BAB I

PENDAHULUAN

I.1. Latar Belakang

Pesatnya perkembangan teknologi informasi telah menjadikan informasi sebagai kebutuhan utama bagi setiap orang atau instansi- instansi, karena informasi adalah hal yang sangat vital untuk membantu individu ataupun instansi untuk berkembang dalam persaingan global.

Untuk menjaga dan menjamin keamanan file tersebut agar tidak jatuh ke tangan orang yang salah, maka orang yang memiliki arsip file .rar tersebut biasanya akan memberi password pada .rar yang ia miliki. Password atau kata sandi adalah kumpulan karakter yang digunakan untuk memverifikasi sesuatu, dapat digunakan juga sebagai pengenal. Ada kalanya kita ingin membuka file .rar yang diberi password tetapi kita tidak mengetahui password tersebut. Ada salah satu cara untuk membobol password .rar, yaitu dengan menggunakan software RAR Password Recovery. Software ini mengimplementasikan algoritma brute force

Oleh karena itu penulis tertarik melakukan penelitian terhadap sistem keamanan berbasis kriptografi RSA dan AES untuk mengamankan file winrar dan zip karena sebelum nya belum ada pengamanan file winrar dan zip menggunakan metode RSA dan AES, biasanya pengamanan file winrar dan zip hanya menggunakan paswoord saja sehingga dapat dengan mudah untuk di crack (di bobol), dengan mempertimbangkan masing-masing kelebihan sistem tersebut

dapat lebih mudah membantu penulis untuk menentukan pasangan kunci public dan private karena proses pembuatan key untuk meng enkripsi file dan men dekripsi file menggunakan satu kunci yang di buat secara random dan tidak bisa di gunakan untuk file yang lain, aplikasi yang hendak di buat penulis di sini akan mengenkripsi file tunggal ataupun multiple file(bukan folder).dalam penelitian ini penulis akan menggunakan bahasa pemrograman microsoft visual studio 2017.

Metode *RSA* adalah salah satu dari kriptografi yang memiliki peranan penting dalam komunikasi elektronik. Metode *RSA* menjadi yang pertama dalam sejarah untuk *crypto system* menggunakan kunci *public* dan *private* dan menjadi satu-satunya metode yang tidak dapat diretas (*uncrackable*) lebih dari 3 dekade. Kunci *public* berfungsi sebagai kunci untuk *enkripsi* dan kunci *private* berfungsi untuk *deskripsi*. Sampai saat ini pun, algoritma *RSA* belum dapat ditembus (*uncrackable*) oleh siapapun. Sifat *uncrackable* ini di karena kan keamanan algoritmanya terletak pada sulitnya memfaktorkan bilangan prima yang besar menjadi faktor-faktor prima dimana pemfaktoran ini dilakukan untuk memperoleh kunci *private*. Selama pemfaktoran bilangan besar prima ini belum berhasil dilakukan, maka selama itu pula keamanan algoritma *RSA* tetap aman.

Sistem keamanan *RSA* masih menjadi pilihan yang lebih baik bila dibandingkan dengan sistem keamanan lain seperti *DES* (*Data Encryption System*). *Bruce Force attack* menjadi ancaman untuk sistem keamanan *DES*. Panjang kunci yang hanya 56-bit menyebabkan sistem keamanan *DES* sangat rawan dan riskan untuk dijebol. Selain itu, struktur *DES* pada bagian *substitution-box* (*S-box*) yang diubah menurut saran *NSA* (*National Security Agency*)

mengakibatkan kita tidak mengetahui kemungkinan adanya kelemahan-kelamahan pada *DES* yang sengaja disembunyikan oleh *NSA*. Ditambah lagi kecurigaan akan kemampuan *NSA* membongkar *cypher* tanpa harus memiliki *key*-nya juga menjadi alasan kurangnya sistem keamanan *DES*. Hal ini disebabkan *DES* sudah didesain secara cermat sehingga bila *S-Box* ini diubah secara acak maka sangat mungkin *DES* justru lebih mudah dijebol.

Selanjutnya, bila dibandingkan dengan sistem keamanan *AES* (*Advanced Encryption System*), sistem *RSA* memang dianggap masih kurang efektif dipandang dari sisi konsumsi waktu *enkripsi* dan sumber daya (*resource)* memori. *RSA* membutuhkan waktu yang lebih lama dalam proses *enkripsi* dan lebih besar dalam penggunaan *memory resource*. Namun, dari sisi keamanan, sistem *AES* sangat berpotensi untuk dijebol atau dipecahkan. *Courtois* dan *Pieprzyk* mengumumkan metode yang berpotensi memecahkan sistem keamanan *AES* adalah "*XSL attack*".

Persamaan logaritma yang tergolong sederhana dari sistem *AES* justru menyebabkan kemungkinan dapat dipecahkannya persamaan logaritma tersebut. Oleh karena itu, penulis tertarik untuk melakukan penelitian terhadap sistem keamanan berbasis kriptografi yang mengkombinasikan atau mengintegrasikan algoritma *RSA* dan *AES* dengan mempertimbangkan masing-masing kelebihan sistem tersebut. Sehingga diharapkan dapat menghasilkan sistem keamanan yang lebih baik. yang nantinya akan menjadi sebuah judul skripsi yang berjudul. **"IMPLEMENTASI METODE *RSA* DAN *AES* UNTUK MENGAMANKAN FILE *WINRAR* DAN *ZIP*".**

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Berdasarkan latar belakang masalah yang di atas, maka dapat di identifikasikan permasalahan yang ada yaitu :

1. Belum adanya Pengamanan *Winrar* dan *Zip* Menggunakan Metode *RSA* dan *AES*
2. Pengamanan *Winrar* dan *Zip* biasanya masih menggunakan *password* sehingga dapat dengan mudah untuk di *Crak* (dibobol).

I.2.2. Rumusan Masalah

Berdasarkan ruang lingkup permasalahan diatas maka, dapat disimpulkan beberapa permasalahan yang ada pada skripsi yaitu :

1. Bagaimana membangun aplikasi *desktop* enkripsi dan deskripsi *file* dengan menggunakan metode *Rivest Shamir Adleman (RSA)* dan metode *Advanced Encryption System (AES)*?
2. Bagaimana cara mengamankan *file Winrar* dan *Zip* menggunakan sistem keamanan metode *RSA* dan *AES*?
3. Bagaimana mempermudah pengguna untuk menentukan pasangan kunci public dan private dengan tingkat akurasi keamanan yang tinggi secara random?

I.2.3. Batasan Masalah

Berdasarkan identifikasi masalah, maka penulis membatasi masalah sebagai berikut :

1. Menggunakan metode *Rivest Shamir Adleman* (*RSA*) dan metode *Advanced Encryption System* (*AES*) yang terdapat pada *library Visual Studio 2017*.
2. Aplikasi akan mengenkripsi *file* tunggal ataupun multiple *file* (bukan *folder*).
3. Aplikasi dibuat dengan menggunakan bahasa pemrograman *C#.*
4. Besaran setiap file yang akan dienkripsi maksimal 30 *Mbytes.*
6. Jenis file yang akan digunakan dalam proses *enkripsi* dan *dekripsi* adalah (*.*rar*), dan (*.*zip*).
7. Program di buat dengan *Visual Studio 2017*.
8. Menggunakan *password* acak untuk meng *enkrip file*.

I.3. Tujuan dan Manfaat Penelitian

I.3.1. Tujuan Penelitian

Adapun tujuan pembuatan skipsi yang dilakukan oleh penulis adalah :

1. Membangun aplikasi kriptografi *file* menggunakan metode *Rivest Shamir Adleman (RSA)* dan metode *Advanced Encryption System (AES)* berbasis *desktop*.
2. Membangun aplikasi yang dapat mengamankan *file* tunggal (bukan *folder*).

3. Membangun aplikasi yang dapat melakukan pergantian pasangan kunci *public* dan *private* secara random sehingga menghemat waktu dan meningkatkan keamanan kunci agar tidak mudah dipecahkan

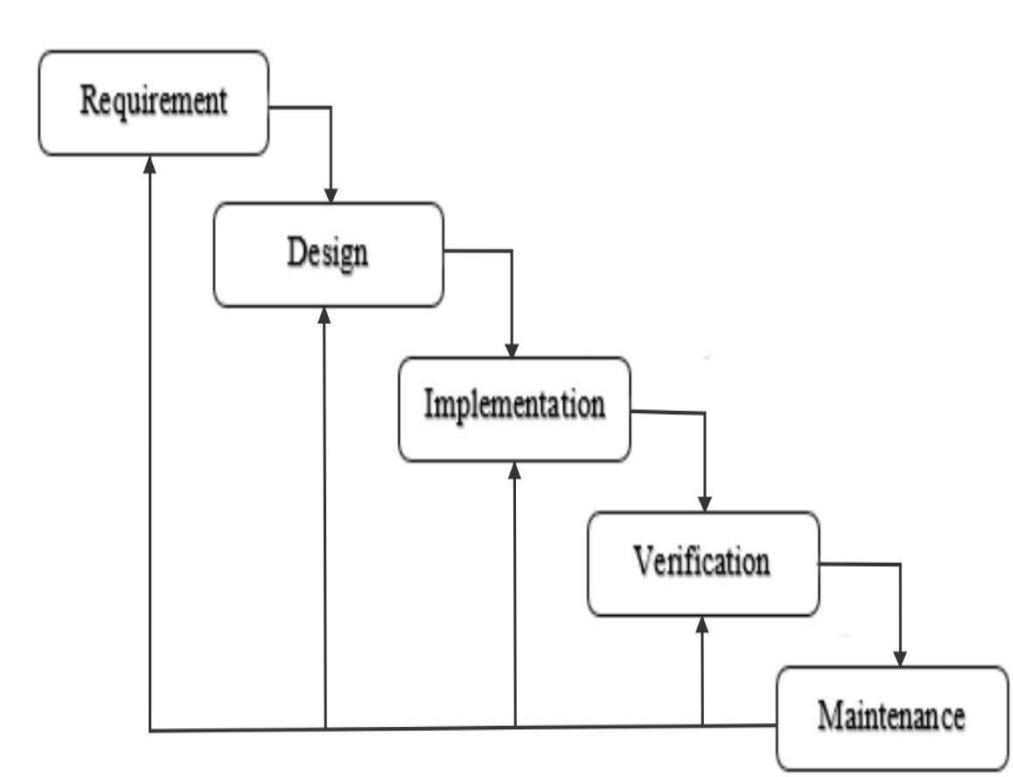
I.3.2. Manfaat Penelitian

Adapun manfaat yang diharapkan dari penulisan skripsi yang dilakukan oleh penulis adalah :

1. Menambah pengetahuan dan wawasan penulis tentang kriptografi khususnya enkripsi dan deskripsi *file* dengan metode *RSA* dan *AES* berbasis *desktop*.
2. Memahami implementasi metode *RSA* dan *AES* pada pengamanan data *file Winrar* dan *Zip*.
3. Membangun aplikasi keamanan dengan kunci *public* dan *private* secara otomatis.

I.4. Metodologi Penelitian

Bagian ini akan membahas mengenai objek penelitian serta metode penelitian bagaimana langkah-langkah penelitian dilakukan. Objek penelitian akan dijelaskan secara lebih jelas pada bagian ini. Metodologi yang digunakan pada perancangan aplikasi ini adalah *Waterfall* yang dijelaskan pada Gambar III.1. berikut ini:



Gambar I.1. Metodologi pengerjaan penelitian.

Dalam pengembangannya metode *waterfall* memiliki beberapa tahapan yang berurut yaitu: *requirement* (analisis kebutuhan), *design system* (desain sistem), *Coding* (pengkodean) *& Testing* (pengujian), Penerapan Program, pemeliharaan. Tahapan tahapan dari metode *waterfall* adalah sebagai berikut :

1. ***Requirement Analisis***

   Tahap ini pengembang sistem diperlukan komunikasi yang bertujuan untuk memahami perangkat lunak yang diharapkan oleh pengguna dan batasan perangkat lunak tersebut. Informasi ini biasanya dapat diperoleh melalui wawancara, diskusi atau survei langsung. Informasi dianalisis untuk mendapatkan data yang dibutuhkan oleh pengguna.

2. ***System Design***

   Spesifikasi kebutuhan dari tahap sebelumnya akan dipelajari dalam fase ini dan desain sistem disiapkan. Desain Sistem membantu dalam menentukan perangkat keras*(hardware)* dan sistem persyaratan dan juga membantu dalam mendefinisikan arsitektur sistem secara keseluruhan.

3. ***Implementation***

   Pada tahap ini, sistem pertama kali dikembangkan di program kecil yang disebut *unit,* yang terintegrasi dalam tahap selanjutnya Setiap *unit,* dikembangkan dan diuji untuk fungsionalitas yang disebut sebagai *unit testing*.

4. ***Integration & Testing***

   Seluruh *unit* yang dikembangkan dalam tahap implementasi diintegrasikan ke dalam sistem setelah pengujian yang dilakukan masing-masing *unit*. Setelah integrasi seluruh sistem diuji untuk mengecek setiap kegagalan maupun kesalahan.

5. ***Operation & Maintenance***

   Tahap akhir dalam model *waterfall* Perangkat lunak yang sudah jadi, dijalankan serta dilakukan pemeliharaan Pemeliharaan termasuk dalam memperbaiki kesalahan yang tidak ditemukan pada langkah sebelumnya. Perbaikan implementasi *unit* sistem dan peningkatan jasa sistem sebagai kebutuhan baru.

I.5. Kontribusi Penelitian

Kontribusi yang dihasilkan penelitian ini yaitu :

1. Penelitian ini dapat menjadi referensi terbaru bagi peneliti berikutnya.
2. Penelitian ini dapat menjadi ide baru untuk peneliti berikutnya.
3. Penelitian ini menerapkan ilmu kriptografi yang dikombinasikan dengan metode *Rivest Shamir Adleman (RSA)* dan *Advanced Encryption System (AES)*.

I.6. Sistematika Penulisan

Adapun sistematika pembahasan laporan ini terdiri dari 5 bab, yaitu:

BAB I : PENDAHULUAN

merupakan bagian kesatu dari laporan ini. Pada bagian ini akan dibahas latar belakang masalah, rumusan masalah, maksud dan tujuan penelitian, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

bab ini membahas mengenai teori-teori yang digunakan penulis untuk membangun sistem yaitu mengenai *kriptografi file* dengan menerapkan metode *Rivest Shamir Adleman* (*RSA*) dan perancangan sistem.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab mengemukakan analisa masalah program yang akan di rancang dan rancangan program yang digunakan pada penulisan skripsi ini.

BAB IV : HASIL DAN PEMBAHASAN

pada bab ini akan dibahas mengenai implementasi rancangan aplikasi sistem mulai dari *hardware*, *software*, dan antarmuka yang siap digunakan.

BAB V : KESIMPULAN DAN SARAN

pada bab ini membahas tentang kesimpulan yang didapat selama pembangunan sistem dan penyusunan laporan tugas akhir serta saran terhadap pembangunan sistem dan penyusunan laporan tugas akhir serta saran terhadap kekurangan yang terdapat pada aplikasi yang telah dibangun.