Proyek Akhir

Enigma Machine

Aldwin Akbar Hermanudin (1306368495)

Teknik Komputer

Untuk Mata Kuliah

Pemrograman Lanjut

FAKULTAS TEKNIK

UNIVERSITAS INDONESIA

DEPOK

2015

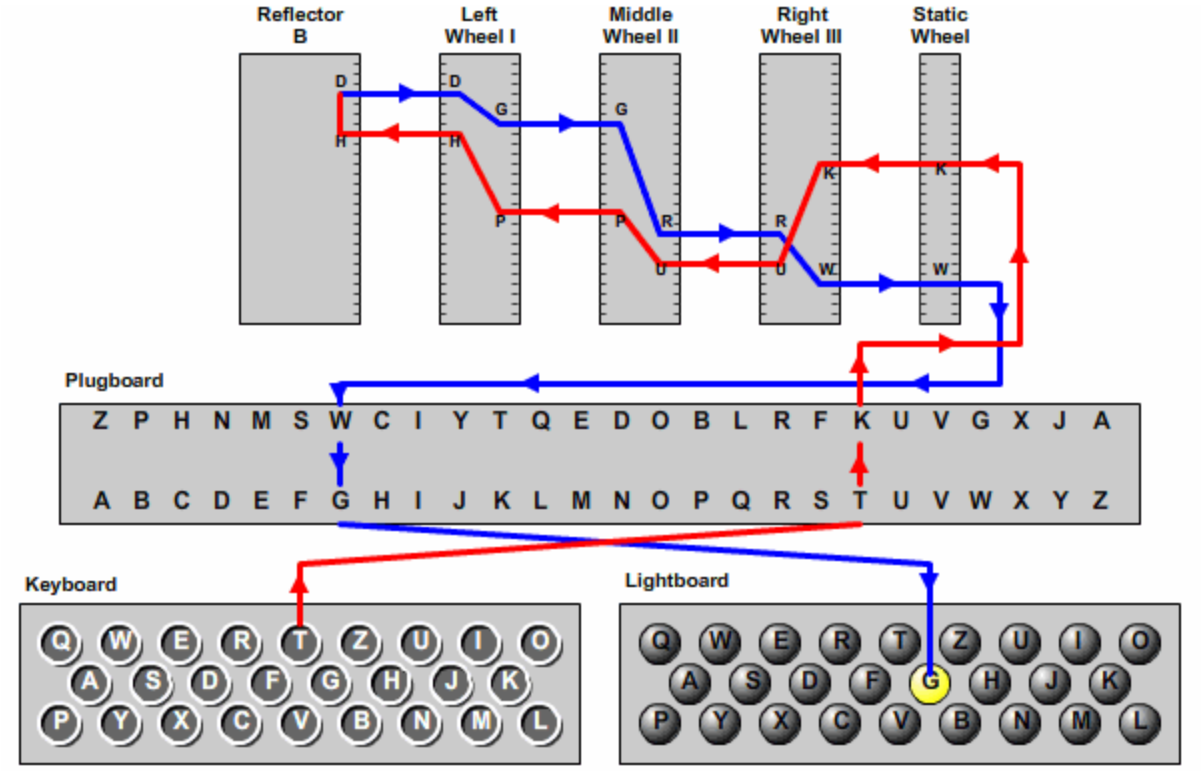
BAB I

PENDAHULUAN

A. GAMBARAN UMUM PROYEK

Pada proyek akhir ini ialah program yang dapat melakukan enkripsi suatu kalimat, kata, huruf, atau Text File. Program ini didasarkan dari cara kerja alat enkripsi yang popular saat perang dunia ke-2 yaitu Enigma. Dengan menggunakan program ini suatu kalimat atau text file akan lebih aman karena tidak dapat dimengerti artinya oleh orang yang membacanya tanpa di dekripsi terlebih dahulu dengan program ini dengan memasukan password yang telah ditentukan saat di enkripsi. Enigma ialah suatu mesin enkripsi yang dipakai saat perang dunia ke-2 oleh Jerman untuk berkomunikasi antara U-Boat dan pangkalan militer-militernya untuk member informasi seperti waktu penyerangan, lokasi setiap battalion atau U-Boat, kondisi battalion dan sebagainya. Pada mesin enigma terdapat 4 macam benda yang melakukan enkripsinya yaitu plugboard, static rotor, scrambler rotor, dan reflector. Cara kerjanya cukup sederhana ialah dengan mengganti suatu huruf dengan huruf lain beberapa kali.

Cara Kerja Enigma Machine

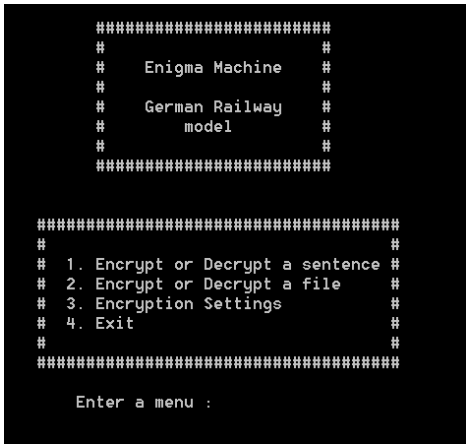


BAB II

ISI

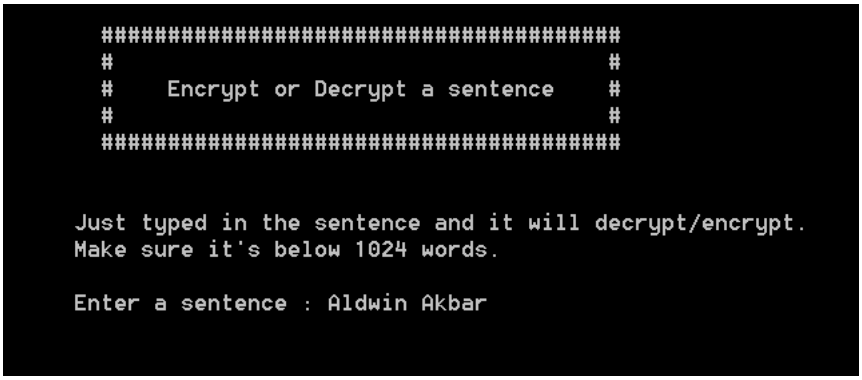
B. PENJELASAN PROYEK

Enigma machine ini mengimplementasikan perulangan,penyeleksian kondisi, pemrograman modular dengan passing variable, dan juga array, linked list, pointer, dan juga rekursif.



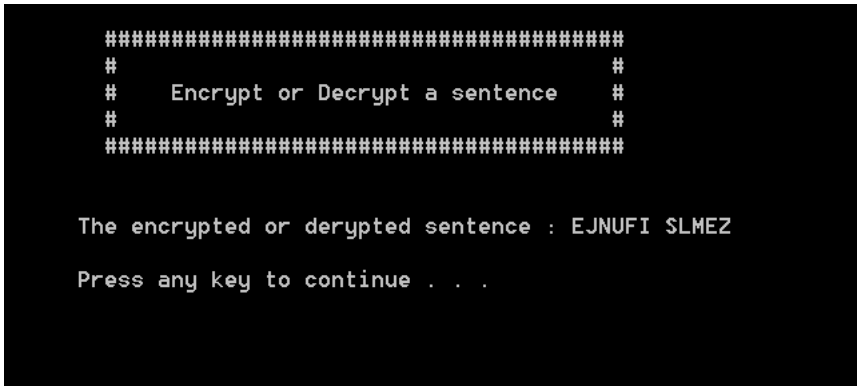
Gambar 1. Interface awal program

Gambar 1. merupakan interface yang pertama saat program pertama kali dijalankan. Terdapat 3 menu, menu pertama untuk enkripsi suatu kalimat, menu kedua untuk enkripsi suatu file, menu ketiga untuk setting dari enkripsi itu sendiri.

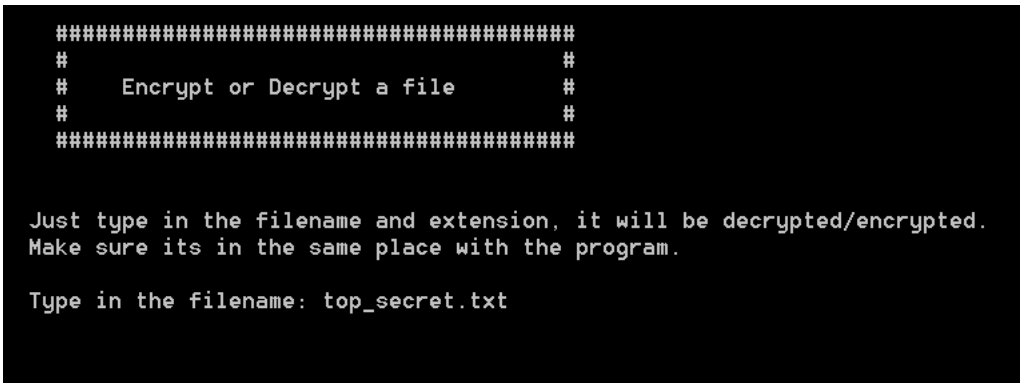


Gambar 2. Enkripsi suatu kalimat

Pada gambar 2 user diminta untuk memasukan kalimat yang ingin di-enkripsi, dan tidak boleh lebih dari 1024 kata, setelah menekan enter maka kalimat yang ter-enrkripsi akan ditampilkan.

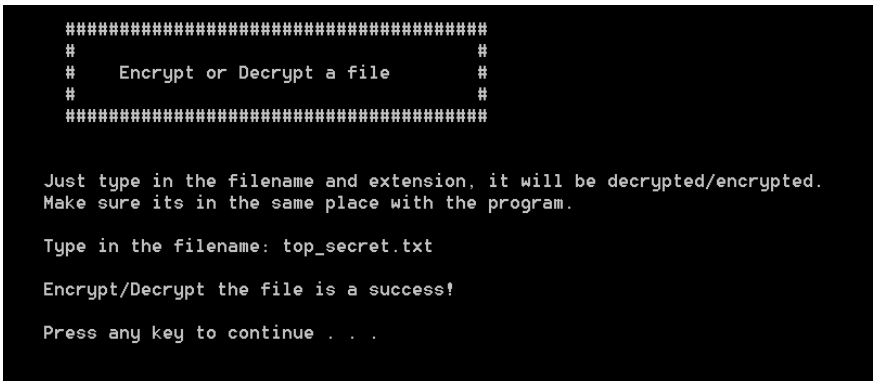


Gambar 3. Kalimat yang telah dienkripsi



Gambar 4. Enkripsi suatu file

Pada gambar 4 user diminta untuk memasukan nama suatu text file yang ingin di-enkripsi. File tersebut tentunya lebih baik harus berada pada lokasi yang sama dengan program enigma machine ini. Jika berhasil, maka akan menampilkan gambar 5.

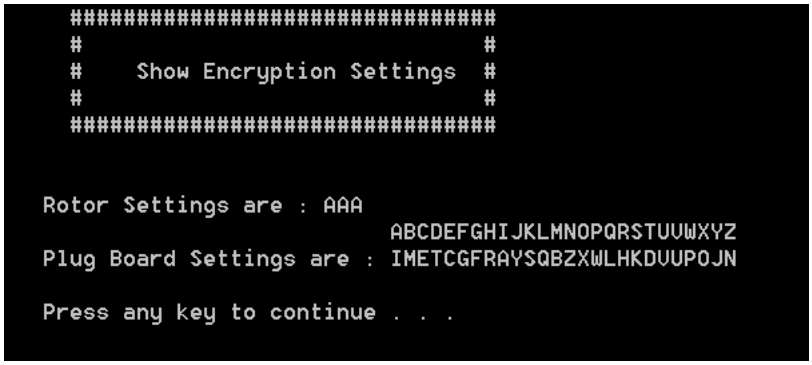


Gambar 5. File berhasil di enkripsi

Bila enkripsi pada file berhasil, maka akan menghasilkan file baru dengan tambahan ekstensi “.enigma” diakhir. Pada gambar diatas contohnya ialah menjadi top_secret.txt.enigma

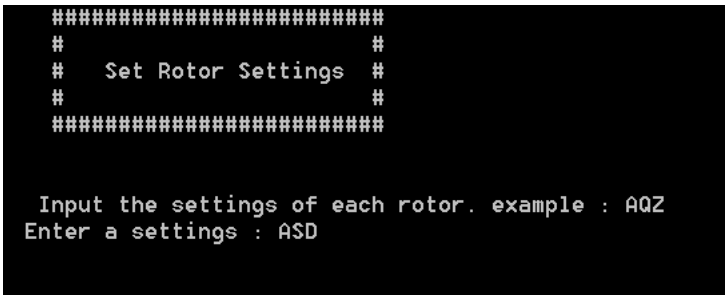
Gambar 6. Submenu Encryption Settings

Pada gambar 6 ialah submenu dari menu *Encryption Settings*. Menu 1 untuk me-cek konfigurasi enkripsi sekarang, menu 2 untuk ubah posisi rotor, menu 3 untuk ubah posisi plug board, menu 4 untuk set semuanya ke konfigurasi awal.



Gambar 7. Menu Show Encryption Settings

Pada gambar 7 ialah konfigurasi mesin engima ada waktu tersebut, rotor settings menunjukan posisi rotor, plug board settings menunjukan colokan plugboard yang terhubung ke setiap huruf, misalkan dari gambar dapat dilihat bahwa A terhubung dengan I dan sebaliknya.

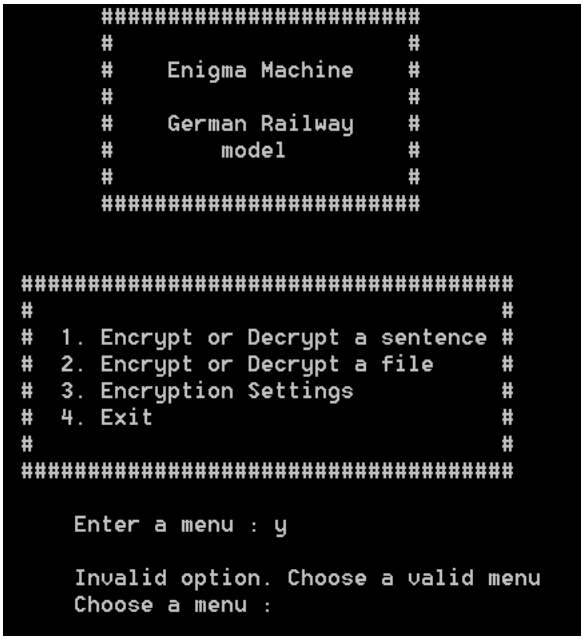


Gambar 8. Menu untuk me-set konfigurasi rotor

Pada gambar 8 user akan diminta untuk meng-input 3 huruf yang merepresentasikan kondisi rotor pada mesin enigma. Huruf yang di-input tidak boleh kurang dan lebih dari 3 dan tidak boleh pula berisi angka. Bila terdapat error, maka konfigurasi tidak akan diupdate dan akan kembali ke menu utama. Posisi ini sangat penting untuk diingat, jika nanti setelah melakukan enkripsi dan ingin melakukan dekripsi, harus me-set konfigurasi rotor yang sama.

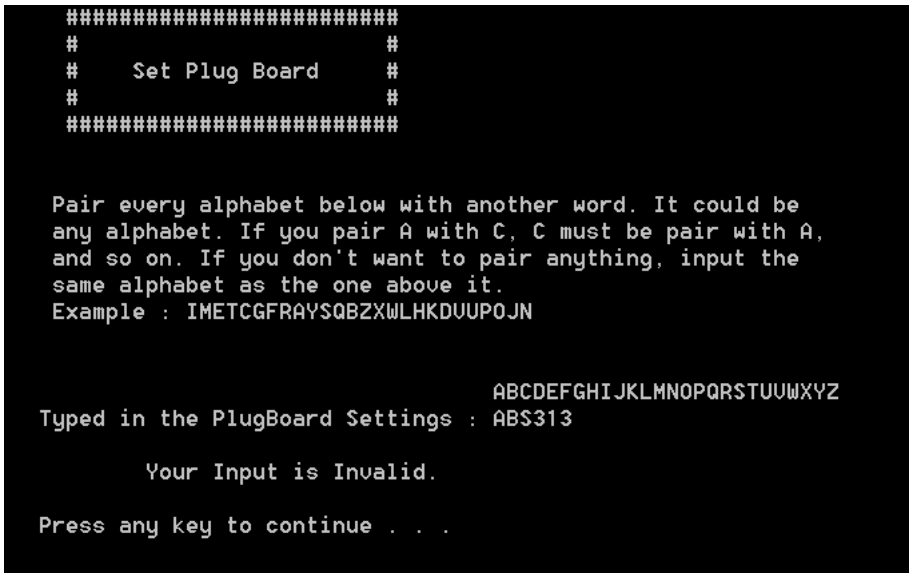
Gambar 9. Menu untuk me-set konfigurasi plugboard

Pada gambar 9 user akan diminta untuk meng-input 26 huruf yang merepresentasikan kondisi plugboard pada mesin enigma, input tidak boleh berupa angka dan tidak boleh pula lebih dan kurang dari 26 huruf. Bila terdapat error, maka konfigurasi tidak akan diupdate dan akan kembali ke menu utama Posisi ini sangat penting untuk diingat, jika nanti setelah melakukan enkripsi dan ingin melakukan dekripsi, harus me-set konfigurasi plugboard yang sama.



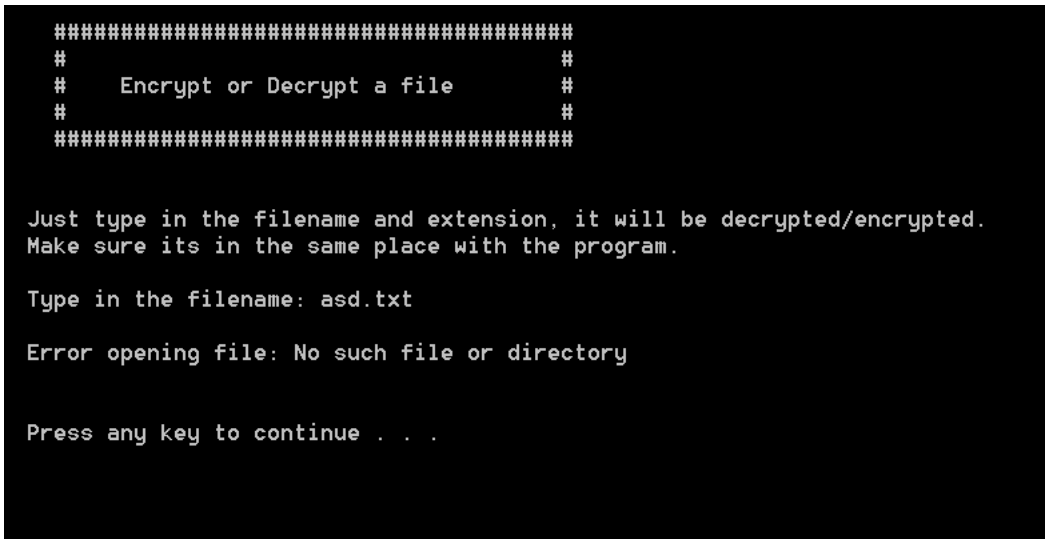
Gambar 10. Kondisi bila terjadi error

Pada gambar 10 ialah saat kondisi program menerima input yang salah, bila ini terjadi program akan terus meminta input hingga inputan tersebut benar.



Gambar 10. Kondisi bila terjadi error

Pada gambar 11 ialah saat melakukan konfigurasi dan input yang dimasukan tidak sesuai dengan yang diperlukan, maka program tidak akan meng-update konfigurasi dan user akan kembali ke menu utama.



Gambar 12. Kondisi saat membuka file error

Pada gambar 12 ialah kondisi saat terjadi error pada pembukaan file, masalah-masalah yang terjadi bisa dikarenakan file tersebut tidak ada, lagi dibuka program lain, tidak mempunyai akses ke file tersebut dan lain-lain

BAB III

PENUTUP

C. KESIMPULAN

Program *Enigma Machine* ini berhasil dibuat dengan bahasa c, dengan menggunakan mekanisme cara kerja mesin tersebut sebagai referensi. Masalah utama yang dihadapi dalam pembuatan mesin enigma ini kedalam enigma yaitu membuat rotor, perputaran rotor, dan mekanisme enkripsinya itu sendiri. Rotor dan Perpindahan rotor dapat diimplementasikan menggunakan linked list, dimana setiap rotor berpindah akan memindahkan pointer pada linked list ke node selanjutnya, dan linked list itu sendiri dibuat dengan mem-point node terakhir ke node pertama, sehingga me-simulasikan sebuah rotor. Untuk enkripsinya itu sendiri cukup mudah yaitu dengan membuat satu fungsi yang men-simulasikan satu buat enkripsi dari kanan ke kiri dan dari kiri kenan, selanjutnya fungsi tersebut hanya perlu digunakan dengan mengubah variable rotor yang digunakan (yaitu rotor[0], rotor[1], rotor[2]).

D. Referensi

- Deitel,H. and Deitel,P. (2011) C++ How to Program. Prentice Hall
- David H., Sullivan, G and Weierud F. "Enigma Variations: An Extended Family of Machines". http://home.comcast.net/~dhhamer/downloads/enigvar2.pdf
- "How Enigma Works". http://enigma.louisedade.co.uk/howitworks.html
- "Working principle of enigma". http://www.cryptomuseum.com/crypto/enigma/working.htm