BAB III
METODE PENELITIAN

Bab ini membahas kerangka penelitian baik itu desain penelitian, metode penelitian serta alat dan bahan yang akan dilakukan selama penelitian berlangsung.

3.1 Desain Penelitian

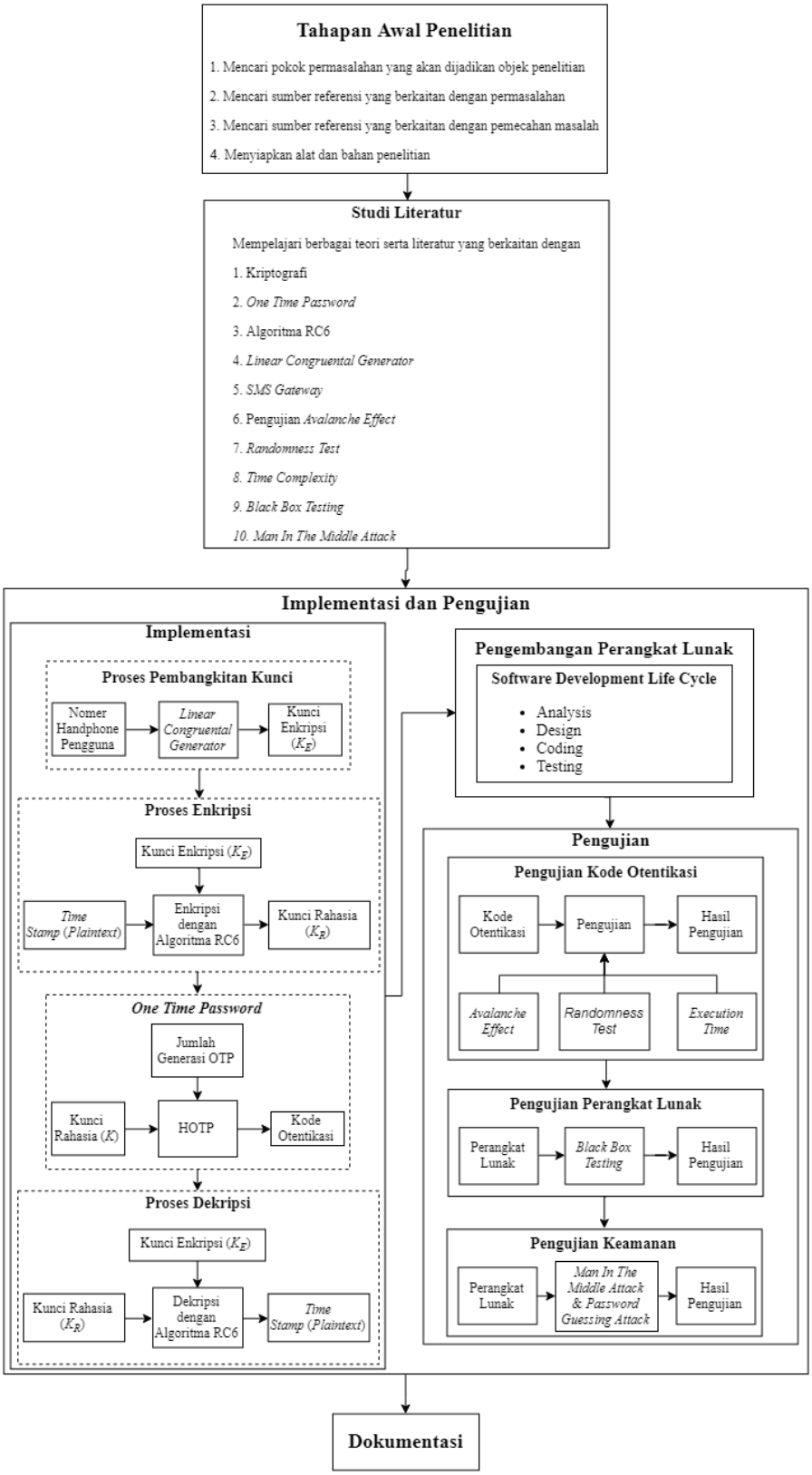
Dalam melakukan penelitian ini, penulis menyusun sebuah kerangka kerja dalam bentuk diagram alur secara terurut dan tersusun, guna mempermudah dalam melakukan penelitian. Kerangka kerja atau desain penlitian ini dapat dilihat pada gambar 3.1

a. Tahap Awal Penelitian

Tahapan ini merupakan tahapan persiapan dari sebuah penelitian. Dimana dalam tahapan ini terdapat sebuah permasalahan yang nantinya akan menjadi tujuan dari penelitian ini. Selain itu, dalam tahapan ini pula perlu dipersiapkan alat dan bahan serta referensi dari permasalahan maupun metode pemecahan dari permasalahan itu sendiri yang nantinya akan menunjang dalam penelitian ini.

b. Studi Literatur

Studi literatur merupakan sebuah tahapan dalam penelitian untuk mendapatkan pemahaman dari literatur-literatur yang telah dikumpulkan pada tahapan sebelumnya baik itu berupa teori maupun pembahasan materi yang berkaitan dengan penelitian ini. Adapun literatur-literatur yaitu berkaitan dengan Kriptografi, *One Time Password*, Algoritma RC6, *SMS Gateway*, Pengujian *Avalanche Effect*, *Randomness Test*, *Execution Time*, *Black Box Testing*, dan serangan *Man In The Middle*. Sumber literatur pada penelitian ini berupa jurnal, teks buku, *website*, dan berbagai sumber lainnya. Selain itu pada tahapan ini pula, dilakukan proses latihan dari alat dan bahan guna mendukung proses penelitian ini.



Gambar 3.1. Desain Penelitian

c. Tahapan Implementasi dan Pengujian

Tahapan implementasi dan pengujian merupakan sebuah tahap inti dari penelitian yang dilakukan dengan membagi kedalam 3 bagian yakni, tahapan implementasi, tahapan pengembangan perangkat lunak serta tahapan pengujian. Pada tahapan implementasi perangkat lunak, langkah pertama yang akan dilakukan adalah dengan membangkitkan kunci untuk proses enkripsi (K_E) dengan menggunakan metode *Linear Congruential Generator* dengan nomer *handphone* pengguna sebagai *seed*-nya. Pemilihan nomer handphone pengguna sebagai *seed*, didasarkan kepada sifat unik nomer handphone yang mana satu nomer handphone hanya dimiliki oleh satu pengguna saja. Setelah kunci enkripsi (K_E) dibangkitkan, langkah kedua adalah melakukan proses enkripsi waktu pembangkitan pada saat kode aktivasi diminta (*Time Stamp*) dengan kunci enkripsi (K_E) menggunakan algroritma RC6. Proses enkripsi ini dilakukan dengan tujuan agar waktu pembangkitan kode aktivasi tidak diketahui oleh siapapun. Karena hasil *ciphertext* yang berupa karakter ASCII, maka, pemanfaatan *ciphertext* sebagai kode aktivasi tidak dapat dilakukan karena pengguna tidak dapat membaca karakter tertentu dan akan menimbulkan kesalahan pada saat pengguna memasukan karakter tersebut dalam proses aktivasi nantinya.

Untuk mengatasi hal tersebut, maka pada penelitian ini digunakan metode HOTP, dimana pada proses pembangkitannya memerlukan dua buah inputan yakni Kunci Rahasia (KR) dan juga pesan. Dalam penelitian ini, penulis menggunakan ciphertext dari proses enkripsi untuk dijadikan sebagai kunci rahasia (KR) dan juga jumlah generasi dari pembangkitan kode aktivasi yang digunakan sebagai pesan. Dari hasil proses pembangkitan kode aktivasi dengan menggunakan HOTP, akan terbentuk 6 digit angka rahasia yang tidak boleh diberikan kepada siapapun. Setelah itu, pengguna akan diminta untuk memasukan kode aktivasi tersebut kedalam sistem. Sistem akan secara otomatis mengecek apakah kode aktivasi tersebut tersimpan didalam database atau tidak. Jika kode aktivasi tersebut tersimpan dalam database, sistem akan melakukan proses dekripsi kunci rahasi (KR) dengan kunci enkripsi (KE) untuk mendapatkan waktu pembangkitan kode aktivasi (Time Stamp) dan akan dibandingkan dengan waktu pada saat user melakukan aktivasi. Proses pembuatan perangkat lunak tersebut

dilakukan dengan menggunakan metode Software Development Life Cycle (SDLC) dengan menerapkan teknik Analysis, Design, Coding dan Testing.

Pada tahapan pengujian, proses pengujian terbagi menjadi 3 bagian, yakni pengujian terhadap kode otentikasi, pengujian terhadap fungsionalitas perangkat lunak serta pengujian keamanan perangkat lunak. Dalam proses pengujian terhadap kode otentikasi, dilakukan 3 buah pengujian yakni pengujian *Avalanche Effect*, *Statistical Randomness Test* dan pengujian *Execution Time*. Pada proses pengujian *Avalanche Effect*, obyek yang diuji adalah ciphertext dari hasil enkripsi algoritma RC6. Tujuan dari pengujian *Avalanche Effect* adalah untuk mengetahui tingkat kerahasian ciphertext yang dihasilkan dari proses enkripsi dengan melakukan perbandingan antara ciphertext yang didapatkan dari kunci dan pesan asli dengan cipherext yang didapatkan dari kunci ataupun pesan yang telah dirubah bit terakhirnya. Selain itu, proses pengujian *Avalanche Effect* dilakukan dua buah skema pengujian, yakni merubah satu bit kunci kemudian melakukan proses perbandingan dan merubah satu bit pesan yang kemudian dilakukan proses perbandingan juga.

Dalam proses *Statistical Randomness Test*, dilakukan 3 kali pengujian, yakni pengujian terhadap kunci enkripsi (K_E) yang diperoleh dari *Linear Congruential Generator*, kunci rahasia (K_R) yang diperoleh dari hasil enkripsi algoritma RC6 serta kode otentikasi yang diperoleh dari HOTP. Tujuan dilakukan *Statistical Randomness Test* adalah untuk mengetahui tingkat keacakan dari hasil yang telah didapat dari tiap-tiap metode yang telah diimplementasikan. Selanjutnya dilakukan pengujian *Execution Time* dengan menjalankan program yang telah diimplementasikan selama 3 menit. Tujuan dilakukannya pengujian *Execution Time* adalah untuk mengetahui waktu yang dibutuhkan sistem untuk membangkitkan kode otentikasi serta jumlah kode otentikasi yang dapat dibangkitkan dalam rentang waktu 3 menit yang mana waktu tersebut adalah waktu tunggu sistem dari pengguna untuk memasukan kode otentikasi pada saat proses aktivasi.

Pada pengujian terhadap fungsionalitas perangkat lunak, proses pengujian dilakukan terhadap fungsi-fungsi dari setiap modul yang telah diimplementasikan dengan melakukan *Black Box Testing* dengan tujuan untuk mengetahui apakah

perangkat lunak sudah berjalan baik atau tidak. Jika terjadi ketidak sesuaian antara fungsi-fungsi yang telah diimplementasikan dengan tujuan dari setiap fungsi-fungsi tersebut, maka akan dilakukan proses *Software Development Life Cycle* kembali. Pada pengujian keamanan, dilakukan pengujian terhadap perangkat lunak dengan membuat dua buah skema serangan, yakni teknik serangan *Man In The Middle* dan *Password Guessing Attack*. Proses serangan *Man In The Middle* ini diterapkan pada saat sistem mengirimkan kode aktivasi melalui layanan SMS serta saat pengguna melakukan aktivasi. Sedangkan, untuk *password guessing attack* dilakukan dengan melakukan pencocokan satu demi satu dari setiap kombinasi kode OTP yang mungkin terbentuk. Tujuan dilakukan dua buah skema serangan ini yakni untuk mengetahui tingkat keamanan dari sistem yang telah diimplementasikan.

d. Tahapan Dokumentasi

Tahapan dokumentasi merupakan sebuah tahapan yang bertujuan untuk mendokumentasikan seluruh kegiatan dan hasil dari penelitian ini.

3.2 Metode Penelitian

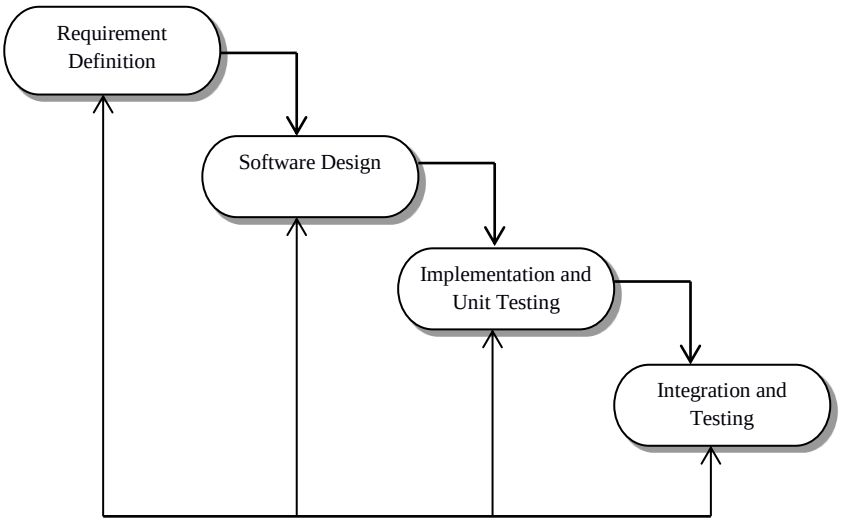
Metode penelitian yang digunakan dalam penelitian ini terbagi menjadi dua bagian yaitu metode yang dilakukan dalam mengumpulkan data serta metode yang dilakukan dalam proses pembuatan aplikasi.

3.2.1 Metode Pengumpulan Data

Proses pengumpulan data dari penelitian ini menggunakan metode studi literatur. Yakni, sebuah metode yang dilakukan dengan mempelajari dan memahami teori dan pembahasan mengenai penelitian ini. Adapaun teori dan pembahasan yang dikumpulkan pada penelitian ini antara lain Kriptografi, *One Time Passoword*, Algoritma RC6, *SMS Gateway*, Pengujian *Avalanche Effect* dan *Randomness Test*. Sumber yang digunakan untuk mengumpulkan literatur-literatur tersebut berasal dari jurnal, buku teks, *website* serta sumber pendukung lainnya.

3.2.2 Metode Pengembangan Perangkat Lunak

Dalam proses pengembangan perangkat lunak dari penelitian ini, digunakan sebuah pendekatan yang digagas oleh Ian Sommerville (Sommerville, 2004) yaitu metode *Waterfall.* Metode tersebut dipilih karena sangat mudah diterapakan dalam pembangunan perangkat lunak dan memudahkan bagi pembuat perangkat lunak untuk melukan pengujian serta mendesain ulang apabila terdapat kesalahan dalam proses pembuatan perangkat lunak tersebut. Berikut ini merupakan metode *waterfall* yang diterapkan pada penelitian ini yang akan ditunjukan oleh gambar 3.2.



Gambar 3.2. Diagram Waterfall (Sommerville, 2004)

a) Requirement Definition

Dalam tahap ini, dilakukan pengumpulan informasi mengenai pembuatan aplikasi Otentikasi baik itu berupa jenis entitas, data, kebutuhan fungsional, kebutuhan non-fungsional serta batasan-batasan apa saja dalam membangun aplikasi otentikasi. Informasi-informasi tersebut didapatkan dari hasil studi literatur yang dilakukan pada tahapan sebelumnya. Tahapan ini dilakukan agar aplikasi yang dirancang memenuhi spesifikasi yang diinginkan sesuai dengan kebutuhan.

b) *Software* Design

Setelah memetakan kebutuhan dan spefisikasi yang akan dibuat, tahapan berikutnya adalah merancang sistem dari aplikasi otentikasi. Tahapan ini

dilakukan untuk memudahkan penerjemahan dari bahasa manusia (kebutuhan dan spesifikasi perangkat lunak) kedalam bahasa program. Adapun alat atau metode yang digunakan dalam memodelkan dan merancang sistem otentikasi ini yaitu dengan menggunakan diagram *Unified Modeling Languange* (UML). Pemilihan UML sebagai alat bantu untuk memodelkan kebutuhan perangkat lunak didasarkan kepada penggunaan *framework* dari bahasa pemrograman PHP yaitu *Code Igniter* yang bersifat pemrograman berbasis objek.

c) Implementation and Unit Testing

Setelah tahapan pemodelan selesai, langkah berikutnya adalah melakukan implementasi kedalam bahasa pemrograma PHP. Pemilihan bahasa tersebut dikarenakan bahasa PHP merupakan satu bahasa *server side* dalam membangkun aplikasi *website*. Dalam proses implentasi antara metode *One Time Passoword* dengan Algoritma RC6 tidak dibuat dari awal akan tetepi menggunakan salah satu *framework* dari bahasa pemrograman PHP yaitu *Code Igniter*. Pemilihan *framework* tersebut didasarkan kepada kemudahan dalam pembangunan aplikasi serta lengkapnya dokumentasi yang dimiliki oleh *Code Igniter*. Selain pembangunan aplikasi, untuk menghindari kesalahan dari sistem, maka pada proses pembangunan aplikasi ini dilakukan *Unit Testing* disetiap modul yang dibuat.

d) Integration and Testing

Setelah memastikan tidak ada kesalahan pada setiap modulnya, langkah berikutnya adalah menyatukan seluruh modul dan melakukan pengujian *Black Box*, baik itu alur dari aplikasi maupun sistem secara keseluruhan. Jika dirasa sudah tidak ada kesalahan lagi, maka proses berikutnya adalah melakukan pengujian *Avalanche Effect* dan *Randomness Test*. Selain itu, untuk mengetahui tingkat keamanan dari perangkat lunak, maka akan dilakukan pengujian dengan melakukan serangan *Man In The Middle* dan *Password Guessing Attack.*

3.3 Alat dan Bahan

Dalam melakukan proses penelitian ini, penulis menggunakan berbagai alat dan bahan guna menunjang proses penelitian baik itu perangkat lunak, perangkat keras, serta bahan materi dan teori.

3.3.1 Alat Penelitian

Adapun perangkat keras (*hardware*) yang digunakan penulis, memilki spesifikasi sebagai berikut:

- *Processor* Intel i5-5200U 2.2 GHz.
- RAM 8 GB.
- *Harddisk Drive* 500GB.
- *Mouse* dan *Keyboard.*
- Layar *Monitor* 14 inch dengan resolusi 1366 x 768.

Sementara, untuk perangkat lunak (*software*) yang digunakan adalah sebagai berikut:

- Text Editor Visual Studio Code versi 1.26.1 (x64 bit).
- WAMP Server 3.1.0 (x64 bit).
- PHP versi 7.1.9.
- Apache versi 2.4.27.
- Mysql versi 5.7.19.
- Mozilla Firefox Developer Edition versi 63.0b6 (64-bit).

3.3.2 Bahan Penelitian

Bahan yang digunakan selama proses penelitian ini antara lain jurnal, teks buku, *website* serta bahan lainnya yang menunjang selama penelitian.