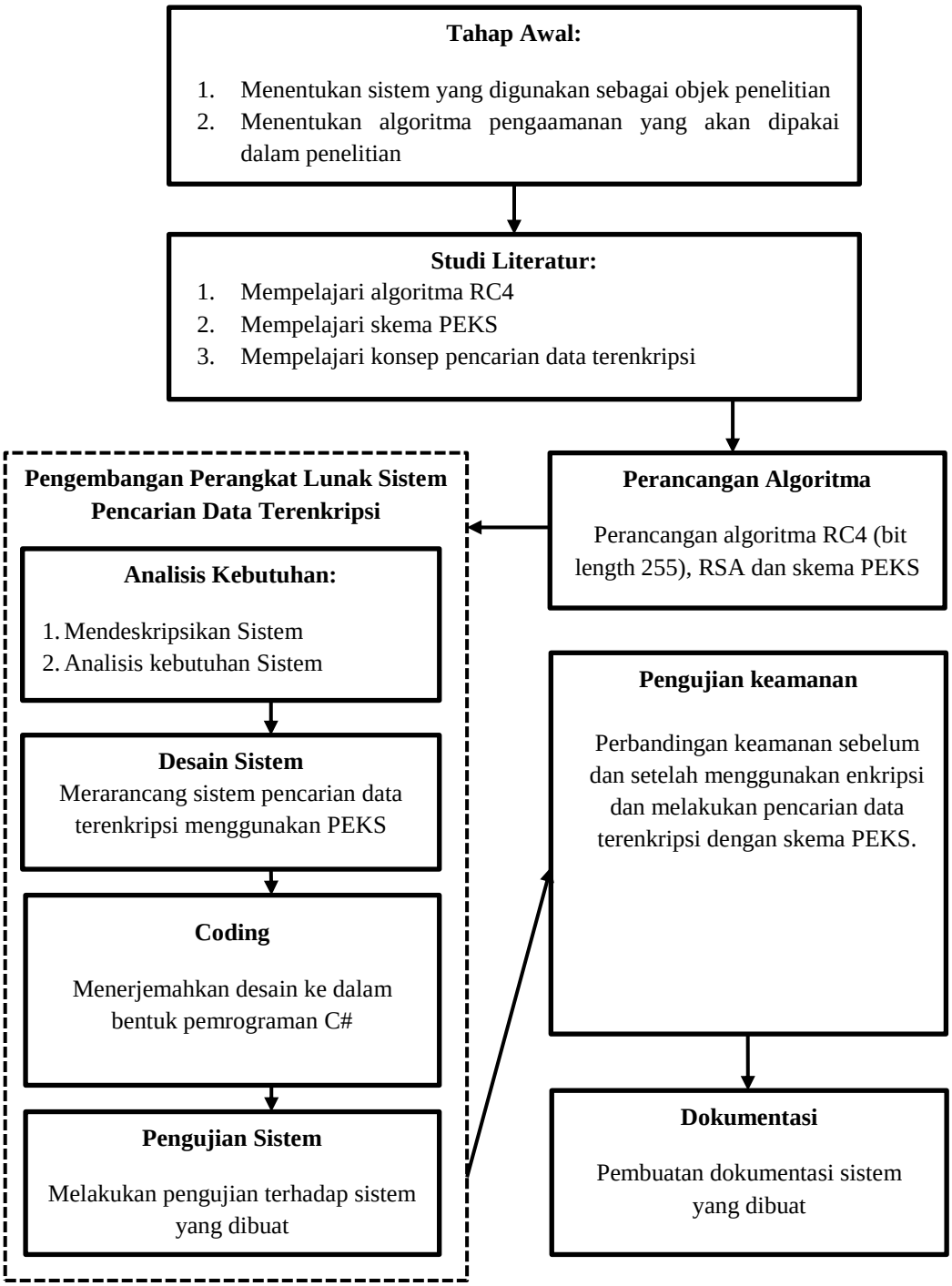
BAB III

METODOLOGI PENELITIAN

3.1. Desain Penelitian



Gambar 3.1 Diagram desain penelitian

3.1.1 Tahap Awal

Ini merupakan tahap penentuan penggunaan bahan terkait dengan penelitan yang dilakukan. Pada tahap ini merupakan proses menentukan sistem yang digunakan dan proses menentukan skema dan algoritma kriptografi yang digunakan. Dalam penelitian ini sistem diterapkan pada media penyimpanan *elearning* dengan menggunakan skema PEKS dan algoritma kriptografi RC4 dan RSA.

3.1.2 Studi Literatur

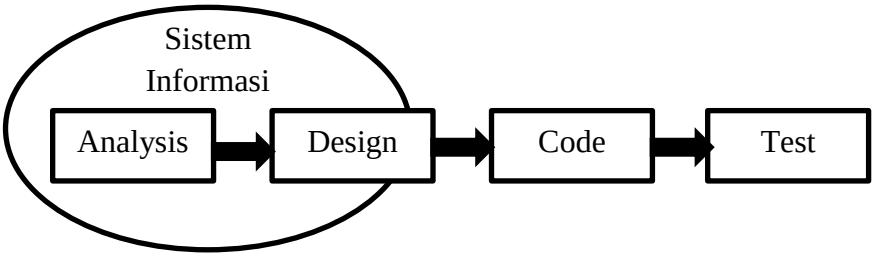
Pada tahap ini merupakan tahap mempelajari terkait dengan penelitian yang dilakukan yaitu mempelajari konsep pencarian data terenkripsi menggunakan skema PEKS, mempelajari algoritma RC4 dan RSA. Sumber yang digunakan ialah buku, jurnal, skripsi dan informasi yang didapat dari internet.

3.1.3 Perancangan Algoritma

Pada tahapan ini dilakukan perancangan dan pembuatan skema PEKS dan algoritma RC4 dan RSA. Perancangan algoritma RC4 ini menggunakan bitlength 256 bit dan RSA menggunakan *bitlength* 1024 bit. Bahasa pemrograman yang digunakan dalam pengembangan sistem ini adalah C#.

3.1.4 Pengembangan Perangkat Lunak

Pada tahapan ini dilakukan pembuatan perangkat lunak *elearning* yang dilengkapi sistem pencarian data terenkripsi menggunakan skema PEKS, algoritma RC4 dan didukung oleh algoritma RSA dengan menggunakan model proses *Sequential Linear* yang dikembangkan oleh Roger. Model ini merupakan model klasku yang bersifat sistematis yang memiliki langkah-langkah dalam membuat perangkat lunak.



Gambar 3.2 Diagram Model *Sequential Linear* (Pressman, 2002)

3.1.5 Analisis

Merupakan tahap menganalisis hal-hal yang diperlukan dalam pelaksanaan proyek pengembangan perangkat lunak *elearning* yang dilengkapi dengan sistem pencarian data terenkripsi.

3.1.6 Desain

Ini merupakan tahap penerjemahan dari data analisi kedalam bentuk yang mudah dimengerti oleh user yaitu pembuatan tampilan antarmuka, arsitektur perangkat lunak, dan detil algoritma. Ini merupakan proses mempersiapkan suatu model perangkat lunak sehingga dapat dilanjutkan pada tahap berikutnya *Coding*.

3.1.7 Coding

Tahap penerjemahan data atau pemecahan masalah yang telah dirancang kedalam bahasa pemrograman, yaitu C#. Sehingga seluruh desain yang telah dirancang dapat berfungsi dan berjalan dengan baik.

3.1.8 Testing

Merupakan tahap pengujian terhadap perangkat lunak yang dibangun yaitu sistem pencarian data terenkripsi pada media

penyimpanan elearning menggunakan skema PEKS, algoritma RC4 dan didukung algoritma RSA secara menyeluruh dari desain antarmuka, alur , hingga fungsi-fungsi yang telah dirancang dapat dipastikan berjalan dengan baik dan benar. Fungsi utama yang akan jadi fokus pengujian adalah pada proses pencarian data terenkripsi oleh algoritma RC4 yang dilakuakan oleh user yang terotentikasi. Pada penelitian ini perangkat lunak akan memperlihatkan keamanan sebelum dan setelah dilakukan enkripsi dan bagaimana penerapan konsep PEKS pada pencarian data terenkripsi.

3.2 Alat dan Bahan Penelitian

3.2.1 Alat Penelitian

Alat penelitian yang digunakan sebagai berikut :

1. Perangkat Keras

   Komputer

   a. *Processor* Intel Pentium M 1.80 GHz
   b. RAM 1 GB
   c. *Hard Disk* 60 GB
2. Perangkat Lunak
   a. Microsoft visual studio 2010

      Microsoft visual studio 2010 ini digunakan sebagai alat untuk mengembangkan perangkat lunak dalam penelitian ini, dalam bahasa pemrograman C#.
   b. Microsoft SQL Server 2008

      Microsoft SQL Server 2008 digunakan untuk membangun database yang akan digunakan oleh sistem.

3.2.2 Bahan Penelitian

Bahan penelitian yang digunakan berupa literature *textbook*, paper, tutorial, artikel dan dokumentasi lainnya yang didapat dari observasi di perpustakaan dan internet mengenai sistem pencarian

data terenkripsi menggunakan skema PEKS pada media penyimpanan elearning.