ABSTRAK

Pada era modern saat ini, keamanan dalam mengirim data menjadi hal yang sangat penting, khususnya dalam bidang teknologi informasi. Teknik untuk mencegah kejahatan dalam pengamanan data disebut kriptographi. Cara kerja kriptographi dengan kunci publik adalah dengan membuat dua buah kunci, yaitu kunci publik dan kunci privat. Kunci publik adalah kunci yang digunakan oleh pengirim *message* (pesan) untuk melakukan proses enkripsi, yaitu proses untuk mengubah *plaintext* (message asli) menjadi *ciphertext* (message yang dikirim, setelah melalui proses enkripsi). Kunci privat digunakan untuk proses dekripsi, yaitu untuk mengubah ciphertext menjadi plaintext (message asli).

Salah satu metode yang menerapkan kriptographi dengan kunci publik adalah algoritma Mc. Eliece. Saat ini belum banyak yang menerapkan algoritma Mc. Eliece dalam pengamanan data. Algoritma Mc. Eliece sangat jarang digunakan karena memiliki rating informasi yang sedikit dan menggunakan matrik bilangan biner yang besar untuk kunci publik dan kunci private (Hung-Min Sun 2000). Algoritma Mc. Eliece menggunakan matrik untuk kunci private dan kunci publik.

Prinsip kerja program Mc. Eliece adalah ketika mengirim sebuah message kepada penerima dalam bentuk karakter, maka pesan yang kita kirim akan diubah terlebih dahulu kedalam kode ASCII, setelah itu kode ASCII yang terbentuk diubah menjadi bilangan biner. Bilangan biner tersebut akan di proses dengan kunci publik penerima dan menghasilkan sebuah ciphertext. Ciphertext yang terbentuk akan dikirim ke penerima. Untuk membaca ciphertext, pertama kali kita harus mengetahui kunci privat dari penerima. Ciphertext tersebut akan diproses dengan kunci privat untuk menghasilkan message asli dalam bentuk biner. Bilangan biner yang terbentuk akan diubah menjadi kode ASCII. Kode ASCII tersebut lalu akan diubah kembali menjadi karakter, sehingga message asli dapat dibaca kembali.

Untuk setiap proses membentuk kunci private, proses enkripsi dan proses dekripsi akan di desain dalam bentuk flowchart dan akan diterapkan dalam bentuk program. Pengubahan dari 1 karakter menjadi 7 bit bilangan biner akan menyebabkan message yang dikirim akan menjadi rata-rata 7 kali lebih besar daripada message yang asli. Oleh karena itu perlu dilakukan uji coba untuk mengetahui kenapa panjang message hasil enkripsi tidak tepat 7 kali lipat.

Batasan tipe file dari program yang dibuat adalah file text dan mengubah satu karakter dari message menjadi bentuk 7 bit bilangan biner. Semakin panjang message yang dikirim akan mengakibatkan iterasi semakin panjang, hal ini akan menyebabkan waktu yang dibutuhkan menjadi lebih lama.