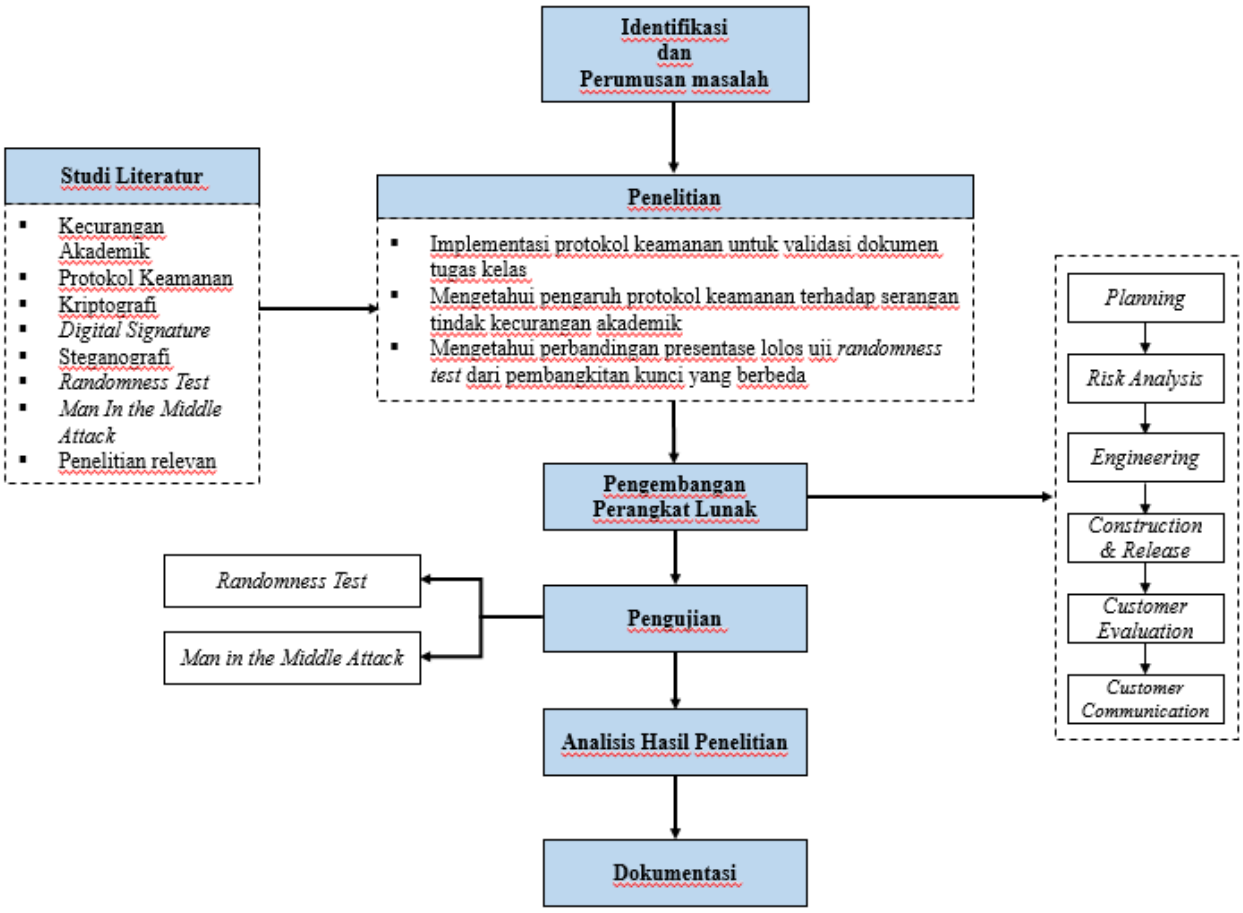
BAB III
METODOLOGI PENELITIAN

Dalam bab ini akan dijelaskan mengenai (1) desain penelitian, (2) metode penelitian, dan (3) alat dan bahan penelitian.

1.1. Desain Penelitian

Pada bagian ini dijelaskan mengenai tahapan yang akan dilakukan untuk memberikan gambaran umum penelitian. Adapun desain penelitian ditunjukan pada gambar di bawah ini:



Gambar 3.1 Desain penelitian

Penjelasan mengenai desain penelitian di atas adalah sebagai berikut:

1. Identifikasi dan perumusan masalah

Tahap ini merupakan tahap awal penelitian. Pada tahap ini dilakukan identifikasi terhadap pemasalahan-permasalahan yang berhubungan dengan kecurangan akademik dan solusi untuk mengatasinya, kemudian dirumuskan masalah yang menjadi dasar dilakukannya penelitian.

2. Studi literatur

Tahap ini dilakukan untuk mempelajari hal-hal teoritis yang mendukung penelitian, seperti kecurangan akademik, protokol keamanan, kriptografi, *digital signature*, steganografi, *Randomness Test*, dan *Man in the Middle Attack*, dan penelitian relevan.

3. Penelitian

Pada tahap ini dilakukan penelitian terhadap masalah yang diangkat dan metode yang diterapkan. Terdapat 3 tujuan penelitian yang menjadikan penelitian yang menjadi kejaran, yaitu: (1) Mengimplementasikan protokol keamanan pada validasi dokumen tugas kelas, (2) Menjadikan protokol keamanan tersebut tahan terhadap serangan kecurangan akademik, dan (3) Mengetahui perbandingan presentase lolos uji *randomness test* pada pembangkitan kunci biasa dengan kunci *message digest*.

4. Pengembangan perangkat lunak

Pada tahap ini dilakukan pengembangan perangkat lunak dengan model *spiral* (Pressman, 2001), yaitu *planning, risk analysis, engineering, construction and realease, customer evaluation,* dan *costumer communication*.

5. Pengujian

Pada tahap ini dilakukan pengujian terhadap perangkat lunak menggunakan *Randomness Test* untuk mengetahui tingkat keacakan *cipherdoc* yang dibangkitkan menggunakan algoritma RC4 dan *Man in the Middle Attack* untuk menguji ketahanan terhadap kecurangan akademik yang dilakukan pihak tidak bertanggung jawab.

6. Analisis hasil penelitian

Pada tahap ini dilakukan analisis berdasarkan rumusan masalah dan hasil pengujian. Kemudian ditarik kesimpulan dari analisis tersebut.

7. Dokumentasi

Tahap ini merupakan tahap akhir penelitian, yaitu pembuatan dokumentasi dari penelitian yang dilakukan.

1.2. Metode Penelitian

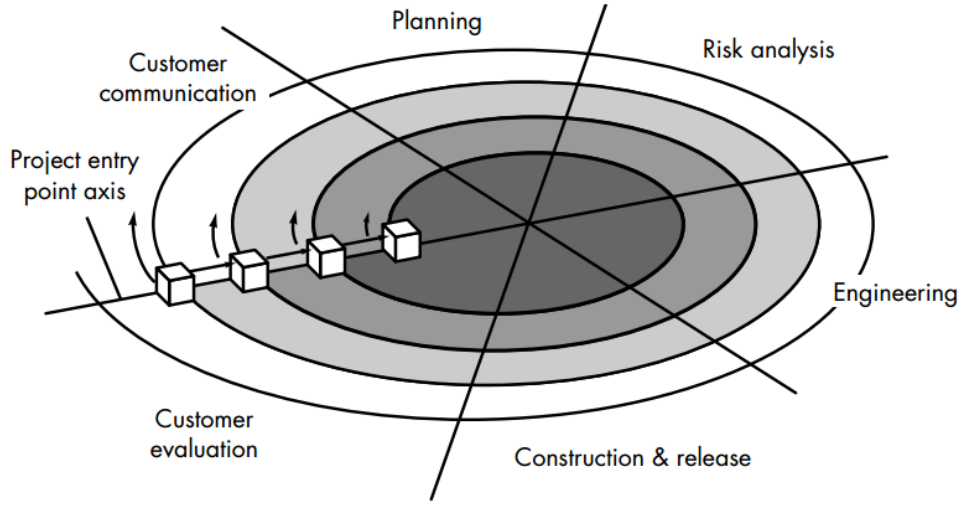
Metode penelitian pada penelitian ini dibagi ke dalam dua bagian, yaitu: (1) metode pengumpulan data, dan (2) metode pengembangan perangkat lunak.

3.2.1. Metode Pengumpulan Data

Dalam penelitian ini, dilakukan pengumpulan data yang menunjang penelitian diantaranya: studi literatur mengenai kecurangan akademik, protokol keamanan, kriptografi, *digital signature*, steganografi, *Randomness Test*, *Man in the Middle Attack* dan penelitian relevan melalui observasi di perpustakaan dan *Worl Wide Web.*

3.2.2. Metode Pengembangan Perangkat Lunak

Dalam penelitian ini, pembangunan perangkat lunak menggunakan model *Spiral* (Pressman, 2001). Pada model ini terdapat kemungkinan untuk kembali ke tahap sebelumnya apabila terjadi kesalahan atau perbaikan. Alur prosesnya seperti terlihat pada gambar berikut:

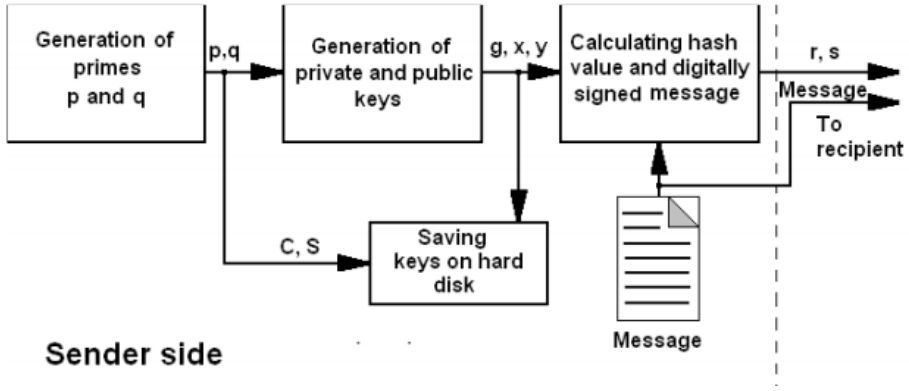


Gambar 3.2 Model *Spiral* (Pressman, 2001)

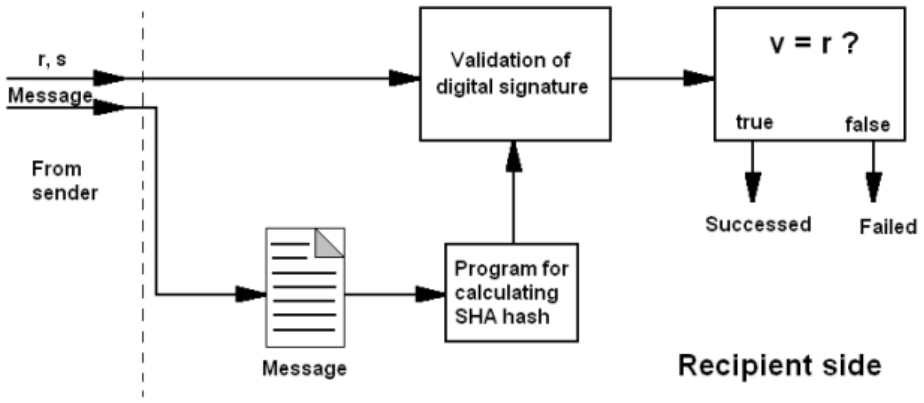
Dalam melakukan pembangunan perangkat lunak pada penelitian ini, dilakukan terlebih dahulu identifikasi perangkat lunak pada penelitian relevan yang dijelaskan pada BAB II. Sehingga pembangunan perangkat lunak pada penelitian ini mengacu pada perangkat lunak penelitian relevan. Adapun mengenai tahap yang akan dijelaskan mengenai pengembangan perangkat lunak model *spiral* penelitian relevan adalah pada tahap *construction and release*.

Penelitian relevan yang dijadikan acuan utama adalah penelitian berjudul "*Analysis of Software Realized DSA Algorithm for Digital Signature*" yaitu mengenai penggunaan DSA pada pembuatan dan verifikasi *digital signature*. Pada tahap *construction and release* dalam penelitian tersebut dijelaskan mengenai diagram sistem *digital signature*, pengembangan perangkat lunak, dan *testing* terhadap perangkat lunak yakni melakukan komparasi DSA dengan metode lain (RSA) dalam hal waktu eksekusi.

Adapun diagram yang menggambarkan perangkat lunak pada penelitian tersebut adalah sebagai berikut:



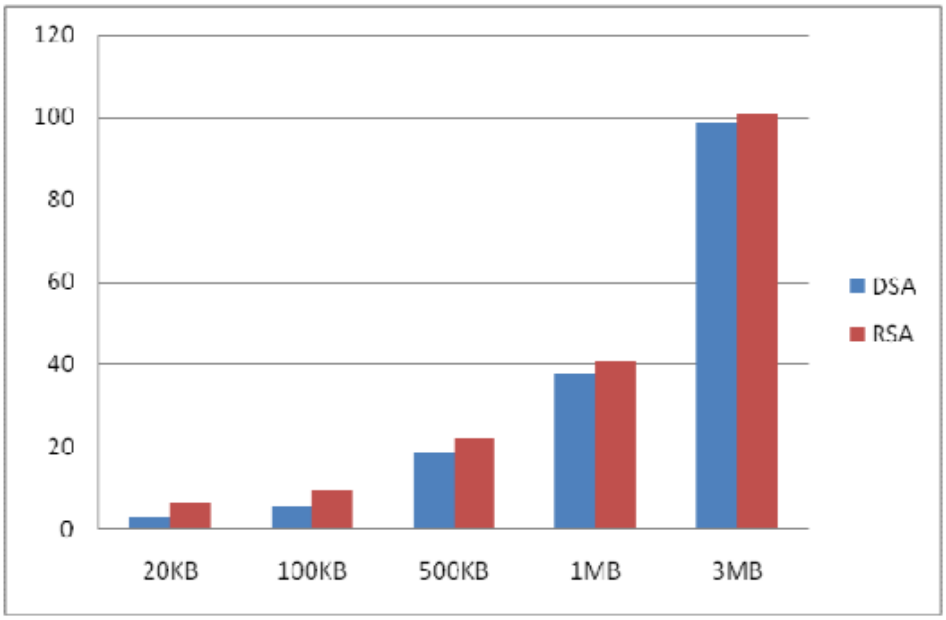
Gambar 3.3 Diagram pembangkitan *digital signature* (Paj & Ivaniš, 2011)



Gambar 3.4 Diagram verifikasi *digital signature* (Paj & Ivaniš, 2011)

Kemudian perangkat lunak pada penelitian tersebut dibangun menggunakan bahasa pemrograman Delphi dan IDE yang digunakan adalah Borland Delphi 7.

Adapun hasil *testing* perangkat lunak dengan membandingkan DSA (metode yang digunakan pada penelitin tersebut) dengan metode lain yaitu RSA dalam hal kecepatan penandatanganan pada ukuran pesan/dokumen yang berbeda-beda, terlihat pada grafik di bawah ini:



Gambar 3.5 Grafik perbandingan DSA dan RSA (Paj & Ivaniš, 2011)

Dari tahap *construction and realease* pada penelitian relevan di atas dapat disimpulkan kelebihan dan kekurangannya sebagai berikut:

Kelebihan:

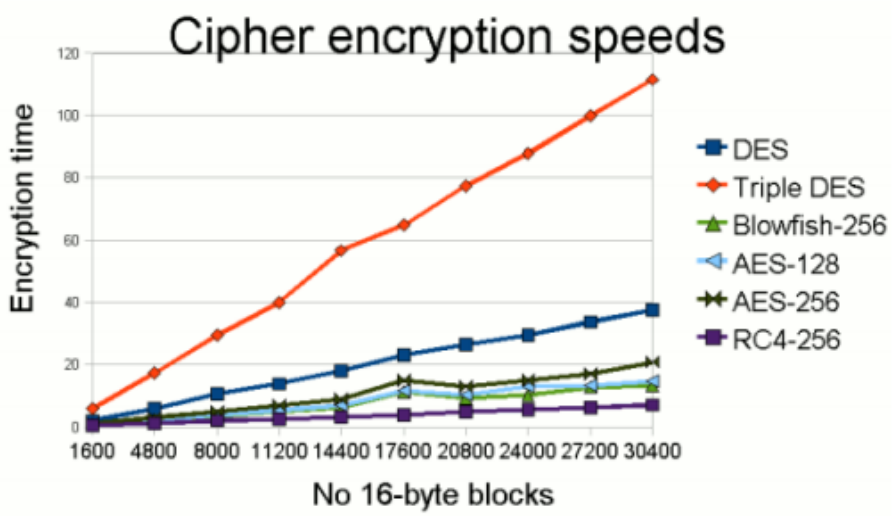
- DSA lebih unggul dari RSA dalam hal kecepatan penandatanganan.
- Seperti yang terlihat pada diagram di atas, bahwa pada DSA dibangkitkan *digital signature* dengan parameter 2 bilangan prima besar yang saling berkaitan satu sama lain.

Kekurangan:

- Pesan/dokumen tidak dapat dienkripsi
- *Digital signature* dikirimkan secara terpisah dari pesan/dokumen

Dari kelebihan dan kekurangan yang telah dijelaskan di atas, maka pada penelitian ini digunakan DSA sebagai metode pembuatan dan verifikasi *digital signature*-nya dan mengatasi kekurangan di atas dengan mengacu pada penelitian berikut:

Penelitian berjudul "Algoritma RC4 Sebagai Metode Enkripsi". Pada penelitian tersebut, perangkat lunak yang dibangun dapat menghasilkan *ciphertext* dengan cara mengenkripsi *plaintext*. Kelebihan dari perangkat lunak tersebut adalah unggul dalam kecepatan eksekusinya dibandingkan dengan metode-metode enkripsi pesan lainnya. Seperti yang terlihat pada tabel di bawah ini.



Gambar 3.6 Grafik perbandingan RC4 dan metode lainnya (Suryani, 2009)

Kemudian pada penelitian berjudul "*An enhanced embedding method using inter-sentence, inter-word, end-of-line and inter-paragraph spacing*", Perangkat lunak yang dibangun memungkinkan penyembunyian teks ke dalam

medium teks (*text steganography*) dengan memanfaatkan spasi antarkalimat, antarkata, akhir baris, dan antarparagraf.

Kemudian dari ketiga penelitian di atas, pada penelitian ini dilakukan putaran *spiral* berikutnya sebagai berikut.

1. *Customer Communication*

   Pada bagian ini dilakukan komunikasi dengan pengguna mengenai kebutuhan perangkat lunak. Pada penelitian ini, pengguna mencakup pengirim dokumen dan penerima dokumen. Dua sisi pengguna tersebut direpresentasikan oleh dosen Departemen Pendidikan Ilmu Komputer Universitas Pendidikan Indonesia yang spesialisasi keilmuannya di bidang kriptografi, yaitu Rizky Rachman J. P. sehingga komunikasi dengan pengguna yang dimaksud dalam penelitian ini adalah komunikasi dengan dosen tersebut.

2. *Planning*

   Pada bagian ini dilakukan perencanaan untuk menentukan sumberdaya, perkiraan waktu pengerjaan, dan informasi lainnya yang dibutuhkan untuk pengembangan perangkat lunak. Perencanaan yang dilakukan pada penelitian ini yakni menentukan *tools* yang akan digunakan, algoritma pendukung sistem, dan menggali referensi pengembangan perangkat lunak yang serupa.

   Pada pengembangan perangkat lunak, direncanakan 1 bulan pengerjaan. Kemudian dilakukan pula perancanaan *tools* yang akan digunakan, dan dipilihlah Matlab, dikarenakan *tools* tersebut memiliki banyak fungsi sehingga pengembangan perangkat lunak banyak terbantu oleh fungsi-fungsi siap pakai pada Matlab tersebut. Adapun algoritma pendukung sistem adalah seperti yang dijelaskan sebelumnya mengenai penelitian relevan, yakni menggunakan DSA, RC4 dan *Text Steganography*.

3. *Risk Analysis*

   Kemudian dilakukan analisis risiko secara teknikal. Pada penelitian ini, dilakukan analisis terhadap kemungkinan-kemungkinan yang bisa terjadi selama pengembangan perangkat lunak dilakukan,

seperti kemungkinan yang terjadi jika algoritma dan metode pada penelitian ini diterapkan pada *tools* yang digunakan, kemudian kemungkinan yang akan terjadi jika format dokumen yang ditentukan pada penelitian ini digunakan pada pengembangan perangkat lunak.

Analisis yang dilakukan adalah penerapan DSA, RC4 dan *Text Steganography* pada Matlab. Adapun hasil analisisnya yaitu bahwa ketiga metode/algoritma tersebut dapat diterapkan pada Matlab dikarenakan Matlab memiliki fungsi yang mendukung implementasi metode/algoritma tersebut, diantaranya Matlab dapat mengeksekusi bahasa pemrograman java yang pada penelitian ini digunakan untuk melakukan fungsi *hash* terhadap teks sehingga DSA yang memerlukan hasil hashing tersebut dapat dijalankan. Begitupun dengan RC4 dan *Text Steganography*, Matlab dapat merealisasikan kedua metode/algoritma tersebut. Adapun analisis format dokumen yakni dilakukan terhadap dokumen berformat .docx dan .txt Kemudian dipilih format .txt dikarenakan ukurannya yang kecil dan mendukung manipulasi *plaintext* yang tidak terdapat pada format .docx.

4. *Engineering*

Pada bagian ini dilakukan pembangunan satu atau lebih representasi dari aplikasi secara teknikal. Pada penelitian ini, dibangun representasi aplikasi secara teknikal yaitu penggambaran langkah-langkah dalam pembentukan *digital signature*, penyembunyian *digital signature*, enkripsi, dekripsi, dan verifikasi *digital signature*.

Adapun langkah-langkah tersebut mengacu pada penelitian relevan yang telah dijelaskan sebelumnya, pada pembentukan digital signature dan penyembunyian digital signature digunakan DSA, kemudian untuk enkripsi dan dekripsi digunakan RC4 dan penyembunyian digital signature ke dalam dokumen digunakan *Text Steganography* dengan memanfaatkan spasi antarkata.

5. *Construction And Release*

Pada bagian ini dilakukan pengembangan perangkat lunak, *testing*, dan instalasi. Pada penelitian ini, pembangunan perangkat lunak

dan instalasi menggunakan Matlab R2013a, testing mengenai *Randomness Test* dilakukan menggunakan Cryptool 1.4.3, sedangkan *Man in the Middle Attack Scenario* dilakukan dengan percobaan di dalam aplikasi yang dibangun menggunakan Matlab itu sendiri.

6. *Costumer Evaluation*

Pada bagian ini dilakukan evaluasi dengan *user* mengenai sistem yang dibangun. Pada penelitian ini, dilakukan evaluasi dengan entitas yang dijelaskan pada *point* 1. Evaluasi yang dilakukan adalah fungsi dari aplikasi dan implikasi terhadap penyelesaian permasalahan.

Adapun fungsi dari aplikasi tersebut adalah melakukan validasi dokumen dengan membubuhkan *digital signature* ke dalamnya. Dan implikasi terhadap masalah yang diangkat adalah aplikasi mampu menyelesaikan masalah penjiplakan dokumen dan pengubahan isi dokumen sesuai skenario yang ditetapkan.

1.3. Alat dan Bahan Penelitian

Alat dan bahan penelitian pada penelitian ini adalah sebagai berikut:

3.3.1. Alat Penelitian

Dalam penelitian ini, digunakan berbagai alat bantu penunjang penelitian, baik berupa perangkat keras, maupun perangkat lunak. Perangkat keras yang digunakan adalah sebagai berikut:

1. *Processor* Intel Core i3 1,8 GHz
2. RAM 4 GB
3. HDD 500 GB
4. NVIDIA Geforce-GT 635M 2GB

Adapun perangkat lunak yang digunakan adalah sebagai berikut:

1. Sistem Operasi Microsoft Windows 8 64 bit
2. Matlab R2013a

3.3.2. Bahan Penelitian

Bahan penelitian pada penelitian ini yaitu jurnal-jurnal penelitian lain yang sudah dipublikasikan, tutorial, *textbook*, bahan ajar, dan dokumentasi lainnya yang didapatkan melalui observasi di perpustakaan dan *World Wide Web* mengenai kecurangan akademik, protokol keamanan, kriptografi, *digital signature*,

steganografi, *Randomness Test, Man in the Middle Attack,* dan penelitian relevan. Kemudian data yang digunakan pada proses penelitian adalah berupa dokumen tugas kelas berformat .txt.