ABSTRAK

Saat ini, pengembangan ilmu pengetahuan pada bidang kriptografi telah menemukan ranah baru dimana ditemukannya kombinasi antara bidang biologi dan kriptografi yang memadukan sifat-sifat DNA dan enkripsi menjadi sebuah bentuk baru yang disebut DNA Kriptografi. DNA kriptografi merupakan ranah baru dari bidang kriptografi yang didasari oleh riset mengenai DNA komputasi dan teknologi baru yaitu : PCR (*Polymerase Chain Reaction*), *microarray*, dll. DNA kriptografi menggunakan sifat-sifat DNA untuk mengenkripsi sebuah *plaintext*. Pada penerapannya diusulkan sebuah metode untuk mengimplementasikan DNA kriptografi yaitu menggunakan metode *One time Pad.*

Algoritma DNA berbasis *One Time Pad* (OTP) ini akan implementasikan, menggunakan dua prosedur algoritma klasik yaitu *vigenere chipher(XOR) dan subtitution table*. Permasalahannya adalah kedua algoritma klasik ini sudah sangat mudah dipecahkan menggunakan metode *kasisi test* (untuk algoritma *vigenere chipher(XOR)*) dan analisis frekuensi (untuk algoritma *subtitution table*). Pada tugas akhir ini, DNA Kriptografi berbasis *One Time Pad* akan diperkuat mengunakan random generator BBS untuk mengatasi permasalahan *kasisi test* dan analisis frekuensi.

Pada pengujian yang dilakukan DNA Kriptografi tahan terhadap kedua attack diatas dan memiliki nilai *Avalanche Effect* mendekati optimal yaitu 53,03%. Namun dari penggunaan memori, hasil enkripsi memiliki besar data hampir 3 kali lipat dari *plaintext* awal. Serta memiliki waktu eksekusi yang lebih lama dari sistem originalnya.

Kata Kunci : Kriptografi, *One-Time-Pads*, DNA Kriptografi, *Vigenere chipher(XOR), Subtitution table*