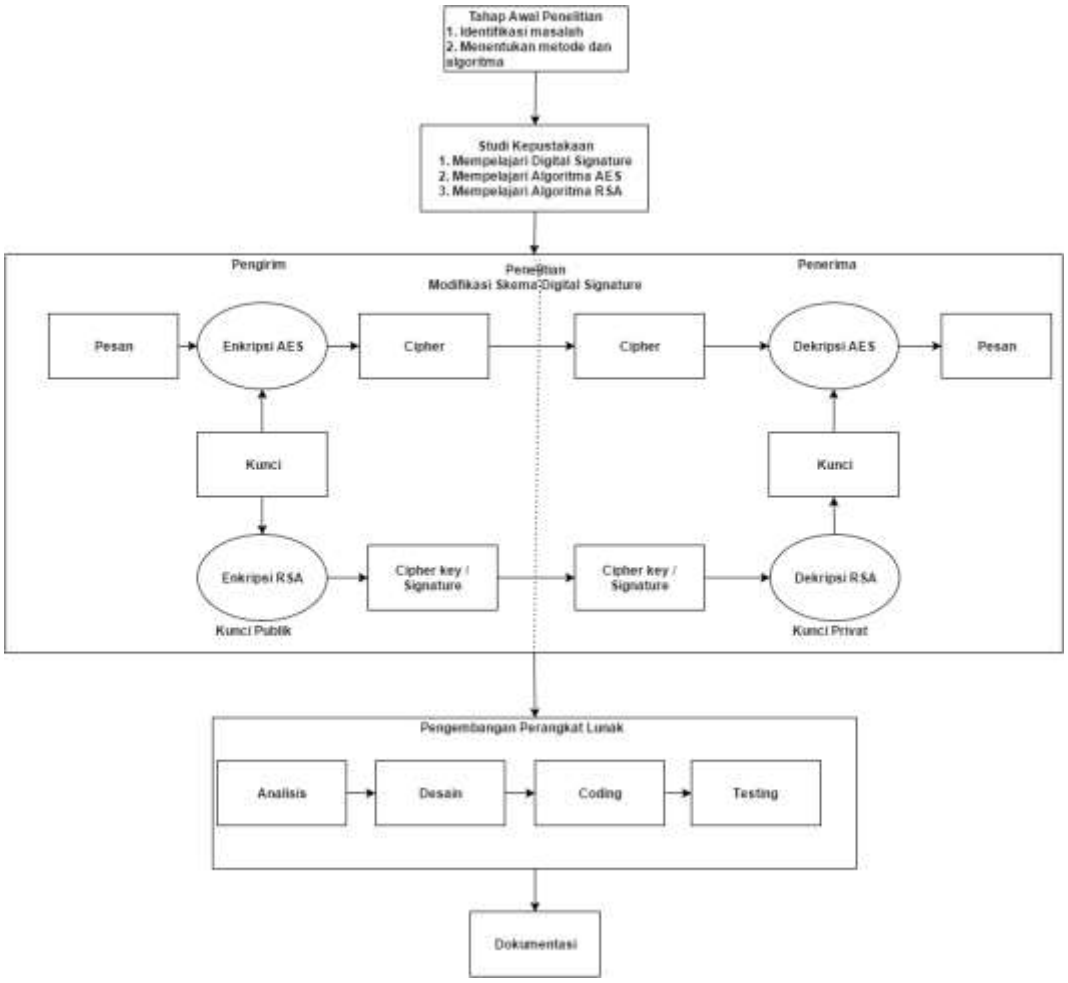
BAB III
METODE PENELITIAN

3.1. Desain Penelitian

Desain penelitian merupakan tahapan yang dilakukan untuk memberikan gambaran serta kemudahan dalam melakukan penelitian. Tahapan penelitian yang akan dilakukan ditujukan pada Gambar 3.1.



Gambar 3. 1 Skema Desain Penelitian

Tahapan penelitian yang akan dilakukan meliputi langkah–langkah berikut:

1. Tahap awal penelitian, yaitu identifikasi permasalahan yang akan diselesaikan dan menentukan metode untuk menyeselaikannya.

2. Studi kepustakaan merupakan tahapan mempelajari metode-metode yang akan digunakan pada penelitian, yaitu mempelajari konsep *digital signature*, mempelajari algoritma RSA dan algoritma AES. Sumber yang digunakan berupa buku, jurnal maupun bahan bacaan yang terdapat pada internet. Buku "Kriptografi" karya Rinaldi Munir pada tahun 2006 menjadi sumber dalam mempelajari konsep *digital signature*. Selain buku tersebut, jurnal milik Wisnu Wedanto (2013), Aji Setiyo Sukarno (2013) dan Ibnu Berliyanto G. A., Amir Hamzah, Suwanto Raharjo (2014) menjadi sumber yang digunakan untuk mempelajadi konsep *digital signature*.

   Untuk sumber yang digunakan dalam mempelajari algoritma AES digunakan buku berjudul "*Cryptography and Network Security: Principles and Practice* 5^{th} *Edition*" milik William Stalling yang diterbitkan pada tahun 2011 dan buku "Kriptografi" milik Rinaldi Munir pada tahun 2006.

   Buku karya Rinaldi Munir yang berjudul "Kriptografi" pada tahun 2006 menjadi sumber yang digunakan dalam mempelajari algoritma RSA. Selain buku tersebut jurnal milik Wisnu Wedanto (2013), Aji Setiyo Sukarno (2013) menjadi sumber yang digunakan untuk mempelajadi algoritma RSA.
3. Memodifikasi skema *digital signature*, *digital signature* pada umumnya hanya memberikan sebuah tanda digital dan tidak merahasiakan isi pesan. Hal tersebut mengakibatkan tidak terjaga kerahasiaan isi pesan. Proses modifikasi dilakukan untuk menambahkan kombinasi algoritma AES dan RSA pada *digital signature*. Algoritma AES bertujuan untuk menjaga kerahasiaan isi pesan, sedangkan algoritma RSA bertujuan untuk menjaga kerahasian kunci yang akan digunakan pada algoritma AES untuk proses mendekripsi pesan.
4. Pengembangan perangkat lunak dengan metode sekuensial linier, yang terdiri dari Analisis, Desain, *Code* dan *Test*.

5. Dokumentasi merupakan pembuatan dokumen skripsi berserta dokumen teknis pembuatan sistem.

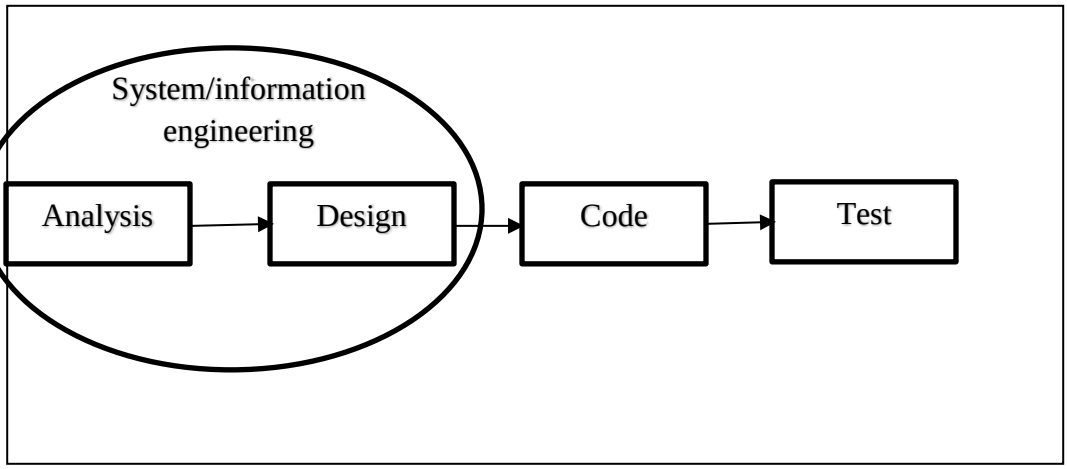
3.2. Metode Penelitian

3.2.1. Metode pengumpulan Data

Dalam penelitian kali ini, data dan informasi yang tersedia dapat menunjang proses penelitian. Pada proses ini dilakukan studi kepustakaan dengan mempelajari *digitalsignature*, algoritma RSA, dan algoritma AES melalui jurnal, *textbook*, tutorial, dan dokumentasi lainnya yang didapat melalui observasi di perpustakaan dan *World Wide Web*.

3.2.2. Proses Pengembangan Perangkat Lunak

Proses pengembangan perangkat lunak menggunakan model sekuensial linier. Berikut adalah tahapan-tahapan dari proses pengembangan perangkat lunak dengan model sekuensial linier pada Gambar 3.2.



Gambar 3. 2 Model Sekuensial linier

a. *Analysis*

Analysis dilakukan untuk menentukan kebutuhan, tujuan dan batasan-batasan apa saja dari perangkat lunak. Sehingga dapat diketahui secara rinci kebutuhan yang akan diperlukan, fungsi-fungsi yang akan digunakan, membutuhkan perangkat lunak tambahan atau tidak dan lain sebagainya.

b. *Design*

Pada tahap ini dilakukan perancangan antarmuka dan basis data yang digunakan pada perangkat lunak, serta perancangan alur proses yang digunakan pada perangkat lunak sehingga semua langkah yang ada dalam sistem disposisi surat yang dimodifikasi dapat dijalankan.

c. *Code*

Dibangun suatu perangkat lunak yang mampu menyelesaikan atau mengolah data-data yang telah terkumpul. Pada tahap ini dilakukan penerjemahan data atau pemecahan masalah yang telah dirancang pada tahap sebelumnya ke dalam bahasa pemrograman.

d. *Test*

Dilakukan pengecekan terhadap perangkat lunak yang telah dibangun apakah sesuai atau tidak dengan kebutuhan menggunakan *blackbox testing*.

3.3. Alat dan Bahan Penelitian

Pada penelitian ini digunakan alat penelitian berupa perangkat keras dan perangkat lunak sebagai berikut:

a. Perangkat Keras

Kebutuhan perangkat keras yang digunakan adalah:

Prosesor : AMD Phenom II X4

Memori : 4 GB RAM

Kapasitas HDD : 500 GB

b. Perangkat Lunak

Peneltian yang dilakukan dibangung di atas Sistem Operasi Windows 7 Ultimate, dan kebutuhan akan perangkat lunak lainnya adalah Web Browser, Web Server, Text Editor dan Hex Editor Neo.

Bahan penelitian yang digunakan adalah jurnal, *textbook*, *tutorial*, dan dokumentasi lainnya yang didapat melalui observasi di perpustakaan dan *World Wide Web* tentang sistem disposisi surat, *digital signature*, algoritma AES dan algoritma RSA.