

BAB III METODOLOGI PENELITIAN

3.1 Tahapan Penelitian



Gambar 3.1 Tahapan Penelitian

Tahapan penelitian untuk perancangan sistem oleh penulis sebagai berikut :

3.1.1 Identifikasi Masalah

Pada tahapan ini peneliti mengidentifikasi masalah yang terjadi agar dapat memberikan solusi yang bermanfaat serta dapat menyelesaikan permasalahan. Merancang latar belakang perlunya penyelesaian permasalahan, merumuskan

permasalahan, mencari tujuan terselesaikannya sebuah masalah tersebut dan mendapat manfaat berdasarkan tujuan penelitian yang didapatkan.

3.1.2 Studi Literatur

Studi literatur dilakukan dengan pengumpulan bahan referensi tentang pengamanan data, dari buku-buku, jurnal dan penelitian tugas akhir sebelumnya yang dapat membantu peneliti untuk memecahkan masalah.

3.1.3 Analisa Kebutuhan Sistem

Analisis kebutuhan pada sistem yang akan dirancang penulis yaitu analisis kebutuhan masukan (*input*), analisis kebutuhan proses dan analisis kebutuhan hasil (*output*).

1. Analisis Kebutuhan *Input*

- a. *Input plaintext* berformat .txt yang akan dijadikan pesan rahasia untuk dilakukan proses enkripsi dengan 2 algoritma.
- b. *Input password* untuk dilakukan proses enkripsi dan dekripsi.
- c. *Input file* keluaran dari proses enkripsi yaitu *ciphertext* berformat .txt yang akan dilakukan proses penyisipan berupa *audio*.
- d. *Input penyisipan file* berupa *audio* yang berformatkan WAV.
- e. *File stego* berupa *audio* dilakukan proses hide yang berisikan pesan rahasia.

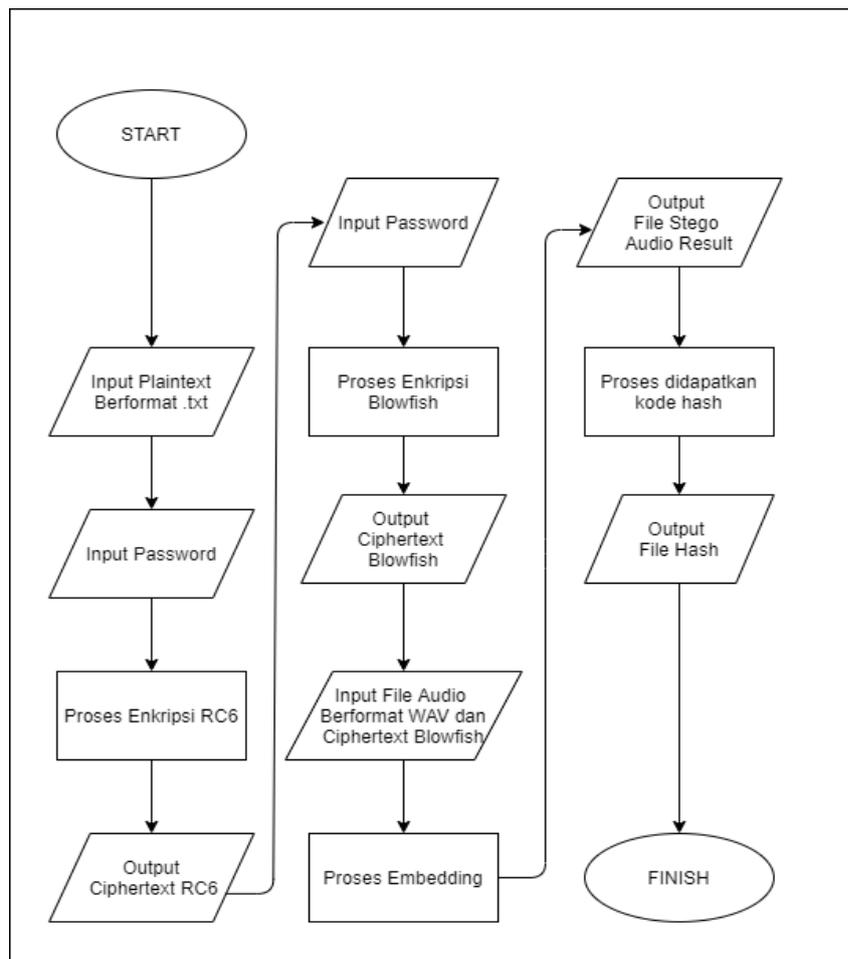
2. Analisis Kebutuhan Proses

- a. Proses enkripsi dilakukan dua kali karena menggunakan 2 algoritma yang berbeda.
- b. Proses enkripsi pesan asli menjadi *ciphertext* dengan memasukan *password* oleh pengirim pesan.
- c. Proses penyisipan pesan dengan menggunakan *ciphertext* dan media *audio* yang akan digunakan.
- d. Proses hash MD5 pada *file stego audio*.
- e. Proses pemisahan *audio result* yang akan menghasilkan file audio WAV dan *file ciphertext*.
- f. Proses dekripsi menggunakan *file ciphertext* hasil dari ekstraksi stego *audio* dan memerlukan *password* untuk proses dekripsi.

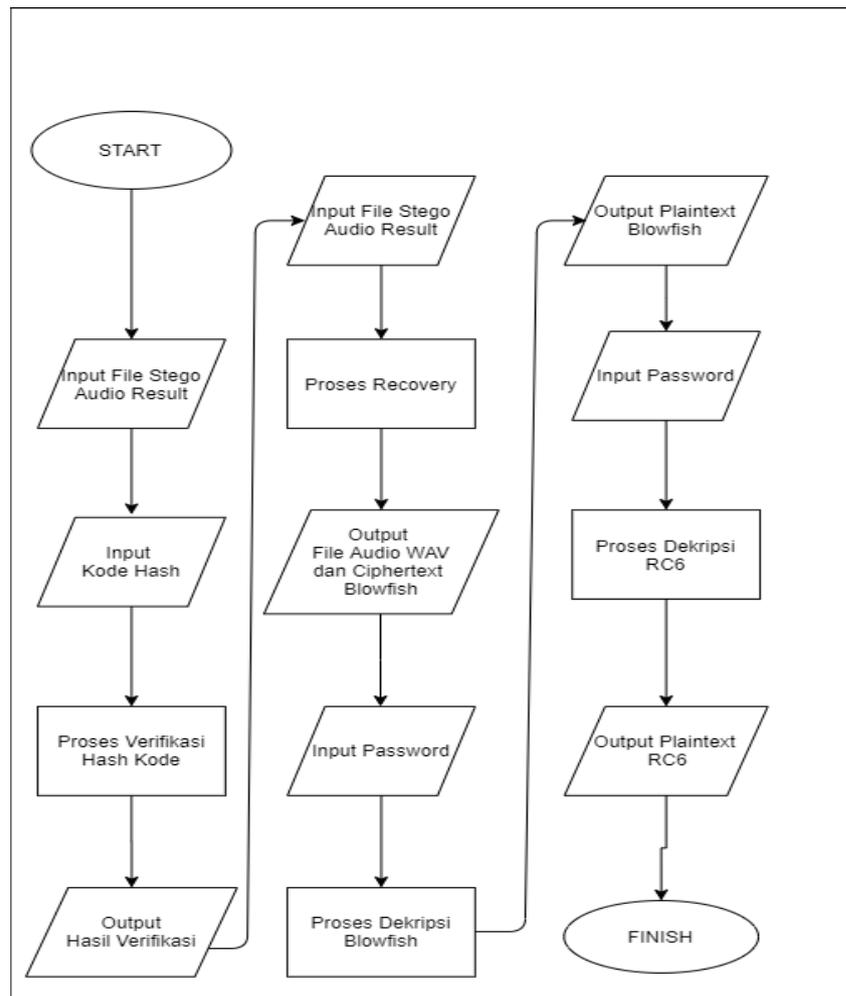
3. Analisis Kebutuhan *Output*

- a. Berkas *file* dari hasil proses enkripsi berupa *ciphertext* berformat .txt.
- b. Berkas *Audio* yang disisipkan dengan pesan rahasia berupa WAV.
- c. Kode hash yang dihasilkan dari proses hash MD5.
- d. *Plaintext* yang diperoleh pada proses dekripsi yang sebelumnya berupa *stego audio* sudah melalui proses *recovery* terlebih dahulu.

3.1.4 Perancangan Sistem



Gambar 3.2 Tahapan Enkripsi pada Sistem



Gambar 3.3 Tahapan Dekripsi pada Sistem

Pada gambar 3.2 menjelaskan tentang Tahapan Enkripsi pada sistem yang akan dibuat. Pada proses Enkripsi RC6, user menginputkan *plaintext* yang berformatkan .txt dan *password*, yang kemudian akan dilakukan proses enkripsi dan menghasilkan *ciphertext* RC6. Kemudian ke tahap selanjutnya yaitu proses Enkripsi Blowfish, dengan menginputkan *ciphertext* RC6 dan *password* setelah itu akan dilakukan proses enkripsi dan menghasilkan *ciphertext* blowfish, yang nantinya akan disisipkan dengan *file audio*. Terdapat proses steganografi, yaitu pada tahap Embedding, maka proses yang dilakukan yaitu menggabungkan *ciphertext* blowfish dengan *file audio* berformat WAV, kemudian dilakukan proses embedding. Pada proses embedding ini akan menghasilkan *output file stego audio* berformat WAV. Kemudian pada proses selanjutnya yaitu cek integritas data, yaitu Get Hash MD5. Tahap get hash MD5, prosesnya menginputkan *file stego audio*,

sehingga menghasilkan *output* kode hash untuk dilakukan verifikasi pesan untuk menjaga keaslian file stego audio.

Pada gambar 3.3 terdapat tahap dekripsi pada system. Pada proses ini dimulai dengan menginputkan *file* stego audio dan kode hash untuk dilakukan proses verifikasi. Dari proses tersebut dihasilkan keterangan jika pesan tersebut diterima secara utuh, akan menampilkan keterangan bahwa adanya kecocokan dengan *file* pesan asli. Tetapi jika pesan yang diterima tidak utuh, maka akan menampilkan keterangan tidak cocok, karena *file* tersebut berbeda dengan *file* pesan yang asli dan kembali ke proses menginputkan *file* hash. Proses selanjutnya yaitu Recovery, proses ini dilakukan untuk memisahkan *file* stego audio dan *ciphertext* blowfish. Kemudian ke tahap dekripsi blowfish, proses yang dilakukan yaitu menginputkan *ciphertext* blowfish, kemudian *input password* dekripsi dan akan dilakukan proses dekripsi. Maka *output* dari proses dekripsi blowfish adalah *plaintext* blowfish. Setelah itu, tahap terakhir yaitu dekripsi RC6 yang prosesnya akan menginputkan *plaintext* blowfish dan *password* dekripsi, lalu dilakukan proses dekripsi, dan menghasilkan *output plaintext* RC6.

3.1.5 Implementasi dan Evaluasi

Pada tahap implementasi lakukan langkah-langkah yang ada pada tahap sebelumnya, yaitu perancangan sistem. Apabila terdapat kekurangan atau kesalahan, sistem dapat dilakukan perbaikan dengan melakukan evaluasi sistem.

3.1.6 Pengujian

Tahap pengujian pada sistem dilakukan untuk membuktikan bahwa aplikasi yang dibangun sesuai dengan kebutuhan yang diperlukan. Pengujian sistem ini dapat ditinjau dengan proses kriptografi dan steganografi. Dengan penggabungan kedua proses ini, sistem akan lebih terjaga keamanannya. Pengujian pada kriptografi diperlukan hasil dari proses enkripsi yaitu *ciphertext*, dimana proses enkripsi tersebut dilakukan dua kali dengan algoritma yang berbeda.

Sedangkan pengujian pada steganografi dengan menggabungkan hasil enkripsi pada kriptografi yaitu *ciphertext* dengan *audio* WAV dan kemudian pengujian integritas data dengan hash MD5, supaya data atau pesan rahasia yang diuji tetap terjaga keutuhan dan keasliannya