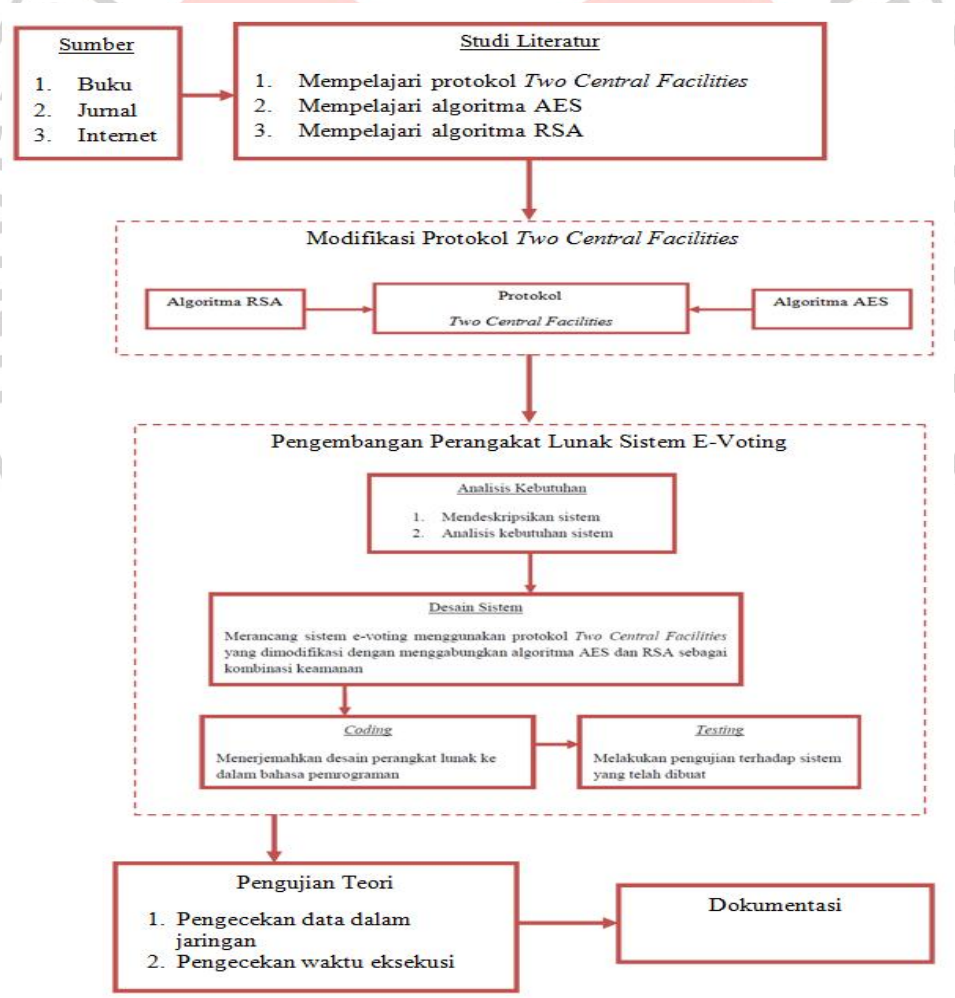
# BAB III

# METODE PENELITIAN

## 3.1. Desain Penelitian

Desain penelitian merupakan tahapan yang akan dilakukan oleh penulis untuk memberikan gambaran serta kemudahana dalam melakukan penelitian. Berikut tahapan penelitian yang dilakukan:




**Gambar 3. 1.** Skema Desain Penelitian

Tahapan penelitian yang akan dilakukan meliputi langkah – langkah berikut:

1. Studi Literatur

   Tahap studi literatur merupakan tahapan mempelajari metode-metode yang akan digunakan pada penelitian, yaitu mempelajari konsep protokol *Two Central Facilities*, mempelajari algoritma AES dan algoritma RSA. Sumber yang digunakan berupa buku jurnal, maupun bahan bacaan yang didapatkan dari internet.

   Buku karya Bruce Scheiner yang berjudul "*Applied Cryptography – Protokol, Algorithms and Source Code in C"* yang diterbitkan pada tahun 1996 menjadi sumber dalam mempelajari konsep dari protokol *Two Central Facilities.* Selain buku tersebut, jurnal milik Dan Dufeu dan Jon Harris(2001), Janga Shireesha dan So-In Chakchai(2005), juga skripsi milik Alfiyan, Erick, dan Fitrah(2012) menjadi sumber yang digunakan untuk mempelajari protokol *Two Central Facilities.*

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

   Buku "*Kriptografi*" karya Rinaldi Munir digunakan sebagai acuan dalam mempelajari algoritma RSA. Selain itu, artikel dari internet yang berjudul "*Implementasi algoritma RSA di PHP*" milik Sakti Dwi Cahyono yang diakses pada tanggal 26 Oktober 2013 pukul 18.30 dengan *url* http://www.saktidwicahyono.name/2010/03/implementasi-algoritma-rsa-di-php.html digunakan untuk mempelajari cara kerja algoritma RSA dalam bahasa pemrograman PHP.

2. Modifikasi Protokol *Two Central Facilities*

   Pada tahap ini dilakukan modifikasi terhadap protokol *Two Central Facilities* yang dikembangkan oleh Dan Dufeu dan Jon Harris. Proses modifikasi dilakukan karena dalam protokol *Two Central Facilities* sistem

yang dibangun terdiri dari tiga subsistem terpisah, yaitu Voter Client yang berperan sebagai penghubung antara pemilih dengan subsistem lainnya, CLA yang merupakan subsistem yang melakukan proses autentikasi pemilih, dan CTF yang melakukan proses tabulasi. Hal tersebut mengakibatkan terjadinya komunikasi data antar subsistem. Dengan adanya proses komunikasi data antar subsistem, mengakibatkan terjadinya kekhawatiran bahwa data tersebut dapat dilihat, diambil, maupun dimodifikasi oleh pihak yang tidak bertanggung jawab.

Proses modifikasi dilakukan dengan menambahkan proses-proses yang digunakan dalam algoritma AES dan RSA ke dalam protokol *Two Central Facilities.* Pada penelitian kali ini, algoritma RSA digunakan untuk proses enkripsi terhadap kunci rahasia yang digunakan oleh AES yang akan dikirimkan ke CLA dan CTF. Sedangkan algoritma AES digunakan untuk proses enkripsi dan dekripsi terhadap data yang akan dikirimkan antar subsistem. Algoritma AES juga digunakan untuk proses enkripsi dan dekripsi data yang akan disimpan di dalam database. Selain itu, proses modifikasi dilakukan untuk membatasi proses-proses yang dapat dilakukan oleh pemilih.

3. Pengembangan Perangkat Lunak.

   Tahap pengembangan sistem dilakukan berdasarkan metode sekuensial linear yang terdiri dari tahapan-tahapan *analysis, design, code, dan testing.*

4. Pengujian Teori

   Pada tahap ini dilakukan untuk melakukan pengujian sistem yang dibangun terhadap teori yang digunakan. Proses yang dilakukan pada tahap ini adalah pengecekan terhadap data yang berada didalam jaringan dengan menggunakan aplikasi tambahan yaitu wireshark untuk melihat apakah data yang berada di dalam jaringan tersebut masih dapat dimengerti oleh orang lain atau tidak. Selain itu, pada penelitian kali ini dilakukan proses percobaan untuk melihat waktu eksekusi terhadap sistem yang dibangun, juga untuk melakukan perbandingan waktu eksekusi antara sistem yang menggunakan proses-proses kriptografi dan sistem yang sama

sekali tidak menggunakan proses-proses kriptografi.

5. Dokumentasi

   Tahap dokementasi merupakan pembuatan dokumen skripsi, dokumen teknis perangkat lunak dan *paper*.

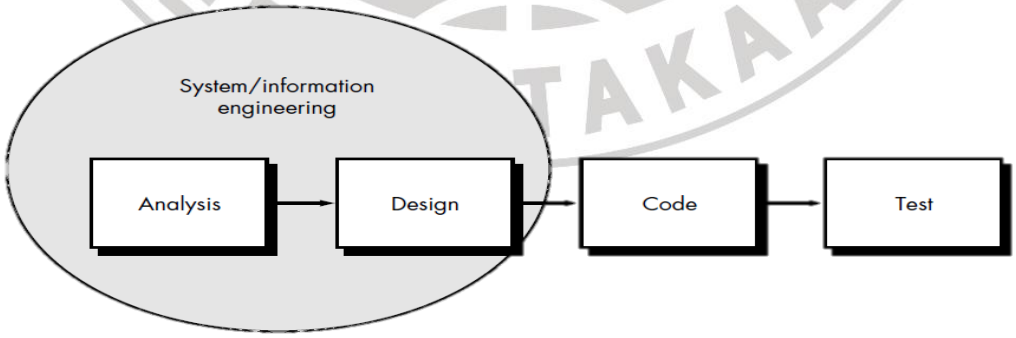
## 3.2 Metode Penelitian

### 1.2.1. Metode Pengumpulan Data

Dalam penelitian kali ini, data dan informasi yang tersedia dapat menunjang proses penelitian. Pada proses ini dilakukan studi literatur dengan mempelajari protokol Two Central Facilities, algoritma AES, dan algoritma RSA melalui jurnal, karya ilmiah, paper, textbook, dan sumber lainnya yang terdapat di internet.

### 1.2.2. Proses Pengembangan Perangkat Lunak

Di dalam proses pembangunan perangkat lunak digunakan model sekuensial linier (Pressman, 2002). Berikut adalah tahapan-tahapan dari proses pengembangan perangkat lunak dengan model sekuensial linier:




**Gambar 3. 2.** Model Sekuensial Linier

(Dikutip dari Rekayasa Perangkat Lunak Pendekatan Praktisi, 2002)

a. *Analysis*

Sistem *e-voting* dibangun berdasarkan protokol *Two Central Facilities* yang telah dimodifikasi pada tahap sebelumnya terdiri atas tiga buah sub program, yaitu *Voter Client*, CLA, dan CTF.

*Voter Client* merupakan sub program yang digunakan sebagai *interface* yang akan digunakan oleh pemilih dalam melakukan proses pemilihan. Proses otentikasi pemilih dilakukan pada sub program CLA, dan proses penghitungan suara dilakukan di dalam sub program CTF. Baik CLA maupun CTF harus dapat diakses oleh *Voter Client* sehingga pemakaian *database* dapat dilakukan secara terpusat.

Untuk menjaga keamanan data yang dikirimkan, digunakan pengenkripsian terhadap data yang dikirim. Sebelum dilakukan proses pengiriman data, *Voter Client* harus bisa melakukan permintaan kunci publik dari CLA dan CTF yang digunakan untuk pengiriman kunci rahasia ke CLA dan CTF.

b. *Design*

Pada tahap ini dilakukan perancangan *interface* yang digunakan pada sub program *Voter Client, database* yang akan digunakan pada sub program CLA dan CTF, serta perancangan alur proses yang akan digunakan pada sistem sehingga semua langkah yang ada dalam protokol *Two Central Facilities* yang dimodifikasi dapat dijalankan.

c. *Code*

Pada tahap ini dilakukan penerjamahan data atau pemecahan masalah yang telah dirancang pada tahap sebelumnya ke dalam bahasa pemrograman PHP.

d. *Test*

Tahap ini merupakan tahap pengujian terhadap perangkat lunak yang dibangun menggunakan *blackbox testing*.

## 3.3 Alat dan Bahan

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

1. 1 Buah komputer yang berfungsi sebagai CLA dengan spesifikasi sebagai berikut :
   - Processor Intel Pentium Core i5
   - Memory DDR3 4 GB
   - Harddisk 250 GB
   - 100 BASE-T Interface Card On-Board (Fast Ethernet 100Mbps)
   - Ip : 192.167.1.2
2. 1 Buah komputer yang berfungsi sebagai CTF dengan spesifikasi sebagai berikut :
   - Processor Intel Pentium Core i5
   - Memory DDR3 4 GB
   - Harddisk 250 GB
   - 100 BASE-T Interface Card On-Board (Fast Ethernet 100Mbps)
   - Ip : 192.167.1.1
3. 1 Buah komputer yang berfungsi sebagai Client dengan spesifikasi sebagai berikut :
   - Processor Intel Pentium Core i5
   - Memory DDR3 4 GB
   - Harddisk 250 GB
   - 100 BASE-T Interface Card On-Board (Fast Ethernet 100Mbps)
   - Ip : 192.167.1.3

Perangkat lunak yang dimanfaatkan dalam penelitian ini baik secara langsung maupun tidak antara lain :

1. Notepad++
2. PHP
3. MySQL
4. Web browser
5. Wireshark

Bahan penelitian yang digunakan adalah *paper*, *textbook*, *tutorial*, artikel majalah, dan dokumentasi lainnya yang didapat melalui observasi di perpustakaan dan *World Wide Web* tentang sistem e-voting, protokol *Two Central Facilities*, algoritma AES dan algoritma RSA.