ABSTRAK

Cryptographically Secure Pseudorandom Number Generator (CSPRNG) adalah pembangkit bilangan acak yang dapat menghasilkan bilangan yang tidak mudah diprediksi pihak lawan. Pembangkit tersebut cocok untuk kriptografi misalnya digunakan untuk pembangkitan elemen-elemen kunci. Kunci inilah yang memegang peranan sangat penting dalam masalah keamanan kriptografi. Semakin sulit kunci itu ditebak oleh pihak lawan maka kriptografi tersebut akan semakin aman dari serangan. Tidak seperti *Pseudorandom Number Generator* (PRNG) lainnya yang biasanya kurang aman terhadap serangan, *Cryptographically Secure Pseudorandom Number Generator* (CSPRNG) hadir dengan performansi lebih baik sehingga dapat mengatasi hal tersebut. Hal ini dimungkinkan karena *Cryptographically Secure Pseudorandom Number Generator* (CSPRNG) dirancang berdasarkan operasi matematika yang sulit seperti pemfaktoran bilangan menjadi faktor prima, logaritma diskrit dan sebagainya.

Blum Blum Shub dan *modified* RSA merupakan dua pembangkit bilangan acak *Cryptographically Secure Pseudorandom Number Generator* (CSPRNG). Kedua macam pembangkit bilangan acak ini dapat menghasilkan bilangan yang tidak mudah diprediksi (*secure*) pihak lawan karena secara statistik memiliki sifat-sifat yang bagus seperti lolos uji keacakan statistik dan tahan terhadap serangan (*attack*) yang serius. Kedua pembangkit bilangan acak ini akan difungsikan sebagai *key* untuk enkripsi pada algoritma RC4.

Setelah itu akan dilakukan pengujian dan analisis terhadap algoritma RC4 dengan parameter seperti variansi, distribusi frekuensi, waktu proses, *avalanche effect* dan *brute force attack.* Dengan demikian dapat diketahui performansi dari kedua pembangkit bilangan acak tersebut dan dapat diambil kesimpulan pembangkit mana yang mempunyai kinerja terbaik.

Dari hasil analisis terhadap parameter tersebut diperoleh bahwa RC4 dengan *Blum Blum Shub* memiliki keunggulan dibandingkan *modified* RSA dalam hal waktu proses yang lebih cepat, variansi yang lebih kecil, distribusi frekuensi yang lebih merata. Sedangkan untuk parameter *avalanche effect*, kedua pembangkit bilangan acak ini memiliki performansi yang sama.