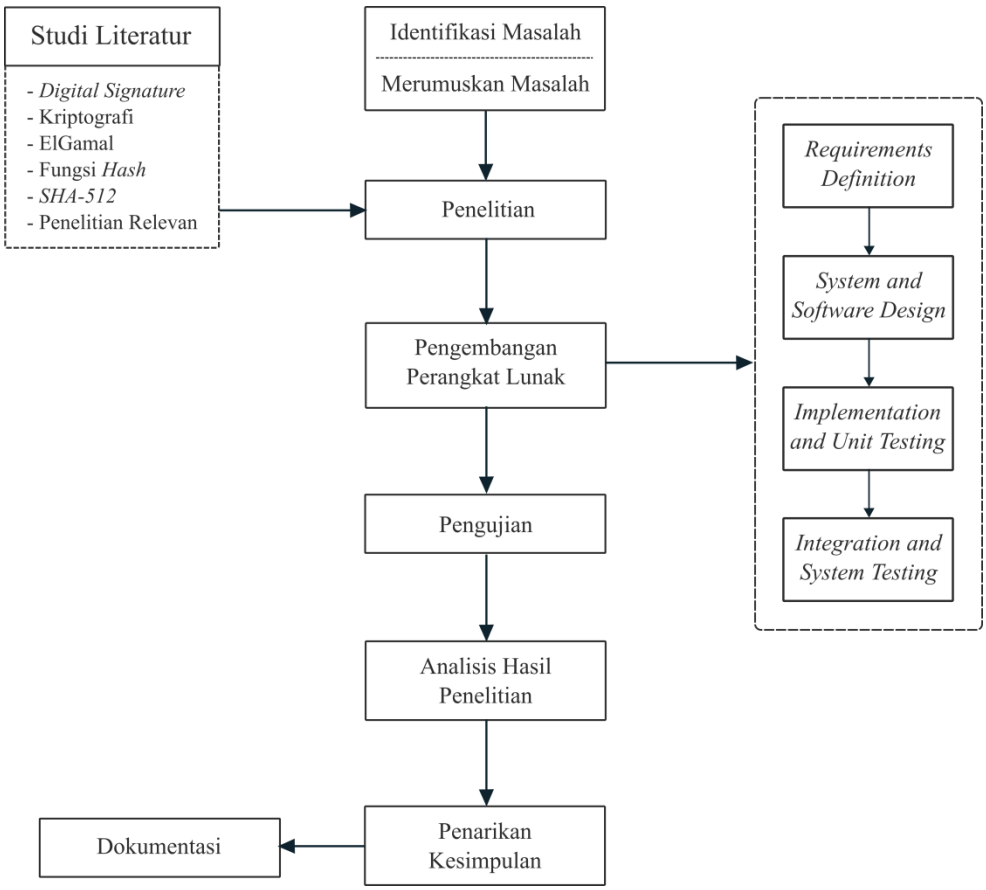
BAB III
METODOLOGI PENELITIAN

Bab ini merupakan bagian yang bersifat prosedural, yaitu bagian yang akan memaparkan serta mengarahkan pembaca agar mengetahui bagaimana peneliti merancang alur penelitiannya, metode penelitian yang diterapkan, serta instrumen yang digunakan.

3.1 Prosedur Penelitian

Prosedur penelitian adalah alur atau tahapan yang akan dilakukan dalam penelitian. Prosedur penelitian ini dibuat untuk memberikan gambaran serta kemudahan dalam melakukan penelitian. Tahapan penelitian yang akan dilakukan dapat dilihat pada Gambar 3.1 berikut :



Gambar 3. 1 Prosedur Penelitian

Berdasarkan Gambar 3.1, berikut adalah tahapan penelitian yang akan dilakukan pada penelitian ini:

1. Identifikasi masalah; merupakan tahapan awal penelitian yang sejalan dengan studi literatur. Pada tahap ini dilakukan identifikasi permasalahan dari penelitian-penilitan yang sudah dilakukan sebelumnya terhadap *digital signature* dan penggunaan algoritma kriptografi, sehingga didapatkan rumusan masalah sebagai landasan untuk dilakukannya penelitian ini.
2. Studi literatur; merupakan tahapan studi pendahuluan terhadap penelitian-penelitian sebelumnya yang terkait dengan penelitian yang akan dilakukan. Selain itu pada tahap ini dilakukan untuk mempelajari hal-hal teoritis mengenai hal-hal yang terkait dengan penelitian yang dilakukan, seperti *digital signature*, kriptografi, kriptosistem ElGamal, fungsi *hash*, dan *SHA-512*.
3. Penelitian; yang dimaksud pada tahap ini yaitu tahapan untuk memulai penelitian setelah adanya rumusan masalah serta hasil studi literature. Pada tahap ini dilakukan analisis awal mengenai *digital signature*, potensi kelemahan yang ada pada *digital signature* dan penerapan algoritma kriptografi, serta solusi yang akan diterapkan untuk menutupi kelemahan tersebut.
4. Pengembangan perangkat lunak; pada tahap ini dilakukan pengembagan perangkat lunak dengan model pengembangan *waterfall* yaitu *requirements definition* (Analisis), *system and software design* (Desain), *implementation and unit testing* (*Coding*), *integration and system testing* (*Testing*). Namum pada penelitian ini tidak menggunakan model pengembangan *waterfall* secara utuh, sehingga tahap *operation and maintenance* (*Maintenance*) tidak dilakukan. Selain penjelasan sebelumnya, tahap ini juga merupakan bagian penerapan Algoritma ElGamal dan SHA-512 sesuai kebutuhan penelitian yang dilakukan.
5. Pengujian; merupakan proses pengujian perangkat lunak guna melakukan penelitian yang dilakukan.

6. Analisis hasil penelitian; merupakan tahapan analisis terhadap hasil penelitian yang dilakukan.
7. Penarikan kesimpulan; merupakan tahapan untuk menentukan kesimpulan-kesimpulan dari hasil penelitian.
8. Dokumentasi; merupakan tahap akhir dari penelitian, yaitu pembuatan dokumentasi.

3.2 Metode Penelitian

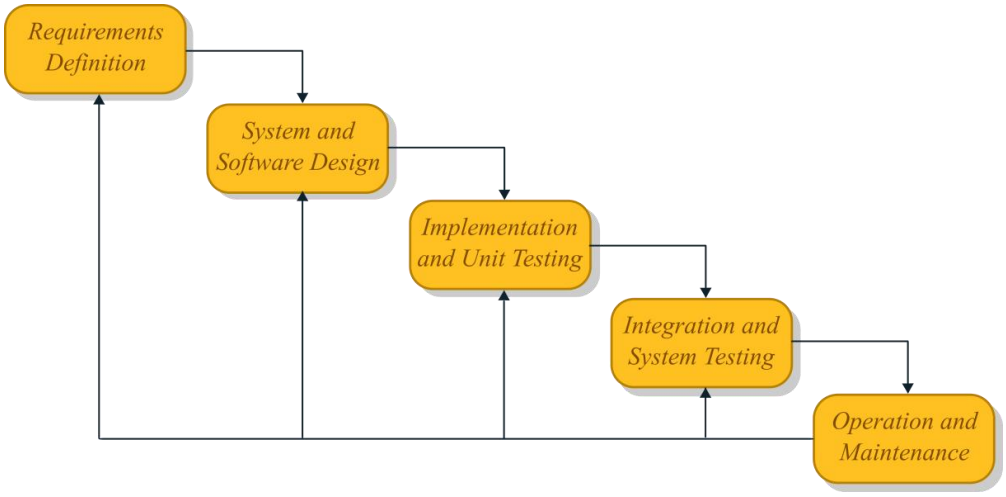
Pada sub bahasan ini akan dipaparkan metode penelitian berupa metode pengumpulan data penelitian dan metode pengembangan perangkat lunak yang digunakan pada penelitian.

3.2.1 Metode Pengumpulan Data

Pada penelitian ini, data berupa bahan studi *literature* berupa *textbook*, jurnal-jurnal penelitian, tutorial beserta dokumen lainnya yang menunjang proses penelitian serta *file* dokumen dan pesan teks yang akan digunakan untuk proses penilitian pada perangkat lunak yang dikembangkan. Pengumpulan data dilakukan melalui observasi di perpustakaan dan *World Wide Web* tentang *digital signature*, kriptografi, algoritma ElGamal, fungsi *hash*, *data collision, Secure Hashing Algorithm (SHA),* implementasi kriptosistem pada *digital signature,* serta perkembangan mengenai *digital signature.*

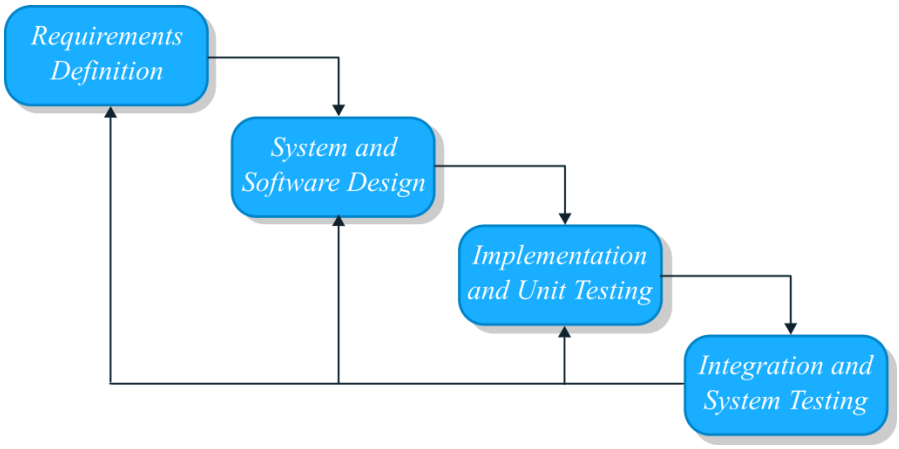
3.2.2 Metode Pengembangan Perangkat Lunak

Metode pengembangan perangkat lunak yang digunakan pada penelitian ini adalah model pengembangan perangkat lunak *waterfall* (Sommerville, 2011). Pada model pengembangan perangkat lunak *waterfall* Sommervile terdapat kemungkinan untuk kembali ke tahap pengembangan sebelumnya apabila terdapat kekurangan dan perlu perbaikan. Berikut adalah tahapan model pengembangan perangkat lunak *waterfall*:



Gambar 3. 2 Model *Waterfall* (Sommerville, 2011)

Namun penelitian ini tidak menggunakan model pengembangan *waterfall* (Sommerville, 2011) secara utuh, sehingga tahapan *maintenance* tidak dilakukan dan tidak termasuk ke dalam lingkup penelitian ini. Maka berikut adalah model pengembangan yang dilakukan pada penelitian ini:



Gambar 3. 3 Model Pengembangan Perangkat Lunak yang Digunakan

1. *Requirement Definition*, merupakan tahapan awal dengan melakukan analisis untuk menentukan kebutuhan, batasan, serta tujuan dari pengembangan perangkat lunak sesuai yang diinginkan. Kemudian hal tersebut didefinisikan secara rinci sehingga menjadi spesifikasi sistem. Pada tahap ini dilakukan penentuan algoritma dan metode untuk penanganan *data collision* pada *digital signature*.

2. *Software Design* merupakan tahap perancangan yang melibatkan identifikasi dan menggambarkan dasar sistem serta hubungan satu sama lain. Pada tahap ini dibuat desain dari implementasi algoritma dan metode yang akan dikembangkan.
3. *Implementation and Unit Testing*, pada tahapan ini *software design* yang telah dilakukan sebelumnya kemudian diimplementasikan dalam bentuk unit program. Setelah unit program dibuat, kemudian dilakukan *testing* pada unit program tersebut untuk memastikan implementasi berjalan dengan baik.
4. *Integration and Testing*, merupakan tahap lanjutan ketika semua unit program berhasil diimplementasikan dan lolos *testing* yaitu dengan mengintegrasikan setiap unit untuk membentuk aplikasi yang diinginkan. Aplikasi yang sudah dibentuk kemudian di tes kembali untuk memastikan unit program dapat berjalan satu sama lain dalam aplikasi dan aplikasi yang dibuat sudah memenuhi kebutuhan.

3.3 Instrumen Penelitian

Berdasarkan kebutuhan yang didefinisikan pada *requirement definition*, maka ditentukan bahwa instrumen penelitian berupa alat dan bahan penelitian beserta skenario pengujian sebagai berikut:

3.3.1 Alat Penelitian

Pada penelitian ini, penulis menggunakan berbagai alat bantu penunjang baik berupa perangkat keras *(hardware)* maupun perangkat lunak *(software)*. Adapun perangkat keras yang digunakan adalah seperangkat komputer yang mempunyai spesifikasi sebagai berikut:

1. *Processor* AMD E-300 APU with Radeon(tm) HD Graphics
2. *RAM* 2 *GB*
3. *Hard disk* 500 *GB*
4. *Mouse* dan *Keyboard*

Kemudian perangkat lunak yang digunakan untuk menunjang penelitian ini adalah sebagai berikut:

1. Sistem Operasi *Windows* 7 32 *bit*
2. Matlab R2013a
3. Mozilla Firefox *Version* 44.0.2 *(x86 en-US)*

3.3.2 Bahan Penelitian

Bahan penelitian yang digunakan pada penelitian ini yaitu jurnal-jurnal penelitian yang sudah dilakukan, *textbook*, *tutorial*, dan dokumentasi lainnya yang didapat melalui observasi di perpustakaan dan *World Wide Web* tentang *digital signature,* kriptografi, algoritma ElGamal, fungsi *hash, data collision, Secure Hashing Algorithm (SHA),* implementasi kriptosistem pada *digital signature,* serta perkembangan mengenai *digital signature.* Sedangkan data yang akan digunakan pada proses penelitiannya yaitu beberapa *file* dokumen atau pesan yang berupa teks.

3.3.3 Skenario Pengujian

Pengujian terhadap sistem yang dibangun akan dilakukan melalui empat skenario, yaitu:

1) Skenario 1, pembuatan *digital signature* dilakukan dengan menggunakan SHA-512 dan Enkripsi ElGamal.
2) Skenario 2, pembuatan *digital signature* dilakukan dengan menggunakan SHA-512 dan tanpa Enkripsi ElGamal.
3) Skenario 3, pembuatan *digital signature* dilakukan tanpa menggunakan SHA-512 tetapi menggunakan Enkripsi ElGamal.
4) Skenario 4, pembuatan *digital signature* dilakukan tanpa menggunakan SHA-512 dan Enkripsi ElGamal.

Pada keempat skenario di atas, akan dilakukan pengujian terhadap suatu dokumen teks untuk mengetahui bagaimana pengaruh implementasi Algoritma ElGamal dan SHA-512 terhadap *data collision* yang terjadi pada isi dokumen yang telah dibubuhi *digital signature* dengan melakukan *Man In The Middle Attack Scenario.* Selain itu pada pembangkitan kunci akan dilakukan *Randomness test* terhadap pasangan kunci. Lebih jelasnya akan dibahas pada BAB IV.