1. Pendahuluan

1.1 Latar belakang

Perkembangan teknologi mengalami kemajuan yang sangat pesat dan semakin hari teknologi semakin canggih. Oleh karena itu, diperlukan pengamanan yang ketat untuk melindungi kerahasiaan data dari orang yang tidak berhak. Salah satu teknologi pengamanan data adalah dengan menggunakan kriptografi yang dewasa ini banyak digunakan oleh masayarakat.

Kriptografi adalah ilmu penyandian data yang dipakai untuk memecahkan masalah keamanan dan kerahasiaan data. Dengan menggunakan kriptografi, data sederhana yang dikirim (plainteks) diubah ke dalam bentuk data sandi (cipherteks), kemudian data sandi tersebut hanya dapat dikembalikan ke bentuk data sebenarnya hanya dengan menggunakan kunci (*key*) tertentu yang dimiliki oleh pihak yang sah saja. Tentunya hal ini menyebabkan pihak lain yang tidak memiliki kunci tersebut tidak akan dapat membaca data yang sebenarnya sehingga dengan kata lain data akan tetap terjaga. Saat ini telah banyak berbagai macam algoritma kriptografi dimana setiap algoritma menawarkan kelebihan dan memiliki kekurangan masing-masing.

Dari sekian banyak algoritma kriptografi, *National Institute of Standards and Technology* (NIST) mencari sebuah algoritma yang akan dijadikan sebuah standard algoritma kriptografi. Dalam sayembara yang diadakan oleh NIST, algoritma kriptografi Rijndael keluar sebagai pemenangnya. Algoritma kriptografi Rijndael merupakan algoritma *cipher* blok (*block cipher*) yang dibuat oleh Joan Daemen and Vincent Rijmen pada tahun 1998. Pada tahun 2000, Vincent Rijmen and Paulo S. L. M. Barreto membuat sebuah algoritma *cipher* blok yang diberi nama Anubis. Teknik enkripsi atau dekripsi antara algoritma kriptografi Anubis dan Rijndael memiliki beberapa kesamaan, antara lain adanya struktur perulangan, menggunakan tabel substitusi, pembangkitan kunci internal. Namun kesamaan ini hanya struktural, karena operasi matematika yang dilakukan di dalamnya berbeda.

Dalam Tugas Akhir ini, alasan penulis memilih untuk membandingkan algoritma kriptografi Anubis dan Rijndael antara lain :

1. Kedua algoritma kriptografi tersebut menggunakan inputan yang sama yaitu 128 bit dan dengan panjang kunci 128, 192 atau 256 bit.
2. Algoritma kriptografi Anubis dan Rijndael memiliki beberapa kemiripan struktural.

1.2 Perumusan masalah

Berdasarkan latar belakang yang dikemukakan di atas, maka permasalahan yang akan dijadikan objek penelitian adalah :

1. Bagaimana mengimplementasikan algoritma kriptografi Anubis dan Rijndael ke dalam sebuah perangkat lunak.
2. Membandingkan antara implementasi algoritma Anubis dan Rijndael berdasarkan waktu proses untuk melakukan enkripsi atau dekripsi, memori yang digunakan dalam proses enkripsi atau dekripsi, dan *avalanche effect*.

Pada penelitian Tugas Akhir ini dibatasi oleh empat batasan masalah, yaitu :

1. Menggunakan inputan file berupa teks.
2. Panjang inputan yang digunakan 128 bit dengan panjang kunci 128 bit.
3. Parameter yang digunakan untuk menganalisa hasil pengujian perangkat lunak adalah waktu proses untuk melakukan enkripsi atau dekripsi, memori yang digunakan dalam proses enkripsi atau dekripsi, dan *avalanche effect*.
4. Kotak Substitusi (*S-Box*), konstanta putaran (*rcon*), dan matriks pengali telah ditetapkan.

1.3 Tujuan

Secara umum, tujuan yang ingin dicapai dalam tugas akhir ini adalah :

1. Merancang dan mengimplementasikan proses penyandian data menggunakan perangkat lunak dengan algoritma kriptografi Anubis dan Rijndael.
2. Menganalisa dan menampilkan hasil perbandingan implementasi algoritma kriptografi Anubis dan Rijndael untuk penyandian data berdasarkan parameter waktu proses enkripsi atau dekripsi, memori yang digunakan dalam proses enkripsi atau dekripsi, dan *avalanche effect*.

1.4 Metodologi penyelesaian masalah

Metodologi yang digunakan dalam melakukan penelitian Tugas Akhir ini mencakup hal-hal sebagai berikut :

1. Mengumpulkan data dan bahan-bahan referensi yang menunjang proses penelitian seperti jurnal-jurnal tentang algoritma kriptografi Anubis dan Rijndael serta semua yang berkaitan dengan ilmu kriptografi secara umum.
2. Identifikasi permasalahan yang akan muncul pada saat melakukan penelitian.
3. Membuat perancangan perangkat lunak algoritma kriptografi Anubis dan Rijndael dan kemudian mengimplementasikannya.
4. Melakukan analisa perbandingan algoritma kriptografi Anubis dan Rijndael.
5. Penyusunan laporan Tugas Akhir dan membuat kesimpulan dari hasil penelitian.