1. Pendahuluan

1.1 Latar Belakang

Saat ini, pengembangan ilmu pengetahuan pada bidang kriptografi telah menemukan ranah baru dimana terdapat 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.*

Permasalahannya, algoritma DNA berbasis *One Time Pad* (OTP) yang akan implementasikan, menggunakan dua prosedur algoritma klasik yaitu *vigenere chipher(XOR) dan subtitution table*. Kedua algoritma klasik ini sudah sangat mudah dipecahkan menggunakan metode *kasisi test* (untuk algoritma *vigenere chipher(XOR)*) dan analisis frekuensi (untuk algoritma *subtitution table*).

Berdasarkan pada masalah diatas, pada tugas akhir ini, DNA Kriptografi berbasis *One Time Pad* akan diperkuat mengunakan *random generator* BBS untuk mengatasi permasalahan *kasiski test* dan analisis frekuensi.

1.2 Perumusan Masalah

Bedasarkan latar belakang di atas, permasalahan dalam tugas akhir ini adalah DNA Kriptografi berbasis *One Time Pad* yang diterapkan menggunakan dua prosedur algoritma klasik yaitu *vigenere chipher(XOR) dan subtitution table* sangat rentan terhadap serangan Kasiski Test dan Analisa Frekuensi.

1.3 Batasan Masalah

Batasan masalah untuk penelitian Tugas Akhir ini adalah :

1. Penerapan DNA Kriptografi dalam sistem tidak menggunakan media transmisi jaringan yang sesungguhnya namun hanya menggunakan simulasi sehingga tidak akan membahas masalah keamanan trafik pada jaringan, misalnya *cell loss*.
2. Aplikasi dibangun menggunakan pemrograman JAVA baik enkripsi maupun dekripsinya.
3. Tidak dilakukan pengamanan terhadap kunci yang dihasilkan. Dengan asumsi bahwa kunci yang dikirimkan dari *sender* ke *receiver* aman.
4. Lingkup sistem yang dibangun hanya sebatas enkripsi dan dekripsi.
5. *Seed key* pada BBS Generator tidak di-*generate* secara otomatis namun diinputkan oleh user
6. Tidak adanya pengecekan terhadap *seed key* yang diinputkan dengan diasumsikan bahwa setiap *seed key* yang diinputkan tidak pernah sama antara satu dengan yang lainnya. Sehingga tidak menyalahi konsep *One Time Pad*.

1.4 Tujuan

Tujuan yang ingin dicapai dari penelitian Tugas Akhir ini adalah menerapkan algoritma DNA Kriptografi berbasis *One Time Pad* y menggunakan *genertor* BBS kemudian mengukur tingkat kekuatan DNA Kriptografi terhadap serangan dari motode Analisis Frekuensi dan *Kasiski Test*.

Hipotesa : pada penerapannya DNA kriptografi menerapkan prosedur algoritma klasik *vigenere chipher* dan *subtitution chipher*. Kedua algoritma klasik ini sudah sangat mudah dipecahkan menggunakan metode *Kasiski Test* (untuk algoritma *vigenere chipher*) dan analisis frekuensi (untuk algoritma *subtitution chipher*).[4] sehingga untuk mengatasi permasalahan ini diajukan BBS Generator agar DNA kriptografi tahan terhadap serangan *Kasiski Test* dan Analisis Frekuensi. BBS dipilih karena merupakan salah satu random number yang kuat.

Dengan penambahan BBS Generator ke dalam sistem maka akan semakin menyulitkan kripanalis dalam melakukan serangan terhadap sistem dan meningkatkan kekuatan sistem.

1.5 Metodologi Penyelesaian Masalah

Tahap penyelesaian dalam Tugas Akhir ini adalah Studi Literatur, Desain Sistem dan Perancangan Sistem, Implementasi, Pengujian Sistem dan Analisis Hasil Pengujian.

Pada studi literatur dilakukan untuk memperlajari konsep dan teori-teori pendukung yang akan digunakan untuk mendesain sistem DNA kriptografi berbasis *One Time Pad.* Pembelajaran yang perlu dilakukan meliputi pencarian referensi dan sumber-sumber yang berhubungan dengan DNA Kriptografi serta pencarian referensi dan sumber-sumber yang berhubungan dengan Blum Blum Shub.

Pada tahap Desain dan Perancangan Sistem dilakukan analisis model sistem yang akan dibuat dan perancangan sistem yaitu desain aplikasi yang akan dibangun. Kemudian, merancang sistem yang sesuai untuk memenuhi kebutuhan. Rancangan ini akan digunakan sebagai panduan untuk implementasi perangkat lunak.

Pada implementasi ini dilakukan implementasi untuk membangun sistem DNA kriptografi. Implementasi dilakukan dengan menggunakan bahasa pemrograman JAVA dan dibangun pada komputer desktop baik proses enkripsi dan dekripsinya. Pada tahap ini dibangun sistem yang dapat melakukan enkripsi dan dekripsi berbasis sifat DNA menggunakan generator BBS.

Kemudian dilakukan Pengujian sistem aplikasi yang telah dibuat terhadap kelayakannya sebagai alat bantu pengamatan tugas akhir. Pengujian dilakukan

dengan mengukur waktu eksekusi sistem, mengukur memori yang digunakan setelah proses enkripsi serta menghitung nilai *avalanche effect*.

Pada tahap terakhir dilakukan analisis hasil pengujian terhadap data yang diambil dari pengamatan parameter-parameter. Parameter tersebut adalah waktu eksekusi, besar memori yang dipakai ketika proses enkripsi dan pola-pola yang dihasilkan untuk mengetahui nilai *avalanche effect*.