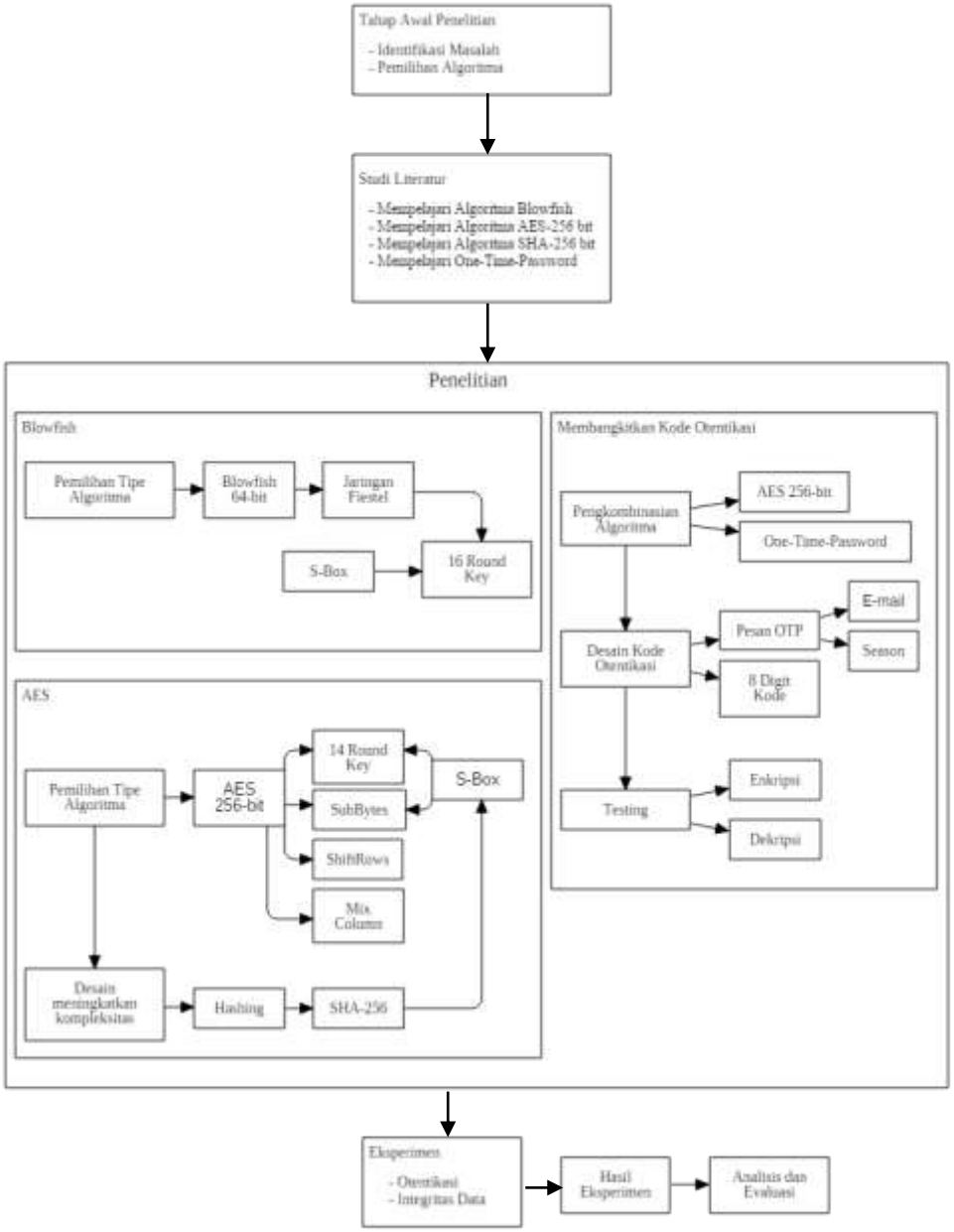
BAB III
METODE PENELITIAN

Pada bab ini akan dijelaskan mengenai metodologi penelitian, mulai dari desain penelitian, metode penelitian, alat penelitian dan data penelitian.

1.1 Desain Penelitian

Desain penelitian (Gambar 3.1) merupakan proses enkripsi dan dekripsi data menggunakan kombinasi algoritma AES dan algoritma blowfish.



Gambar 3.1 Desain Penelitian

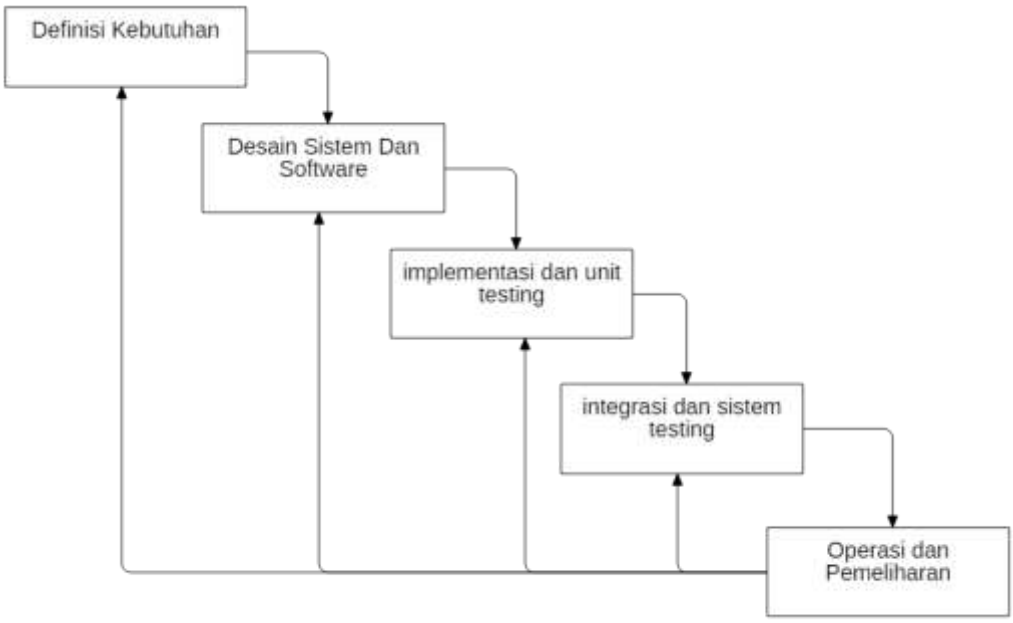
Penelitian yang akan dilakukan meliputi langkah-langkah berikut:

1. Identifikasi Masalah merupakan tahap awal dalam penelitianyang dapat membantu penentuan tujuan penelitian yang dilakukan, masalah dapat ditemukan dengan mengikuti isi-isi dan perkembangan teknologi saat ini, serta mempelajari penelitian yang sudah dilakukan dan dipublikasikan melalui jurnalF ilmiah. Dan pada masalah yang ditemukan pada identifikasi ialah ditemukannya pencurian data terhadap identitas para anggotanya.
2. Studi literatur merupakan tahapan mempelajari metode-metode yang akan digunakan pada penelitian, yaitu mempelajari tentang algoritma Blowfish, mempelajari algoritma AES-256, mempelajari algoritma SHA-256 untuk *hashing* terhadap kunci AES-256, dan mempelajari *One-Time-Password* baik melalui buku literature atau jurnal ilmiah.
3. Melakukan penelitian untuk keamanan data menggunakan kode otentikasi dengan memanfaatkan ilmu kriptografi.
    a. Penelitian pertama dilakukan untuk mengamankan data menggunakan algoritma Blowfish, dimana data tersebut akan di enkripsi dan disimpan didalam database, selain itu hasil enkripsi dari algoritma Blowfish akan dianalisis melalui tes *Randomness Test*.
    b. Penelitian yang kedua dilakukan untuk membangkitkan kode otentikasi, dimana kode otentikasi mengkombinasikan *uppercase*, *lowercase*, dan *number* akan di enkripsi oleh algoritma AES-356 ditambah dengan *One-Time-Password* sehingga kode memiliki jangka waktu pakai, kemudian hasil *One-Time-Password* ini memiliki 8 digit untuk dijadikan kode otentikasi.
4. Eksperimen yang dilakukan mengimplementasikan hasil penelitian dengan data .pdf dan .docx untuk data masukan. Data tersebut hanya bisa diunduh apabila user mempunyai kode otentikasi yang dikirimkan melalui email sebagai aksesnya.
5. Setelah ekperimen dilakukan hasilnya akan di analisis dan di evaluasi apakah pengamanan terhadap data menggunakan kode otentikasi dengan

menguji keacakan terhadap hasil enkripsi dan kunci yang telah di-*hashing*.

1.2 Metode Penelitian

Rancangan penelitian (Gambar 3.2) merupakan pedoman untuk melakukan penelitian dengan prinsip *waterfall* yang meliputi definisi kebutuhan, desain sistem dan software, implementasi dan unit testing, integrasi dan sistem testing, serta operasi dan pemeliharaan



Gambar 3.2 Model *Waterfall* (Sommerville, 2011)

1. Definisi kebutuhan, tahap dimana adanya analisis untuk kebutuhan, tujuan, analisis masukan dan analisis keluaran dari perangkat lunak yang diinginkan pada tahap ini dilakukan framework apa yang akan digunakan sebagai koding.
2. Desain sistem dan software, pada tahap ini merupakan proses perancangan yang melibatkan identifikasi dan menggambarkan sistem hubungan satu sama lain. Pada tahap ini dibuat desain dan implementasi algoritma yang digunakan
3. Implementasi unit dan testing, pada tahap ini desain sistem dan software dilakukan sebelum diimplementasikan dalam bentuk unit program. Setelah unit program dibuat, kemudian akan dilakukan testing

pada unit program untuk memastikan implementasi berjalan dengan baik.

4. Integrase dan sistem testing, setelah semua unit berhasil diimplementasikan dan berhasil lolos *testing* maka langkah selanjutnya mengintegrasikan semua unit untuk membentuk aplikasi. Aplikasi yang telah dibuat akan di tes kembali untuk memastikan unit program berjalan satu sama lain dalam aplikasi yang dibuat terhadap aplikasi.
5. Operasi dan perawatan

   Tahap ini merupakan tahap dimana aplikasi sudah diterapkan kemudian melakukan perbaikan apabila terjadi kesalahan atau *error* yang tidak ditemukan pada saat pengembangan aplikasi.

1.3 Alat Penelitian

Penelitian ini menggunakan seperangkap laptop yang dilengkapi perangkat lunak pendukung, dengan spesifikasi perangkat keras sebagai berikut:

1. Prosesor Intel® Core™ i5-2520M CPU @ 2.50 GHz
2. Kartu Grafis Intel® HD *Graphics* 3000
3. *Random Access Memory* (RAM) 4 GB
4. *Hard Disk Drive* 500 GB
5. Monitor 14 inci dengan resolusi 1366x768 piksel

Adapun perangkat lunak yang digunakan adalah:

1. *Sistem Operasi Mocrosoft Windows* 10 64-bit
2. *Sublime* 64-bit
3. PHP 7.0
4. Framework *Laravel*
5. Xampp v3.2.2

Alat-alat penelitian tersebut digunakan untuk mengembankan aplikasi yang nantinya akan digunakan untuk eksperimen, penciptaan studi kasus enkripsi dan dekripsi *file* menggunakan kombinasi algoritma *blowfish* sedangkan untuk pembuatan OTP hasilnya akan di enkripsi oleh algoritma AES-256 kemudian hasil dari enkripsi algoritma AES dikirimkan melalui e-mail. Tidak menutup

kemungkinan akan ada perubahan terkait perangkat keras dan lunak yang akan digunakan di dalam penelitian ini.

1.4 Data Penelitian

Data yang akan digunakan dalam penelitian ini diperoleh dengan pencarian *file* original yang cukup memadai untuk digunakan, pengambilan *file* yang merupakan berekstensi .docx dan .pdf akan digunakan dalam penelitian ini.

1.4.1 Data Masukan

Data yang digunakan sebagai masukan untuk penelitian ini adalah *file* pelamar pekerjaan yang alami *file* yang original yang tidak mengalami perubahan terhadap isinya). Dengan ketentuan ukuran *file* tidak dibatasi seberapa besar. Hal ini dilakukan agar performa proses enkripsi dan dekripsi dari aplikasi kombinasi algoritma ini masih dapat di evaluasi. Namun tidak menutup kemungkinan akan ada data masukan yang memiliki ukuran yang kecil.

1.4.2 Data Keluaran

Data keluaran dari eksperimen diharapkan berupa *file* yang terenkripsi oleh algoritma blowfish. Sehingga dapat di evaluasi dan dinilai lebih lanjut mengenai tingkat keamanan dan kecepatan dari kombinasi algoritma tersebut