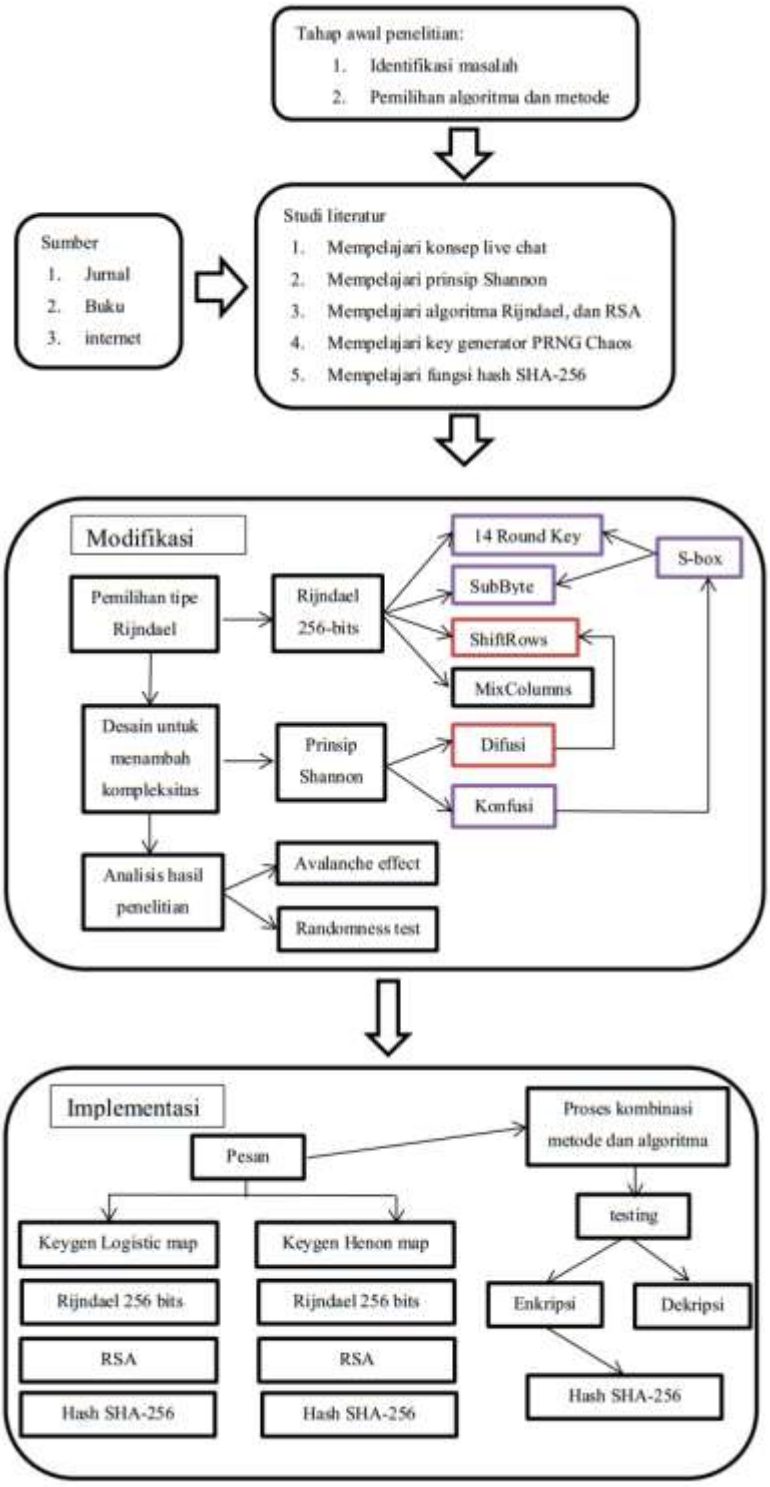
BAB III
METODOLOGI PENELITIAN

3.1 Desain Penelitian

Dalam penelitian ini, peneliti akan menggunakan metode "Library Research" dimana metode yang akan digunakan dalam penelitian ini akan menggunakan teori-teori yang diambil dari buku literature yang mendukung dan relevan dengan topic skripsi ini. Berikut ini desain penelitian yang akan peneliti lakukan.

1. Menentukan kebutuhan data yang akan digunakan, seperti data yang akan digunakan untuk enkripsi dan dekripsi berupa teks, data mengenai algoritma Rijndael, RSA, SHA-256, data mengenai perhitungan avalanche effect, dan data mengenai pengujian menggunakan randomness test.
2. Setelah data ditentukan, peneliti akan mengumpulkan data-data tersebut untuk kemudian diproses. Data yang dikumpulkan merupakan data yang diperoleh melalui studi literatur.
3. Setelah data terkumpul, peneliti mempersiapkan alat dan data penelitian. Alat yang akan digunakan merupakan perangkat keras dan perangkat lunak, sedangkan data yang akan digunakan merupakan data yang telah terkumpul untuk kemudian diproses dalam penelitian.

Gambaran umum mengenai desain penelitian yang akan peneliti lakukan dapat dilihat pada Gambar 3.1.



Gambar 3. 1 Desain Penelitian

3.1.1 Tahap Awal

Pada tahap awal akan dilakukan penentuan penggunaan bahan-bahan yang terkait dengan penelitian yang akan dilakukan. Tahap awal yang akan dilakukan adalah mengidentifikasi maslah yang akan diselesaikan dan masalah yang akan diteliti. Masalah utama dari penelitian ini adalah tingkat keamanan pada system live chat pada e-commerce. Sebagaimana kita tahu bahwa semakin banyak penggunaan e-commerce, dan salah satu service yang diberikan kepada pengguna adalah live chat. Hal ini menunjukkan bahwa tingkat keamanan pada system live chat harus lebih ditingkatkan karena sangat rentan terhadap pencurian data dan perubahan data. Pengamanan system live chat yang akan peneliti lakukan menggunakan teknik enkripsi dan fungsi hash. Algoritma yang akan digunakan adalah algoritma Rijndael 256-bits, RSA, dan fungsi SHA 256.

3.1.2 Proses Modifikasi

Pada tahap ini akan dilakukan modifikasi pada Algoritma Rijndael pada bagian S-Box dan ShiftRows dan kunci yang akan digunakan akan digenerate menggunakan dua generator kunci yang berbeda yaitu Logistic Map dan Henon Map. Dilanjutkan dengan tahap perancangan dan pembuatan aplikasi menggunakan Algoritma-algoritma yang akan digunakan.

3.1.3 Proses Implementasi

Pada tahap proses implementasi akan dilakukan pengimplementasian algoritma yang sudah di rancang dan dimodifikasi ke dalam aplikasi live chat berbasis web yang menggunakan bahasa pemrograman PHP.

3.1.4 Proses Testing

Pada tahap proses testing, akan dilakukan pengujian tingkat keamanan pesan menggunakan teknik *avalanche effect*. Kemudian dilakukan juga pengujian tingkat keacakan pesan menggunakan teknik

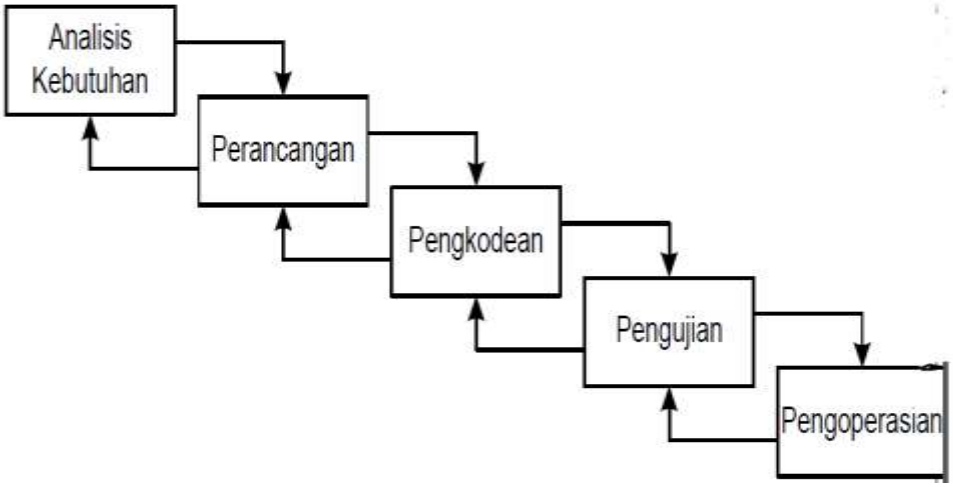
randomness test, dan dilakukan pengujian serangan man-in-the-middle attack dengan metode brute force pada aplikasi live chat.

3.2 Metode Pengumpulan Data

Pengumpulan data dilakukan melalui studi literature yang bersumber dari buku, jurnal, maupun internet. Peneliti melakukan studi literature demi mengumpulkan data yang akan digunakan pada penelitian, karena penting bagi peneliti untuk mengumpulkan data yang relevan dengan penelitian yang akan dilakukan. Data yang dikumpulkan dan dipelajari yaitu konsep live chat. Peneliti menemukan banyak kelemahan dari konsep live chat itu sendiri dari segi keamanan. Peneliti menemukan kelemahan dari konsep live chat dari berbagai sumber, diantaranya jurnal dan penelitian sebelumnya yang dilakukan oleh Anggita pada tahun 2017. Hal lain yang peneliti pelajari diantanya, yaitu konsep algoritma Rijndael, dan juga kelemahan dan kelebihan dari algoritma Rijndael. Selanjutnya peneliti mempelajari mengenai prinsip Shannon. Seperti yang kita tahu bahwa prinsip Shanon terdiri dari dua prinsip yaitu Difusi dan Konfusi. Menurut penelitian sebelumnya yang dilakukan oleh Anggita pada tahun 2017, beliau membandingkan tingkat keamanan yang dilakukan terhadap algoritma Rijndael yang dimodifikasi pada bagian Shiftrows dan S-box. Anggita menemukan bahwa tingkat keamanan yang lebih tinggi, ditunjukkan pada proses modifikasi bagian ShiftRows sebesar 50.2232%. Peneliti pun mempelajari mengenai RSA, key generator PRNG chaos dan juga fungsi hash SHA-256. Pengumpulan data dilakukan melalui studi literature yang bersumber dari buku, jurnal, maupun internet.

3.3 Metode Pengembangan Perangkat Lunak

Metode pengembangan perangkat lunak dalam penelitian ini akan menggunakan model pengembangan perangkat lunak waterfall. Dalam model ini terdapat kemungkinan untuk mengulang tahap sebelumnya guna meminimalisir kesalahan dan melakukan perbaikan. Alur proses yang akan dilakukan dapat dilihat pada Gambar 3.2.



Gambar 3. 2 Model Waterfall

Dalam pengembangannya, model waterfall ini memiliki beberapa tahapan yang berurut, yaitu analisis kebutuhan, perancangan, pengkodean, pengujian, pengoperasian, dan pemeliharaan. Tahapan-tahapan pada model ini akan dijelaskan sebagai berikut.

1. Analisis kebutuhan

   Pada tahap ini pengembang system menganalisis data yang dibutuhkan untuk pengembangan perangkat lunak. Data-data yang dibutuhkan adalah mengenai algoritma Rijndael, konsep live chat, algoritma RSA, Key generator PRNG, dan fungsi hash SHA-256.
2. Perancangan

   Spesifikasi kebutuhan dari tahap sebelumnya akan dipelajari pada tahap ini, lalu disiapkan desain sistemnya. Desain system sangat membantu dalam menentukan arsitektur system secara menyeluruh. Pada tahap ini akan dibuat desain pengimplementasian algoritma Rijndael dan RSA untuk proses enkripsi.
3. Pengkodean

   Pada tahap ini, peneliti akan mulai mengembangkan system dan menerapkan arsitektur system yang telah dirancang pada tahap 2.
4. Pengujian

Setelah system dikembangkan dalam tahap pengkodean, akan dilakukan pengujian menggunakan teknik randomness test. Seluruh system akan diuji untuk meninjau setiap kegagalan atau kesalahan.

5. Pengoperasian

   Tahap ini merupakan tahap akhir dalam model waterfall. Perangkat lunak yang sudah melewati tahapan-tahapan sebelumnya akan dioperasikan dan dilakukan pemeliharaan atau peninjauan kembali.

3.4 Fokus Penelitian

Adapun fokus penelitian yang akan dilakukan adalah sebagai berikut.

1. Memodifikasi algoritma Rijndael pada bagian S-Box dan ShiftRows
2. Membandingkan dua generator kunci yaitu Logistic Map dan Henon Map
3. Melakukan pengujian terhadap algoritma yang sudah dimodifikasi menggunakan randomness test.
4. Mengimplementasikan algoritma yang telah termodifikasi pada system live chat yang akan dibuat.
5. Pengujian keseluruhan system

3.5 Alat dan Data Penelitian

Berdasarkan kebutuhan-kebutuhan penelitian yang telah dianalisis oleh peneliti, maka dari itu akan ditentukan kebutuhan alat dan bahan yang akan digunakan pada penelitian ini.

3.5.1 Alat Penelitian

Untuk menunjang keberhasilan penelitian ini, peneliti membutuhkan alat bantu yang berupa perangkat keras maupun lunak. Perangkat keras yang digunakan oleh peneliti adalah komputer yang memiliki spesifikasi sebagai berikut:

1. Processor Intel i3.
2. RAM 4GB.
3. Hard disk 464 GB.
4. Mouse dan keyboard.

Adapun perangkat lunak yang digunakan adalah sebagai berikut:

1. System Operasi Microsoft Windows 7, 32-bit.
2. Sublime text
3. XAMPP v3.2.1
4. Chrome
5. Matlab R2013a
6. Cryptool 1.4.30

3.5.2 Data Penelitian

Salah satu penunjang keberhasilan penelitian ini adalah data penelitan yang akan digunakan. Data penelitian yang digunakan salah satunya adalah hasil penelitian yang telah dilakukan dan juga data yang didapat dari jurnal penelitian yang sudah pernah dilakukan(penelitian terkait, penelitian sebelumnya), buku, e-book, video tutorial dan data informasi lainnya yang didapatkan dari internet maupun perpustakaan mengenai live chat, algoritma Rijndael, RSA, key generator PRNG, prinsip Shannon dan fungsi hash SHA-256.