

**PEMBUATAN FILE ENKRIPSI DAN DEKRIPSI MENGGUNAKAN
PRINSIP KERJA MESIN ENIGMA**

TUGAS AKHIR

**Diajukan Untuk Memenuhi Salah Satu Syarat
Menyelesaikan Program Diploma III
Politeknik Universitas Andalas**

Oleh:

SATRIA AGUNG WJAYA AZMIR

BP. 06 075 001

**Program Studi Teknik Telekomunikasi Multimedia
Jurusan Teknik Elektro**



POLITEKNIK UNIVERSITAS ANDALAS PADANG

2009

ABSTRAK

Pembuatan File Enkripsi – Dekripsi Menggunakan Prinsip Kerja Mesin Enigma

Oleh

Satria Agung Wijaya Azmir
06075001

Perkembangan teknologi berkembang sangat cepat terutama dalam bidang telekomunikasi. Melalui komunikasi segala sesuatu dapat terpecahkan. Untuk menjaga kerahasiaan data para programmer telah mengembangkan berbagai software untuk mengamankan data atau file agar data bisa dirahasiakan dan tidak mudah untuk diketahui oleh pihak – pihak yang tidak diinginkan.

Mesin enigma adalah salah satu alat yang digunakan pada zaman dahulu sebagai alat pengacak data atau data yang dirahasiakan atau disebut juga dengan istilah kriptografi. Untuk melakukan proses kriptografi ini ada beberapa proses yang dinamai dengan Enkripsi dan Dekripsi. Enkripsi yaitu proses pengubahan text asli menjadi text acak sedangkan dekripsi proses pengembalian text acak menjadi text asli. Sedangkan enigma itu sendiri adalah salah satu metode kriptografi dengan mensubstitusi suatu karakter menjadi karakter lain.

Pada tugas akhir ini didapatkan hasil enkripsi dari suatu karakter menghasilkan karakterlain yang telah diacak dengan penggunaan kunci (key). Karakter yang telah diacak dapat dikembalikan seperti semula bagaimana karakter aslinya dengan menggunakan key yang sama.

Key word : Kriptografi, Enigma, Enkripsi, Dekripsi, Key

BAB I PENDAHULUAN

I. Latar Belakang

Enkripsi merupakan suatu proses pengubahan pesan asal menjadi karakter yang tidak dapat dibaca sedangkan dekripsi merupakan proses pengembalian text enkripsi menjadi text asli. Ada beberapa algoritma enkripsi – dekripsi yang biasa digunakan seperti DES, Triple DES, Blowfish, IDEA dan sebagainya. Algoritma-algoritma tersebut begitu rumit dan sulit dimengerti dengan dalih faktor keamanan, katanya semakin sulit suatu algoritma dimengerti, maka semakin aman. Namun bagi para pengguna mereka tidak memikirkan seberapa sulit algoritma dan aplikasinya, yang mereka inginkan adalah menjaga kerahasiaan data.

Teknik enkripsi – dekripsi yang sangat terkenal, digunakan oleh tentara Jerman ialah Mesin Enigma, yang diciptakan oleh Arthur Scherbius pada tahun 1918. Pada dasarnya, tujuan dari enkripsi – dekripsi ini ialah untuk menyembunyikan pesan (data atau informasi) dari pihak yang tidak berkepentingan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna.

Mesin Enigma yang merupakan mesin pengenkripsi dan dekripsi pesan, diciptakan oleh pihak Jerman berdasarkan metode enkripsi – dekripsi tersebut. Konsep dasar dari enkripsi – dekripsi mesin ini, ialah dengan menggunakan metode *Caesar chipper*, yaitu dengan mensubstitusi huruf dengan huruf lainnya.

Dengan adanya program ini, maka kita dapat mengenkripsi dan dekripsi file dengan prinsip mesin enigma tanpa harus menggunakan mesin enigma.

Dengan menggunakan prinsip kerja mesin enigma tersebut maka pada tugas akhir ini dibuat metode enkripsi – dekripsi yang berdasarkan pada prinsip kerja mesin enigma. Untuk membuktikan keluaran dari proses enkripsi harus dilakukan proses dekripsi dari cipher text menjadi plain text lagi.

II. Tujuan

Adapun tujuan yang ingin dicapai dalam pembuatan tugas akhir ini adalah:

1. Dapat mengetahui konsep dari mesin enigma dan metode enkripsi dan dekripsi yang digunakan.
2. Membuat program enkripsi sebuah file, sehingga file tersebut tidak bisa dimengerti oleh pihak yang tidak diizinkan untuk mengakses file tersebut.

III. Perumusan Masalah

Adapun permasalahan yang diangkat adalah bagaimana cara kerja dari mesin enigma dan bagaimana menerapkannya dalam bentuk *software*. Serta pembuatan program dengan menggunakan Visual Basic.

IV. Batasan Masalah

Batasan masalah dari metode enkripsi dan dekripsi dengan menggunakan prinsip kerja mesin enigma ini adalah untuk file dengan format .doc,txt,rtf,xls.

BAB V

PENUTUP

5.1 Kesimpulan

Setelah dilakukan pengujian dan analisa terhadap program file enkripsi menggunakan prinsip kerja mesin enigma, maka dapat diambil kesimpulan :

1. Generator key yang digunakan untuk pengujian ini menghasilkan key yang acak, sehingga key yang digunakan tidak dapat diketahui oleh pihak yang tidak diinginkan.
2. Hasil enkripsi dari plain text tergantung kepada kunci yang digunakan.
3. Proses dekripsi pada tugas akhir ini harus menggunakan kunci yang sama dengan kunci proses enkripsi tersebut.

5.2 Saran

Untuk maksimalnya program yang dibuat ini, maka penulis memberikan beberapa saran, diantaranya sebagai berikut :

1. Perlu dikembangkan program enkripsi ini dengan metode lain yang lebih baik.
2. Diharapkan program enkripsi ini dapat mengkombinasikan beberapa metode enkripsi lainnya. Sehingga data atau file hasil enkripsi – dekripsi lebih aman lagi.
3. Perlu penambahan inputan untuk pengembangan selanjutnya sehingga semua jenis file dapat dienkripsi dan didekripsi.

DAFTAR PUSTAKA

- Divisi Penelitian dan Pengembangan LPKBM MADCOMS, Panduan Pemrograman dan Referensi Kamus Visual Basic 6.0, CV Andi Offset, Madiun, 2005
- Muhammad Sadeli, 81 Trik Tersembunyi Visual Basic 2005, Maxicom, Palembang, 2009.
- Pengertian kriptografi. 12 November 2009. [http : informatika.org/ ~ rinaldi / Kriptografi / 2008 - 2009/ Makalah1/ MakalahIF30581 -2009- a016. Pdf](http://informatika.org/~rinaldi/Kriptografi/2008-2009/Makalah1/MakalahIF30581-2009-a016.Pdf)
- Enkripsi – Dekripsi. 12 November 2009. [http : // tedi.heriyanto.net/papers.html](http://tedi.heriyanto.net/papers.html)
- Teori Enigma. 20 Desember 2009. [http : // www.informatika.org/ ~rinaldi/ Madris/2007- 2008/Makalah/MakalahIF2153-0708-019.pdf](http://www.informatika.org/~rinaldi/Madris/2007-2008/Makalah/MakalahIF2153-0708-019.pdf)
- Prinsip Kerja Mesin Enigma. 20 Desember 2009 : [// www.skma.org/skmaorg/topik main menu-156/i-t-mainmenu 160/86.html](http://www.skma.org/skmaorg/topik/main%20menu-156/i-t-mainmenu%20160/86.html)