BAB III

METODOLOGI PENELITIAN

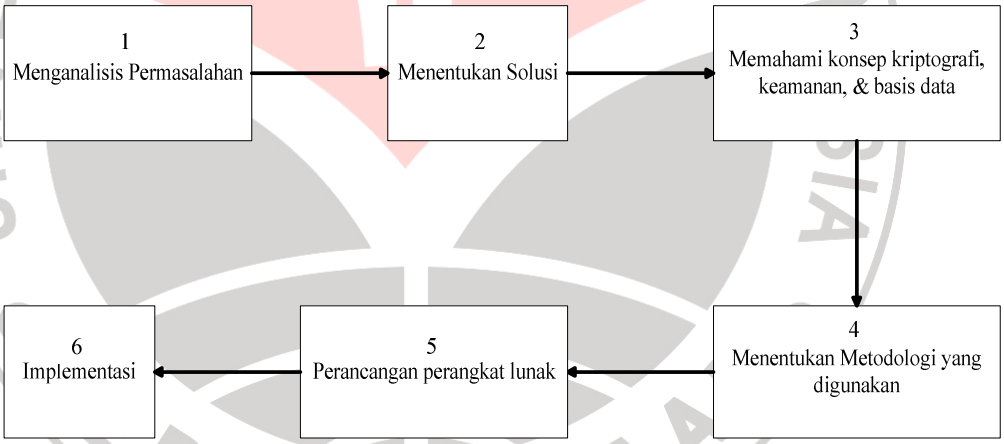
3.1 Alat dan Bahan Penelitian

Dalam melakukan penelitian ini, berikut alat dan bahan penelitian yang digunakan:

1. Literatur: yaitu buku, jurnal, *paper*, dan artikel ilmiah yang berhubungan dengan kriptografi (khususnya algoritma kriptografi RC4), Basis data (khususnya mengenai *query* dan *PL/SQL* (*Programming Language*/*Structured Query Language*) .
2. Adapun dari sisi *hardware*, rekomendasi spesifikasi yang bisa digunakan adalah:
    - Prosesor *Dual Core* 64*bit* AMD *Athlon* X2 5400+ (*clock* 2.8 Ghz) atau yang setara.
    - Memori RAM 1GB
    - Kapasitas *Harddisk* 160GB dengan ruang kosong sekitar 10GB
    - Antarmuka Jaringan: *Realtek* RTL8168/8111C(P) *Gigabit Ethernet* NIC dan kabel LAN sepanjang 5 M
3. Sedangkan dari sisi *software*, rekomendasi spesifikasi yang digunakan adalah:
    - XAMPP 1.7.2 (*Apache* 2.2.12 sebagai *web service*, PHP 5.3.0 sebagai *server side scripting*)

- *Micosoft Sql Server* 2005 *Developer Edition*, sebagai DBMS (*Database Management System*)
- *Micosoft Visual* C# 2005 *Profesional Edition* (*tools* bahasa pemrograman C#)
- Sistem Operasi: *Windows* XP *Profesional* SP3
- *Internet Browser*: *Mozilla Firefox* 3.5.3
- *Text editor: Notepad++*
- *Javascript* (sebagai *Client Side Scripting*)

3.2 Desain Penelitian



Gambar 3.1 Desain Penelitian

1. Dalam penelitian ini, permasalahan yang dianalisis adalah permasalahan keamanan, dimana di dalam arsitektur perangkat lunak yang ada, menggunakan arsitektur *client-server*, dimana basis data diakses secara *remote* melalui suatu jaringan komputer. Pengaksesan basis data,

khususnya secara *remote*, dapat menimbulkan masalah keamanan, seperti *sniffing*, di mana data-data yang melewati jaringan dapat dilihat, seperti *query* yang digunakan, dan hasil *retrieve* dari *query* tersebut (data-data pribadi, struktur tabel, dan sebagainya).

2. Salah satu cara untuk melakukan pengaman data selama dalam jaringan yaitu dengan melakukan enkripsi. Untuk aplikasi berbasis *web*, pengamanan jaringan ini dilakukan antara *server web* dengan *server* basis data. Pengamanan dengan enkripsi ini dilakukan untuk menjaga data agar data terjaga kerahasiannya. Enkripsi akan mempersulit penyadap, karena data hasil *sniffing* tidak akan dimengerti oleh penyadap.
3. Penulis mencoba memahami konsep kriptografi, keamanan, dan basis data.
4. Dalam penelitian untuk skripsi ini, penulis memilih metodologi *research and development* (R&D) untuk perangkat lunak.
5. Penulis akan melakukan perancangan perangkat lunak Kontrak Kuliah *Online* (KoKiNe) di mana algoritma RC4 ini akan diimplementasikan. Pendekatan yang digunakan dalam melakukan perancangan ini adalah pendekatan berorientasi objek (*objek oriented*) dengan model proses yang dipilih adalah model *prototipe*. Pembahasan secara lengkap mengenai tahapan-tahapan dalam melakukan perancangan perangkat lunak ini akan dibahas secara terperinci di dalam dokumen teknis perangkat lunak, sedangkan mengenai enkripsi RC4 tersebut akan dibahas pada skripsi ini.
6. Implementasi yang dilakukan merupakan implementasi penggunaan algoritma kriptografi RC4 dalam mengamankan data selama dalam

transmisi di jaringan komputer antara *client* (*web server*) dengan server (*server* basis data).

3.3 Metode Penelitian

Penulis melakukan beberapa tahapan penelitian yang dilaksanakan. Tahapan-tahapan yang dilakukan yaitu pengumpulan data, perancangan perangkat lunak, dan pembangunan perangkat lunak.

3.3.1 Metode Pengumpulan Data

a. Studi Kepustakaan

Mempelajari literatur-literatur yang berkaitan dengan teori dan konsep atas masalah yang diteliti agar diperoleh suatu pemahaman yang mendalam serta menunjang proses pembahasan mengenai masalah-masalah yang telah diidentifikasi.

b. Oberservasi

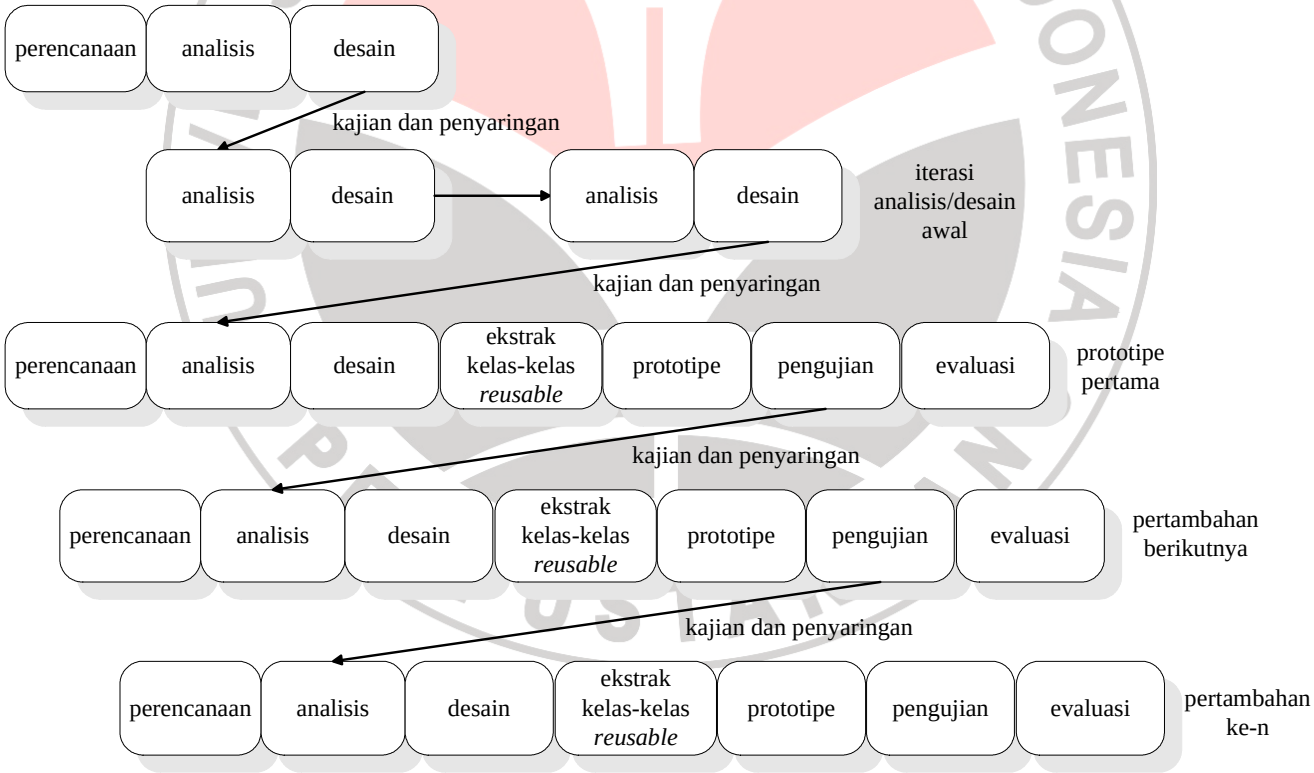
Melakukan pengamatan terhadap kenyataan yang ada di lapangan, seperti melihat proses yang ada dalam transaksi kontrak mata kuliah secara manual dan mencoba memetakannya secara *online*

c. Wawancara

Mencari apa yang dirasakan pengguna dalam menggunakan kontrak mata kuliah secara manual, baik kekurangan ataupun kelebihan, dan harapan-harapan yang diinginkan pengguna bila konrak mata kuliah dilakukan secara *online*.

3.3.2 Metode Pembangunan Perangkat Lunak

Pengembangan perangkat lunak ini menggunakan pendekatan berorientasi objek yang terfokus pada “informasi dan perilaku yang dimiliki suatu objek sehingga kemudian pengembang dapat mengembangkan sistem/perangkat lunak yang fleksibel dalam menghadapi perubahan-perubahan informasi dan/atau perilaku yang dituntut pengguna” (Nugroho, 2005, h. 6). Berikut adalah urutan proses tipikal berorientasi objek menurut Pressman (1997, h. 677)



Gambar 3.2 Urutan proses tipikal untuk pendekatan berorientasi objek menurut Pressman

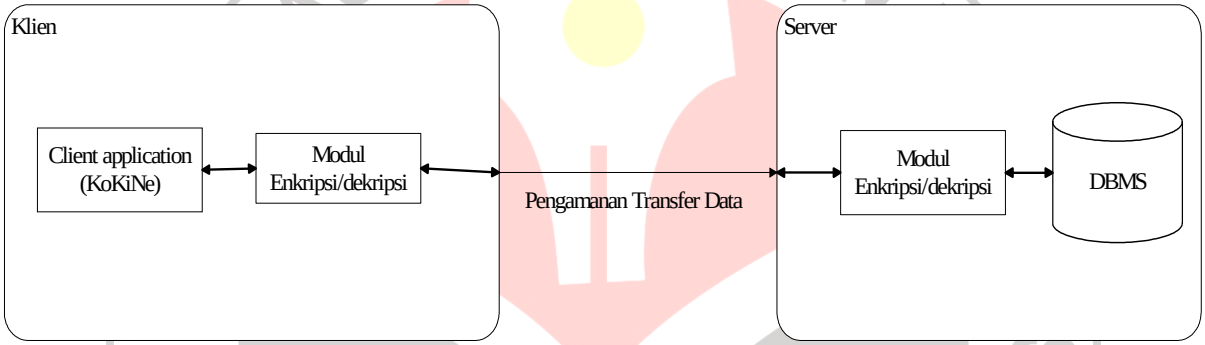
Menurut Ed Berard dan Grady Booch (Pressman, 1997, h. 674) cara kerja pemodelan tersebut adalah:

- Melakukan analisis secukupnya untuk mengisolasi koneksi dan kelas-kelas masalah utama
- Melakukan sedikit desain untuk menentukan apakah kelas dan koneksi tersebut dapat diimplementasi dengan cara yang praktis
- Mengekstrak objek *reusable* dari suatu pustaka untuk membangun *prototipe* kasar
- Melakukan beberapa pengujian untuk mengungkap kesalahan pada *prototipe*
- Melakukan evaluasi mengenai *prototipe* itu
- Memodifikasi model analisis yang didasarkan pada apa yang telah dipelajari dari *prototipe* tersebut, dari pembuatan desain, dan dari hasil evaluasi
- Menyaring desain untuk mengakomodasi perubahan yang ada
- Merekayasa objek khusus (yang tidak dapat diperoleh dari pustaka)
- Memasang *prototipe* baru dengan menggunakan objek pustaka dan objek baru yang telah diciptakan
- Melakukan beberapa pengujian untuk mengungkap kesalahan pada *prototipe*
- Melakukan evaluasi mengenai *prototipe* tersebut

Pendekatan ini berlanjut sampai *prototipe* berkembang ke dalam aplikasi produksi/siap pakai.

3.4 Implementasi

Implementasi yang dilakukan adalah pengamanan transmisi *query* dan hasil *query* basis data menggunakan algoritma kriptografi RC4. Hasil dari implementasi tersebut adalah *prototipe* dari perangkat lunak untuk memperlihatkan penggunaan algoritma kriptografi RC4 tersebut. Berikut adalah gambaran umum dari perangkat lunak yang dimaksud:



Gambar 3.3 Gambaran Umum Perangkat Lunak