BAB III
METODELOGI PENELITIAN

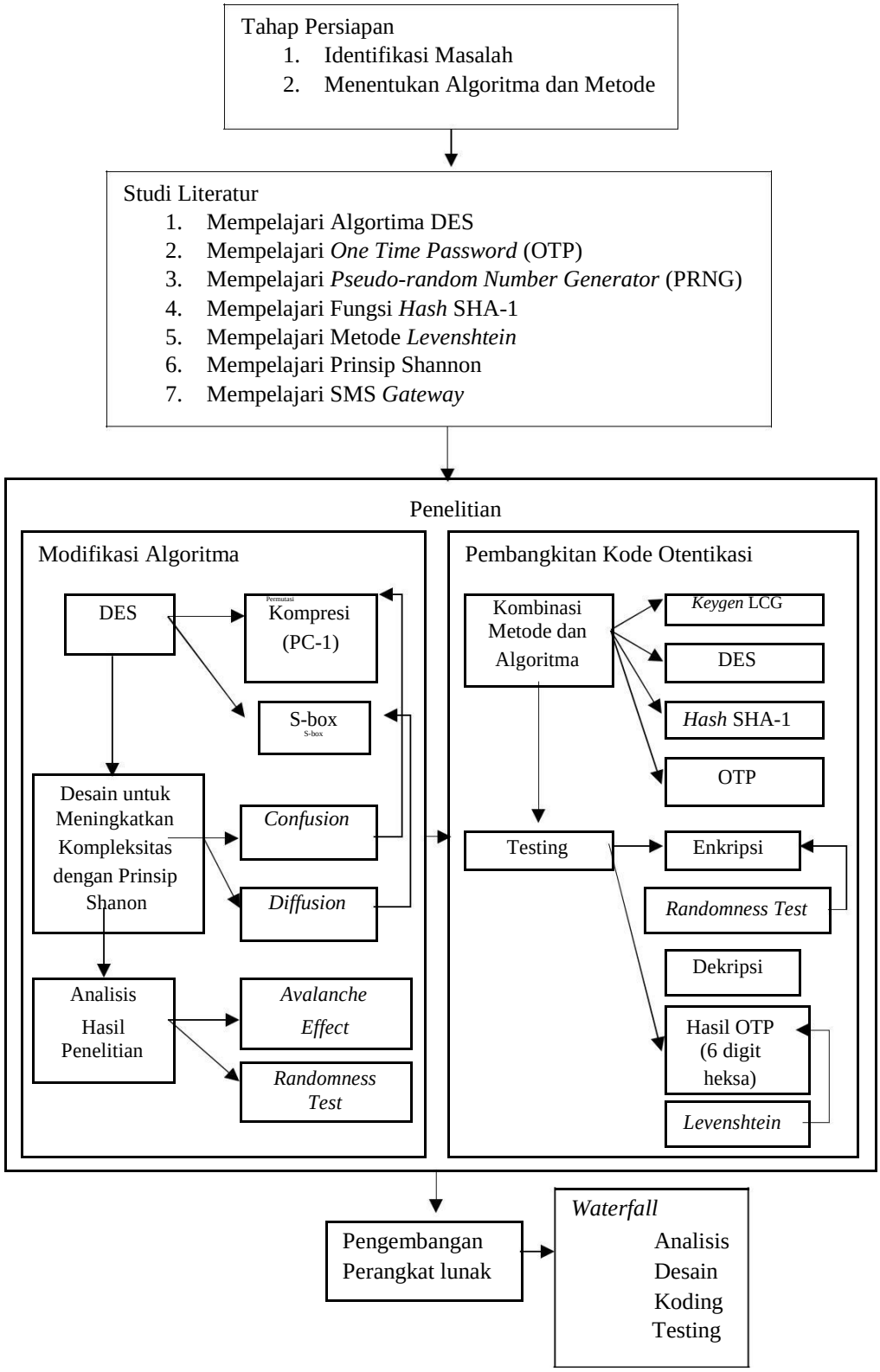
Bab ini akan menjelaskan tentang metodelogi penelitian, mulai dari desain penelitian, alat dan bahan penelitian, dan metode penelitian.

3.1. Desain Penelitian

Desain penelitian adalah kerangka kerja yang digunakan untuk melakukan penelitian. Desain penelitian dari modifikasi algoritma DES dengan pengujian *avalanche effect* dan *randomness test* serta implementasi fungsi *hash* dan metode OTP untuk dijadikan kode otentikasi dibuat untuk memberikan gambaran serta kemudahan dalam melakukan penelitian. Berikut ini persiapan yang dilakukan sebelum penulis mulai melakukan penelitian.

1. Menentukan kebutuhan data yang digunakan, seperti data teks yang digunakan untuk enkripsi-dekripsi, algoritma DES, fungsi *hash* SHA-1, metode OTP, perhitungan *avalanche effect*, pengujian dengan *randomness test* dan Analisis Levenshtein.
2. Mengumpulkan data yang dibutuhkan, data yang sudah ditentukan diatas kemudian dikumpulkan untuk diproses. Data dapat diperoleh melalui studi literatur.
3. Mempersiapkan alat dan bahan penelitian. Alat disini adalah perangkat keras (hardware) dan perangkat lunak (software) yang akan digunakan untuk memodifikasi algoritma DES dengan perhitungan *avalanche effect* dan pengujian *randomness test* sedangkan datanya berupa data-data yang telah dikumpulkan, untuk diproses ke dalam program.

Desain Penelitian yang penulis lakukan digambarkan pada gambar 3.1.



Gambar 3.1. Desain Penelitian

Gambar 3.1 menjelaskan proses penelitian yang akan dilakukan sebagai berikut:

1. Tahap persiapan adalah tahap awal dari penelitian, tahap ini dimulai dari identifikasi masalah, masalah ditemukan dengan mengikuti isu-isu dan perkembangan teknologi saat ini, serta mempelajari penelitian yang sudah dilakukan dan dipublikasikan melalui jurnal ilmiah. Masalah yang diangkat pada penelitian ini adalah mengenai pembangkitan kode otentikasi sebagai salah satu cara untuk dapat meningkatkan keamaanan pada saat melakukan registrasi akun suatu sosial media untuk mencegah pembuatan akun palsu, dan penyerangan terhadap data login, algoritma yang digunakan pada penelitian ini adalah algoritma DES, fungsi *hash* SHA-1 dan OTP.
2. Studi literatur merupakan bagian dari tahap persiapan. Studi literatur dilakukan dengan memperlajari dan memahami teori yang akan digunakan untuk melakukan penelitian. Beberapa teori harus dipahami dalam melakukan penelitian ini yaitu memahami kriptografi, memahami algoritma DES, memahami fungsi *hash* SHA-1, memahami metode OTP, memahami metode LCG, dan memahami bagaimana penggunaan SMS Gateway. Teori-teori tersebut didapatkan dari literatur yang telah dikumpulkan seperti, jurnal, *text book*, *paper*, dan artikel yang topiknya terkait dengan penelitian.
3. Tahap Penelitian, penelitian yang pertama yaitu membuat program enkripsi dan dekripsi algoritma DES untuk mengetahui nilai *avalanche effect* dari algoritma dengan menggunakan aplikasi matlab R2013a. Kemudian dilakukan penelitian untuk memodifikasi DES, dimana modifikasi bertujuan untuk meningkatkan kompleksitas dari DES standar dengan meningkatkan nilai *confusion* dan *diffusion* sesuai dengan prinsip Shannon pada bagian permutasi kompresi (PC-1) dan *S- box* dari algoritma DES. Algoritma DES yang telah dimodifikasi dianalisis melalui tes *avalanche effect* dengan aplikasi yang dibuat di matlab R2013a.

   Tahap selanjutnya setelah modifikasi algoritma DES selesai, masuk ketahap implementasi yang mana pada tahap implementasi menerapkan metode LCG untuk membangkitkan nilai kunci sebagai *key generator*, algoritma DES yang telah dimodifikasi tersebut diimplementasikan dengan SHA-1, dan metode OTP sebagai kontrol untuk waktu validasi yang kemudian di implementasikan

pada saat pembangkitan kode otentikasi, setelah itu dilakukan tes *randomness test* untuk hasil enkripsi dengan menggunakan Cryptool 1.4.30.

4. Pengembangan aplikasi dilakukan dalam beberapa tahap sesuai dengan model pengembangan perangkat lunak *waterfall*. Yang pertama analisis, pada tahap ini dilakukan analisis bagaimana *software* akan dibuat. Kemudian masuk ke tahap desain, tahap desain ini mencakup desain aplikasi, desain database, dan desain interface. Setelah itu masuk ke implementasi (*coding*).

3.2. Fokus Penelitian

Fokus penelitian pada skripsi ini adalah:

1. Modifikasi Algoritma DES pada bagian permutasi kompresi (PC-1) dan S-box.
2. Pengujian modifikasi algoritma dengan *avalanche effect* dan *randomness test.*
3. Mengimpelentasikan algoritma DES yang telah dimodifikasi, SHA-1, dan Metode OTP kedalam sistem registrasi.

3.3. Alat dan Bahan Penelitian

Bagian ini menjelaskan secara detail alat dan bahan yang digunakan untuk melakukan penelitian.

3.3.1. Alat Penelitian

Dalam penelitian ini, peneliti menggunakan berbagai alat bantu penunjang baik berupa perangkat keras maupun perangkat lunak. Adapaun Perangkat Keras (*Hardware*) yang digunakan memiliki spesifikasi sebagai berikut:

- *Processor* Intel Pentium inside
- RAM 2 GB
- *Harddisk Drive* 512 GB
- *Mouse* dan *Keyboard*

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

- Notepad ++
- XAMPP
- MySQL
- Matlab R2013a
- Chrome
- Cryptool 1.4.30
- SMS Gateway Gammu

3.3.2. Bahan Penelitian

Bahan yang diperlukan untuk melakukan penelitian yaitu mengenai penerapan algoritma DES pada berbagai macam sistem agar dapat mengetahui kelebihan dan kekurangan dari algoritma tersebut sehingga algoritma yang di modifikasi akan menghasilkan kinerja yang lebih baik. Penggunaan OTP untuk otentikasi *password,* penggunaan metode LCG dalam membangkitkan bilangan acak untuk dijadikan inputan kunci, dan SMS gateway untuk mendukung pengembangan aplikasi.

3.4. Metode Penelitian

Adapun metode yang dilakukan dalam penelitian ini dibagi kedalam dua bagian, yaitu metode pengumpulan data dan metode pengembangan perangkat lunak.

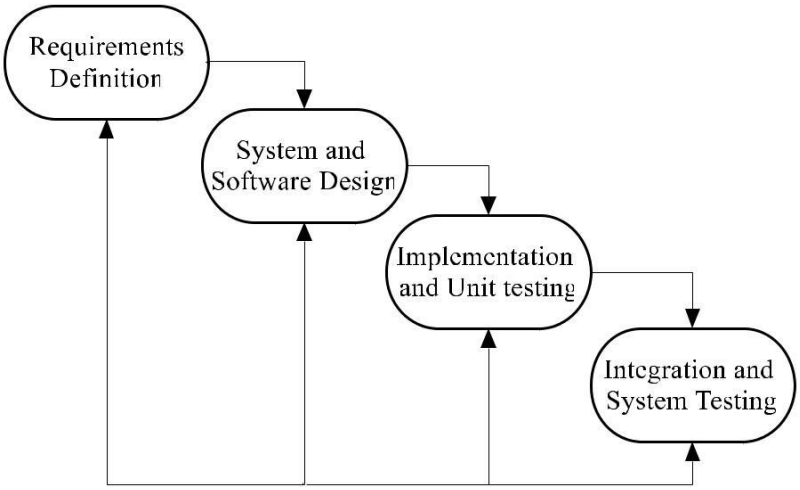
3.4.1. Metode Pengumpulan Data

Penulis berusaha mendapatkan data yang akurat dan mampu menunjang penelitian, adapun metode pengumpulan datanya adalah sebagai berikut:

1. Studi Literatur

   Studi literatur dilakukan dengan mempelajari teori dan konsep yang menjadi pendukung dalam penelitian ini, yaitu kriptografi, algoritma DES, metode OTP, metode LCG, dan SMS gateway, *Avalanche Effect* dan *Randomness Test* melalui jurnal, *textbook*, dan artikel dari internet.

3.4.2. Metode Penggembangan Perangkat Lunak



Gambar 3.2. Metode *Waterfall* (Sommerville, 2011)

Metode pengembangan perangkat lunak dilakukan dengan metode *waterfall*. Model SDLC air terjun (*waterfall*) sering juga disebut model sekuensial linier (sequential linier). Model *waterfall* menyediakan pendekatan alur hidup perangkat lunak secara sekuensial atau urut dimulai dari analisis, desain, pengkodean, pengujian dan tahap support (Sukamto & Shalahuddin, 2011). Penulis menggunakan metode *modern waterfall* seperti pada gambar 3.2 agar jika suatu saat ada kesalahan pada salah satu tahap, bisa dikembalikan ke tahap sebelumnya. Berikut pengertian dari tahap-tahap pada model *waterfall* pada gambar 3.2 menurut Ian Sommerville (2011) :

1. *Requirements Analysis and Definition* (Analisis)

   Analisis adalah tahap menentukan aplikasi atau *software* seperti apakah yang akan dibuat. Analisis merupakan tahapan penetapan fitur, kendala dan tujuan sistem melalui konsultasi dengan pengguna sistem. Semua hal tersebut akan ditetapkan secara rinci dan berfungsi sebagai spesifikasi sistem.

2. *System and Software Design* (Desain)

   Dalam tahapan ini akan dibentuk suatu arsitektur sistem berdasarkan persyaratan yang telah ditetapkan. Dan juga mengidentifikasi dan menggambarkan abstraksi dasar sistem perangkat lunak dan hubungan-hubungannya.

3. *Implementation and Unit Testing* (*Coding*)

   Coding adalah tahap proses implementasi dari desain, dalam tahapan ini, hasil dari desain perangkat lunak akan direalisasikan sebagai satu set program atau unit program. Setiap unit akan diuji apakah sudah memenuhi spesifikasinya.

4. *Integration and System Testing* (Testing)

   Proses testing atau pengujian dilakukan pada logika internal untuk memastikan semua pernyataan sudah diuji. Dalam tahapan ini, setiap unit program akan diintegrasikan satu sama lain dan diuji sebagai satu sistem yang utuh untuk memastikan sistem sudah memenuhi persyaratan yang ada. Setelah itu sistem akan dikirim ke pengguna sistem.