ABSTRAK

Random Number Generator memiliki peranan penting dalam bidang kriptografi. RNG seringkali digunakan utuk membangkitkan seed dari berbagai algoritma kriptografi yang ada, misalnya saja untuk membangkitkan seed yang akan digunakan dalam algoritma block cipher atau membangkitkan bilangan prima untuk algoritma RSA. Skripsi ini akan membahas mengenai dua algoritma pembangkit bilangan acak, yaitu Blum Blum Shub dan Linear Congruential Generator, baik itu cara algoritmanya, cara kerjanya serta perbandingan kedua algoritma tersebut.

ABSTRACT

Random Number Generator has an important role of cryptography. RNG is often used to generate seeds from various existing cryptographic algorithms, for example to generate seeds that will be used in block cipher algorithms or generate prime numbers for the RSA algorithm. This thesis will discuss two random number generator algorithms, namely Blum Blum Shub and Linear Congruential Generator, both the way the algorithm works, how it works and the comparison of the two algorithms.