BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Dalam era konektifitas sekarang ini, dimana setiap informasi dapat di akses dengan mudah, maka keamanan data benar – benar menjadi permasalahan yang sangat penting. Perkembangan sistem komputer dan interkoneksinya melalui jaringan telah meningkat sehingga membutuhkan keamanan data dan informasi yang handal agar terhindar dari serangan (*attack*). Salah satu cara untuk mengamankan data atau pesan adalah dengan menyandikan informasi tersebut.

Cabang ilmu pengetahuan yang mempelajari penyandian adalah *kriptologi*, kriptologi terdiri dari dua bagian yaitu *kriptografi* dan *kriptoanalis.* Kriptografi adalah seni untuk mengamankan informasi atau *plainteks* dengan menggunakan teknik penyandian sedangkan kriptoanalis adalah seni untuk memecahkan sandi. Dalam kriptografi terdapat sistem kriptografi yang disebut *kriptosistem* yang melibatkan dua pihak yaitu pihak pengirim dan penerima. Pengirim akan mengubah informasi asli (*plainteks*) sebelum mengirimkan kepada penerima. Proses penyandian informasi disebut *enkripsi* sedangkan informasi yang diperoleh dari proses enkripsi disebut *ciperteks*. Kemudian penerima akan menguraikan ciperteks untuk mendapatkan kembali informasi asli (*plainteks*). Proses tersebut disebut *dekripsi*.

Mengingat informasi yang dikirim melalui jaringan komunikasi maka diperlukan kunci dalam proses enkripsi dan dekripsi. Dalam proses enkripsi dan dekripsi dapat menggunakan kunci berbeda. Enkripsi menggunakan kunci yang

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

diketahui oleh umum disebut dengan kunci publik (*public key*) sedangkan dekripsi menggunakan kunci rahasia (*private key*) yang hanya diketahui pihak penerima.

Salah satu metode dalam kriptografi yang menggunakan kunci berbeda adalah *Algoritma LUC*, yang diberi nama sesuai penemu barisan Lucas yaitu Edouard Lucas. Algoritma LUC adalah metode penyandian yang menggunakan bilangan prima sebagai pembangkit kunci untuk enkripsi maupun dekripsi dan barisan Lucas untuk melakukan proses enkripsi maupun dekripsi.

1.2 PERUMUSAN MASALAH

Perumusan masalah yang akan diangkat dalam tugas akhir ini adalah bagaimana menerapkan algoritma LUC dalam kriptografi dan implementasinya dalam menyandikan teks.

1.3 PEMBATASAN MASALAH

Dalam tugas akhir ini yang akan dibahas adalah cara kerja algoritma LUC dalam kriptografi dan tidak dibahas proses pengiriman ciperteks. Sumber kode yang digunakan adalah kode ASCII (*American Standard Code for Information Interchange*) dari bilangan desimal 32 sampai 126 yang dimodifikasi menjadi 01 sampai 95.

1.4 TUJUAN

Tujuan penulisan tugas akhir ini adalah :

1. Memahami algoritma LUC dalam menyandikan suatu string berupa teks

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

2. Pembangkitan kunci enkripsi dan dekripsi dengan algoritma LUC
3. Mengimplementasikan algoritma LUC untuk penyandian teks dalam bahasa pemrograman Turbo Pascal.

1.5 SISTEMATIKA PENULISAN

BAB I berisikan latar belakang, perumusan masalah, pembatasan masalah, tujuan dan sistematika penulisan

BAB II berisikan dasar teori meliputi fungsi, teori bilangan berupa pembagi dan aritmatika modulo, sistem bilangan biner serta barisan Lucas

BAB III berisikan pembahasan meliputi konsep dasar kriptografi, kriptografi kunci umum, barisan Lucas dalam kriptografi, algoritma LUC dan implementasi algoritma LUC

BAB IV berisi kesimpulan

DAFTAR PUSTAKA

LAMPIRAN

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)