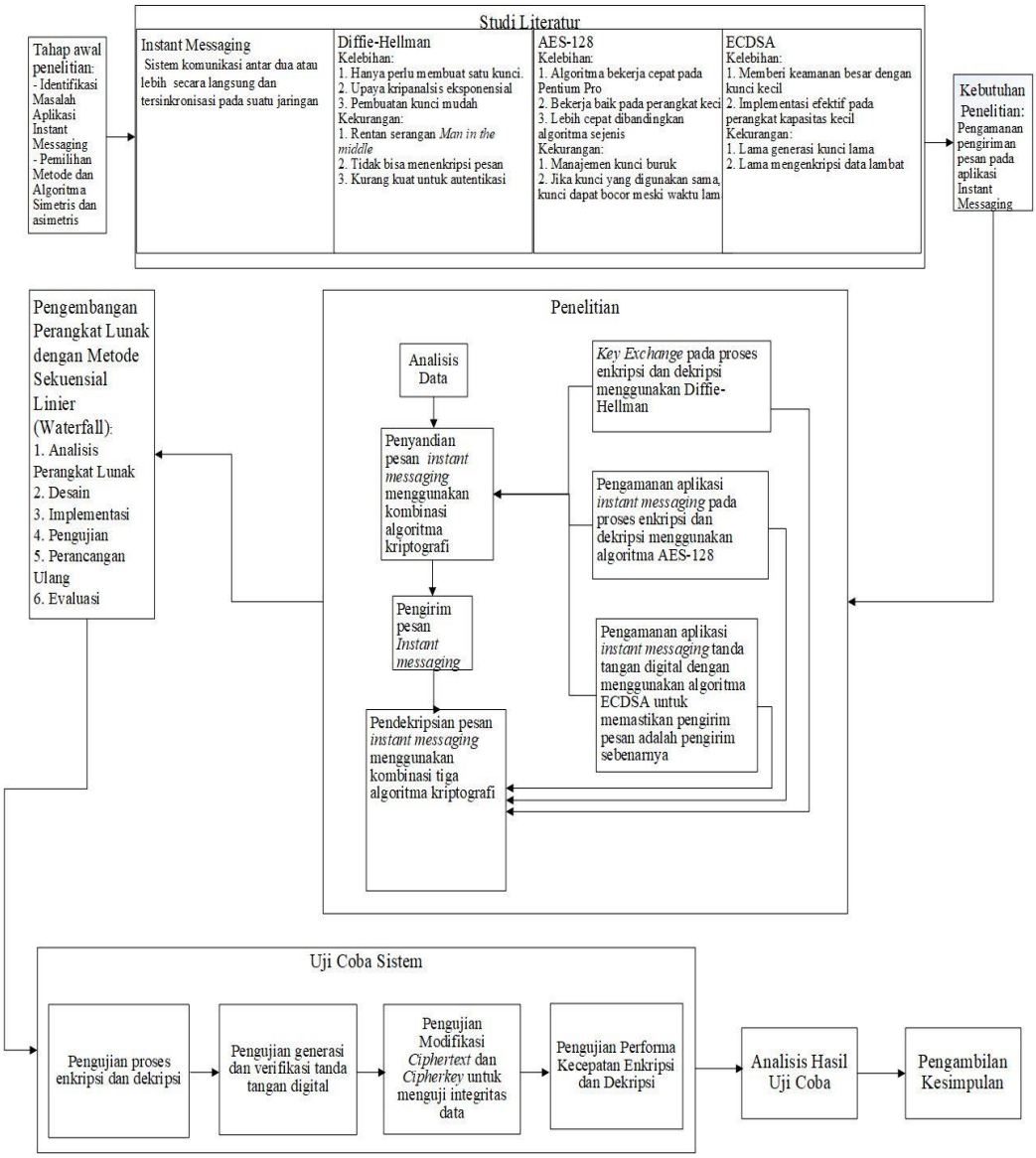
BAB III
METODOLOGI PENELITIAN

3.1 Desain Penelitian

Desain penelitian yang akan dilakukan pada penelitian ini dimulai dari tahap awal penelitian, studi literatur, kebutuhan penelitian, penelitian, pengembangan perangkat lunak, uji coba sistem, sampai pengambilan kesimpulan. Gambaran desain penelitian disajikan pada Gambar 3.1.



Gambar 3.1 Skema Desain Penelitian

Berikut merupakan penjelasan dari tahapan desain penelitian:

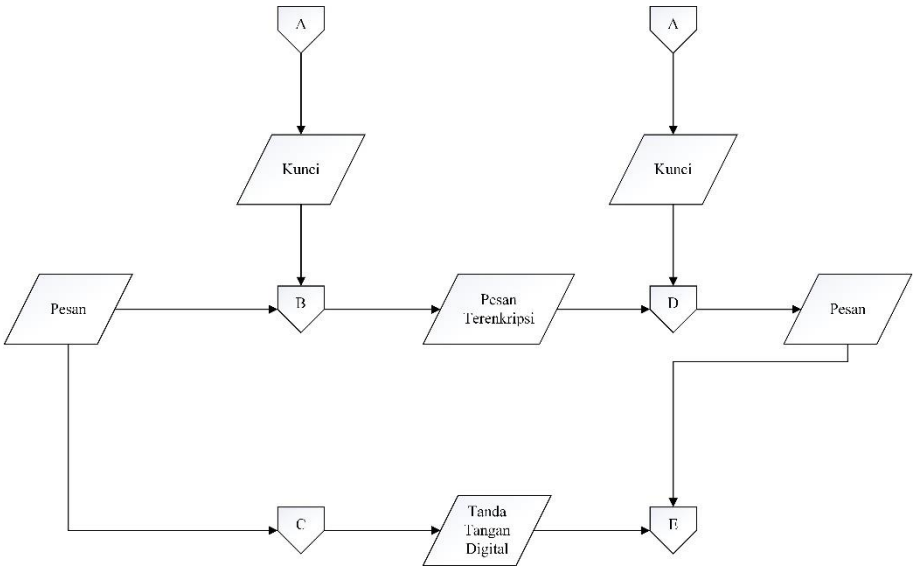
1. Tahap awal penelitian dengan melakukan identifikasi permasalahan yang akan diselesaikan dan menentukan metode yang akan digunakan untuk menyelesaikannya.
2. Melakukan studi literatur mengenai proses pengkodean algoritma Diffie-Hellman sebagai pengaman kunci untuk enkripsi pesan, proses pengkodean algoritma AES-128 sebagai pengaman isi pesan, proses pengkodean algoritma ECDSA sebagai autentikasi pesan yang diterima, cara kerja aplikasi *instant messaging*, dan lain-lain yang berhubungan dengan penelitian ini. Sumber yang digunakan berupa buku, jurnal, dan sumber-sumber yang relevan dengan penelitian dari internet.
3. Kebutuhan dari penelitian untuk melakukan pengamanan pengiriminan pesan pada aplikasi *instant messaging*.
4. Melakukan penelitian pada pengamanan dan pengiriman pesan aplikasi *instant messaging* menggunakan kombinasi tiga algoritma kriptografi.
    a. Data penelitian berupa pesan pada aplikasi *instant messaging*
    b. Dalam pengenkripsian isi pesan terdapat tiga proses yang dilakukan, yaitu: *key exchange* menggunakan algoritma Diffie-Hellman, enkripsi isi pesan menggunakan algoritma AES-128 dan penandaan pesan dengan menggunakan algoritma ECDSA. Pengirim dan penerima akan membuat kunci privat dan kunci publik yang akan digunakan untuk melakukan pertukaran kunci. Pengirim dan penerima kemudian saling mengirim kunci publik yang dibuat oleh masing-masing pengirim dan penerima untuk kemudian dihitung masing-masing pada masing-masing sisi dengan menggunakan algoritma Diffie-Hellman, hasil perhitungan tersebut kemudian akan digunakan untuk mengenkripsi pesan 1. Isi pesan l akan dikonversi menjadi bilangan desimal dan diubah menjadi 128 bit/blok. Kumpulan blok ini akan dikenakan proses enkripsi menggunakan algoritma AES-128 dan menghasilkan suatu *ciphertext*. Algoritma AES-128 membutuhkan sebuah kunci yang pada penelitian ini akan didapat dari hasil perhitungan algoritma Diffie-Hellman. Pesan yang sudah dienkripsi

AES-128 akan diberi penanda dari algoritma ECDSA yang menggunakan kunci publik dari generator kunci acak. *Ciphertext* dan *signature* akan dikirim kepada penerima dalam satu pesan.

c. Dalam pendekripsian isi pesan terdapat tiga proses yang dilakukan, yaitu: *key exchange* dengan algoritma Diffie-Hellman, verifikasi penanda yang ada pada pesan dengan algoritma ECDSA dan pendekripsian *ciphertext* menggunakan algoritma AES-128.

5. Setelah perancangan dari kombinasi tiga algoritma kriptografi dilakukan, langkah selanjutnya yaitu mengimplementasikannya ke dalam kode program dan setiap proses dijadikan fungsi pada perangkat lunak. Pengembangan perangkat lunak menggunakan metode pendekatan berorientasi objek dengan model proses sekuensial linier (*waterfall*). Terdapat 4 proses dalam model tersebut, yaitu analisis, desain, *coding* dan *testing* terhadap sistem yang dibuat.
6. Pengujian yang dilakukan pada penelitian ini yaitu pengujian proses enkripsi dan dekripsi, pada proses dekripsi memodifikasi berupa perubahan, pengurangan dan penambahan satu bit *ciphertext* dan *cipherkey*. Selain itu pengujian dilakukan juga terhadap lama waktu proses enkripsi dan dekripsi pada berbagai ukuran *plaintext* dan *ciphertext*.
7. Analisis hasil uji coba yaitu analisis terhadap hasil uji coba yang sudah dilakukan, yaitu hasil uji coba proses enkripsi dan dekripsi, hasil uji coba generasi dan verifikasi tanda tangan digital, hasil uji coba modifikasi *ciphertext* dan *cipherkey*, dan hasil uji coba performa kecepatan enkripsi dan dekripsi.
8. Pengambilan kesimpulan berdasarkan analisis hasil uji coba.

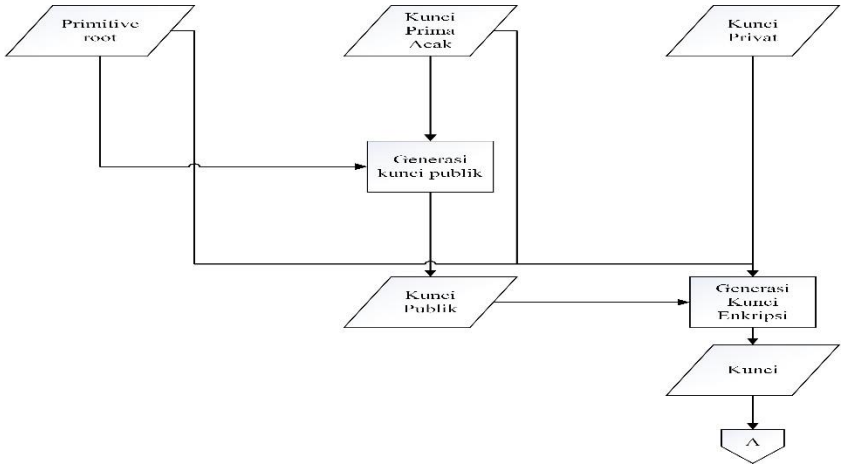
Adapaun alur penggunaan algoritma kriptografi pada pengamanan aplikasi *instant messaging* secara umum disajikan pada Gambar 3.2.



Gambar 3.2 Alur Umum dari Penggunaan Algoritma Kriptografi Pada Aplikasi *Instant Messaging*

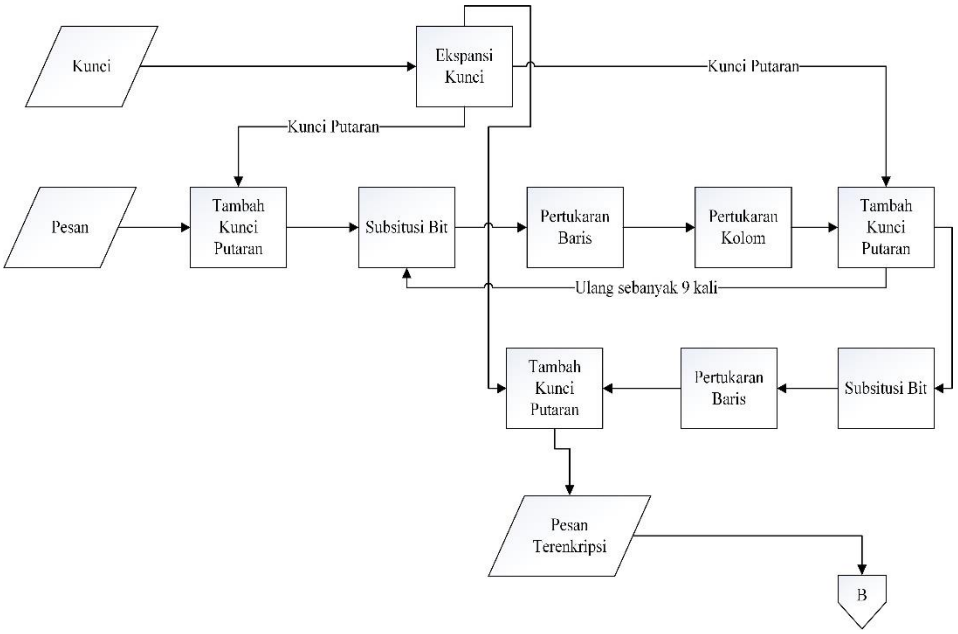
Pada Gambar 3.2 Pesan akan diolah menjadi tanda tangan digital dan pesan terenkripsi. Pada proses enkripsi pesan, akan melibatkan algoritma Diffie-Hellman seperti pada proses (A) dan algoritma enkripsi dengan menggunakan algoritma AES-128 seperti pada proses (B). Selain itu, juga dibuat tanda tangan digital dengan algoritma ECDSA pada proses (C). Setelah pesan terenkripsi dan tanda tangan digital dikirim, pesan terenkripsi akan didekripsi oleh AES-128 seperti pada proses (D) dan tanda tangan digital akan diverifikasi seperti pada proses (E).

Proses (A) yang berisi proses pertukaran kunci, disajikan pada Gambar 3.3.



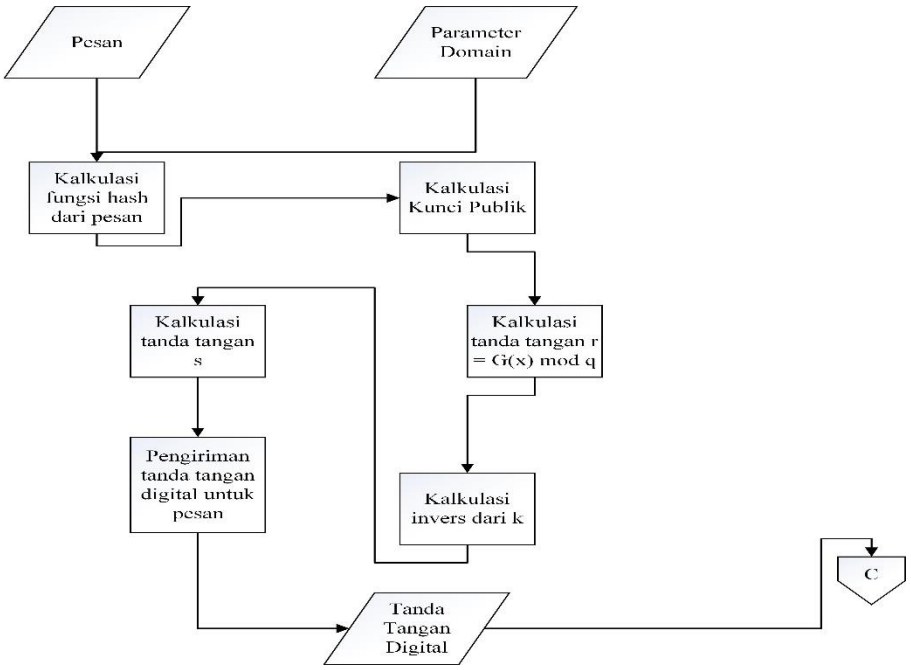
Gambar 3.3 Algoritma Pertukaran Kunci

Algoritma pertukaran kunci seperti terlihat pada Gambar 3.3, pada proses (A) dilakukan pertukaran kunci dengan algoritma Diffie-Hellman. Dimana *primitive root* dan kunci prima acak digunakan untuk melakukan generasi kunci publik. Selanjutnya, kunci publik yang dibuat dan kunci privat akan dioperasikan pada Generasi Kunci Enkripsi sehingga akan menghasilkan Kunci yang selanjutnya akan digunakan dalam proses enkripsi. Alur proses enkripsi disajikan pada Gambar 3.4.



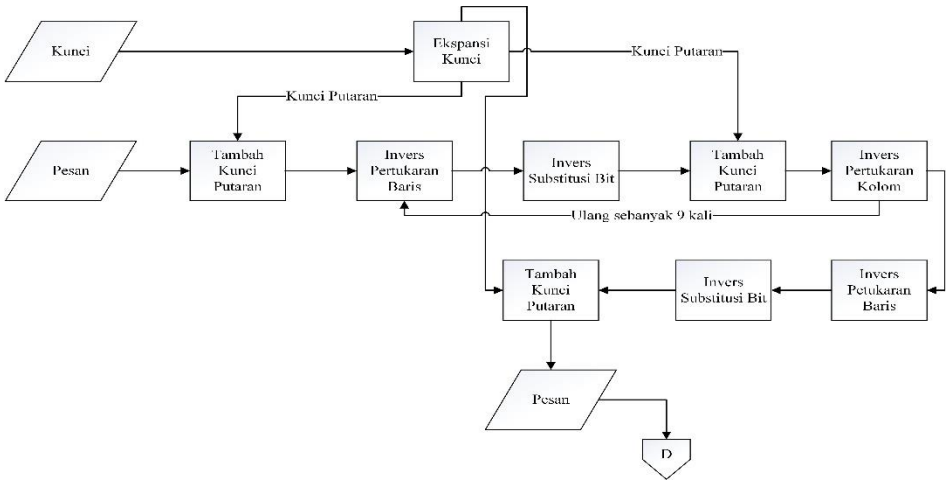
Gambar 3.4 Algoritma Enkripsi Pesan

Pada proses enkripsi pesan, masukan berupa Kunci dan Pesan yang akan digunakan sebagai masukan pada proses enkripsi. Selanjutnya, kunci akan diolah di proses ekspansi kunci, untuk kemudian selanjutnya membantu proses enkripsi pesan. Pesan yang belum terenkripsi selanjutnya akan menjalani proses Tambah Kunci Putaran, Substitusi Bit, Pertukaran Baris, dan Pertukaran Kolom berulang-ulang hingga proses selesai. Hasil dari pengolahan tersebut adalah berupa pesan yang sudah dienkripsi. Selain itu, ada juga proses generasi tanda tangan yang terdapat pada proses (C), yang disajikan pada Gambar 3.5.



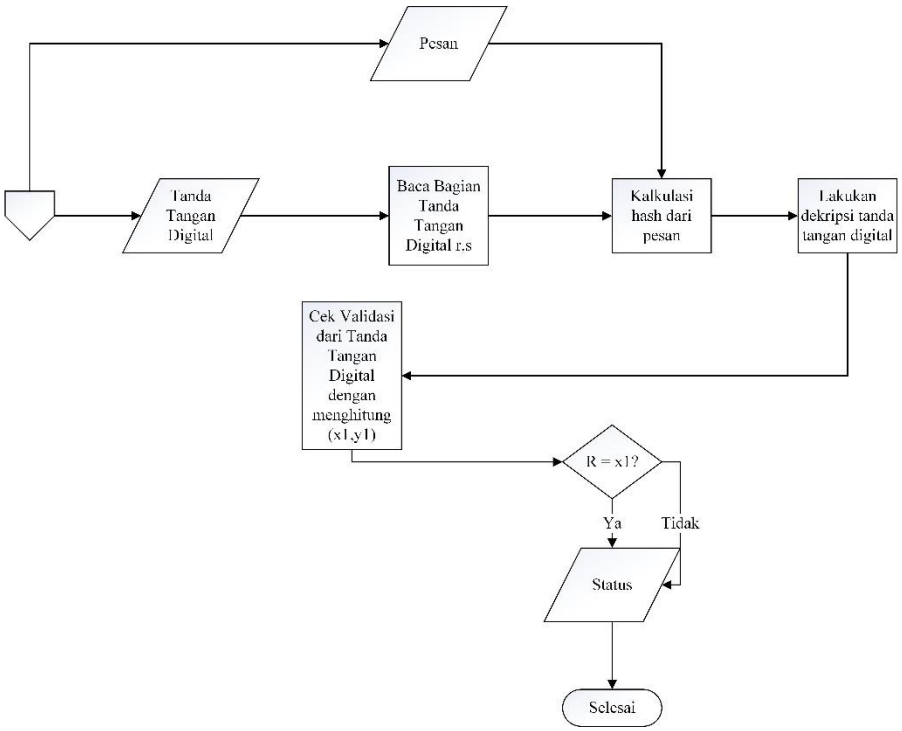
Gambar 3.5 Algoritma Generasi Tanda Tangan Digital

Proses (C), yaitu proses generasi tanda tangan, seperti terlihat pada Gambar 3.5, membutuhkan masukan berupa Pesan dan Parameter domain. Pertama pesan akan diubah ke dalam bentuk *hash* yang selanjutnya akan menghasilkan kunci publik. Kemudian, dilakukan generasi tanda tangan digital berupa koordinat r dan s, r dan s inilah yang akan berperan sebagai tanda tangan digital yang dihasilkan oleh proses (C). Selanjutnya, adalah proses (D) yang melakukan proses dekripsi pesan, disajikan pada Gambar 3.6.



Gambar 3.6 Algoritma Dekripsi Pesan

Pada proses dekripsi pesan, masukan berupa Kunci dan Pesan terenkripsi yang akan digunakan sebagai masukan pada proses dekripsi. Selanjutnya, kunci akan diolah di proses ekspansi kunci, untuk kemudian selanjutnya membantu proses dekripsi pesan terenkripsi. Pesan yang terenkripsi selanjutnya akan menjalani proses Tambah Kunci Putaran, Invers Pertukaran Baris, Inverse Substitusi Bit, dan Inverse Pertukaran Kolom secara berulang-ulang hingga proses selesai. Hasil dari pengolahan tersebut adalah berupa pesan yang sudah didekripsi. Selain itu, ada juga proses verifikasi tanda tangan yang terdapat pada proses (E), disajikan pada Gambar 3.7.



Gambar 3.7. Algoritma Verifikasi Tanda Tangan Digital

Pada proses (E) dilakukan proses verifikasi tanda tangan digital yang melakukan verifikasi dari tanda tangan yang diterima. Proses membutuhkan Pesan dan Tanda Tangan Digital, proses pertama adalah proses membaca tanda tangan digital r dan s. Selanjutnya, dilakukan kalkulasi *hash* dari pesan. Kemudian, dilakukan dekripsi tanda tangan digital. Dan terakhir adalah dilakukan pengecekan validasi dari tanda tangan digital. Jika tervirifikasi, maka statusnya menjadi ya. Jika tidak terverifikasi, maka status menjadi tidak.

3.2 Metode Pengumpulan Data

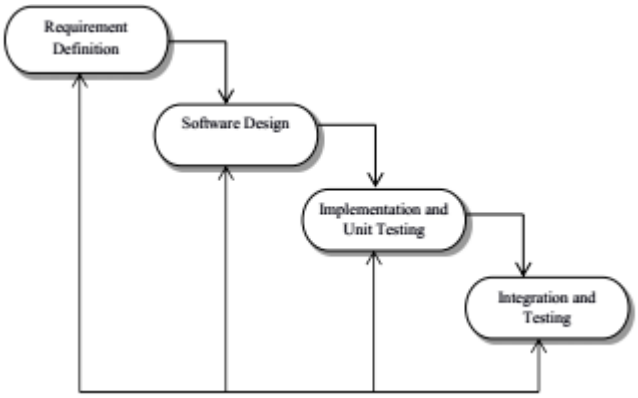
Metode penelitian ini dibagi menjadi dua, yaitu metode pengumpulan data dan metode pengembangan perangkat lunak.

3.2.1. Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan adalah eksplorasi dan studi literatur. Eksplorasi dan studi literatur dilakukan dengan mempelajari konsep dasar yang berkaitan dengan penelitian ini, seperti teknik *key exchange* dengan Diffie-Hellman, algoritma teknik pengenkripsian dan pendekripsian pesan dengan algoritma AES-128, dan teknik penandaan pesan dengan algoritma ECDSA. Berbagai macam metode penngumpulan yang dilakukan pada penelitian ini melalui literatur-literatur berupa buku, jurnal, skripsi dan sumber ilmiah lain.

3.2.2. Metode Pengembangan Perangkat Lunak

Metode Proses Pengembangan Perangkat Lunak yang akan digunakan merupakan metode *Waterfall*, yang disajikan pada Gambar 3.8.



Gambar 3.8. Diagram Waterfall (Sommerville, 2016)

Tahap-tahapan *Waterfall*, yaitu:

1. Analisis Perangkat Lunak.

   Menganalisa data penelitian serta alat dan bahan untuk digunakan dalam penelitian. Menentukan fitur-fitur yang akan dibuat di dalam perangkat lunak tersebut.

2. Desain.

   Perancangan dan antarmuka perangkat lunak. Perancangan perangkat lunak menggunakan *Block Diagram, Flow Chart Diagram, Use Case Diagram,Class Diagram, Activity Diagram, Sequence Diagram, Deployment Diagram,* dan *Collaaboration Diagram.*

3. Implementasi

   Pembuatan perangkat lunak menggunakan bahasa pemrograman

4. *Testing*/Pengujian.

   Pengujian perangkat lunak dilakukan oleh penulis untuk memeriksa perangkat lunak tersebut sudah berjalan dengan baik atau belum dengan melakukan percobaan dari semua fitur yang telah dibuat.

5. Perancangan ulang

   Perancangan ulang dilakukan setelah mendapatkan hasil dari pengujian dan juga dari sisi yang dilihat bisa dikembangkan.

6. Evaluasi

   Melakukan evaluasi dari rancangan yang sudah diperbaiki/modifikasi apakah sudah memenuhi kebutuhan atau belum.

3.3 Instrumen Penelitian

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

3.3.1. Alat Penelitian

Dalam penelitian ini, peneliti menggunakan alat bantu penunjang penelitian berupa perangkat keras dan perangkat lunak. Adapun perangkat keras yang digunakan dalah seperangkat komputer yang mempunyai spesifikasi sebagai berikut:

1. Processor Intel Core i5-8250U 1.6 GHz
2. RAM 8GB
3. Kapasitas HDD 1000 GB

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

1. Sistem Operasi Windows 10
2. Android Studio
3. StarUML
4. Firebase

3.3.2. Bahan Penelitian

Bahan penelitian yang digunakan pada penelitian ini adalah jurnal penelitian yang telah dilakukan, *textbook*, tutorial, dan dokumentasi lainnya yang terdapat pada perpustakaan dan jurnal tentang keamanan data, algoritma Diffie Hellman, algoritma AES-128, algoritma ECDSA, aplikasi pengiriman pesan pada *instant messaging.*

3.3.3. Pengujian

Setelah dilakukannya kode program, tahap berikutnya adalah pengujian. Pengujian terhadap sistem yang dibangun akan dilakukan melalui metode *black box*. Sedangkan untuk pengujian penelitian dilakukan dengan cara pengujian proses enkripsi dan dekripsi, pengujian generasi dan verifikasi tanda tangan digital, pengujian pada proses dekripsi dengan memodifikasi berupa perubahan, pengurangan dan penambahan satu bit *ciphertext* dan *cipherkey*. Selain itu, pengujian dilakukan juga terhadap lama waktu proses enkripsi dan dekripsi pada berbagai ukuran *plaintext* dan *ciphertext*. Hal tersebut dilakukan untuk melihat pengaruh kombinasi tiga algoritma kriptografi terhadap tujuan kriptografi, yaitu kerahasiaan (*confendiality*), integritas data (*data integrity*), autentikasi (*authentication*), dan non-penyangkalan (*non-repudiation*).