

BAB I

PENDAHULUAN

I.1. Latar Belakang

Keamanan komputer merupakan suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada komputer. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian atau pemeliharaan ketersediaan, seperti dijabarkan dalam kebijakan keamanan. Untuk menjaga keamanan dan terutama bagi suatu perusahaan, institusi atau organisasi yang mempunyai dokumen - dokumen rahasia dan penting. Mereka mengamankan dokumen - dokumen tersebut agar terhindar dari gangguan orang lain. Saat ini, sebagian besar dokumen - dokumen menggunakan aplikasi *Microsoft Word*. Sebagian besar terbiasa dengan aplikasi *Microsoft Office* yang sangat memudahkan siapa saja ketika menggunakan aplikasi ini. Pengolah kata *Microsoft Word*, begitu mudah digunakan sehingga siapapun yang menggunakannya akan merasa nyaman dengan pengolah kata ini. Dalam aplikasi *Microsoft Office* pengolah kata disimpan sebagai *file Microsoft Word*, pengolah angka sebagai *file Microsoft Excel*, dan sebagainya. Memang tidak ada yang aneh dalam sistem penyimpanan seperti ini karena memang sebagian besar di antara kita menggunakan semua aplikasi yang ada pada *Microsoft Office*.

Salah satu teknik untuk pengamanan data adalah dengan menggunakan algoritma penyandian data. Algoritma penyandian data saat ini semakin banyak jumlahnya sejalan dengan berkembangnya ilmu yang mempelajari data tersebut,

ilmu ini biasa disebut Kriptografi. Dalam kriptografi terdapat beberapa metode yang cukup penting dalam pengamanan data, untuk menjaga kerahasiaan suatu data salah satunya adalah enkripsi (*encryption*). Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan aslinjadi *ciphertext*. Sedangkan suatu proses yang dilakukan untuk mengubah pesan tersembunyi menjadi pesan biasa (yang mudah dibaca) disebut dekripsi. Pesan biasa atau pesan asli disebut *plaintext* sedangkan pesan yang telah diubah atau disandikan supaya tidak mudah dibaca disebut dengan *ciphertext*.

Algoritma *kriptografi modern*, seperti *Massey-Omura Cryptosystem* ini, dapat mengatasi masalah tersebut dengan menggunakan kunci, yang dalam hal ini algoritmanya tidak lagi dirahasiakan, tetapi kunci harus di jaga kerahasiaannya. Sehingga setiap kali ada anggota kelompok yang keluar, maka algoritma yang dipakai tidak perlu diganti, namun cukup mengganti kuncinya saja. Oleh sebab itu penulis mencoba untuk menggunakan Algoritma *Massey-Omura* yang pengimplementasiannya menggunakan *Three Pas Protocol* untuk membangkitkan bilangan prima karena algoritma *Massey-Omura* ini merupakan salah satu algoritma simetri yang melakukan pemfaktoran bilangan besar untuk mendapatkan kunci privat. Dengan perkataan lain, diperlukan algoritma *kriptografi modern* yang dapat digunakan dan gampang dimengerti oleh semua orang, juga algoritma yang menyediakan keamanan cukup tinggi yang tidak didasarkan atas kerahasiaan algoritmanya.

Berdasarkan latar belakang di atas, maka pada penelitian ini penulis akan membangun sebuah aplikasi yang dapat digunakan untuk mengamankan sebuah

file dokumen. Sehingga pada penelitian ini akan ditarik sebuah judul **“Implementasi Pengamanan File Dokumen Word Menggunakan Algoritma Massey-Omura”**.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Berdasarkan latar belakang masalah, maka penulis mengambil pokok permasalahan yang dihadapi yaitu:

1. Banyaknya pihak-pihak yang melakukan modifikasi file dokumen word yang bertujuan negatif sehingga merugikan pihak tertentu.
2. Kurangnya keamanan file dokumen word dan perlindungan pemeliharaan ketersediaan.
3. Terjadinya penyalahgunaan file dari orang-orang yang tidak bertanggung jawab untuk meretas dan mengganggu pekerjaan orang lain.

I.2.2. Rumusan Masalah

Berikut rumusan masalah yang akan dicari pemecahannya melalui penulisan skripsi ini yaitu:

1. Bagaimana cara mengatasi modifikasi file dokumen word?
2. Bagaimana menerapkan algoritma *Massey-Omura* dalam melindungi file dokumen word?
3. Bagaimana merancang dan membangun sebuah aplikasi pengamanan file dokumen word menggunakan algoritma *Massey-Omura* ?

I.2.3. Batasan Masalah

Penulis membatasi masalah yang akan dibahas dalam skripsi ini diantaranya:

1. Metode yang digunakan pada aplikasi ini adalah *Massey-Omura*.
2. Perancangan menggunakan bahasa pemrograman Microsoft Visual Studio 2010.
3. Penelitian ini hanya membatasi masalah pada keamanan file dokumen word.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut :

1. Melindungi informasi terhadap modifikasi atau pemeliharaan ketersediaan.
2. Membantu menjaga keamanan file dokumen word sehingga dapat terhindar dari pencurian atau kerusakan pada file dokumen word dari orang yang tidak bertanggung jawab.
3. Menghasilkan sebuah aplikasi untuk mengamankan sebuah file dokumen word.

I.3.2. Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut :

1. Agar dapat menambah wawasan dan kemampuan berfikir mengenai metode *Massey-Omura*.

2. Memperkecil tingkat pencurian file dokumen word atau modifikasi pada file dokumen word.
3. Agar dapat digunakan sebagai aplikasi untuk mengamankan sebuah file dokumen word.

I.4. Metodologi Penelitian

Dalam pembuatan laporan ini, penulis membutuhkan data-data yang akan dijadikan bahan pertimbangan dalam pembuatan laporan ini. Untuk itu penulis menggunakan *Massey-Omura* sebagai metode studi.

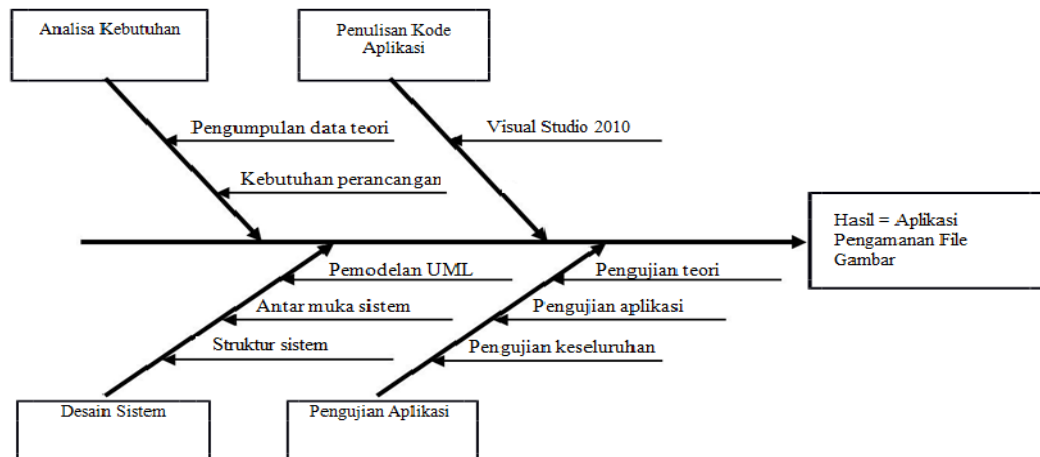
I.4.1. Metode Pengumpulan Data

Sistem yang dirancang tentunya memerlukan pengumpulan data, dalam proses pengumpulan data terdapat beberapa cara sebagai berikut:

1. Studi Literatur, dengan cara mempelajari buku-buku acuan dan literatur yang berhubungan dengan materi dalam penulisan skripsi. Buku-buku acuan yang digunakan umumnya adalah tentang cara penyusunan skripsi pada Universitas Potensi Utama dan juga buku-buku tentang studi pustaka yang digunakan dalam penulisan skripsi.
2. Pengamatan, yaitu pengumpulan data dan informasi yang dilakukan dengan cara pengamatan langsung beberapa contoh aplikasi media pembelajaran. Pengamatan yang dilakukan adalah dengan melihat contoh-contoh *script* program bahasa pemrograman yang selanjutnya akan dituangkan kedalam bahasa pemrograman Visual Studio 2010.

I.4.2. Metode Perancangan Sistem

Dalam merancang sistem dilakukan tahap-tahap sebagai berikut :



Gambar I.1. Diagram Fishbone Prosedur Perancangan

1. Analisa Kebutuhan

Setelah melalui tahap prosedur perancangan, maka tahap selanjutnya adalah analisa kebutuhan yaitu hal-hal yang diperlukan untuk perancangan sistem berupa perangkat lunak yaitu Visual Studio 2010 yang digunakan untuk merancang aplikasi untuk perangkat keras seperti komputer atau laptop yang dibutuhkan untuk membangun aplikasi.

2. Desain Sistem

Pada tahap ini dirancang sebuah desain dari aplikasi pengamanan file dokumen menggunakan *Massey-Omura*. Bagaimana desain yang akan digunakan pada antarmuka perangkat berbasis *Desktop* Setelah dilakukan perancangan desain aplikasi selanjutnya melakukan implementasi terhadap desain antarmuka dari aplikasi berbasis *Desktop* yang telah dirancang kedalam bahasa pemrograman visual studio 2010.

3. Penulisan Kode Aplikasi

Pada proses ini rancang bangun aplikasi pengamanan file dokumen menggunakan *Massey-Omura* dituangkan kedalam bahasa pemrograman dan mulai dibangun menggunakan visual studio 2010 untuk menghasilkan sebuah aplikasi sesuai dengan perancangan. Seluruh fungsi dan antarmuka yang terdapat pada perancangan akan disesuaikan dengan aplikasi yang akan dihasilkan.

4. Pengujian Aplikasi

Pada tahap ini dilakukan pengujian aplikasi pengamanan file dokumen menggunakan *Massey-Omura* secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan aplikasi. Pengujian fungsional dilakukan untuk mengetahui bahwa aplikasi pengamanan file dokumen menggunakan *Massey-Omura* telah berjalan dengan sesuai dengan perancangan. Pengujian ketahanan merupakan kemampuan aplikasi untuk berjalan dengan baik pada spesifikasi minimum komputer.

5. Hasil

Pada tahap ini akan diambil kesimpulan dari rancang bangun aplikasi pengamanan file dokumen menggunakan *Massey-Omura* yang telah dihasilkan, seperti apa saja kelebihan dan kekurangan dari aplikasi pengamanan file dokumen menggunakan *Massey-Omura*.

I.5. Kontribusi Penelitian

Disini penulis akan mengangkat judul “Implementasi Pengamanan File Dokumen Word Menggunakan Algoritma Massey-Omura” yang akan menghasilkan sebuah aplikasi yang dapat mengubah file asli kedalam file rahasia, penelitian ini juga bermanfaat sebagai referensi bagi penulis lain yang ingin membuat sebuah penelitian yang berhubungan dengan *Massey-Omura*.

I.6. Sistematika Penulisan

Penulisan skripsi ini disusun secara sistematika untuk memudahkan mahasiswa dalam penyusunan skripsi. Adapun sistematika penulisan skripsi ini adalah:

BAB 1 : PENDAHULUAN

Dalam bab ini penulis menguraikan mengenai latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian, kontribusi penulisan dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Dalam bab ini mencakup uraian penyelesaian secara teoritis serta konsep baru dalam penyelesaian masalah berkenaan dengan sistem dan fokus kajian. Adapun landasan teori yang diuraikan oleh penulis adalah penjelasan mengenai sistem, informasi, materi yang digunakan, serta metode yang menggambarkan cara kerja dari sistem yang akan dirancang.

BAB III : ANALISIS DAN PERANCANGAN

Pada bab ini berisi analisa sitem yang sedang berjalan, perancangan proses dalam bentuk diagram UML yang mencakup analisa dan perancangan sistem pengolahan data yang mencakup seluruh aktivitas yang terjadi pada sistem yang akan dibangun.

BAB IV : HASIL DAN UJI COBA

Dalam bab ini penulis menguraikan tentang tampilan hasil sistem yang dirancang beserta pembahasannya, kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini penulis menguraikan tentang kesimpulan dan saran untuk meningkatkan kualitas dari aplikasi yang sudah dirancang.

