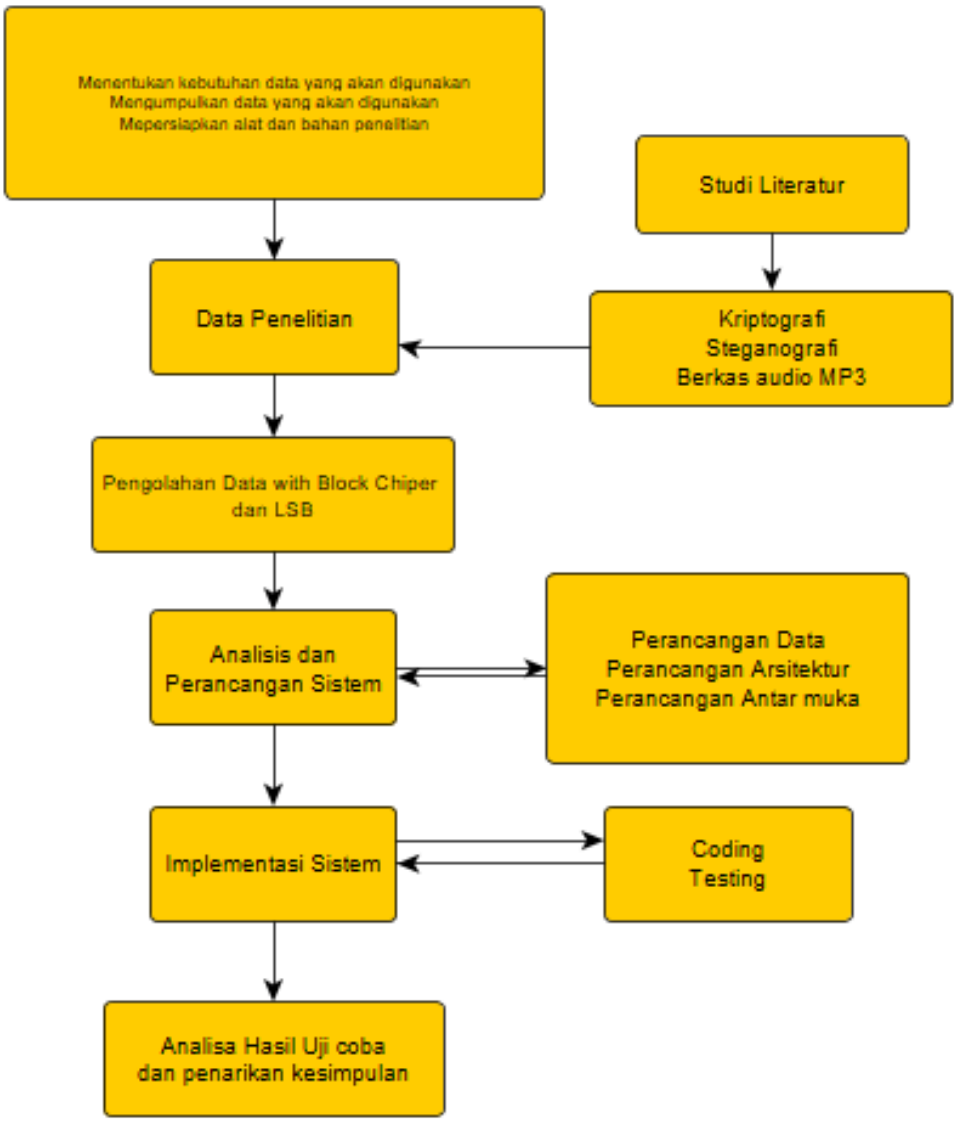
BAB III
METODOLOGI PENELITIAN

1.1. Desain Penelitian

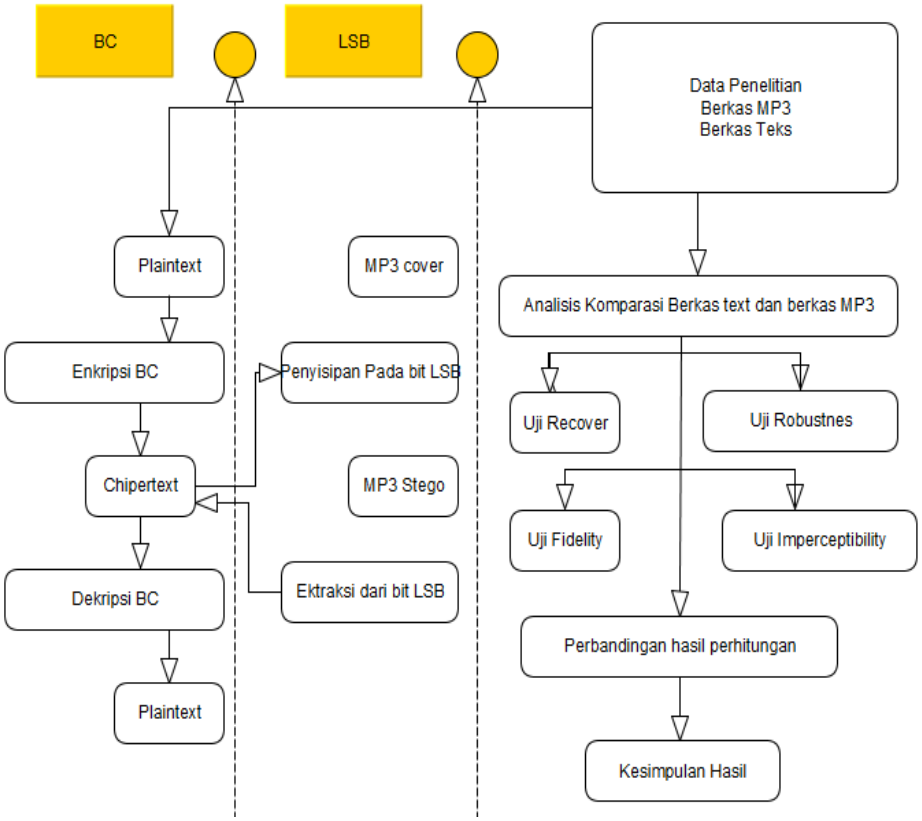
Berikut ini adalah desain penelitian yang akan digunakan pada proses implementasi algoritma *Block Cipher* pada audio steganografi berbasis MP3.



Gambar 3. 1 Desain Penelitian

Berikut ini adalah penjelasan dari tahapan desain penelitian:

1. Menentukan dan mengumpulkan kebutuhan data yang akan digunakan meliputi jumlah berkas MP3 maupun jenis berkas MP3 yang akan digunakan sebagai bahan penelitian.
2. Mempersiapkan alat dan bahan penelitian. Alat disini merupakan perangkat yang digunakan untuk membuat perangkat lunak, sedangkan bahan merupakan data-data yang telah dikumpulkan untuk digunakan sebagai bahan pembuatan penelitian ini.
3. Setelah data penelitian terkumpul, kemudian data penelitian tersebut digunakan untuk mengembangkan perangkat lunak dengan menggunakan metode pendekatan berorientasi objek dengan model proses sekuensial linear (*waterfall*).
4. Perangkat lunak yang dihasilkan kemudian digunakan untuk pengujian data yang hasilnya lalu dianalisa untuk ditarik kesimpulan akhir.



Gambar 3. 2 Diagram Proses Pengolahan Data

Berikut penjelasan tahapan-tahapan proses pada gambar 3.2 diatas:

1. Tahapan Audio Steganografi Block Cipher MP3 dimulai dengan proses penentuan data penelitian berupa berkas teks dan berkas MP3.
2. Tahapan Analisa Komparasi Berkas Teks dan Berkas MP3

   Pada tahapan ini dilakukan penelitian mengenai uji recover, uji fidelity, uji imperceptibility dan uji robustness. Hasil dari pengujian tersebut lalu dianalisa untuk diambil kesimpulan akhir.
3. Tahapan pada bagian Block Cipher

   Pada tahapan ini dijelaskan mengenai proses enkripsi plainteks menggunakan algoritma Block Cipher hingga menjadi cipherteks. Terdapat 2 proses utama di dalam algoritma Block Cipher, yaitu pembuatan subkunci dan enkripsi data. Proses pembuatan subkunci di dalam algoritma Block Cipher adalah sebagai berikut:

   A. Round Function

Pada round function akan dilakukan beberapa proses diantaranya adalah pertukaran blok, rotasi, XOR, dan subtitusi dengan mengunakan S-Box. Alur yang digunakan pada round function adalah sebagai berikut :

1. Pertukaran byte

   pertukaran byte dilakukan dengan menukarkan suatu byte dengan bit yang berada di sampingnya. Byte yang sudah ditukar tidak diproses lagi. Contohnya pada blok berukuran 8 byte berikut:

10	fa	6b	10	00	ff	5c	6b

Setelah dilakukan pertukaran bit, maka blok akan menjadi seperti berikut:

fa	10	10	6b	ff	00	6b	5c

2. Lakukan XOR antara blok dengan kunci

3. Rotasi blok

Rotasi blok akan dilakukan dengan menggeser blok ke kanan sebanyak satu kali secara siklik. Misalkan pada blok dengan 8 bit berikut :

10	fa	6b	10	00	ff	5c	6b

Setelah dilakukan pergeseran, maka blok akan menjadi seperti berikut:

6b	10	fa	6b	10	00	ff	5c

4. Substisusi dengan S-Box

Substitusi blok akan dilakukan dengan menggunakan S-Box sehingga menghasilkan blok yang lebih teracak. S-Box dibangun secara acak dengan bantuan kakas random.org. Berikut adalah S-Box yang penulis gunakan pada algoritma ini:

```
8a f6 a9 51 12 b7 0e 83 54 53 06 2e e7 9d 3f f1
3e a9 1e e0 de e2 b8 eb 1b 48 0c 17 63 b2 b5 c2
49 e3 c5 e2 25 f0 f9 50 26 e9 1d ad fb ed bb 7f
0b 78 96 8b e3 e7 7f eb 2a 1f 62 58 f1 e5 df 73
fd df 4e b7 8a aa c0 03 f2 6a ea 0f 17 19 20 b3
35 ef 73 fb 46 fe 31 33 5f 42 a0 92 ee 6e 22 e1
99 f7 42 e7 bf 71 e0 7e ed 17 1e 88 d7 04 4c 0e
3c 96 ac cc 69 a9 43 53 b6 b4 76 f3 35 81 84 9c
bd 78 49 f8 c4 33 83 23 d7 75 39 f3 bc 4f 2d 95
75 c0 bd 9c 00 ff 26 a7 7e 78 af 49 58 56 c3 a8
36 b0 54 ac 1f a3 f7 f0 bb 63 e7 6d 04 12 84 dc
2d 91 89 1a cb 39 ed 85 0a 76 53 61 8c 74 0c 4d
f3 ac 7f 74 32 2e 7a ad 48 eb b3 9c 8e a7 7c dd
c8 cf 5e 78 6f 12 f4 72 58 f1 ff b3 d7 d9 90 64
84 48 8a 81 23 c5 11 1c eb be 44 5a 07 70 88 99
2e 5f a7 65 85 1f a1 d1 9c 68 7f 36 43 aa c4 cc
```

Gambar 3. 3 S-Box

5. Lakukan XOR kembali antara blok dengan kunci

C. Key Schedule

Pembangkitan kunci internal dilakukan dengan menggeserkan byte kunci ke kanan sebanyak perputaran jaringan feistel. Jika jaringan feistel berada pada perputaran pertama, maka kunci yang akan digunakan adalah kunci hasil pergeseran ke kanan sebanyak satu pergeseran, jika jaringan feistel berada pada putaran ke dua, maka kunci yang digunakan adalah

kunci hasil pergeseran ke kanan sebanyak 2 pergeseran. Hal yang sama dilakukan juga pada putaran berikutnya.

Setelah proses pembuatan subkunci selesai, masuk ke dalam proses enkripsi seperti yang digambarkan pada gambar 2.4. Data cipherteks ini yang kemudian disisipkan menggunakan metode Low Bit Coding. Lalu pada proses ekstraksi MP3, bit-bit LSB yang diekstraksi didekripsi kembali menggunakan algoritma Block Cipher untuk didapatkan pesan awal yang disisipkan.

1. Tahapan pada bagian Low Bit Coding

   Pada tahapan ini dilakukan proses penyisipan pesan terenkripsi (cipherteks) ke dalam berkas MP3 pada bagian bit-bit yang paling tidak berpengaruh (LSB).

1.2. Metode Penelitian

Metode penelitian yang digunakan pada penyusunan skripsi ini yaitu:

1.2.1. Metode Pengambilan Data

Penulis berusaha untuk mengumpulkan data dan informasi akurat yang mampu menunjang proses penelitian. Adapun metode pengumpulan data yang dilakukan tersebut adalah:

a. Eksplorasi dan Studi Literatur

Eksplorasi dan studi literatur dilakukan dengan mempelajari konsep-konsep yang berkaitan dengan penelitian ini, seperti teori tentang teknik steganografi, metode-metode dalam steganografi, teknik enkripsi maupun struktur berkas audio melalui literatur-literatur seperti

buku (textbook), paper, dan sumber ilmiah lain seperti situs internet ataupun artikel dokumen teks yang berhubungan.

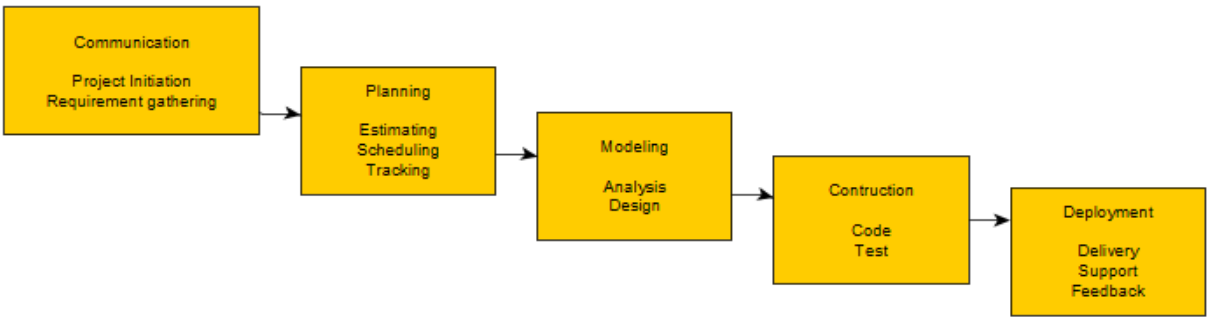
1.2.2. Metode Pengembangan Perangkat Lunak

1.2.2.1. Metode Pendekatan Pengembangan Perangkat Lunak

Metode pendekatan perangkat lunak yang digunakan pada penelitian ini adalah metode pendekatan berorientasi objek. Metode pendekatan perangkat lunak berorientasi objek adalah sebuah pendekatan pengembangan perangkat lunak yang komponen-komponennya dienkapsulasi menjadi kelompok data dan fungsi yang dapat mewarisi sifat dan atribut dari komponen lainnya serta terdapat interaksi diantara komponen-komponen tersebut. Proses pemodelan dan perancangan yang digunakan pada metode berorientasi objek ini adalah UML (*Unified Markup Language*).

1.2.2.2. Model Proses Pengembangan Perangkat Lunak

Model proses yang digunakan dalam penelitian ini adalah model *waterfall* atau dikenal juga dengan model proses sekuensial linear. Model *waterfall* merupakan sebuah model pengembangan perangkat lunak yang sistematik dan sekuensial atau berurutan mulai dari proses *communication*, *planning*, *modeling*, *construction* hingga proses *deployment*. Berikut ini merupakan tahapan dalam model *waterfall*:



Gambar 3. 4 Model Waterfall (Sekuensial Linear) *(Sumber: Pressman, Roger S.* Software Engineering: A Practitioner's Approach, Seventh Edition. *2010:* chapter *2-39)*

1. *Communication*

Tahapan awal dari proses pengembangan perangkat lunak ini menitikberatkan pada proses pengumpulan informasi dari setiap pihak yang terlibat (*stakeholder*). Pendefinisian target, masalah, dan batasan sistem merupakan bagian dari tahapan ini. Pada tahapan ini juga ditentukan kebutuhan-kebutuhan apa saja yang harus dipenuhi oleh perangkat lunak yang akan dikembangkan.

2. *Planning*

Pada tahapan planning didefinisikan mengenai aktivitas-aktivitas manajerial dan teknis yang diperlukan untuk mencapai tujuan pengembangan perangkat lunak. Aktivitas tersebut diantaranya adalah *estimating*, *scheduling* dan *tracking*. Pada tahapan ini dihasilkan *road map* yang dijadikan panduan dalam aktivitas pengembangan perangkat lunak.

3. *Modeling*

Tahapan *modeling* terdiri dari aktivitas analisis dan desain. Proses analisis dilakukan untuk menentukan fitur-fitur apa saja yang akan dikembangkan dan data apa saja yang dibutuhkan dalam pengembangan perangkat lunak. Proses desain meliputi aktivitas perancangan data, perancangan antar muka hingga arsitektur perangkat lunak. Tahapan ini dilakukan agar dihasilkan sebuah model yang representatif dari perangkat lunak yang akan dikembangkan.

4. *Construction*

Pada tahapan ini dilakukan proses pengimplementasian dari hasil perancangan yang sudah dilakukan. Proses *coding* menerjemahkan hasil perancangan kedalam bahasa pemrograman yang dipahami oleh komputer. Pada tahapan ini pula dilakukan *testing* yakni pengujian terhadap perangkat lunak yang sudah dikembangkan untuk memastikan bahwa semua kebutuhan sudah diimplementasikan dan berfungsi sebagaimana mestinya.

5. *Deployment*

Pada tahapan akhir ini perangkat lunak yang sudah dikembangkan dikirimkan kepada pengguna untuk digunakan dan pengguna memberikan umpan balik (*feedback*) dari hasil evaluasi atau penggunaan perangkat lunak tersebut.

1.3. Alat dan Bahan Penelitian

1.3.1. Alat Penelitian

Pada penelitian ini menggunakan alat penelitian berupa perangkat keras dan perangkat lunak, yaitu:

1. Perangkat keras
    a. *Processor* AMD E-350 1.6 Ghz
    b. RAM 3 GB
    c. *Harddisk* 320 GB
    d. *Display* beresolusi 1366 x 768 px
    e. *Mouse* dan *keyboard*
2. Perangkat lunak
    a. Windows 10
    b. yEd Graph Editor

c. Php Native

d. wxHexEditor v 0.23

1.3.2. Bahan Penelitian

Bahan penelitian yang dibutuhkan pada penelitian ini adalah beberapa berkas audio MP3 yang akan disisipi pesan dan juga dijadikan bahan pada proses pengujian. Penulis menggunakan berkas MP3 yang banyak tersedia di jaringan internet setelah terlebih dahulu memilah sesuai dengan kebutuhan penelitian