ABSTRACT

Cryptographically Secure Pseudorandom Number Generator (CSPRNG) is a random number generator that can generate the unpredictable number from the attacker. The generator is suitable for cryptography for example used for generating key elements. This key has important role on security of cryptography. If the key is increasingly difficult predictabled, the cryptography is increasingly secure from the attacker. Not likely any other Pseudorandom Number Generator (PRNG) that usually is not enough secure from attack, Cryptographically Secure Pseudorandom Number Generator (CSPRNG) come with better performance so that can solve this matter. This is possible because Cryptographically Secure Pseudorandom Number Generator (CSPRNG) is built based on difficult mathematical operation for example getting the primes factor of any number, discrete logarithm and so on.

Blum Blum Shub and modified RSA are two random number generator of Cryptographically Secure Pseudorandom Number Generator (CSPRNG). Both of this random number generator can generate the unpredictable number from the attacker because have good characteristic statistically like pass the random test and powerful from serious attack. Both of this random number generator will be functioned as key for encryption in RC4 algorithm.

After that all, test and analysis will be done for RC4 algorithm with parameter such as variance, frequency distribution, time processing, avalanche effect and brute force attack. So that the performance from both of the random number generator can be known and which generator has the best performance can be concluded.

From the analysis for those parameter can be obtained that RC4 using Blum Blum Shub has better performance than modified RSA for these case such as faster time processing, smaller variance, smooth frequency distribution. Whereas for avalanche effect parameter, both of these key has same performance.