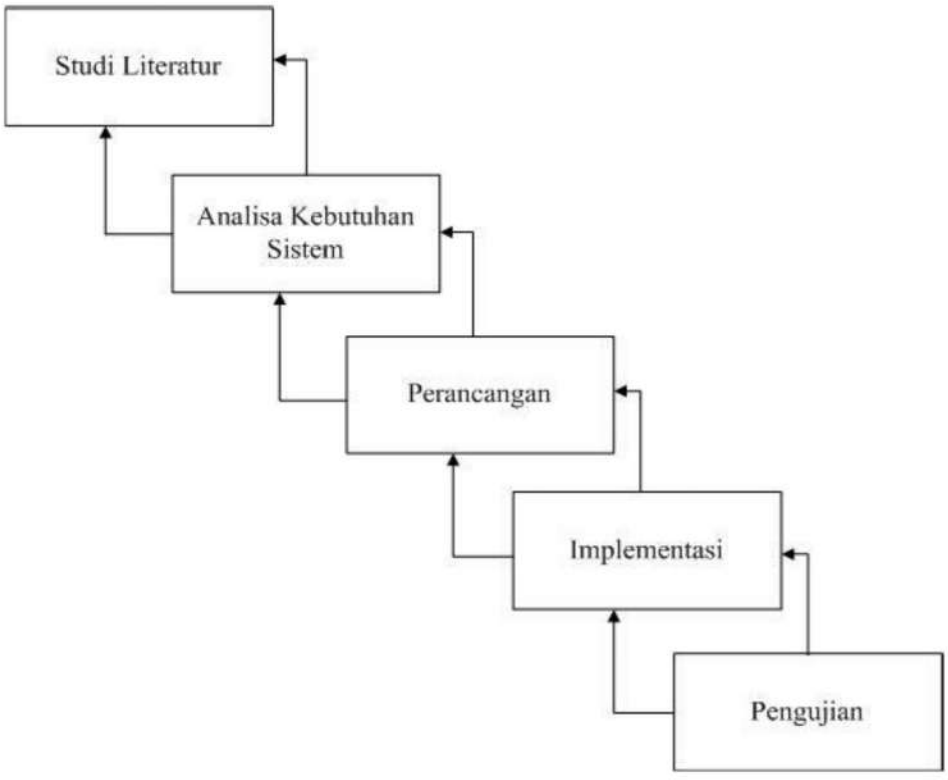
BAB III. METODOLOGI PENELITIAN

Dalam bab ini akan dijelaskan mengenai langkah-langkah yang akan membimbing penulis dalam memilih metode, teknik, prosedur, dan tools apa saja yang digunakan sehingga tiap tahap penelitian dapat dilakukan dengan tepat. Beberapa uraian yang ada di dalam metodologi penelitian antara lain metode pengambilan data dan metode pengembangan sistem. Dalam metode penelitian ini, akan dijelaskan langkah-langkah yang dilakukan untuk Rancang Bangun Alpikasi Desain dan Implementasi Algoritma Kriptografi RSA pada Telkom Bojonegoro untuk Meningkatkan Keamanan Sistem Jaringan sebagai berikut:

3.1 Metode Perancangan Sistem

Metode yang digunakan dalam perancangan aplikasi ini menggunakan Metode *Waterfall* atau Metode Air Terjun. Adapun tahapan-tahapan dalam Metode *Waterfall* ini dapat dilihat pada gambar 3.1:



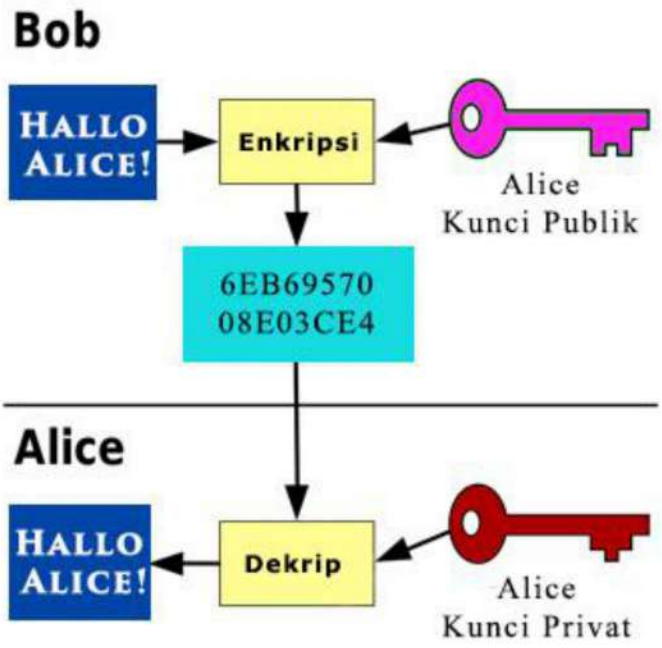
Gambar 3. 1 Metode Perancangan Sistem

3.2 Studi Literatur

Pada tahap ini penulis melakukan analisis dengan menggunakan studi keamanan informasi dan komunikasi data menggunakan kriptografi dengan algoritma enkripsi

RSA berdasarkan sumber dari artikel, jurnal, serta *e-book* dari internet yang akan di implementasikan pada sistem komunikasi untuk Telkom Bojonegoro.

Berdasarkan buku yag berjudul "Kriptografi Untuk Keamanan Jaringan" menjelaskan tentang konsep sistem kriptografi kunci publik di mana kunci-kunci yang berbeda digunakan untuk enkripsi dan dekripsi, Berikut Proses aplikasi *file transfer* yang mengamankan data-data penting atau *Critical Data* dengan menarapkan Enkripsi yang di implementasikan menggunakan algoritma kriptografi RSA pada program Berbasis *file transfer* pada jaringan *client server* dapat dilihat pada gambar 3.2:



Gambar 3. 2 *Requiremen*

Gambar 3.2 menjelaskan tentang *Plaintext* yang di kirim kepada Alice akan di enkrisi menggunakan kunci publik kemudian menghasilkan *cyper text* yang merupakan data yang telah di sandikan atau secara acak. Kemudian *cyper text* di kirimkan dan di dekrip menggunakan kunci privat pada node pengguna yang terkirim kepada Alice yang mempunyai kunci privat tersebut. Pada intinya, yang bisa membuka hanya pihak terkirim atau Alice.

3.3 Analisa Kebutuhan Sistem

Pada tahap ini implementasi dilakukan pengujian aplikasi kepada *user* untuk mengetahui apakah Sistem ini dapat benar dapat mengamankan *data critical* atau data penting yang akan di kirimkan ke sistem komunikasi yang ada di Telkom Bojonegoro.

3.4 Perancangan

Pada tahap ini menjelaskan bagaimana meningkatkan keamanan informasi dan komunikasi data menggunakan kriptografi dengan algoritma enkripsi Rsa pada protocol FTP yang memiliki kerentanan terhadap pihak yang tidak berkepentingan mendapatkan informasi maka akan dilakukan penambahan metode RSA sebelum melewati protocol FTP atau sebelum proses upload data akan di enkripsi.

3.5 Implementasi

Pada tahap ini, penulis akan menerapkan algoritma kriptografi RSA pada sistem aplikasi berbasis *file* transfer berdasarkan desain sistem yang telah di buat pada Desain dan Implementasi Algoritma Kriptografi RSA pada Telkom Bojonegoro Untuk Meningkatkan Keamanan Sistem Jaringan.

3.6 Pengujian

Pada tahapan ini dimana sistem diuji kemampuan dan ke efektifannya sehingga didapatkan kekurangan dan kelemahan sistem yang kemudian dilakukan pengkajian ulang dan perbaikan terhadap aplikasi menjadi lebih baik lagi.