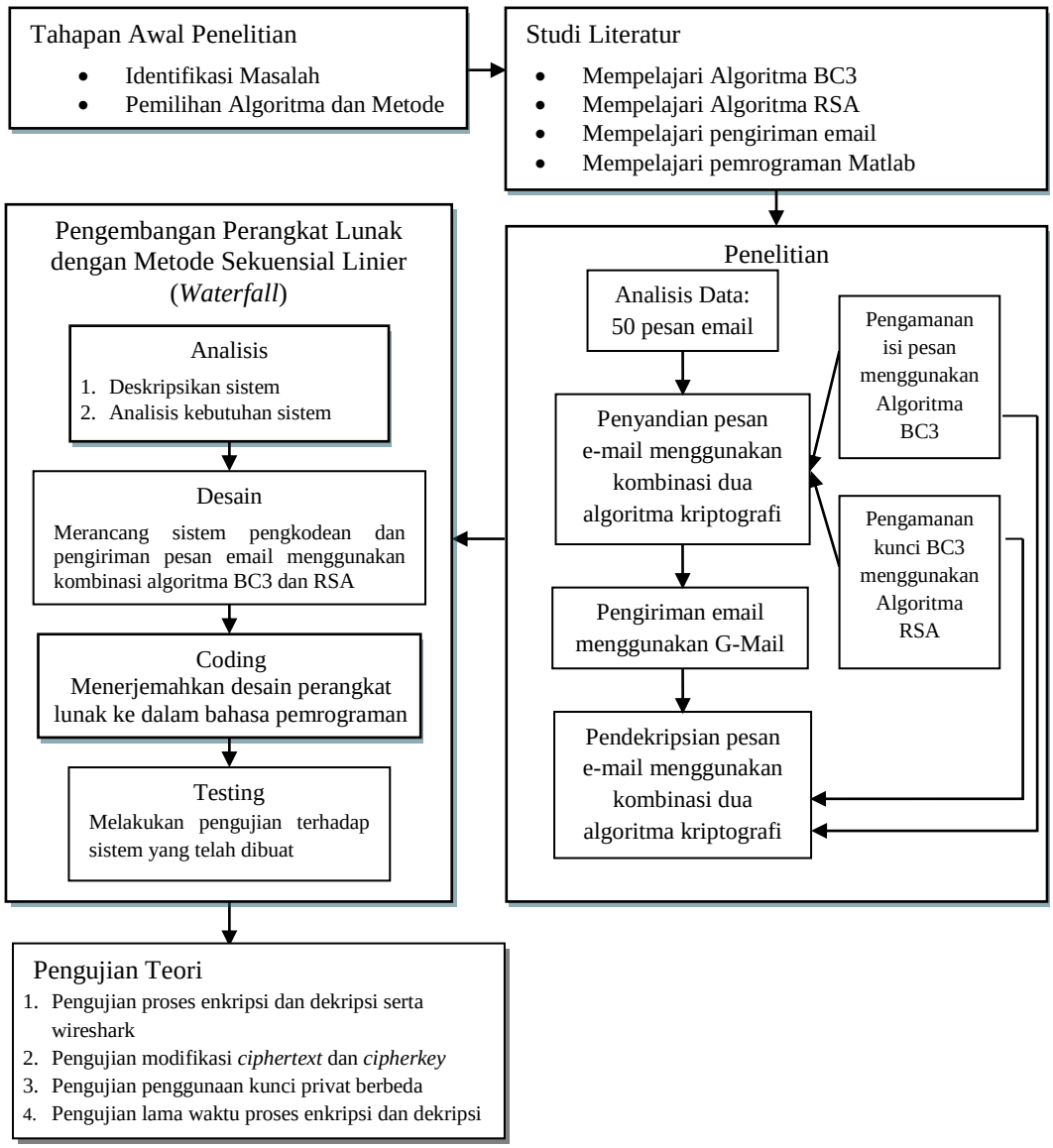
BAB III
METODOLOGI PENELITIAN

3.1. Desain Penelitian

Desain penelitian adalah tahapan atau gambaran yang akan dilakukan dalam penelitian. Desan penelitian dibuat untuk memberikan kemudahan dalam melakukan penelitian. Gambar 3.1 merupakan desain penelitian yang akan di gunakan:



Gambar 3. 1 Skema Desain Penelitian

Berikut merupakan penjelasan dari tahapan desain penelitian:

1. Tahap awal penelitian, yaitu identifikasi permasalahan yang akan diselesaikan dan menentukan metode untuk menyelesaikannya.
2. Melakukan studi literatur mengenai proses pengkodean algoritma BC3, proses pengkodean algoritma RSA, proses pengiriman email, dan lain-lain yang berhubungan dengan penelitian ini. Sumber yang digunakan berupa buku, jurnal, dan bacaan yang terdapat pada internet.
3. Melakukan penelitian pada pengamanan dan pengiriman pesan e-mail menggunakan kombinasi dua algoritma kriptografi.
    a. Data penelitian berupa pesan e-mail sebanyak 50 pesan dengan format teks. Pesan tersebut diambil dari 4 akun G-Mail dengan cara *copy-paste* dari *inbox* dan memiliki variasi panjang pesan yang berbeda-beda.
    b. Dalam penyandian isi pesan email terdapat dua proses yang dilakukan, yaitu: penyandian isi pesan email menggunakan algoritma BC3 dan pengamanan kunci BC3 menggunakan algoritma RSA. Isi pesan email akan dikonversi menjadi bilangan desimal dan diubah menjadi 64 bit/blok. Kumpulan blok ini akan dikenakan proses enkripsi menggunakan algoritma BC3 dan menghasilkan suatu *ciphertext*. Algoritma BC3 membutuhkan sebuah kunci yang pada penelitian ini akan didapat dari masukan pengirim pesan. Kunci BC3 ini akan dienkripsi menggunakan algoritma RSA dengan bantuan kunci publik yang diketahui sebelumnya sehingga menghasilkan *cipherkey*. *Ciphertext* dan *cipherkey* akan dikirim kepada penerima dalam satu pesan.
    c. Terdapat dua proses pengiriman email yang dilakukan, yaitu pengiriman kunci RSA dan pengiriman pesan email terenkripsi. Pengiriman kunci RSA dilakukan sebelum adanya penyandian isi pesan email. Server email yang digunakan pada penelitian ini adalah server Google Mail (G-Mail). Hal tersebut diambil berdasarkan hasil survei yang dilakukan APJII (Isparmo, 2016) bahwa G-Mail

merupakan layanan email terpopuler di Indonesia pada tahun 2016. Selain itu, masih terdapat kasus peretasan yang terjadi pada akun G-Mail yang dilakukan oleh pihak ketiga.

d. Dalam pendekripsian isi pesan email terdapat dua proses yang dilakukan, yaitu: pendekripsian *cipherkey* menggunakan algoritma RSA dan pendekripsian *ciphertext* menggunakan algoritma BC3. *Cipherkey* akan dikenakan algoritma RSA untuk dikembalikan menjadi kunci BC3 dengan bantuan kunci privat RSA yang telah diketahui sebelumnya. Kunci BC3 tersebut digunakan untuk mendekripsi *ciphertext* agar menjadi pesan email semula.

4. Setelah perancangan dari kombinasi dua algoritma kriptografi dilakukan, langkah selanjutnya yaitu mengimplementasikannya ke dalam kode program dan setiap proses dijadikan fungsi pada perangkat lunak. Bahasa pemrograman yang digunakan adalah bahasa Matlab. 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.
5. Pengujian yang dilakukan pada penelitian ini yaitu pengujian proses enkripsi dan dekripsi, pengujian aplikasi wireshark, pada proses dekripsi memodifikasi berupa perubahan, pengurangan dan penambahan satu bit *ciphertext* dan *cipherkey*, serta penggunaan kunci privat dari pasangan kunci RSA yang berbeda. Selain itu pengujian dilakukan juga terhadap lama waktu proses enkripsi dan dekripsi pada berbagai ukuran *plaintext* dan *ciphertext*.

3.2. Metode Penelitian

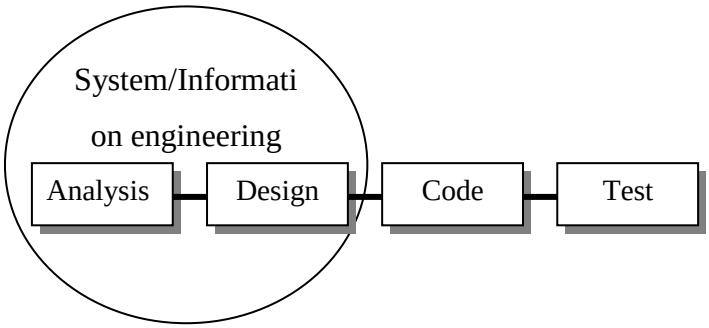
Metode penelitian ini dibagi menjadi dua, yaitu metode pengumpulan data dan metode pengembangan perangkat lunak.

3.2.1. Metode Pengumpulan Data

Adapun 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 pengenkripsian pesan berupa teks dengan algoritma BC3 dan RSA, teknik pendekripsian pesan dengan algoritma BC3 dan RSA, proses pengiriman email pada Matlab, berbagai macam metode pengujian yang dapat 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 sekuensial linier (*waterfall*).



Gambar 3. 2 Tahap-tahapan metode *Linier Sequence* (*Waterfall*)
Sumber: **(Pressman, 2001)**

Tahap-tahapan *Linier Sequence* seperti pada Gambar 3.2, yaitu:

1. Analisis Perangkat Lunak. Menganalisa data penelitian serta alat dan bahan untuk digunakan dalam penelitian. Menentukan fitur-fitur yang akan dibuat didalam perangkat lunak tersebut.
2. Desain. Perancangan dan antarmuka perangkat lunak. Perancangan perangkat lunak menggunakan *Data Flow Diagram* (DFD).
3. *Code Generation/ Coding.* Pembuatan perangkat lunak menggunakan bahasa pemrograman Matlab.
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.

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 i3-2330M 2.20 GHz
2. RAM 2GB
3. Kapasitas HDD 500 GB

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

1. Sistem Operasi Windows 7 Ultimate 32-bit
2. Matlab R2013a
3. Microsoft Office Outlook 2007
4. Wireshark
5. Mozila Firefox
6. Power Degisner
7. Microsoft Office Excel 2007

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 *World Wide Web* tentang keamanan data, algoritma BC3, algoritma RSA, pengiriman email pada matlab.

Sedangkan bahan penelitian berupa 50 pesan email untuk pengujian didapatkan dari 4 akun Google *Mail*.

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 aplikasi wireshark, pada proses dekripsi memodifikasi berupa perubahan, pengurangan dan penambahan satu bit *ciphertext* dan *cipherkey*, serta penggunaan kunci privat dari pasangan kunci RSA yang berbeda. 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 dua algoritma kriptografi terhadap dua tujuan kriptografi, yaitu kerahasiaan (*confendiality*) dan integritas data (*data integrity*).