# BAB 1

# PENDAHULUAN

## 1.1.Latar Belakang

Seiring dengan semakin berkembangnya teknologi jaringan komputer dan internet banyak orang yang memanfaatkan internet tersebut untuk saling bertukar dokumen/*file*. Pertukaran *file* di dunia maya merupakan salah satu hal yang sangat sering terjadi didalam kehidupan kita saat ini. Ada saat dimana suatu *file* tersebut bersifat rahasia sehingga tidak boleh ada orang lain yang mengetahui informasi selain orang yang dituju. Oleh karena itu metode pertukaran *file* melalui internet harus dibuat sedemikian rupa sehingga tidak ada orang lain selain orang yang dituju yang dapat mengambil ataupun mencuri *file* tersebut. Dengan demikian, tingkat keamanan yang tinggi juga semakin diperlukan untuk menghindari pencurian *file* pada saat terjadinya proses pertukaran *file* yang mungkin saja bisa terjadi dan tentunya kejadian seperti itu tidak kita kehendaki karena mungkin saja *file* tersebut bersifat sangat rahasia dan dikhawatirkan *file* tersebut dicuri seseorang dan kemudian disalahgunakan untuk merusak ataupun melakukan tindak kejahatan lainnya. Maka dengan itu dibutuhkan suatu sistem keamanan yang mengimplementasikan kriptografi data untuk menjaga kerahasiaan *file* dengan teknik enkripsi dan dekripsi.

Kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi, seperti kerahasiaan, keutuhan data, dan otentikasi entitas. Kriptografi menjamin kerahasiaaan pesan ataupun dokumen-dokumen yang ingin disampaikan dari orang yang satu ke orang yang lain. Kriptografi telah menjadi bagian penting dalam dunia teknologi informasi saat ini. Hampir semua penerapan teknologi informasi menggunakan kriptografi sebagai alat untuk menjamin keamanan dan kerahasiaan dokumen. Karena itu pulalah, kriptografi menjadi ilmu yang berkembang pesat. Dalam waktu singkat, amat banyak bermunculan algoritma-algoritma baru yang dianggap lebih unggul daripada pendahulunya.

Dalam kriptografi data asli disebut dengan *plaintext*. Pengamanan *plaintext* dalam kriptografi dapat dilakukan dengan 2 macam teknik, yaitu dengan menggunakan penyandian kunci simetris dan penyandian kunci asimetris. Algoritma simetris adalah algoritma yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Sedangkan, algoritma asimetris memiliki dua kunci, yaitu kunci *private* yang berguna untuk dekripsi yang hanya diketahui oleh penerima pesan dan kunci publik yang berguna untuk enkripsi yang diumumkan kepada publik. Algoritma asimetris yang digunakan untuk proses penyandian ini adalah algoritma *Multi-Power RSA*, algoritma ini memiliki sifat menarik tidak hanya cepat tapi juga menghemat memori dibandingkan dengan algoritma *Multi-Factor* lainnya dan algoritma simetris yang digunakan adalah algoritma *Blowfish* dengan proses enkripsi dan dekripsi dilakukan dengan cara satu kali proses untuk masing-masing algoritma.

Algoritma *Blowfish* mempunyai kriteria sebagai berikut (Schneier, 1996):

1) Cepat, pengenkripsian data *Blowfish* dilakukan pada*microprocessors*32-bit dengan*rate*26*clock cycles*per*byte*.
2) Ringan, pada memori lebih kecil dari 5K *Blowfish*masih dapat dijalankan.
3) Sederhana, *Blowfish*hanya menggunakan operasi-operasi sederhana: penambahan, XOR, dan*lookup* tabel pada operan 32-bit.
4) Memiliki tingkat keamanan yang bervariasi, panjang kunci yang digunakan oleh *Blowfish* dapat bervariasi dan bisa sampai sepanjang 448 bit.

Algoritma asimetris memiliki kelebihan yaitu sangat bagus dalam hal enkripsi namun membutuhkan waktu proses yang cukup lama karna menggunakan perhitungan yang sangat rumit. Sedangkan pada algoritma simetris mempunyai kelebihan yaitu waktu enkripsinya yang cepat sehingga dapat meningkatkan performa sistem sedangkan kelemahan algoritma simetris yaitu sulitnya melakukan pertukaran kunci sehingga proses enkripsi dan dekripsi menjadi kurang aman. Selain itu jika pada tahap tertentu dibutuhkan perubahan kunci, maka proses pertukaran kunci perlu diulang. Dari kelebihan dan kelemahan tersebut perlunya mengkombinasikan algoritma asimetris dan simetris untuk menguatkan dan menutupi kelemahan masing-masing algoritma. Metode kombinasi ini disebut dengan *hybridcryptosystem* yang proses enkripsi dan dekripsi pesannya menggunakan algoritma simetris dan asimetris (Gutub & Khan, 2012).

## 1.2.Rumusan Masalah

Teknik enkripsi menggunakan algoritma asimetris, dalam hal ini menggunakan algoritma *Multi-Power RSA* lebih lambat dibandingkan enkripsi dengan menggunakan algoritma simetris dalam hal ini meggunakan algoritma *Blowfish* karena pada algoritma *Multi-Power RSA* menggunakan perhitungan matematika yang sangat rumit, untuk itu algoritma *Multi-Power RSA* perlu dikombinasikan dengan algoritma *Blowfish* untuk menutupi kelemahan dari algoritma *Multi-Power RSA*. Maka, penelitian ini akan membahas tentang pengamanan teksdengan menggunakan algoritma asimetris yaitu *Multi-Power RSA* dan algoritma simetris yaitu *Blowfish* menggunakan metode *Hybrid Cryptosystem.*

## 1.3.Tujuan Penelitian

1. Untuk mengimplementasikan *Hybrid Cryptosystem* dalam sebuah aplikasi yang menggunakan kombinasi algoritma *Multi-Power RSA*dan algoritma *Blowfish*dalam pengamanan teks.
2. Menganalisa waktu nyata (*real time*) enkripsi dan dekripsi pada pengamanan teks dalam *millisecond.*

### a. Batasan Penelitian

Batasan masalah dalam penelitian ini antara lain adalah sebagai berikut:

1. Teks dapat diambil pada format *file* .txt, .doc, dan .docx.
2. *Plaintext* dan *ciphertext* menggunakan karakter ASCII (*American Standard Code for Information Interchange*) 8 bit.
3. Menghitung *Real Running Time (ms).*
4. Bilangan prima yang digunakan maksimal 32 bit.
5. Konsep *hybrid* yang digunakan adalah dengan menggunakan algoritma asimetris *Multi-Power RSA* untuk membangkitkan *public key* dan *private key* dan algoritma simetris *Blowfish* untuk mengenkripsi dan dekripsi pesan.
6. Percobaan/simulasi dilakukan pada *Personal Computer*yang sama.
7. Menggunakan bahasa pemrograman C#.

b. **ManfaatPenelitian**

Penelitian ini diharapkan mampu memberikan kemudahan kepada masyarakat dalam merahasiakan pesan yang mereka kirimkan dan mendapatkan kembali pesan seperti semula.

c. **Metodologi Penelitian**

Metode penelitian yang dilakukan dalam penelitian ini adalah:

1. Studi Literatur

   Pada tahap ini penelitian dimulai dengan peninjauan pustaka berupa buku, artikel-artikel ilmiah, skripsi, dan penelitian-penelitian yang didokumentasikan dalam bentuk jurnal yang berhubungan dengan *Hybrid Cryptosystem*, Algoritma *Multi-Power RSA* dan Algoritma *Blowfish*.
2. Analisis dan Perancangan

   Berkaitan dengan batasan masalah, pada tahap ini dianalisa apa saja yang dibutuhkan dalam penelitian ini dan selanjutnya dirancang dalam sebuah model *flowchart*, *use case diagram*, *activity diagram*, dan *sequencediagram*sehingga menjadi sebuah informasi.
3. Implementasi

   Pada tahap ini perancangan diagram alir diimplementasikan dengan menggunakan bahasa pemrograman C#.
4. Pengujian

   Pada tahap ini prototipe yang telah dirancang dilakukan pengujian dengan menggunakan *file* teks berekstensi .txt, .doc, dan .docx.
5. Dokumentasi

   Pada tahap ini dilakukan pendokumentasian penelitian yang telah dilakukan mulai dari tahap analisa sampai kepada pengujian dalam bentuk skripsi.

**d. Sistematika Penulisan**

Sistematika penulisan skripsi in iterdiri dari beberapa bagian utama, yaitu:

**BAB 1 PENDAHULUAN**

Bab ini berisi latar belakang pemilihan judul skripsi "Pengamanan *File* Dengan *Hybrid Cryptosystem* Algoritma *Multi-Power RSA* dan Algoritma *Blowfish*", rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

**BAB 2 LANDASAN TEORI**

Bab ini menjelaskan tentang sistem kriptografi secara umum, teori dan dasar-dasar perhitungan serta contoh algoritma *Multi-Power RSA*, algoritma *Blowfish*, dan mekanisme *Hybrid Cryptosystem*.

**BAB 3 ANALISIS DAN PERANCANGAN**

Bab ini berisi analisis terhadap masalah penelitian dan perancangan sistem yang akan dibangun sebagai solusi permasalahan tersebut.

**BAB 4 IMPLEMENTASI DAN PENGUJIAN**

Bab ini berisi implementasi algoritma *Multi-Power RSA*dan algoritma *Blowfish*, selanjutnya pengujian terhadap sistem yang telah dibangun dengan beberapa sampel *file* teks serta pembahasan hasil pengujian dan analisisnya.

**BAB 5 KESIMPULAN DAN SARAN**

Bab ini memuat kesimpulan dari uraian penjelasan bab-bab sebelumnya dan saran berdasarkan hasil pengujian yang diharapkan dapat bermanfaat untuk pengembangan sistem selanjutnya.