# BAB III

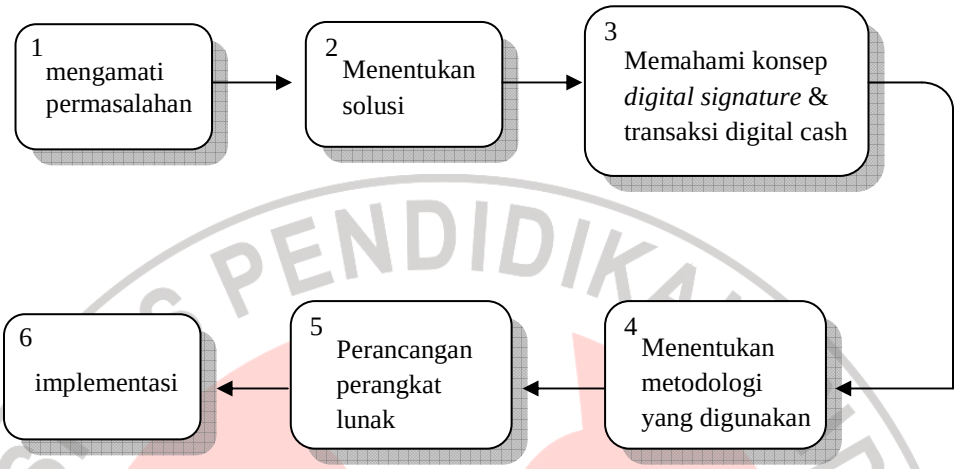
# METODOLOGI PENELITIAN

## 3.1 Alat dan Bahan Penelitian

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

1. Literatur yakni : buku, jurnal, paper dan artikel ilmiah yang berhubungan dengan *digital signature*, *digital cash payment* , kiptografi dan RSA. Adapun literatur yang digunakan sebagai acuan utama dalam penelitian ini adalah : Digital Payment Sistems with Passive Anonymity-Revoking Trustees oleh Canebish dan Jan m Ueli Maurer serta Digital Cash oleh Jahanian Farsi.
2. PC dengan spesifikasi , intel pentium *dual core* 1.8 GHz,RAM 1 Gb dan hardisk 120 GB .
3. Software XAMPP 1.7.0 ( Mysql, Apache, php yang telah dipaketkan ), power designer 9, dreamweaver 8, photoshop CS , Microsoft Office 2007

## 3.2 Desain Penelitian




**Gambar 3.1** *model desain penelitian*

1. Dalam menentukan permasalahan untuk penelitian ini, penulis mengamati kondisi *cyberfraud* untuk transaksi *online* saat ini yang melibatkan penggunaan kartu kredit dalam transaksinya, terdapat fenomena dan kasus-kasus yang penulis dapatkan mengenai kasus penipuan ( cyberfraud ), pencurian data kartu kredit kustomer, hack *database* paypal dalam mencuri data privasi kustomer yang melibatkan kartu kredit dalam transaksinya.
2. Dari hasil pengamatan tersebut, penulis mencoba untuk mencari solusi dalam bertransaksi *online* saat ini, agar privasi kustomer untuk data yang bersifat pivasi ini dapat terjaga keamanannya. Dalam hal ini penulis mencoba membuat transaksi *online* dengan menggunakan *property anonymous* seperti pada transaksi menggunakan uang kertas. Dalam model

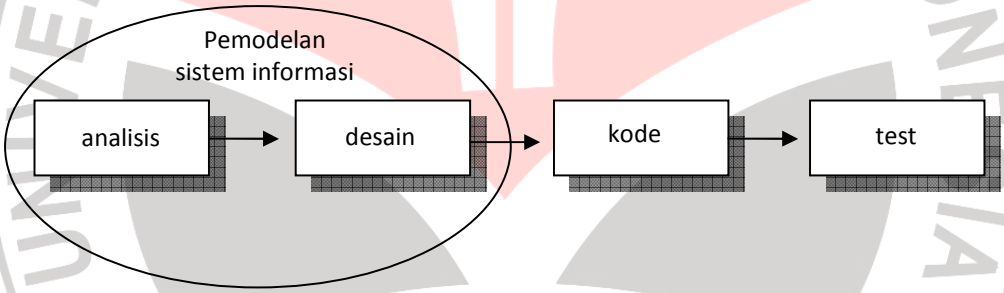
transaksi yang dibuat ini penulis melengkapi *digital signature* untuk otentikasi keamanan dalam bertransaksi menggunakan algoritma RSA.

3. Penulis mencoba memahami untuk konsep *digital signature*, algoritma RSA dan.transaksi *digital cash*. .
4. Dalam penelitian skripsi ini, penulis memilih menggunakan metodologi *research and development* (R&D) untuk perangkat lunak.
5. Penulis akan melakukan perancangan untuk transaksi *online* menggunakan uang digital yang disertai dengan penggunaan RSA *digital signature*. Pendekatan yang digunakan untuk melakukan perancangan ini adalah pendekatan terstruktur ( *process oriented* ) dengan model proses yang di pilih adalah *sequensial linear*. Pembahasan secara lengkap untuk tahapan tahapan dalam melakukan perancangan perangkat lunak ( SDLC ) ini akan dibahas secara terperinci pada dokumen teknis perngkat lunak untuk perangkat lunak yang akan dibuat, adapun untuk konsep RSA *digital signature* dalam transaksi *digital cash* ini, secara lengkap akan dibahas pada skripsi ini.
6. Implementasi yang dilakukan merupakan implementasi RSA *digital signature* pada transaksi digital cash dengan membuat *prototype* untuk transaksi *digital cash* menggunakan RSA *digital signature*.

## 3.3 Metodologi Penelitian Perangkat Lunak

Dalam proses analisis dan perancangan yang dilakukan, digunakan pendekatan berbasis proses (*process oriented approach* ) dengan model proses yang digunakan adalah *Sequential Model*/*waterfall* model.

Model ini adalah model klasik yang besifat sistematis, berurutan dalam membangun perangkat lunak. Berikut skema dan aktifitas - aktivitas dalam model sekuensial linear (Presman,2004:37):




**Gambar 3.1** *Model sequensial linear*

1. Rekayasa dan pemodelan sistem/informasi

   Rekayasa dan analisis sistem mencakup pengumpulan kebutuhan pada tingkat bisnis strategis dan tingkat area bisnis.dalam penelitian ini akan dibuat frame work sistem dalam transaksi menggunakan uang digital .

2. Analisis kebutuhan perangkat lunak
3. Desain

a. Membuat ERD untuk object data yang dimodelkan.
b. Membuat DFD untuk menggambarkan aliran informasi dan transformasi data.
c. Membuat PSPEC untuk menggambarkan semua model proses yang nampak pada tingkat akhir penyaringan dengan disertai algoritma di setiap proses yang ada.
d. Membuat Kamus Data

4. Generasi kode
5. testing

## 3.4 Impelementasi

Implementasi yang dilakukan dalam penelitian ini adalah mengimplementasikan keilmuan kriptografi untuk *digital signature* yang menggunakan algoritma RSA 64 bit ini pada transaksi *digital cash* yang menggunakan uang digital dalam transaksinya. Hasil dari pengimplementasian tersebut akan dibuat *prototype* perangkat lunak untuk mempelihatkan penggunaan RSA *digital signature* dalam transaksi *digital cash* ini.