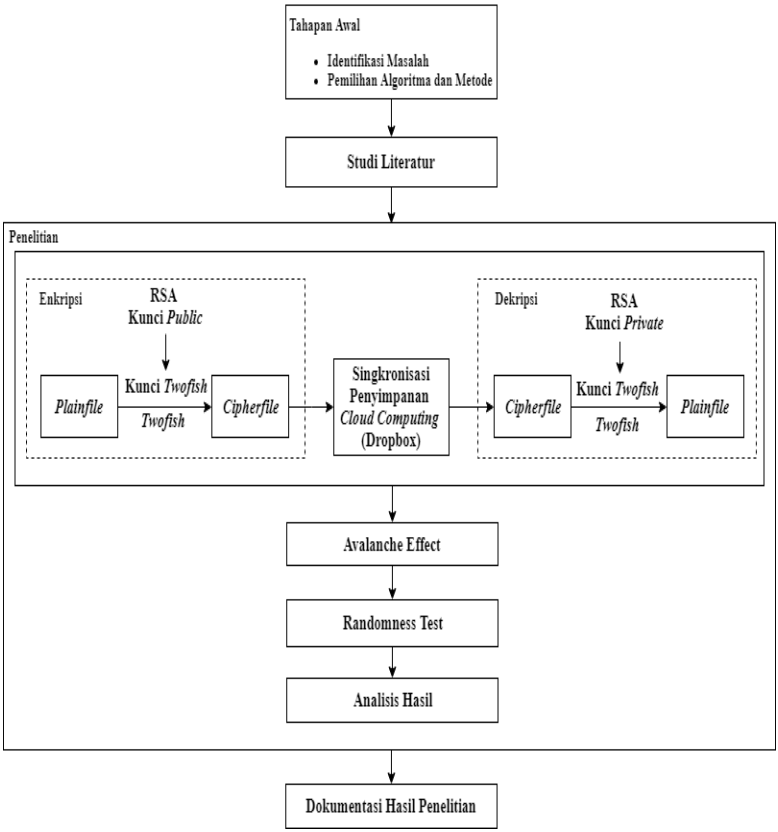
BAB III
METODE PENELITIAN

3.1 Desain Penelitian

Desain penelitian adalah tahapan atau gambaran yang akan dilakukan dalam penelitian. Desain dibuat untuk memberikan gambaran serta kemudahan dalam melakukan penelitian. Gambaran umum mengenai desain penelitian yang penulis lakukan dapat dilihat pada gambar 3.1



Gambar 3. 1 Desain Penelitian

Berikut merupakan penjelasan dari tahapan penelitian :

3.1.1 Tahap Awal

Tahap Awal merupakan penentuan penggunaan bahan terkait dengan penelitian yang dilakukan. Pada tahap ini akan dilakukan identifikasi masalah dan pemilihan algoritma dan metode untuk menyelesaikannya. masalah ditemukan dengan mengikuti isu-isu dan perkembangan teknologi saat ini, serta mempelajari penelitian yang sudah dilakukan dan dipublikasikan melaui jurnal ilmiah. masalah yang akan diteliti adalah bagaimana mengamankan data yang disimpan pada *cloud computing* karena keamanan data merupakan salah satu permasalahan pada *cloud computing*.Untuk menghindari pencurian atau kebocoran data pada penyimpanan cloud maka di terapkan sistem enkripsi hybrid cryptosystem. Algoritma yang akan dipakai adalah Algoritma *Twofish* dan RSA.

3.1.2 Studi literatur

Studi literatur merupakan tahapan mempelajari metode-metode yang akan digunakan pada penelitian, yaitu mempelajari *cloud computing*, kriptografi, hybrid cryptosystem, algoritma *Twofish*, algoritma RSA, pengujian *avalanche effect* dan randomness tess baik melalui buku literatur atau jurnal ilmiah.

3.1.3 Penelitian

Pada tahap ini, dilakukan penelitian dengan membuat unit program. Setelah unit program dibuat, kemudian dilakukan testing pada unit program tersebut untuk memastikan implementasi berjalan dengan baik. Pelaksanaan penelitian dilakukan dengan beberapa tahap, yaitu :

1. Pembuatan aplikasi enkripsi dekripsi *file* dengan menerapkan metode hybrid cryptosystem yang tersingkron dengan penyimpanan *cloud computing*. Pada saat menguplod *file* ke penyimpanan Dropbox *file* dienkripsi terlebih dahulu kemudian hasil dari enkripsi di upload kepenyimpanan Dropbox sedangkan pada saat mendownload *file*, *file* yang didownload akan didekripsi sehingga *file* kembali ke bentuk semula. Proses enkripsi dan dekripsi menggunakan *hybrid cryptosystem* algoritma *Twofish* dan RSA. Algoritma *Twofish* kunci simetri untuk enkripsi dan *file*. Sedangkan algoritma RSA kunci asimetri untuk enkripsi kunci *Twofish*.
2. *Avalanche effect*

Tahap ini menghitung *avalanche effect* dari algoritma *Twofish* dan RSA untuk melihat ketahanan algoritma *Twofish* dan RSA terhadap *cryptanalisys.*

3. *Randomness test*
   Tahap ini melakukan pengujian *randomness* terhadap ciphertext yang dihasilkan oleh algoritma *Twofish* dan RSA apakah menghasilkan ciphertext yang random atau tidak
4. Analisis hasil
   Pada tahap ini dilakukan analisis hasil dari penerapan *hybrid cryptosystem* algoritma *Twofish* dan RSA untuk mengamankan data yang tersimpan di *cloud computing*. Analisis yang dilakukan yaitu perubahan ukuran *file* sebelum dan sesudah dienkripsi, waktu yang dibutuhkan untuk enkripsi dan dekripsi serta analisis hasil dari *avalanche effect* dan *randomness test* dari algoritma *Twofish* dan RSA.

2.1.4 Dokumentasi Hasil Penelitian

Dokumentasi hasil penelitian yang berupa tulisan dalam bentuk dokumen teknis, jurnal, dan skripsi.

2.2 Flowchart Sistem

Flowchart adalah suatu bagan yang menggambarkan urutan proses secara detail dan hubungan antara satu proses dengan proses laiinya dalam suatu program. Berikut adalah flowchart dari aplikasi pengamanan *file* pada *cloud computing.*

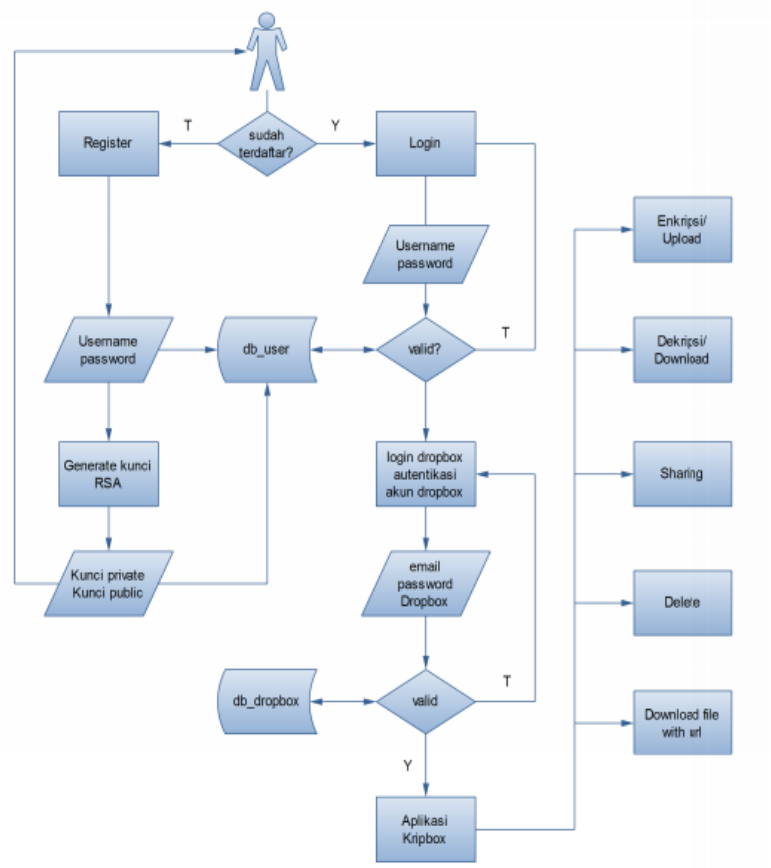
3.2.1 Flowchart Gambaran Umum Sistem

Gambar 3.2 menjelaskan gambaran umum sistem . Berikut penjelasannya :

1. User yang menggunakan aplikasi ini harus mendaftar terlebih dulu agar bisa login
2. Pada saat register user akan diberikan kunci private dan kunci publik RSA. Kunci publik ,username dan password disimpan di database aplikasi sedangkan kunci private hanya disimpan oleh user yang terdownload otomatis saat selesai melakukan register
3. Setelah melakukan register user bisa login ke aplikasi menggunakan username dan password yang telah di daftarkan.jika tidak valid user akan kembali ke halaman login dan jika valid maka akan ditampilkan halaman login Dropbox
4. Halaman login dropbox ini untuk autentikasi akun user dropbox yang akan di singkronkan ke aplikasi ini.jika valid maka akan

didapatkan token user yang digunakan untuk proses singkronisasi dan user masuk ke halaman dashboar aplikasi

5. Pada aplikasi user dapat melakukan upload *file* ke penyimpanan dropbox dengan di enkripsi terlebih dahulu,download dan dekripsi *file* yang tersimpan didropbox, sharing *file* melalui url, download *file* melalui url yang dibagikan dan delete *file* yang diingkan.

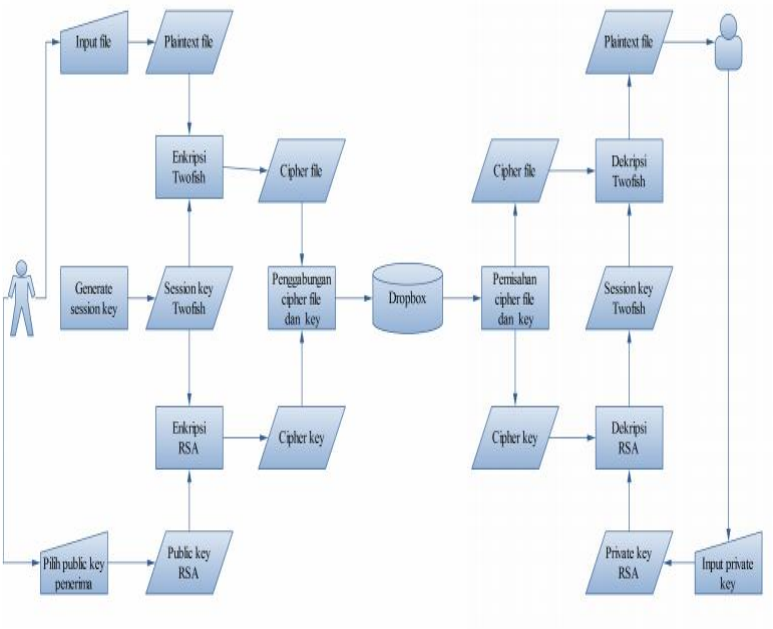


Gambar 3. 2 Flowchart Gambaran Umum Sistem

3.2.2 Flowchart Proses Enkripsi dan Dekripsi *File*

Pada penelitian ini, algoritma Enkripsi digunakan untuk mengamankan *file* Sedangkan algoritma RSA digunakan untuk

mengamankan kunci *Twofish*. Gambar 3.3 merupakan gambaran proses enkripsi dan dekripsi *file*.



Gambar 3. 3 Flowchart Proses Enkripsi dan Dekripsi *file* yang tersimpan di *Cloud Computing* Dropbox

2.3 Alat dan Bahan Penelitian

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

3.3.1 Alat Penelitian

Pada penelitian ini digunakan alat penelitian berupa perangkat keras dan perangkat lunak sebagai berikut:

a. Perangkat keras
   1. *Processor* Intel Core i5 4210U up to 2,7 GHz
   2. RAM 4GB
   3. *Harddisk* 1 TB
   4. Monitor 14’ HD (1366 x768).

5. *Mouse dan keyboard*

b. Perangkat lunak
   1. Sistem Operasi Microsoft Windows 8.1 64 bit
   2. Notepad++
   3. Xampp
   4. Dropbox
   5. Chrome
   6. Cryptool 1.4.30

3.3.2 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 *cloud computing*, kriptografi, *hybrid cryptosystem*, algoritma *Twofish* dan RSA, pengujian *avalanche effect* dan *randomness test.*