BAB I
PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan dan kerahasiaan data merupakan suatu aspek yang penting. Pesan, data, atau informasi akan tidak berguna lagi apabila di tengah jalan disadap atau dibajak oleh orang yang tidak berkepentingan. Kriptografi merupakan solusi dalam menangani masalah keraharasiaan dan keamanan data. Kriptografi merupakan ilmu dan seni untuk mengamankan pesan. Seiring dengan perkembangan zaman, metode kriptografi diterapkan dalam berbagai aspek kebutuhan manusia seperti untuk mengamankan data sehingga saat ini banyak bermunculan algoritma modern.

Stream chiper adalah salah satu metode kriptografi modern yang populer karena di samping prosesnya yang memakan waktu lebih singkat, *stream chiper* juga menggunakan memori yang lebih sedikit. *Stream chiper* melakukan penggabungan sebuah *plaintext* dan bit semu acak dengan menggunakan operasi eksklusif *or* untuk mendapatkan sebuah *chipertext* pada proses enkripsi dan untuk mendapatkan kembali *plaintext* awal, *chipertext* cukup digabungkan dengan bit semu acak yang sama menggunakan operasi eksklusif *or* kembali.

LFSR (*Linear Feedback Shift Register*) adalah salah satu jenis generator yang dapat menghasilkan bit semu acak. LFSR sering digunakan karena mampu menghasilkan bit semu acak dengan periode maksimal yang panjang dan mudah diaplikasikan dalam berbagai hal. Namun seiring dengan perkembangan zaman, penggunaan sebuah LFSR sebagai generator bit semu acak rawan terhadap serangan kriptanalisis karena bit semu acak yang dihasilkan generator LFSR akan mengalami perulangan di setiap periodenya. Oleh karena itu diperlukan fungsi-fungsi tambahan karena kekuatan algoritma *stream cipher* terletak pada keacakan rangkaian bit semu acak yang dihasilkan bukan tergantung pada kerahasiaan algoritmanya.

LFSR menggunakan polinomial dalam menghasilkan bit semu acak. Polinomial berfungsi sebagai fungsi *feedback* dari generator LFSR. Penggunaan

jenis polinomial mempengaruhi tingkat keacakan bit semu acak yang dihasilkan LFSR. Berdasarkan semua hal yang telah dijabarkan di atas, maka pada skripsi ini dilakukan pengembangan algoritma enkripsi dekripsi berbasis LFSR dengan menggunakan polinomial primitif sebagai generator yang mampu menghasilkan bit semu acak yang lebih tahan terhadap serangan kriptanalisis.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka diperoleh rumusan permasalahan pada tugas akhir ini yaitu bagaimana merancang sebuah algoritma enkripsi dekiripsi berbasis LFSR dengan menggunakaan polinomial primitif yang mampu menghasilkan bit semu acak yang lebih tahan terhadap serangan kriptanalisis?

1.3 Tujuan

Penelitian ini bertujuan untuk merancang sebuah algoritma enkripsi dekripsi berbasis LFSR dengan menggunakan polinomial primitif yang mampu menghasilkan bit semu acak yang lebih tahan terhadap serangan kriptanalisis.

1.4 Batasan Masalah

Batasan masalah yang didefinisikan dalam pelaksanaan tugas akhir ini adalah:

1. Algoritma yang akan dibuat dalam skripsi ini berbasis *Linear Feedback Shift Register*.
2. Data masukan berupa *plaintext*

1.5 Sistematika Penulisan

Sistematika penulisan dokumen skripsi adalah sebagai berikut:

BAB 1 – Pendahuluan

Bab Pendahuluan membahas latar belakang penulisan tugas akhir, rumusan permasalahan, tujuan tugas akhir, ruang lingkup dan batasan permasalahan yang ditangani, metodologi pengerjaan tugas akhir yang digunakan, serta sistematika pembahasan.

BAB II – Tinjauan Pustaka

Bab Tinjauan Pustaka berisi teori-teori yang menguraikan konsep-konsep yang mendasari dan mendukung masalah Tugas Akhir. Konsep yang akan dibahas meliputi definisi kriptografi, bilangan semu acak, generator LFSR (*Linear Feedback Shift Register*), multi register, dan test uji statistik.

BAB III – Metodologi

Bab Metodologi berisi tentang metode-metode yang dipakai dalam melakukan perancangan, pengujian, dan analisis data.

BAB IV – Perancangan

Bab Perancangan berisi perancangan dan perealisasian alat yang meliputi spesifikasi, perencanaan diagram blok, prinsip kerja dan realisasi alat.

BAB V– Implementasi dan Algoritma

Bab Implementasi dan Algoritma memuat aspek implementasi, instruksi penggunaan alat, serta algoritma yang dipakai dalam pembuatan alat

BAB VI -- Pengujian dan Analisis

Bab Pengujian dan Analisis memuat aspek pengujian meliputi penjelasan tentang cara pengujian dan hasil pengujian. Aspek analisis meliputi penilaian atau komentar terhadap hasil-hasil pengujian. Pengujian dan analisis ini terhadap alat yang telah direalisasikan berdasarkan masing-masing blok dan sistem secara keseluruhan.

BAB VII Kesimpulan dan Saran

Bab Kesimpulan dan Saran memuat intisari hasil pengujian dan menjawab rumusan masalah serta memberikan rekomendasi untuk perbaikan kualitas penelitian dimasa yang akan datang.