1. Pendahuluan

1.1 Latar belakang

Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting dalam komunikasi data, baik untuk tujuan keamanan bersama, maupun untuk privasi individu. Mereka yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikan. Ketika suatu pesan dikirim dari satu tempat ke tempat lain, isi dari pesan tersebut kemungkinan dapat disadap oleh pihak lain. Untuk menjaga keamanan pesan, maka pesan tersebut dapat diacak atau diubah menjadi kode yang tidak dimengerti orang lain, namun dapat dikembalikan menjadi pesan semula. Perlindungan terhadap kerahasiaan datapun meningkat, salah satu caranya adalah dengan penyandian data atau enkripsi. Sebagai media komunikasi umum, Internet sangat rawan terhadap penyadapan, pencurian, dan pemalsuan informasi. Karena itu eksploitasi Internet oleh sektor-sektor strategis seperti bisnis, perbankan, atau pemerintahan sangat memerlukan teknologi penyandian Informasi.

Ada beberapa teknik yang dapat digunakan untuk menerapkan sistem kriptografi, yaitu konvensional dan kunci publik. Pada kriptografi konvensional, untuk mengubah *plaintext* ke bentuk chipertext dan proses kebalikannya menggunakan kunci yang sama atau disebut juga *symetric*, sedangkan pada kriptografi kunci publik atau disebut juga kriptografi *asymetrik*, diperlukan 2 buah kunci. Satu kunci yang disebut kunci publik (*publik key*) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (*private key*) harus dirahasiakan. Algoritma DES (Data Encryption Standard) sebagai salah satu algoritma kriptografi *symetric*, memiliki blok kunci 64 bit tetapi yang digunakan dalam eksekusi hanya 56 bit dan merupakan algoritma enkripsi yang paling banyak digunakan di dunia, karena secara teori blok kunci 56 bit termasuk algoritma enkripsi yang mudah yang kuat dan tidak mudah di terobos [8]. Algoritma DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. Dengan demikian, DES termasuk keluarga block *chiper*. Dengan tahapan dan kunci yang sama, DES digunakan untuk membalik enkripsi. Algoritma DES sangat banyak digunakan untuk melindungi data dalam dunia elektronik khususnya di bidang perbankan, finansial, dan *e-commers.* Hingga kini algoritma DES masih kebal terhadap *cryptanalysis* baik yang berjenis *linier cryptoanalysis* maupun *differential cryptanalysis*, dua teknik yang dikenal sebagai cara yang paling ampuh untuk memecahkan sandi modern [4].

Algoritma kunci publik yang paling umum digunakan adalah RSA(Rivest Shamir Adleman). RSA dianggap aman karena sulitnya pemfaktoran bilangan yang sangat besar meskipun tidak pernah dibuktikan aman tidaknya [7]. Dilihat dari persamaan matematisnya, algoritma RSA sulit dipecahkan karena sulitnya pemfaktoran bilangan prima yang sangat besar. Jumlah bilangan prima yang tersedia pada bilangan 512 bit adalah sekitar 10 pangkat 151, jika terdapat mendapatkan 1000 bilangan prima, maka diperlukan hanya 1000 milyar (10 pangkat 12) bilangan prima yang berbeda untuk memenuhinya. Jumlah ini cukup

kecil jika dibandingkan bilangan prima yang tersedia pada 512 bit (sekitar 10 pangkat 151), apalagi jika menggunakan 1024 bit (tersedia sekitar 10 pangkat 305 bilangan prima) [9].

Pada kenyataanya RSA dianggap aman karena memiliki pemfaktoran bialangan prima yang besar, walaupun belum pernah ada yang membuktikan, sedangkan algoritma DES banyak diterapkan dalam dunia nyata terutama dalam dunia perbankan. Oleh karena itu diperlukan suatu pengujian terhadap algoritma DES sebagai algoritma *symetrik* dan membandingkannya dengan algoritma *asymetrik* yang umum digunakan yaitu algoritma RSA. Pengujian dilakukan terhadap file (*.txt) menggunakan perangkat lunak sebagai simulasi suatu sistem kriptografi yang menggunakan algoritma DES dan RSA.

1.2 Perumusan masalah

Dalam tugas akhir ini dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana membangun prangkat lunak berdasarkan algoritma kriptografi DES dan algoritma RSA.
2. Menganalisis performansi implementasi perangkat lunak kriptografi algortima DES dan RSA berdasarkan parameter tertentu.

Adapun batasan masalah tugas akhir ini adalah sebagai berikut :

1. Data atau pesan yang dienkripi atau didekripsi berupa text.
2. Perangkat lunak yang dihasilkan merupakan simulasi dari kedua algoritma.
3. Algoritma RSA yang digunakan memiliki kunci 8 bit, 16 bit, dan 24 bit.
4. Algoritma DES enkripsi data pada 64 bit

1.3 Tujuan

1. Mengimplementasikan Algoritma DES dan RSA dalam bentuk perangkat lunak
2. Menganalisis performansi algoritma RSA berdasarkan jumlah kunci, pembengkakan *chipertext*, dan pemakaian memori pada saat proses enkripsi dan dekripsi. Yang kemudian dibandingkan dengan algoritma DES

1.4 Metodologi penyelesaian masalah

Metode yang digunakan dalam penyelesaian tugas akhir ini adalah menggunakan metode studi pustaka atau studi literatur dan analisis dengan langkah kerja sebagai berikut:

1. Studi Literatur:
   a. Pencarian referensi
      Mencari referensi dan sumber-sumber lain yang layak yang berhubungan dengan materi kriptografi terutama mengenai algoritma DES dan algoritma RSA.

b. Pendalaman materi
   Mempelajari dan memahami materi yang berhubungan dengan tugas akhir ini.

2. Mempelajari konsep dasar dari kedua algoritma (algoritma DES dan RSA) secara detail yang digunakan sebagai langkah awal dalam mendesain perangkat lunak.
3. Melakukan perancangan dan implementasi perangkat lunak. Bertujuan merancang perangkat lunak yang dibuat, metode pengembangan perngkat lunak yang digunakan adalah model *waterfall* yang disebut juga *clasic life cycle*.
4. Pengujian dan analisis. Bertujuan menganalisis apakah perangkat lunak yang dibuat sesuai dengan spesifikasi yang diinginkan. Analisis dilakukan terhadap kedua algoritma setelah perangkat lunak selesai dibuat.
5. Pengambilan kesimpulan dan penyusunan laporan tugas akhir. Merupakan hasil analisis perbandingan dari kedua algoritma berdasarkan perangkat lunak yang telah dibuat.