ABSTRAKSI

Dalam era informasi, pemanfaatan informasi menjadi sesuatu yang vital. Nilai suatu keputusan suatu organisasi maupun suatu individu sangatlah tergantung dari kekayaan informasi yang dimilikinya. Saat ini informasi telah menjadi basis pengetahuan dalam pengambilan keputusan, dan tentunya hal ini merupakan kekuatan bagi individu maupun organisasi yang memilikinya. Oleh karena itu, upaya mendapatkan informasi menjadi kebutuhan yang mendasar bagi suatu individu maupun organisasi. Disatu hal ini mendorong timbulnya kriminalitas, yaitu mendapatkan informasi secara tidak sah. Salah satu cara untuk mengamankan data dan menjaga kerahasiaan data dari pengguna yang tidak sah adalah dengan menggunakan kriptografi yaitu ilmu yang mempelajari penulisan secara rahasia. Dengan kriptografi data diubah ke bentuk yang tidak dapat dipahami sehingga tidak dapat dibaca oleh orang tidak berkepentingan.

Dalam tugas akhir ini mempelajari dan mengimplementasikan algoritma kriptografi GOST dengan menggunakan mode operasi ECB *(Electronic Code Blok)* dan CBC *(Cipher Blok Chaining)*. Selain itu juga dilakukan beberapa analisa terhadap hasil implementasi seperti *Avallanche effect*, *Weak key* dan *Semi weak key*, disamping analisa terhadap struktur algoritma GOST itu sendiri.

Kesimpulan yang diperoleh dari implementasi dan analisa terhadap algoritma kriptografi GOST antara lain : Kelebihan dari struktur *fiestal network* adalah modul untuk proses enkripsi dan dekripsi adalah sama hanya saja urutan sub – kunci yang digunakan terbalik, GOST memiliki *avallanche effect* yang baik, hal ini diperlihatkan dari hasil proses enkripsi terhadap dua *plaintext* yang berbeda satu bit menyebabkan *ciphertext* yang berbeda kurang lebih 46% dari total satu blok.

Kata kunci : Kriptografi, *Blok Cipher*, "GOST", *Avallanche effect*