BAB I

PENDAHULUAN

I.1. Latar Belakang

Perkembangan teknologi informasi dan komunikasi saat ini memudahkan manusia untuk mengakses berbagai sumber data/informasi dari berbagai belahan dunia. Penyajian dan penyimpanan informasi atau data kini dapat disimpan dalam *format digital* dan merniliki beragam bentuk dalam hal ini data atau informasi di simpan kedalam database.

Akhir-akhir ini, semakin banyak muncul berbagai *software* untuk mengedit dan memodifikasi data dengan mudah, bahkan kalangan awampun bisa menggunakannya . Hasil modifikasi mereka pun tidak sedikit yang bernada negatif baik untuk membuat fitnah, pengambaran buruk seseorang atau sekelompok orang dan berbagai maksud lainnya. Hal ini tentunya akan mengganggu para pemilik data, dan Juga pihak yang ingin berkornunikasi dalam rangka bertukar informasi baik kepentingan pribadi maupun kelompok. Sehingga dapat dikatakan bahwa perlindungan orisinalitas suatu data atau informasi menjadi kebutuhan yang penting dan mendesak saat ini. Untuk itu diperlukan usaha pengamanan data tersebut supaya keaslian dan kerahasiannya bisa terjaga. Untuk itu diperlukan usaha pengamanan data tersebut supaya keaslian dan kerahasiannya bisa terjaga Usaha perlindungan data dapat dilakukan dengan berbagai cara, salah satunya dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. *Kriptografi* telah ada dan digunakan sejak

berabad-abad yang lalu dikenal dengan istilah *kriptografi* klasik, yang bekerja pada mode karakter *alfabet*. Kelemahan *kriptografi* klasik adalah mudah dipecahkan dengan metode analisis *frekuensi*, karena keterbatasan kunci yang sedikit yaitu 26 kunci. Salah satu teknik *kriptografi* klasik adalah *algoritma Vigenère*. Pada saat ini, *algoritma kriptografi* telah berkembang secara *modern* dengan bantuan teknologi komputasi digital. *Kriptografi modern* menggunakan gagasan yang sama seperti *kriptografi* klasik, namun tidak beroperasi dalam modus karakter *alfabet* seperti pada *algoritma kriptografi* klasik. *Kriptografi modern* beroperasi pada mode *bit*, yang berarti semua data dan informasi (kunci, *plainteks*, maupun *cipherteks*) dinyatakan dalam rangkaian (*string*) *bit biner*, 0 dan 1. Salah satu teknik *kriptografi* modern adalah *algoritma RC4.*

Kriptografi klasik dan modern secara teori dapat digabungkan dengan bantuan teknologi komputasi modern, agarmendapatkan proteksi ganda dalam melindungi pesan rahasia. *Algoritma kriptografi Vigenère* dan *RC4* dapat dikombinasikan secara digital untuk menghasilkan dua lapis keamanan yang dapat memberi perlindungan lebih pada *database* rahasia. Dan oleh sebab itu berdasarkan uraian diatas penulis ingin membuat Skripsi kuliah ini dengan merancang dan membuat sebuah aplikasi komputer dengan judul **" Perancangan Aplikasi Keamanan Database Menggunakan Algoritma Vigenere dan Algoritma RC4".**

I.2. Ruang Lingkup Masalah

I.2.1. Indentifikasi Masalah

Berdasarkan latar belakang di atas, maka masalah dapat diidentifikasikan sebagai berikut:

1. Banyaknya pihak-pihak yang melakukan modifikasi data atau *database* yang bertujuan mengubah data yang ada sehingga merugikan pihak-pihak tertentu.
2. Terjadinya *interupsi* yang dapat mengganggu ketersediaan *database* yaitu data yang ada dapat dihapus sehingga pihak yang membutuhkan data atau informasi tersebut tidak dapat menemukan data atau informasi tersebut
3. Seringnya terjadi ancaman *intersepsi* yaitu merupakan ancaman terhadap kerahasiaan data atau informasi yang ada dalam *database.*

I.2.2. Rumusan Masalah

Rumusan masalah dalam pembahasan dan permasalahan yang akan dihadapi dalam perancangan aplikasi ini :

1. Bagaimana konsep *algoritma Vigenere* dan *Algoritma RC4* secara umum?
2. Bagaimana menerapkan *algoritma Vigenere* dan *Algoritma RC4* dalam melindungi *database*?
3. Bagaimana membangun program aplikasi *algoritma Vigenere* dan *Algoritma RC4* dalam implementasinya terhadap pengamanan *database*?

.I.2.3. Batasan Masalah

Sesuai dengan topik yang diangkat dalam penelitian ini, maka pembatasan masalah yang akan dibahas hanya meliputi :

1. Implementasi *algoritma Vigenere* dan *Algoritma RC4 pada database* .

2. Pengamanan hanya pada *database SQL Server*.
3. Perancangan menggunakan bahasa pemrograman *VB.Net*.
4. *Desains* sistem menggunakan UML (*Unified Modeling Language*).

I.3. Tujuan Dan Manfaat Penelitian

I.3.1. Tujuan

Adapun tujuan dari penelitian penulis ini adalah :

1. Untuk merancang suatu aplikasi keamanan *database* agar dapat terhindar dari ancaman *modifikasi,interupsi dan intersepsi*.
2. Untuk menyajiikan database yang dijamin keaslian datanya.
3. Untuk memperkenalkan aplikasi implementasi *Algoritma Vigenere* dan *Algoritma RC4.*

I.3.2. Manfaat

Adapun manfaat yang akan diperoleh dari aplikasi yang akan dibangun ini adalah:

1. Agar dapat terhindar dari ancaman modifikasi mengakibatkan perubahan *database* yang tidak diinginkan.
2. Dapat menyajiikan data atau informasi yang ada pada *database* yang dijamin keasliannya.
3. Diharapkan dengan adanya aplikasi ini dapat menjaga dari ancaman terhadap kerahasiaan *database*.

I.4. Metodologi Penelitian

Metode merupakan suatu cara atau teknik yang *sistematik* untuk mengerjakan suatu kasus. Didalam menyelesaikan Skripsi ini penulis menggunakan 2 (dua) metode *studi* yaitu :

1. Studi Lapangan

Merupakan metode yang dilakukan dengan mengadakan studi langsung ke lapangan untuk mengumpulkan data yaitu peninjauan langsung ke lokasi studi.

Adapun teknik pengumpulan data yang dilakukan penulis adalah

a. Pengamatan (*Observation*)

Merupakan salah satu metode pengumpulan data yang cukup efektif untuk mempelajari suatu sistem. Kegiatannya dengan melakukan pengamatan langsung terhadap kegiatan yang sedang berjalan.

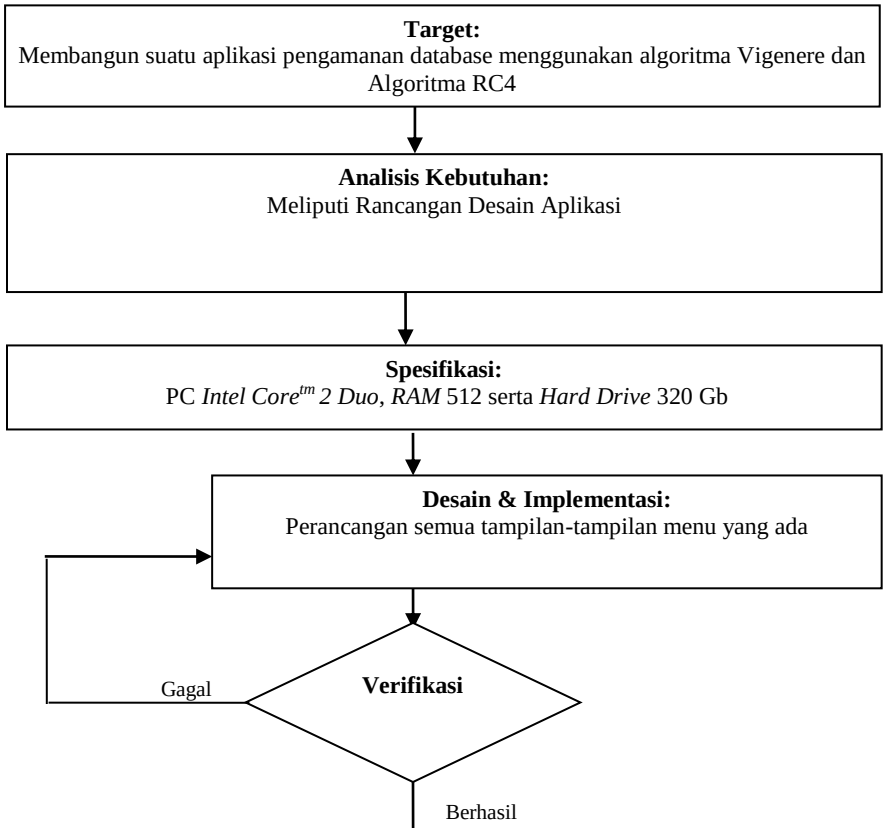
b. Sampel (*Sampling*)

Mengambil contoh – contoh data yang diperlukan khususnya *E-mail* berbentuk *plaintext.*

2. Studi Kepustakaan (*Library Research*)

Penulis melakukan studi pustaka untuk memperoleh data yang ada hubungan dengan penulisan Skripsi dari berbagai sumber bacaan seperti: buku, internet, dan lain – lain.

1. Analisa Sistem Yang Ada



Gambar 1.1 : Prosedur Perancangan

1. Target

Target merupakan tujuan dibuat skripsi ini. Adapun target dari dirancangnya aplikasi ini adalah merancang dan membangun suatu aplikasi pengamanan database menggunakan *algoritma Vigenere* dan *Algoritma RC4*

2. Analisis Kebutuhan

Adapun analisa yang penulis lakukan terhadap kebutuhan yang diharapkan dari aplikasi yang dirancang dan dibuat adalah sebagai berikut:

1. Aplikasi yang dibangun diharapkan menjaga *database* dari pihak-pihak yang tidak di inginkan
2. Aplikasi harus dapat memberikan manfaat yang lebih agar dapat banyak dipergunakan oleh banyak *user*.

3. *Spesifikasi* dan *Desain*

Berikut *spesifikasi* alat yang membantu perancangan dan pembuatan aplikasi adalah sebagai berikut:

1. *Spesifikasi Hardware*

a. *Processor Intel Pentium P6100.*

b. Memori *1 GB DDR3.*

c. *HardDisk 320 GB.*

d. *Keyboard* dan *mouse standar* komputer.

2. *Spesifikasi Software*

a. Sistem operasi *Microsoft Windows XP*.

b. *Microsof Visual Studio* 2010.

Pendesain yaitu merancang dan membuat aplikasi ini, dimana didalamnya berisikan interface atau tampilan yang menarik dan menggambarkan bagaimana aplikasi berinteraksi dengan sistem yang berintegrasi dengan pengguna yang akan menggunakannya, dan memberikan berbagai informasi yang dibutuhkan.

Berikut desain aplikasi yang penulis rancang agar pengguna dapat berinteraksi dengan perangkat lunak yang dirancang antara lain sebagai berikut:

1. Tampilan Menu Utama
2. Tampilan menu pilihan untuk enkripsi
3. Tampilan pesan yang telah dienkripsi
4. Tampilan konfirmasi bahwa pesan berhasil didekripsi
5. Tampilan hasil dekripsi

3. Membangun/Membuat Aplikasi

Tahapan dalam membangun dan membuat aplikasi ini adalah sebagai berikut:

1. Melakukan Implementasi *desain Form*/Tampilan

Pada tahap ini, penulis melakukan implementasi *desain Form* dengan membuat *Form* sesuai dengan desain yang dirancang pada bahasa pemrograman *VB.NET*.

2. Melakukan *Coding Program*

Pada tahap ini, dilakukan proses menterjemahkan dari keperluan data atau pemecahan masalah yang telah dirancang ke dalam bahasa pemrograman komputer. Proses penulisan program menggunakan bahasa pemrograman VB.NET.

4. Pengujian Sistem

Pada tahap ini dilakukan pengujian sistem secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan sistem. Pengujian fungsional dilakukan untuk mengetahui bahwa sistem dapat bekerja dengan baik sesuai dengan prinsip kerjanya. Dari pengujian sistem ini dapat diketahui kesesuaian hasil perancangan dengan analisis kebutuhan yang diharapkan.

I.5. Keaslian Penelitian

Sebagai bukti penelitian yang akan dibuat, maka penelitian akan dibandingkan terhadap penelitian sejenis yang pernah dilakukan. Penelitian pertama yang diangkat oleh Wiwiek Nurwiyati dan Indra Yatini dari STMIK AKAKOM Yogyakarta dengan judul "Enkripsi Dekripsi Data Menggunakan *Metode Stream* Dan *Vigenere Cipher*" dan penelitian kedua diangkat oleh Derwin Suhartono dari Unversitas BINUS Jakarta dengan judul "Aplikasi Penyembunyian Pesan Pada Citra JPEG Dengan *Algoritma* F5 Dalam Perangkat *Mobile* Berbasis Android" perbandingannya dapat dilihat pada tabel I.1. dibawah ini :

Tabel I.1. Keaslian Penelitian

No	Materi Perbandingan	Instrumen
Penelitian pertama : Enkripsi Dekripsi Data Menggunakan Metode Stream Dan Vigenere Cipher		
1.	Target	aplikasi pengamanan data
2.	Solusi	Solusi didapat dengan Menggunakan Metode Stream Dan Vigenere Cipher
3.	Bahasa pemrograman	*Visual Basic* 6.0

Penelitian kedua : Aplikasi Penyembunyian Pesan Pada Citra JPEG Dengan Algoritma F5 Dalam Perangkat Mobile Berbasis Android		
1.	Target	Merancang aplikasi steganografi
2.	Solusi	Solusi didapat dengan Algoritma F5
3.	Bahasa pemrograman	*Java Mobile*
Penelitian yang akan dibuat : Perancangan Aplikasi Keamanan Database Menggunakan Algoritma Vigenere dan Algoritma RC4		
1.	Target	Merancang aplikasi pengamanan database
2.	Solusi	Solusi didapat dengan Algoritma Vigenere dan Algoritma RC4
3.	Bahasa pemrograman	*VB.Net*

I.6. Sistematika Penulisan

Sistematika penulisan Skripsi ini adalah sebagai berikut.

BAB I : PENDAHULUAN

Pada bab ini akan menjelaskan tentang latar belakang, tujuan, metodologi penulisan yang digunakan, batasan masalah dan sistematika penulisannya.

BAB II : LANDASAN TEORI

Dalam bab ini diuraikan tentang teori-teori yang digunakan sebagai dasar untuk melakukan pemecahan masalah yang telah dirumuskan.

BAB III : DESKRIPSI PERUSAHAAN

Bab ini menguraikan mengenai gambaran umum perusahaan yang meliputi: sejarah berdirinya perusahaan, struktur organisasi dan struktur sistem yang digunakan.

BAB IV : ANALISIS DAN IMPLEMENTASI SISTEM

Bab ini menguraikan seluruh uraian mengenai pengolahan data dan data yang telah dikumpulkan dan dikaitkan dengan cara berfikir guna mendapatkan pemecahan masalah.

BAB V : PENUTUP

Bab ini berisi tentang berisi kesimpulan dari pembahasan dan saran-saran yang diharapkan dapat memberikan masukan.