ABSTRAK

SYAHRUL MAULIDIN

Rancangan Sistem Keamanan Algoritma Gronsfeld Cipher dengan Pembangkit Bilangan Acak LCG (*Linear Congruential Generator*)

2019

Untuk menjaga keamanan data supaya data tidak disalahgunakan oleh orang yang tidak bertanggungjawab, salah satu cara yang bisa digunakan yaitu dengan menggunakan metode kriptografi untuk mengenkripsi *file*, sehingga tidak dapat disalahgunakan oleh orang yang tidak berhak. Salah satu algoritma kriptografi adalah Gronsfeld yang merupakan algoritma *plaintext* kriptografi *modern* kunci simetris berbentuk cipher *block*. Enkripsi dilakukan dengan menggunakan penggabungan antara Gronsfeld dengan pembangkit bilangan acak LCG (*Linear Congruential Generator*). Aplikasi yang dibangun ini dapat mengenkripsi *plaintext* sehingga menghasilkan *ciphertext*. *Ciphertext* tersebut dapat dikembalikan seperti semula jika didekripsi menggunakan kunci yang sama sewaktu mengenkripsi *plaintext* tersebut. Kunci yang digunakan tidak membutuhkan batasan maksimum karakter. Metode yang digunakan untuk membangun aplikasi ini adalah metode deskriptif. Perangkat lunak yang digunakan untuk *user system interface*-nya adalah Visual Studio 2012.

Keywords : Dekripsi, Enkripsi, Gronsfeld, LCG (*Linear Congruential Generator*)