BAB I

PENDAHULUAN

I.1. Latar Belakang Masalah

Metode kriptografi digunakan untuk mengamankan data yang bersifat rahasia agar tidak diketahui oleh orang lain. Metode kriptografi yang dapat digunakan untuk mengamankan data ada bermacam-macam. Setiap metode memiliki kelebihan dan kekurangannya masing-masing. Namun, masalah utamanya adalah bagaimana mengetahui dan memahami cara kerja atau algoritma dari metoda kriptografi tersebut. Penulis memilih metode kriptografi RC5 karena menurut Rivest metode RC5 ini merupakan algoritma *state table* yang terbaik dan teraman yang disediakan untuk *secure socket layer*.

Data dokumen merupakan data yang dapat digolongkan sebagai data pribadi. Salah satu cara mengamankan data dokumen itu memberikan pengamanan *file* tersebut. *File* dokumen yang berjenis teks di aplikasikan dengan perangkat lunak *Microsoft word*. Data ini isinya sebenarnya sifatnya rahasia karena seseorang yang menggunakan aplikasi untuk surat menyurat, isi dari surat menyurat ini sifatnya sangat rahasia sekali jika tidak dilakukan pengamanan maka isi surat tersebut bisa dirusak orang bukan itu saja tetapi isi dari surat itu dapat dibaca seseorang dan itu bisa disalahgunakan bagi orang yang tidak bertanggung jawab.

Berdasarkan uraian diatas penulis mengangkat judul ”**Perancangan Aplikasi Keamanan Data Teks Menggunakan RC5**”.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Adapun identifikasi masalah pada penulisan skripsi ini adalah :

1. Mengamankan data teks dengan memberikan sandi menggunakan metode RC5.
2. Untuk menggunakan isi *file* dari data yang asli.

I.2.2. Rumusan Masalah

Berdasarkan identifikasi masalah diatas adapun yang menjadi rumusan masalah pada penulisan skripsi ini adalah :

1. Bagaimana merancang pembuatan sistem keamanan data teks metode RC5 ?
2. Bagaimana membangun aplikasi keamanan data teks menggunakan RC5 ?

I.2.3. Batasan Masalah

Agar pembahasan tidak menyimpang dari tujuannya maka dilakukan pembatasan masalah sebagai berikut:

1. Aplikasi dalam penanganan keamanan data teks menggunakan metode RC5.
2. Sistam keamanan data yang dibangun berformat teks.
3. Perancangan aplikasi menggunakan bahasa pemrograman C# 2010.

I.3. Tujuan dan Manfaat Penelitian

I.3.1. Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Membangun aplikasi kemananan data teks dengan menggunakan metode RC5.
2. Mengetahui proses keamanan *file* data teks menggunakan metode RC5
3. Mengetahui kelebihan dan kekurangan metode RC5.

I.3.2. Manfaat Penelitian

Manfaat dari penelitian ini adalah

1. Aplikasi RC5 dapat digunakan sebagai fasilitas pendukung dalam proses sistem keamanan data teks.
2. Dengan aplikasi RC5 ini maka isi dari data tersebut tidak dapat dibaca lagi tanpa seijin pemiliknya.
3. Sebagai bahan referensi bagi peneliti lain yang ingin merancang pengembangan aplikasi tentang RC5.

I.4. Metodologi Penelitan

Berisi langkah-langkah diperlukan untuk mencapai tujuan perancangan yang dilakukan. Adapun metodologi dalam pengumpulan data adalah:

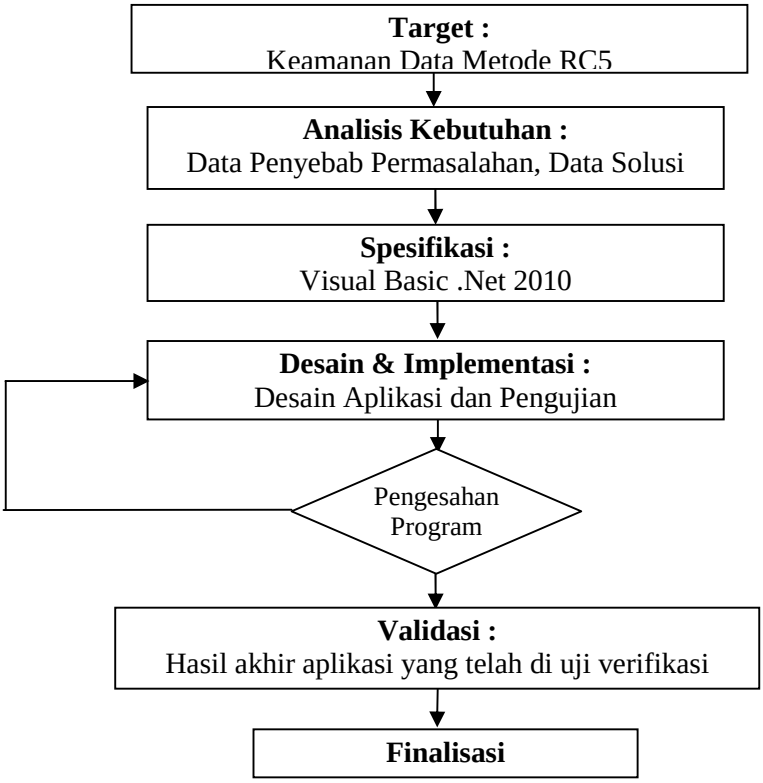
1. Studi Pustaka dan Literatur

Pada tahap ini dilakukan pengumpulan informasi yang diperlukan untuk sistem keamanan data dengan RC5. Untuk keperluan implementasi, penulis melakukan *study literature* terhadap pemrograman *action script* sebagai bahasa pemrograman yang akan digunakan dalam tahap implementasi.

2. Implementasi

Implementasi yang dilakukan meliputi implementasi bangun ruang. Selain itu perancangan pengujian terhadap hasil implementasi juga dilakukan untuk mengetahui efektifitas dari suatu algoritma.

Setelah melakukan penelitian lapangan dan penelitian kepustakaan penulis melanjutkan penelitian dengan prosedur sebagai berikut :



Gambar 1.1. Prosedur Perancangan

a. Target

Membuat sistem keamanan data dengan RC5 dengan maksud agar data lebih aman dari pencurian dan kerusakan.

b. Analisa kebutuhan

Untuk mencapai penyelesaian masalah, kebutuhan pokok yang harus ada pada sistem yang akan di bangun adalah :

1. Sistem keamanan data dengan RC5 yang akan dibangun harus dapat di mengerti dengan mudah digunakan oleh pengguna.
2. Sistem dapat menampilkan hasil yang sebenarnya dari proses pengamanan data, dan mengeluarkan *output* berupa enkripsi dan deskripsi data.

c. Spesifikasi

Secara umum sistem keamanan data memiliki spesifikasi sebagai berukut :

a. Dalam Implementasi rancang program dibangun dengan menggunakan pemrograman C# 2010.
b. Analisa yang mendeskripsikan perangkat yang dibutuhkan dalam pembangunan sistem yang terdiri dari komponan perangkat keras dengan perangkt lunak komponen perangkat keras yang dibutuhkan oleh sistem adalah sebuah PC dan Laptop.

d. Implementasi dan Verifikasi

Setelah jelas apa saja yang menjadi spesifikasi dan desain yang dirancang, maka langkah selanjutnya mengatur posisi yang tepat untuk form-form pada sistem, kemudian membentuk suatu logika yang diimplementasikan dengan bahasa pemrograman. Untuk mengetahui apakah sistem yang dirancang sudah dapat bekerja dengan baik maka perlu dilakukan verifikasi. Dengan demikian bila ada kesalahan atau kekurangan dapat diperbaiki terlebih dahulu.

e. Validasi

Setelah melewati tahap implementasi dan verifikasi maka tahap selanjutnya adalah validasi. Pada tahap ini dilakukan pengujian sistem secara menyeluruh, meliputi pengujian fungsional dan ketahanan sistem. Dari validasi ini dapat di ketahui kesesuain hasil perancangan dengan analisis kebutuhan yang diharapkan.

d. Finalisasi

Sistem sudah dapat digunakan dan dipublikasikan.

I.5. Keaslian Penelitian

Sepengetahuan penulis, penelitian tentang rancang bangun Sistem keamanan data teks menggunakan RC5. Penelitian yang terkait dengan penelitian ini adalah :

Tabel 1.1. Daftar Keaslian Penelitian

No	Penelitian	Judul Penelitian	Hasil Penelitian
1.	Ernita Sitohang (2013)	Perangkat Aplikasi Keamanan Data Text Menggunakan Electronic Codebook Dengan Algoritma Des	Algoritma DES dalam mengamankan data elektronic codebook
2.	Tarbudi (2011)	Membangun Aplikasi Keamanan Transmisi Data Multimedia Menggunakan Kriptografi Algoritma Data Encryption Standard (Des)	Algoritma DES dalam mengamankan data transmisi multimedia
3.	Rohmat Nur Ibrahim (2012)	Kriptografi Algoritma Des, Aes/Rijndael, Blowfish Untuk Keamanan Citra Digital Dengan Menggunakan Metode Discrete Wavelet Transformation (Dwt)	Keamanan Citra Digital Menggunakan Algoritma DES, AES, Blowfish Metode DWT

I.6. Sistematika Penulisan

Adapun sistematika penulisan dari skripsi ini adalah sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini penulis akan menjelaskan mengenai latar belakang masalah dan ruang lingkup permasalahan yang terdiri dari : identifikasi masalah, perumusan masalah serta batasan masalah, tujuan dan manfaat penelitian, metodologi penelitan dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini berisi uraian mengenai teori-teori yang terkait dengan masalah yang diteliti, yaitu : pengertian sistem, penguasaan aplikasi dan UML.

BAB III : ANALISA DAN PERANCANGAN SISTEM

Pada bab ini penulis menjelaskan tentang analisis sistem yang terdiri dari : *input*, proses dan *output* serta evaluasi sistem yang berjalan dan desain sistem yang dibangun.

BAB IV : HASIL DAN UJI COBA

Pada bab ini penulis membahas tentang tampilan interface dan hasil serta pembahasan tentang simulasi pembelajarang tekni-teknik dasar sepakbola yang dirancang serta kelebihan dan kekurangannya daripada sistem tersebut.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini penulis menguraikan kesimpulan dari keseluruhan penulisan dan saran yang membantu dalam penulisan.