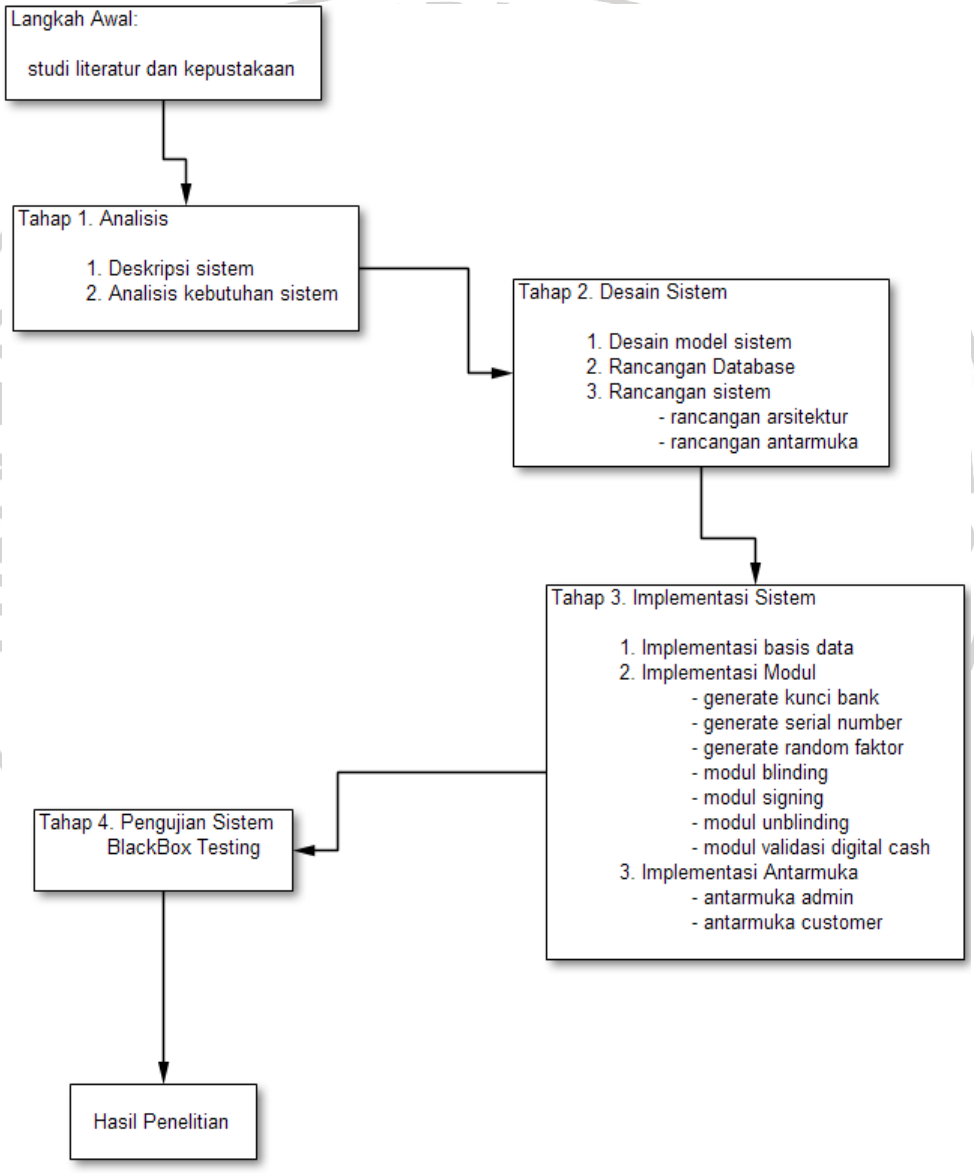
BAB III

METODOLOGI PENELITIAN

3.1 Desain Penelitian



Gambar 3.1*Desain Penelitian*

Metode rekayasa sistem (perangkat lunak) yang digunakan dalam penelitian ini berdasarkan konsep pendekatan terstruktur. Konsep ini merupakan pemodelan pendekatan yang baku dengan menerapkan tahapan-tahapan yang sistematik. Konsep ini mengenalkan beberapa alat yang dibutuhkan dalam pembangunan sistem, antara lain :

1. Context Diagram

   Digunakan sebagai penjelasan event-event pada sistem, tiap proses event dijelaskan pada *function breakdown*-nya.
2. Diagram Alir Data (DFD)

   Menggambarkan transformasi perpindahan data yang terjadi di dalam sistem.
3. Kamus Data (*Data Dictionary*)

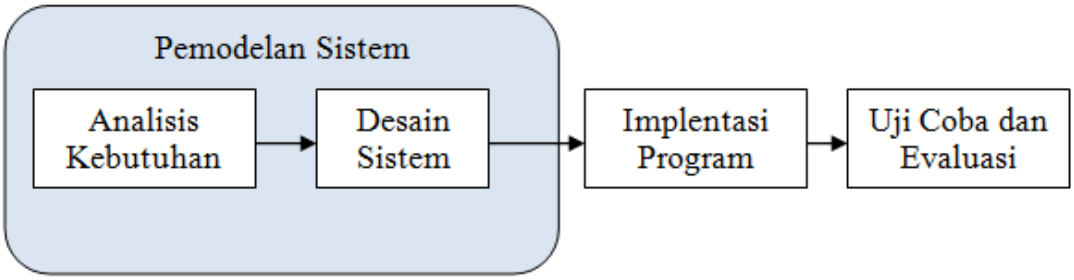
   Menyimpan deskripsi objek data yang digunakan dan yang dihasilkan oleh sistem.
4. Spesifikasi Proses

   Penjelasan setiap proses yang ada pada DFD.
5. Diagram Keterhubungan Entitas (ERD)

   Menggambarkan hubungan antar objek di dalam sistem.

Pengembangan sistem ini menggunakan model sekuensial linier atau model *waterfall*. Model ini merupakan model klasik yang bersifat sistematis, berurutan membangun perangkat lunak.

Berikut skemaaktivitasnya (Presman, 2004:37):



Gambar 3.2*Model Sekuensial Linear*

Desain penelitian sitem ini melingkupi aktivitas berikut ini:

1. Pemodelan sistem

   Bertujuan untuk menemukan batasan-batasan masalah pada penerapan sistem.

   Pemodelan sistem terdiri dari 2 tahap, yaitu:

   a. Analisis kebutuhan

      Dalam menganalisa kebutuhan, penulis mengamati permasalahan yang terkait dengan *transaksi online* dan *digital cash*. Bentuk–bentuk *digital cash*, syarat atau property dari *digital cash*, proses penggunaan serta ancaman yang menyerang kemanan *digital cash.*

b. Desain sistem

Dari hasil analisa kebutuhan, penulis mencoba mencari solusi lalu mendesain sistem yang sesui dengan solusi atas permasalahan yang dihadapi. Proses pada tahap ini berfokus pada struktur data, arsitektur sistem, representasi antarmuka, dan prosedur algoritma. Tahap ini menterjemahkan kebutuhan ke dalam representasi sistem yang akan dibangun.

2. Implementasi program

Implementasi yang dilakukan disini adalah mengimplementasikan *blind signature* dengan menggunakan skema algoritma RSA dalam proses penarikan *digital cash*, dengan menerapkan modul-modul yang sudah di rancang agar menjadi satu kesatuan sistem yang utuh.

3. Uji coba dan evaluasi

Uji coba dan evaluasi berfokus pada logika internal sitem. Proses uji coba dilakukan untuk menguji apakah *blind signature* mampu membuat *digital cash* menjadi tidak terindentifikasi baik oleh bank maupun oleh *vendor*. Selain itu melakukan *verifikasi* dan *validasidi gital cash*, baik dari keaslian *signature* maupun nominalnya.

3.2 Alat Penelitian

Penelitian ini dilakukan dengan menggunakan :

1. PC dengan spesifikasi , Prosesor AMD Phenom (tm) II X4 840 Processor 3,2 GHz, RAM 4GB , VGA 1024 MB 128 Bit, dan hardisk 120 GB
2. Sistem operasi Windows 7, software xampp-win32-1.7.7 (MySql, Apache, PHP), Eclipse Helios, dan browser.

3.3 Implementasi

Implementasi yang dilakukan adalah dengan mengimplementasikan algoritma RSA dan *blind signature* dalam transaksi *digital cash.*