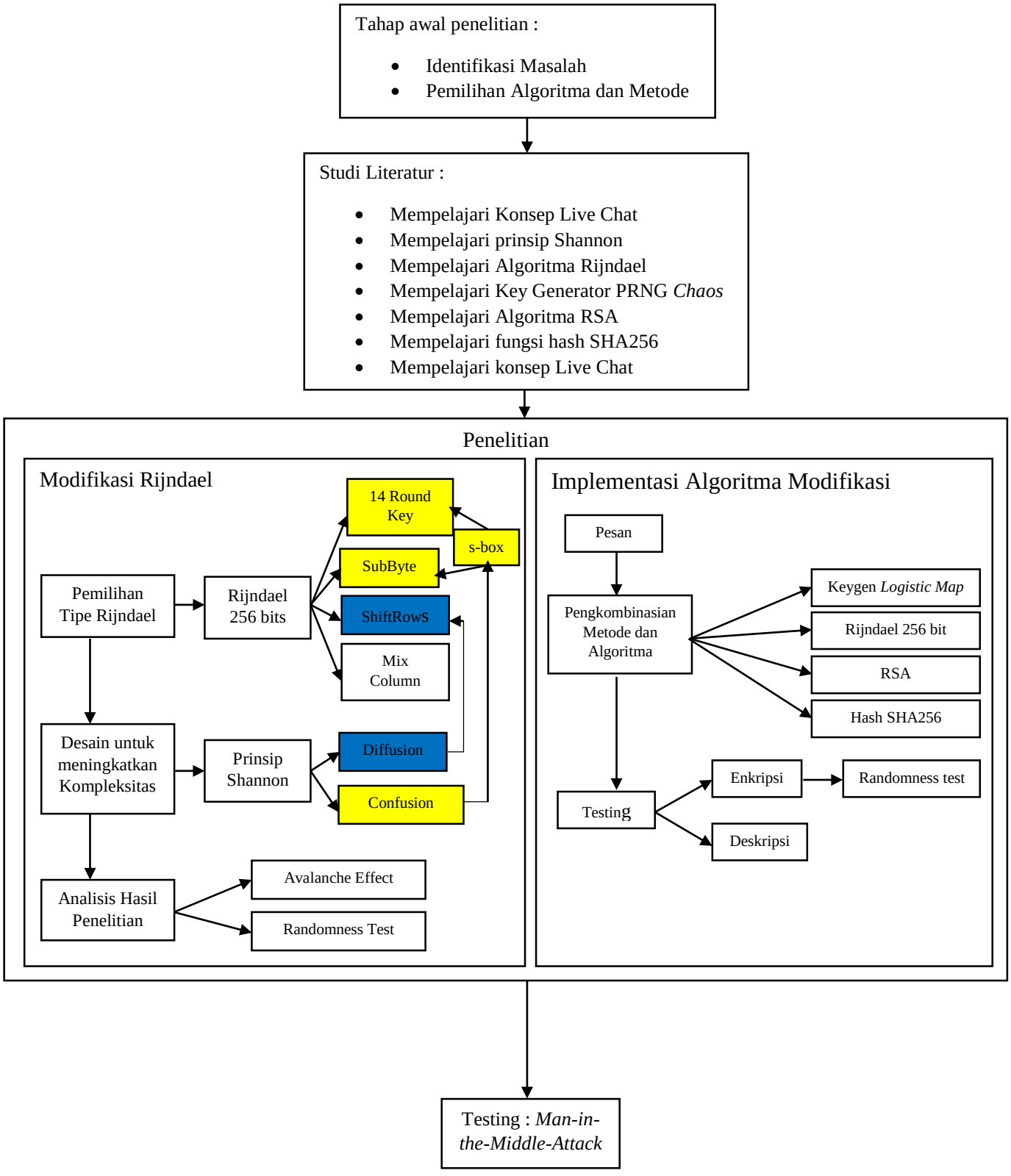
BAB III
METODOLOGI PENELITIAN

3.1 Desain Penelitian

Desain penelitian adalah tahapan atau gambaran yang akan dilakukan dalam penelitian untuk mempermudah penelitian. Desain penelitian "Modifikasi Algoritma Rijndael dengan Pengujian Randomness Test, Avalanche Effect, serta implementasi algoritma RSA dan SHA256 untuk pertukaran kunci dan pengujian menggunakan *Man-in-the-Middle-Attack*" 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 Rijndael, algoritma RSA, SHA256, perhitungan avalanche effect, pengujian dengan randomness test.
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 memodifikasi algoritma Rijndael dengan pengujian randomness test dan avalanche effect, sedangkan datanya berupa data-data yang telah dikumpulkan, untuk diproses ke dalam program.

Gambaran umum mengenai desain penelitian yang penulis lakukan dapat dilihat pada gambar 3.1.



Gambar 3. 1 Desain Penelitian

3.1.1 Tahap Awal

Pada tahap ini merupakan penetuan penggunaan bahan terkait dengan penelitian yang dilakukan. Pada tahap ini akan dilakukan identifikasi masalah yang akan diselesaikan, masalah yang akan diteliti adalah semakin banyaknya penggunaan *e-commerce* semakin banyak juga pengguna yang akan berinteraksi dengan *customer service.* Maka semakin banyak yang menggunakan *Live Chat,* dengan begitu tingkat keamanannya harus lebih ditingkatkan untuk menghindari pencurian data dan perubahan data dengan cara menerapkan sistem enkripsi dan fungsi hash. Algoritma yang akan dipakai adalah Algoritma Rijndael 256 bit, Algoritma RSA, dan fungsi hash SHA256.

3.1.2 Studi Literatur

Pada tahap ini merupakan tahapan yang mempelajari terkait dengan penelitian yang dilakukan yaitu mempelajari Konsep *Live Chat,* Prinsip Shannon, Algoritma Rijndael, Key generator PRNG *Chaos,* Algoritma RSA, dan mempelajari fungsi hash SHA256 dengan menggunakan Bahasa pemograman PHP dan Matlab. Sumber yang digunakan ialah, buku, jurnal, skripsi dan informasi yang didapat dari internet.

3.1.3 Perancangan Algoritma Rijndael

Pada tahap ini dilakukan modifikasi pada Algoritma Rijndael yaitu modifikasi pada bagian S-Box, dan *ShiftRows* . Setelah itu, ke tahap perancangan dan pembuatan Algoritma Rijndael dan RSA yang langsung diterapkan pada Live Chat berbasis Web. Bahasa pemograman yang dipakai adalah PHP.

3.2 Fokus Penelitian

Fokus penelitian pada skripsi ini adalah:

1. Memodifikasi bagian S-box dan *ShiftRows* Algoritma Rijndael.
2. Pengujian modifikasi algoritma dengan *avalanche effect* dan *randomness test.*
3. Pengimplementasian Algoritma Rijndael 256bit yang sudah dimodifikasi, Algoritma RSA, dan fungsi hash SHA256 ke dalam *Live chat.*
4. Pengujian keseluruhan sistem menggunakan *Man-in-the-Middle-Attack.*
5. File yang akan diolah hanya berupa data teks.

3.3 Metode Penelitian

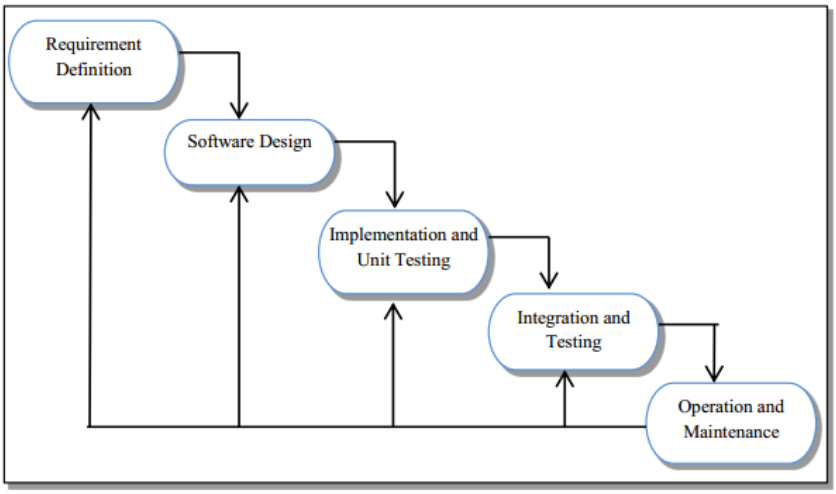
Metode penelitian ini dibagi menjadi dua, yaitu metode pengumpulan data dan metode pengembangan perangkat lunak.

3.3.1 Metode Pengumpulan Data

Dalam penelitian kali ini, data dan informasi yang tersedia dapat menunjang proses penelitian. Pada proses ini dilakukan studi literatur dengan mempelajari Konsep *Live Chat,* Prinsip Shannon, Algoritma Rijndael, Key generator PRNG *Chaos,* Algoritma RSA, dan mempelajari fungsi hash SHA256, struktur Rijndael, modifikasi algoritma Rindael, *Avalanche Effect*, *Hamming Weight* dan *Randomness Test* melalui jurnal, textbook, tutorial serta dokumentasi lainnya yang didapat melalui observasi di perpustakaan dan *World Wide Web.*

3.3.2 Metode Pengembangan Perangkat Lunak

Pembangunan perangkat lunak dalam penilitian ini menggunakan model *waterfall* (Sommerville, 2011). Dalam model *waterfall* Sommerville terdapat kemungkinan untuk kembali ke tahap sebelumnya apabila terjadi kesalahan atau perbaikan, dimana alur prosesnya seperti pada Gambar 3.2.



Gambar 3. 2 Model Waterfall *(Sommerville, 2011)*

Berikut beberapa tahapan dari metode *waterfall* sommerville :

1. *Requirement Definition*, Tahap awal dimana adanya analisis untuk menentukan kebutuhan, batasan, dan tujuan (*goal*) dari perangkat lunak sesuai yang diinginkan. Dalam tahap ini penulis mengidentikasi masalah, dan memilih metode yang cocok untuk menyelesaikan masalah tersebut. Algortima yang dipakai adalah algoritma kriptografi Rijndael, algoritma kriptografi RSA dan hashing SHA256.
2. *Software Design* merupakan proses perancangan yang melibatkan identifikasi dan menggambarkan dasar sistem serta hubungan satu sama lain. Pada tahap ini dibuat desain algoritma rijndael dengan memodifikasi di bagian *S-boxes* nya dan *ShiftRows*. Setelah itu menggabungkan dengan algoritma RSA untuk mengenkripsi kunci dari algoritma rijndael. Algoritma yang sudah dibuat di uji terlebih dahulu dengan *Avalanche effect* dan *Randomness test.*
3. *Implementation and Unit Testing*, Pada tahap ini, *software design* yang telah dilakukan sebelumnya kemudian diimplementasikan dalam bentuk unit program. Dari hasil perancangan algoritma, kita masuk kedalam pengimplementasian ke dalam aplikasi *Live Chat* dengan

Bahasa pemograman PHP. Lalu, aplikasi diuji dengan teknik penyadapan yaitu Man-In-The-Middle-Attack.

4. *Integration and Testing*, Setelah semua unit program berhasil diimplementasikan dan lolos *testing* maka dilanjutkan dengan mengintegrasikan setiap unit untuk membentuk aplikasi yang diinginkan. Aplikasi yang sudah dibentuk kemudian di tes kembali untuk memastikan unit program dapat berjalan satu sama lain dalam aplikasi dan aplikasi yang dibuat sudah memenuhi kebutuhan.

3.4 Alat dan Bahan Penelitian

Berdasarkan kebutuhan-kebutuhan di atas, maka ditentukan bahwa alat dan bahan yang digunakan pada penelitian ini adalah sebagai berikut:

3.4.1 Alat Penelitian

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

1. *Processor* Intel i3
2. RAM 6 GB
3. *Hard disk* 512 GB
4. Mouse dan Keyboard

Sementara itu perangkat lunak yang digunakan adalah sebagai berikut:

5. Sistem Operasi Microsoft Windows 10 64 bit
6. Sublime Text
7. XAMPP v3.2.2
8. Chrome
9. Matlab R2013a
10. Cryptool 1.4.30

3.4.2 Bahan Penelitian

Bahan penelitian yang digunakan adalah jurnal penelitian yang sudah dilakukan, *textbook*, *tutorial*, dan dokumentasi lainnya yang didapat melalui observasi di perpustakaan dan *World Wide Web* tentang, Konsep *Live Chat*, Prinsip Shannon, Algoritma Rijndael, Key generator PRNG *Chaos*, Algoritma RSA, dan fungsi hash SHA256.