BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Banyaknya permintaan akan program aplikasi membuat badan-badan usaha yang bergerak dibidang rekayasa perangkat lunak saling berlomba-lomba dalam memproduksi *software*. Hal ini membuat perkembangan pasar program memiliki nilai saing yang tinggi. Dengan meningkatnya kebutuhan akan program maka meningkat juga resiko akan pembajakan dan duplikasi program aplikasi secara ilegal.

Program-program yang dipasarkan dapat mempunyai nilai jual tinggi, pastinya memiliki resiko yang tinggi untuk digandakan secara ilegal. Agar kasus-kasus duplikasi secara ilegal dapat dikurangi, dan untuk mewujudkan itu maka dibutuhkan sebuah konsep yang dapat mengamankan program tersebut agar tidak mudah untuk diduplikasi. Proses pengamanan sebuah program dapat dilakukan dengan membuat "serial number" dimana satu serial hanya berlaku untuk satu unit komputer. Dalam dunia rekayasa perangkat lunak terdapat metode yang khusus dibuat untuk mengamankan data atau berkas.

Keamanan data dan berkas merupakan sesuatu yang sangat penting dijaman sekarang ini. Kerahasiaan, keaslian, dan integritas data atau berkas juga perlu dijaga. Umumnya, setiap orang memiliki data atau berkas yang penting dan bersifat rahasia yang tidak semua orang berhak mengetahui keberadaan data atau berkas

tersebut selain pemiliknya. Oleh karena itu, diperlukan teknik untuk mengamankannya.

Banyak teknik yang bisa dilakukan untuk mengamankan data atau berkas, baik dengan penyandian, penyembunyiaan kedalam media digital lainnya, maupun penggabungan keduanya yaitu penyandian dan penyembunyiaan.

Teknik penyandian berkas atau data disebut dengan kriptografi. Banyak algoritma-algoritma yang dapat digunakan untuk menyediakan berkas atau data, salah satunya yaitu menggunakan algoritma *Advanced Encryption Standard* (AES), yang dinilai merupakan algoritma yang paling aman untuk proses penyandian.

Berdasarkan dari uraian latar belakang diatas maka diperolehlah beberapa masalah yang terjadi dalam pengamanan program seperti yang akan dipaparkan dibawah ini:

1. Kurangnya kode pengamanan pada program sehingga dapat dengan mudah diduplikasi.
2. Program-program yang dibuat dapat diamankan dengan menggunakan metode algoritma kriptografi.

Dari uraian masalah-masalah diatas, maka diangkatlah tema penelitian untuk skripsi dengan judul Analisis dan Pemanfaatan Algoritma Kriptografi untuk Pengkodean *Serial Number* pada Aplikasi berbasis Desktop.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas dapat dibuat rimusan masalah, antara lain sebagai berikut:

1. Bagaimana cara membuat kode pengamanan pada program sehingga tidak dapat dengan mudah diduplikasi?
2. Bagaimana cara memanfaatkan algoritma kriptografi untuk mengamankan program yang akan dibuat?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telh dijelaskan diatas, maka dapat dibuat batasan masalah antara lain sebagai berikut:

1. Menggunakan algoritma AES128 *Rijndael* untuk mengenkripsi data yang akan diproses.
2. Sistem yang dibuat hanya membuat dan mengunci serial number sebagai nomor seri aplikasi.
3. Menggunakan analisis SWOT sebagai alat bantu untuk menganalisa masalah yang ada.
4. Menggunakan *Unified Modeling Language* 2.0 (UML) untuk rancangan pemodelan sistem.
5. Pembuatan aplikasinya menggunakan bahasa pemrograman csharp (C#) berbasis desktop aplikasi.
6. Alat yang digunakan untuk menulis dan mengkompilasi adalah Microsoft Visual Studio 2015 Community.

1.4 Maksud dan Tujuan Penelitian

Maksud dan tujuan dari pembuatan aplikasi ini antara lain sebagai berikut:

1. Menerapkan algoritma kriptografi *Advanced Encryption Standard* (AES) untuk penyandian info berkas pada sebuah program.
2. Membangun sebuah aplikasi yang dapat menyandikan info berkas pada program dengan menggunakan algoritma kriptografi *Advanced Encryption Standard* (AES).

1.5 Metode Penelitian

1.5.1 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan antara lain sebagai berikut:

1. Metode Observasi

   Metode ini digunakan untuk mengetahui bagaimana menyandikan informasi suatu berkas pada pada sebuah program sehingga program tersebut tidak dapat digandakan dengan cara melakukan pengamatan dari aplikasi-aplikasi sejenis.

2. Metode Studi pustaka

   Studi pustaka yaitu teknik pengumpulan data yang dilakukan dengan literatur-literatur, buku-buku pendukung, catatan, dan laporan- laporan untuk mendapat konsep teori mengenai masalah yang diteliti. Metode ini dilakukan untuk mendapatkan informasi tentang pembuatan aplikasi untuk penyandian informasi suatu berkas pada sebuah program.

1.5.2 Metode Analisis

Pada tahap ini dilakukan alalisis dengan metode SWOT. Selain itu juga terdapat analisis kebutuhan dan asalisis kelayakan. Analisis kebutuhan mencakup kebutuhan fungsional dan kebutuhan non fungsional. Dan analisis kelayakan mencakup kelayakan operasional, kelayakan teknis, kelayakan jadwal, dan kelayakan ekonomis.

1.5.3 Metode Perancangan

Pada tahap ini dilakukan perancangan terhadap aplikasi yang akan dibuat dengan menggunakan UML untuk pemodelan aplikasinya, algoritma kriptogarfi *Advanced Encryption Standard* (AES) untuk penyandian.

1.5.4 Metode Pengembangan

Setelah melakukan perancangan, selanjutnya ialah menerapkan rancangan tersebut dengan pembuatan sistem menggunakan bahasa pemrograman C#. Metode yang digunakan adalah metode *waterfall*. dengan tahapan analisis, *design*, pengkodean (*coding*), dan pengujian. Penyempurnaan aplikasi dilakukan berdasarkan metode pengembangan yang dilakukan terhadap aplikasi yang dibuat.

1.5.5 Metode Testing

Pada tahap ini dilakukan pengujian terhadap aplikasi yang dihasilkan yaitu menggunakan metode *black-box* dan metode *white-box*.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunkan penulis dalam pembuatan aplikasi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini menguraikan latar belakang masalah,rumusan masalah, batsan masalah, tujuan penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini akan dijelaskan tentang teori-teori dasar yang digunakan dalam pembuatan aplikasi ini

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini akan menguraikan tentang metode pengumpulan data, input data, perancangan program, dan proses analisis.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas tentang implementasi dari aplikasi penyandian informasi berkas pada program, pengujian sistem, dan hasil analisa yang didapatkan

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran yang didapat dari pembuatan aplikasi penyandian info berkas pada program.