidak ada
Tabel	Tidak ada
Gambar	Ada
Persamaan Matematis /Rumus	Ada
Format kolom	2 kolom

Berikut ini adalah tampilan dari file input dokumen pada percobaan 1 ditunjukkan pada gambar 6

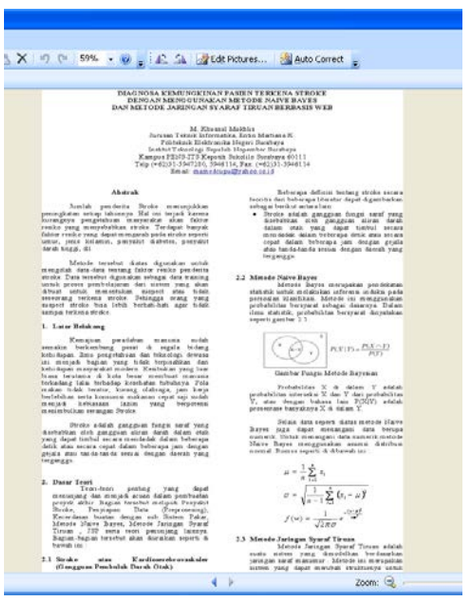


Gambar 6. Dokumen Input

Setelah dilakukan proses konversi maka akan dihasilkan 3 file yang digunakan sebagai perbandingan yaitu :

1. File gambar, sebagai output dari proses konversi dokumen ke gambar, berekstensi .GIF.
2. File Teks hasil proses encoding base64 sebagai hasil dari proses encoding file gambar menjadi plain text (string), berekstensi .txt
3. File ebook, sebagai hasil proses enkripsi dari plain text menjadi file dokumen ebook, berekstensi .eff (Eepis File Format)

- File Gambar



Gambar 7. Dokumen Input

- File Teks

Dengan fungsi *convert to base64 string* maka gambar yang dihasilkan dari proses sebelumnya dikonversi menjadi string lalu kemudian disimpan dalam file Percobaan1.txt berikut adalah tampilan file Percobaan1.txt apabila dibuka dengan program teks editor notepad. Seperti diperlihatkan pada gambar 8

Gambar 8. Hasil File Teks Encoding Base64

- File Ebook

Setelah proses encoding dari gambar ke string proses selanjutnya adalah enkripsi menggunakan hill chipper berikut adalah hasil dari proses enkripsi yang kemudian disimpan dengan ekstensi .eff. dan apabila file ebook tersebut dibuka dengan program teks editor notepad maka komposisi datanya akan terlihat seperti pada gambar

Gambar 9. Hasil File Ebook

Analisa Percobaan

Dari hasil output yang terlihat pada aplikasi EFF Reader maka didapatkan data spesifikasi seperti pada tabel 2

Gambar 10. Hasil Output File Ebook yang Dibaca Lewat Program EFF Reader

Tabel 2. Spesifikasi Dokumen Input Percobaan

Spesifikasi	Keterangan
Ekstensi file output	.eff
Ukuran kertas	Tidak Ada
Header/footer	Tidak Ada
Tabel	Tidak Ada
Gambar	Ada
Persamaan Matematis /Rumus	Ada
Format kolom	2 Kolom

Apabila dibandingkan dengan data spesifikasi dokumen input pada tabel 1 maka didapatkan analisa bahwa dokumen ebook telah dapat menampilkan Gambar, Persamaan Matematis,dan Format Kolom. Namun sekali lagi baru bisa menampilkan satu halaman depannya saja dari file input yang dimasukkan. Dan belum bisa untuk mengatur ukuran ebook sesuai dengan ukuran kertas yang sama dengan file input.

Analisa Secara Umum

1. Aplikasi hanya bisa melakukan *capture* pada halaman awal dari dokumen input
2. Aplikasi dapat menampilkan keseluruhan isi teks dari halaman awal dokumen
3. Aplikasi tidak dapat menampilkan header/footer seperti pada dokumen input
4. Aplikasi dapat menampilkan isi dokumen yang berupa tabel, gambar, chart, format kolom dan persamaan matematika.
5. Aplikasi dapat menghandle tipe dokumen input dari microsft word baik yang berekstensi.doc maupun .docx

5 Kesimpulan dan Saran

KESIMPULAN

Pada bagian ini akan di ulas tentang kesimpulan dan analisa dari seluruh percobaan proyek akhir Aplikasi Ebook untuk Karya Ilmiah PENS-ITS.

Berikut beberapa kesimpulan yang dapat diambil dari percobaan dan pengujian proyek akhir ini :

1. Keberhasilan pada proses *capturing* file input mempengaruhi hasil dari output file yang ditampilkan.
2. Hasil output dari proyek akhir ini hanya bisa menampilkan halaman pertama dari file input yang dikonversi.
3. Pada proyek ini fungsi encoding dan decoding base64 dari gambar ke string maupun sebaliknya dapat berfungsi dengan baik sehingga tidak terjadi kehilangan data atau kerusakan data pada proses konversi.
4. Metode hill chipper dalam tahap enkripsi berpengaruh dalam mengacak data sehingga data yang dihasilkan dari proses encoding base64 yang dihasilkan semakin acak.

SARAN

Dalam penyempurnaan proyek akhir ini disarankan untuk perbaikan pada beberapa bagian. Diharapkan proyek akhir ini dapat diteruskan agar didapatkan hasil yang maksimal. Perbaikan dalam penyempurnaan yang dimaksudkan diantaranya adalah :

1. Untuk dapat membuat aplikasi reader ebook yang dapat menampilkan multipage dari file input yang di konversi
2. Untuk membuat aplikasi ebook yang lebih lengkap dengan fitur-fitur tambahan yang lebih fungsional.
3. Untuk dapat menambahkan teknik kompresi data sehingga didapatkan ukuran file ebook yang lebih kecil.

6 Daftar Pustaka

1. Ivan Nugraha, Studi dan Perbandingan Performansi Algoritma Simetri *Chipper Binner* dan *Hill Chipper Binner*, 2007.
2. Forouzan, Behrouz, *Cryptography And* Nikken Prima Puspita, Nurdin Bahtiar Kriptografi Hill Cipher Dengan Menggunakan Operasi Matriks, 2010.
3. Amogh Mahapatra, Rajballav Dash *Data Encryption And Decryption By Using Hill Cipher Technique And Self Repetitive Matrix* National Institute Of Technology Rourkela, 2007.
4. http://www.rasamautau.co.cc/2010/04/enkripsi-hill-chiper.html
5. http://www.dreamincode.net/forums/topic/216719-convert-doc-to-image/
6. http://en.wikipedia.org/wiki/base64
7. http://en.wikipedia.org/wiki/hill_cipher