

BAB III METODE PENELITIAN

3.1 Tempat dan Waktu Penelitian

Tempat penelitian merupakan objek dimana peneliti melakukan penelitian guna untuk memperoleh data-data yang diperlukan. Waktu penelitian merupakan rincian mengenai jadwal pelaksanaan penelitian. Tempat dan waktu penelitian dapat dijelaskan pada sub bab selanjutnya.

3.1.1 Tempat Penelitian

Tempat penelitian dan pengumpulan data tidak terikat karena didasarkan dari pengujian karena sifat penelitian ini menggunakan rancang bangun sistem, yaitu kegiatan menerjemahkan hasil analisis kedalam bentuk perangkat lunak yang kemudian menciptakan atau memperbaiki sistem yang sudah ada.

3.1.2 Waktu & Jadwal Pelaksanaan Penelitian

Waktu yang digunakan untuk penelitian ini dilaksanakan sejak tanggal dikeluarkannya izin penelitian.

Tabel 3.1 Jadwal Pelaksanaan Penelitian

No.	Jenis Kegiatan	Waktu Kegiatan																			
		Oktober 2022				November 2022				Desember 2022				Januari 2023				Februari 2023			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Identifikasi Masalah	■	■	■	■																
2.	Pengajuan Judul			■	■	■	■														
3.	Penyusunan Proosal				■	■	■	■													
4.	Bimbingan Proposal						■	■	■	■											
5.	Seminar Proposal										■	■	■								

2. *Microsoft Office Word 2010* digunakan untuk membantu pembuatan penulisan laporan skripsi.
3. *Microsoft Office Visio 2007* digunakan untuk membantu pembuatan rancangan sistem.
4. *PHP, HTML, dan Javascript* sebagai bahasa pemrograman untuk membuat aplikasi *web*.
5. *XAMPP* sebagai *tools* untuk mengontrol *web server apache*.
6. *Framework Bootstrap5* sebagai *library CSS (Cascading Style Sheets)* untuk membantu dalam mendesign tampilan aplikasi *web*.
7. *Visual Studio Code* sebagai teks editor untuk menulis *coding program*.
8. *Google Chrome* sebagai *web browser* untuk menjalankan plikasi *web*.

3.3 Cara Kerja

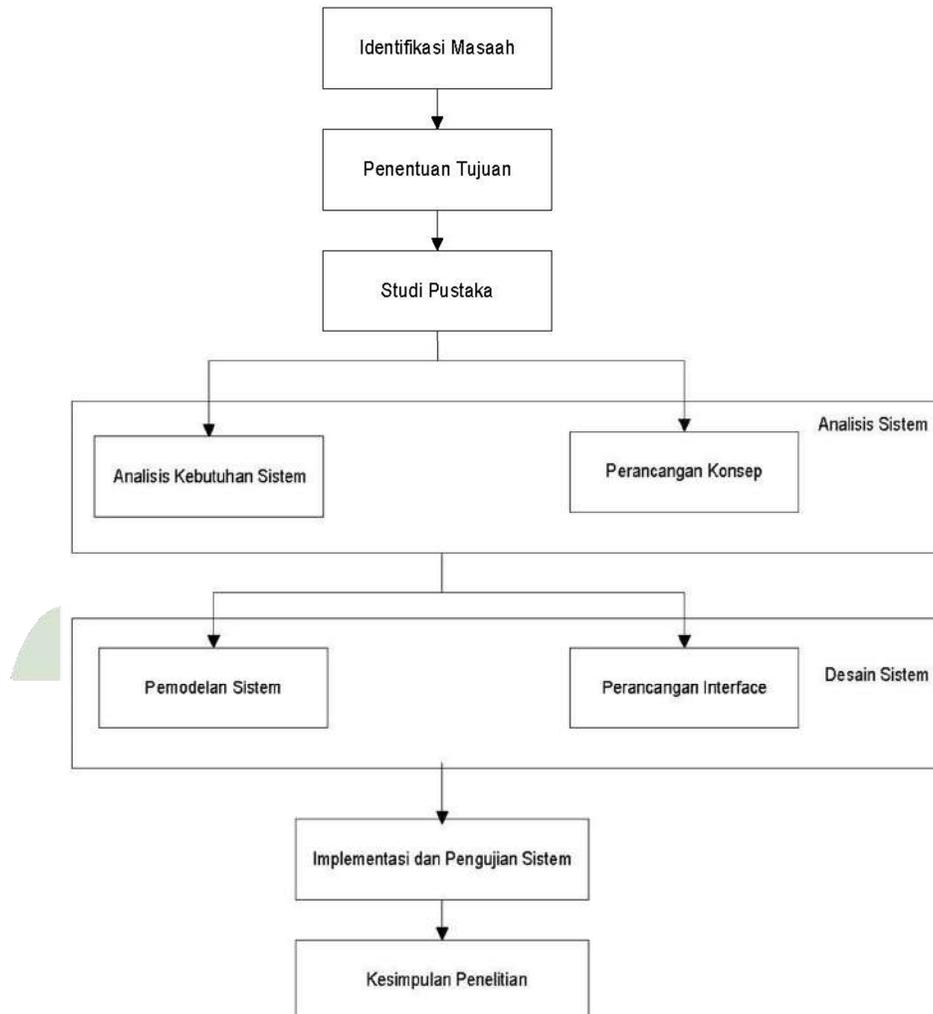
Cara kerja merupakan tahapan yang dilakukan dalam penelitian, yang mana tahapan ini akan dibahas mengenai perencanaan dalam penelitian, teknik pengumpulan data yang digunakan dalam penelitian, analisis kebutuhan sistem, perancangan sistem serta pengujian sistem. Rincian dari cara kerja penelitian dapat dijelaskan pada sub bab selanjutnya.

3.3.1 Perencanaan

Dalam mendukung jalannya penelitian terkait dengan pengamanan data pada *file* teks menggunakan teknik kriptografi super enkripsi agar lebih terarah dan sistematis, maka dibutuhkan suatu tahapan perencanaan penelitian yang disusun dengan baik. Adanya tahapan ini juga dapat memudahkan dalam melakukan penulisan proposal penelitian. Perencanaan merupakan tahapan yang dilakukan dalam penelitian, yang mana tahapan ini bertujuan untuk memberikan ketentuan bentuk masalah dan tujuan.

Dalam proses perencanaan ada beberapa hal yang akan dilakukan yaitu identifikasi masalah, penentuan tujuan penelitian, studi pustaka, analisis sistem, desain sistem, implementasi dan pengujian sistem dan kesimpulan penelitian.

Adapun tahapan-tahapan yang dilakukan pada penelitian ini dapat dilihat pada gambar 3.1.



Gambar 3.1 Tahapan Penelitian

Berdasarkan gambar 3.1, berikut merupakan keterangan mengenai tahapan penelitian yaitu sebagai berikut:

1. Identifikasi Masalah

Tahap identifikasi masalah merupakan tahap awal dan persiapan dari sebuah penelitian. Pada tahap ini penulis mengidentifikasi apa-apa saja yang menjadi permasalahan dan mengambil permasalahan tersebut menjadi topik penelitian sehingga penulis dapat mencari solusi yang nantinya akan menjadi tujuan dari

penelitian ini. Permasalahan yang diangkat dalam penelitian ini terkait dalam hal meningkatkan keamanan data pada *file* teks. Keamanan dan kerahasiaan sebuah informasi pada *file* teks merupakan hal yang sangat penting untuk dilakukan, terutama informasi sensitif atau pribadi yang hanya boleh diakses oleh pihak yang berhak saja, baik pada saat disimpan dalam media penyimpanan (*hard drive*) ataupun pada saat akan dikirimkan. Salah satu cara yang dapat dilakukan untuk mengamankan informasi tersebut adalah dengan teknik kriptografi. Dalam penelitian ini, akan menggabungkan teknik kriptografi dalam skema super enkripsi dengan menerapkan kombinasi algoritma kriptografi simetris *Beaufort Cipher* dan algoritma asimetris RSA. Identifikasi masalah merupakan bentuk pernyataan atau pertanyaan yang jelas mengenai penelitian.

2. Penentuan Tujuan

Penentuan tujuan ini memperkuat tentang perlunya dilaksanakan suatu penelitian sehingga pemecahan masalah yang diuraikan pada perumusan masalah dapat dicapai setelah penelitian selesai dilakukan. Setelah masalah ditentukan, maka penulis menentukan tujuan dari penelitian ini, yaitu untuk menyelesaikan masalah yang ada dengan membuat sebuah aplikasi yang dapat digunakan untuk mengamankan data pada *file* teks dengan teknik super enkripsi menggunakan kombinasi algoritma simetris *Beaufort Cipher* dan algoritma asimetris RSA.

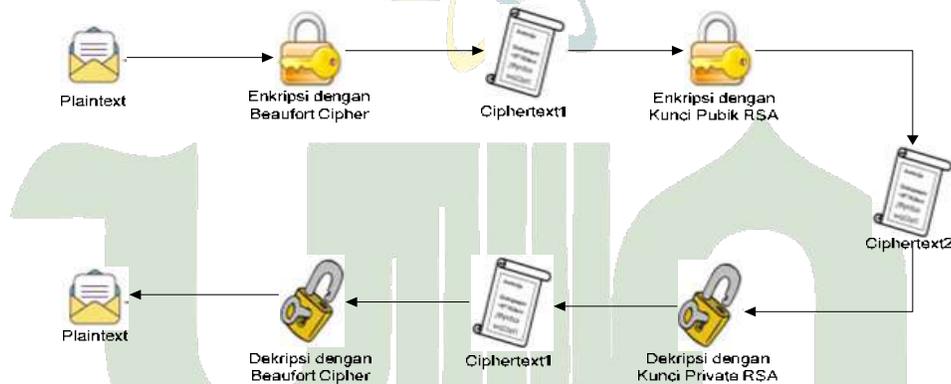
3. Studi Pustaka

Studi pustaka merupakan hal yang mendukung sebagai landasan teori penelitian dalam membahas penelitian yang sedang dilakukan. Studi pustaka dilakukan untuk mendapatkan berbagai informasi yang relevan terkait dengan penelitian yang akan dilakukan dengan cara *browsing* di *internet*, membaca berbagai literatur seperti buku dan jurnal, hasil kajian dari penelitian terdahulu, catatan perkuliahan, serta sumber-sumber lain yang relevan dengan pokok permasalahan pada penelitian ini.. Informasi tersebut antara lain terkait dengan algoritma *Beaufort Cipher*, algoritma RSA, dan penelitian-penelitian

sebelumnya terkait dengan penelitian yang dilakukan. Hasil dari kajian pustaka yang telah dilakukan dapat dilihat pada bagian tinjauan pustaka.

4. Analisis Kebutuhan Sistem dan Perancangan Konsep

Sebelum merancang sebuah sistem, tahapan yang terlebih dahulu harus dilakukan adalah dengan menganalisis sistem yang ingin dibuat. Analisis sistem yang dibahas mencakup kebutuhan fungsional sistem dan kebutuhan non fungsional. Setelah melakukan analisis sistem, langkah selanjutnya adalah melakukan perancangan konsep pengamanan data pada *file* teks. Konsep pengamanan akan menggunakan perpaduan antara algoritma *Beaufort Cipher* dan algoritma RSA. Konsep pengamanan tersebut dapat dilihat lebih lanjut pada gambar 3.2.



Gambar 3.2 Arsitektur Umum Sistem

Pada gambar 3.2, terlihat bahwa terdapat 9 tahapan dalam melakukan proses enkripsi dengan memanfaatkan algoritma *Beaufort* dan RSA. Langkah pertama diawali dengan menentukan *plaintext* atau data berupa teks yang akan diacak melalui proses enkripsi. Pada tahap ini juga harus ditentukan kunci yang akan digunakan dalam proses enkripsi. Langkah selanjutnya merupakan proses enkripsi tahap pertama dengan menggunakan algoritma *Beaufort Cipher*. Hasil dari proses enkripsi ini berupa *ciphertext1*, yang akan mengalami proses enkripsi lagi dengan menggunakan algoritma RSA dan akan menghasilkan berupa *ciphertext2*. Untuk mendekripsi maka tahap pertama dengan menggunakan algoritma RSA sehingga menghasilkan *ciphertext1*,

yang akan mengalami proses dekripsi lagi dengan menggunakan algoritma *Beaufort Cipher* sehingga diperoleh pesan asli berupa *plaintext*.

5. Desain Sistem

Tahapan desain sistem dilakukan untuk mendapatkan gambaran yang jelas tentang apa yang dikerjakan pada analisis sistem dan dilanjutkan dengan mempertimbangkan bagaimana membentuk sistem tersebut. Perancangan sistem dilakukan dengan membuat *flowchart* sistem dan tampilan *interface* (antarmuka) sistem yang akan diintegrasikan dengan aplikasi pada tahap implementasi sistem.

6. Implementasi dan Pengujian Sistem

Pada tahap ini akan dilakukan pengkodean (*coding*) yang mengacu pada perancangan sistem yang telah dibuat sebelumnya dengan menggunakan *PHP*, *HTML*, dan *Javascript* sebagai bahasa pemrograman untuk membuat aplikasi *web*. Selanjutnya melakukan pengujian terhadap sistem yang telah dirancang apakah sistem tersebut berjalan sesuai dengan yang diharapkan. Metode pengujian yang digunakan adalah *black box*, yaitu sebuah metode yang digunakan untuk mendemonstrasikan fungsional aplikasi saat dioperasikan, apakah *input* diterima dengan benar dan *output* yang dihasilkan telah sesuai dengan yang diharapkan.

7. Kesimpulan Penelitian

Langkah terakhir dari penelitian adalah melakukan penarikan kesimpulan terhadap hasil dari penelitian yang telah dilakukan yang menjawab tujuan akhir dari penelitian berdasarkan hasil analisis data sampai pengujian sistem yang telah dilakukan.

3.3.2 Teknik Pengumpulan Data

Metode pengumpulan data digunakan untuk memperoleh data yang dapat mendukung permasalahan yang akan dibahas. Sehubungan dengan hal ini maka digunakan metode pengumpulan data yang meliputi:

1. Studi Pustaka

Pengumpulan data melalui metode ini diperoleh dengan *browsing* di *internet*, membaca berbagai literatur seperti buku dan jurnal, hasil kajian dari penelitian terdahulu, catatan perkuliahan, serta sumber-sumber lain yang relevan dengan pokok permasalahan pada penelitian ini.

2. Observasi

Observasi dilakukan untuk tahapan pengumpulan data yang akan digunakan sebagai masukan untuk penelitian ini adalah *file* teks dengan format **.txt* dengan ketentuan ukuran *file* atau jumlah karakter yang bervariasi. Hal ini dilakukan agar performa skema super enkripsi dengan kombinasi algoritma *Beaufort Cipher* dan algoritma RSA dapat di evaluasi. Namun tidak menutup kemungkinan akan ada data masukan yang memiliki ukuran atau jumlah karakter yang kecil atau sedikit.

3. Pengujian Lab

Pada tahap ini, penulis melakukan pembuatan aplikasi berbasis *web*, setelah aplikasi berjalan selanjutnya melakukan tahap uji coba langsung terhadap data yang akan di enkripsi dan dekripsi..

3.3.3 Analisis Kebutuhan

Tahap ini bertujuan untuk mengumpulkan informasi dan spesifikasi tentang kebutuhan sistem. Dalam analisis kebutuhan ini terdapat dua bagian, yaitu kebutuhan fungsional sistem dan kebutuhan non-fungsional sistem. Kebutuhan fungsional sistem mendeskripsikan fungsi-fungsi yang harus dilakukan oleh sebuah sistem untuk mencapai tujuan. Sedangkan kebutuhan non-fungsional sistem mendeskripsikan fitur lain seperti karakteristik, batasan sistem, performa, dokumentasi dan yang lainnya agar sistem berjalan sukses.

3.3.3.1 Analisis Kebutuhan Fungsional

Kebutuhan fungsional merupakan jenis kebutuhan yang berkaitan dengan proses yang akan dikerjakan oleh sistem dan juga berisi informasi tentang apa saja yang harus ada dan dihasilkan oleh sistem. Kebutuhan fungsional dari sistem yang

mengimplementasikan kombinasi algoritma kriptografi simetris *Beaufort Cipher* dan kriptografi asimetris RSA dalam skema super enkripsi adalah sebagai berikut:

1. Bangkitkan Kunci

Sistem dapat membangkitkan kunci publik (*public key*) dan kunci privat (*private key*) algoritma RSA secara acak (*random*). Selanjutnya juga dapat menyimpan kunci publik untuk selanjutnya digunakan pada proses enkripsi dan kunci privat untuk selanjutnya digunakan pada proses dekripsi.

2. Menerima *Input* Pesan Teks (*Plaintext*)

Sistem dapat mencari dan membaca isi *file* teks yang berekstensi **.txt* yang tersimpan pada perangkat yang digunakan dan hanya dapat membaca berupa teks (*string*) yang terdapat dalam *file* teks. Sistem juga dapat menerima *input plaintext* langsung dari pengguna secara manual.

3. Mengenkripsi Pesan Teks (*Plaintext*)

Sistem dapat mengenkripsi berupa teks (*string*) yang terdapat dalam *file* teks dengan menggunakan algoritma *Beaufort Cipher* kemudian menghasilkan *ciphertext* pertama, lalu *ciphertext* yang didapat sebelumnya dienkripsi lagi dengan menggunakan kunci publik algoritma RSA dan menghasilkan *ciphertext* kedua sebagai hasil akhir enkripsi.

4. Menyimpan Hasil Enkripsi Pesan Teks (*Ciphertext*)

Sistem akan menyimpan pesan teks yang telah dienkripsi sebelumnya (*ciphertext*). Setelah itu sistem akan membaca pesan yang disimpan tersebut untuk melakukan proses dekripsi.

5. Mendekripsi Pesan Teks (*Ciphertext*)

Sistem dapat mendekripsi pesan teks (*ciphertext*) dengan menggunakan kunci privat algoritma RSA kemudian menghasilkan *ciphertext* pertama, lalu *ciphertext* yang didapat sebelumnya didekripsi lagi dengan menggunakan algoritma *Beaufort Cipher* dan menghasilkan *plaintext* asli.

3.3.3.2 Analisis Kebutuhan Non Fungsional

Kebutuhan non fungsional berisi tentang perilaku yang dimiliki oleh sistem seperti operasional dan kinerja dari sistem. Adapun kebutuhan non

fungsional dari sistem yang mengimplementasikan kombinasi algoritma kriptografi simetris *Beaufort Cipher* dan kriptografi asimetris RSA dalam skema super enkripsi adalah sebagai berikut:

1. Dokumentasi, sistem yang akan dibangun memiliki panduan (*help*) penggunaan aplikasi sehingga pengguna dapat menggunakan sesuai panduan.
2. Pengendalian, sistem yang akan dibangun akan menampilkan pesan *error* untuk setiap masukan yang tidak sesuai.
3. Kinerja, sistem melakukan proses enkripsi dan dekripsi pada pesan teks dengan waktu yang relatif singkat.
4. *User Friendly*, sistem menggunakan tampilan yang mudah digunakan dan dipelajari.

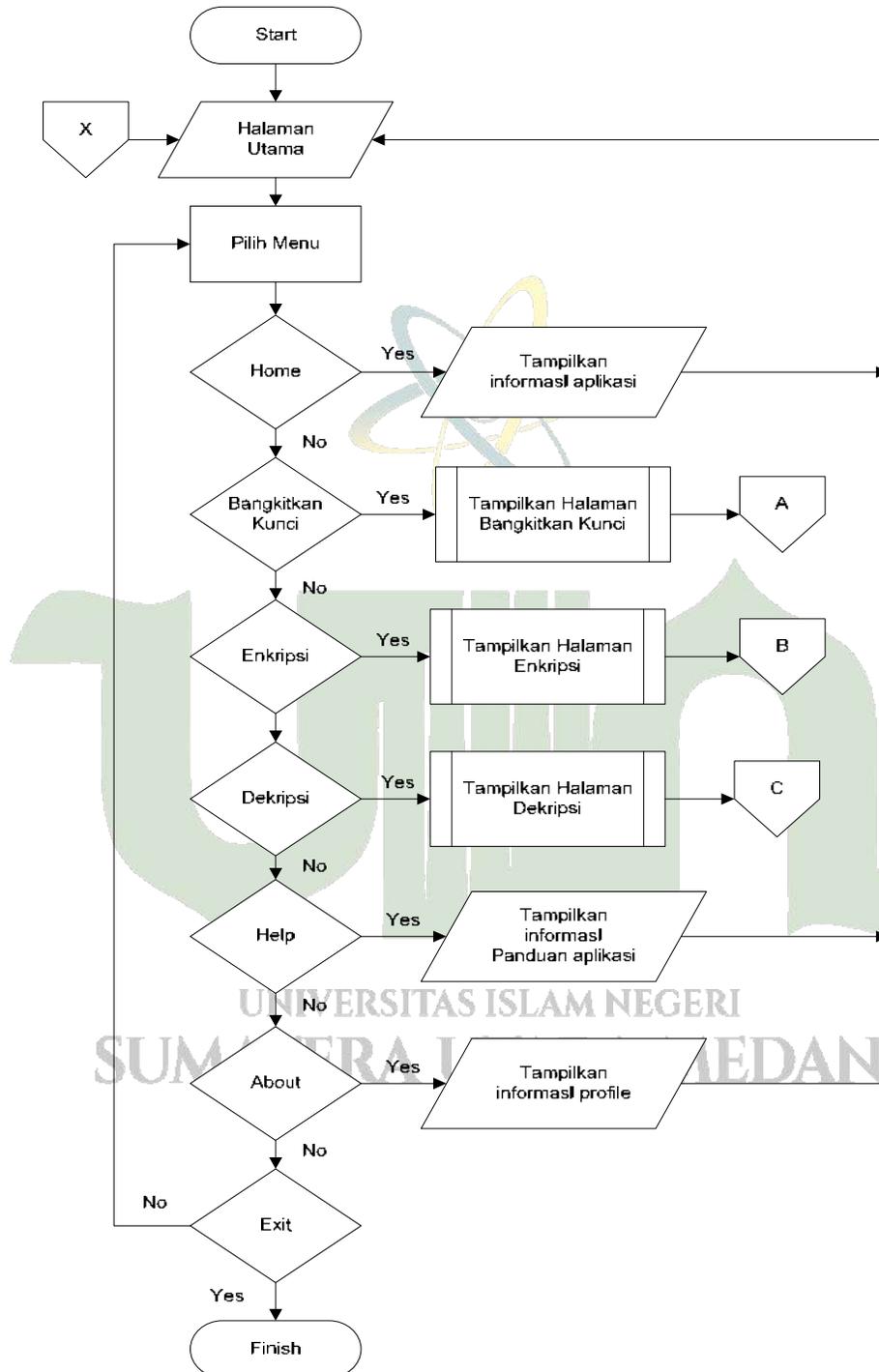
3.3.4 Perancangan

Perancangan sistem merupakan wujud dari implementasi sistem secara teknis. Perancangan sistem bertujuan untuk menggambarkan semua kondisi dan bagian-bagian yang berperan dalam sistem yang dirancang. Tujuan dari perancangan antarmuka yaitu membuat tampilan sistem yang sederhana dan mudah digunakan (*user friendly*) sehingga *user* dapat lebih mudah dalam menggunakan sistem. Dalam perancangan sistem ini menggunakan *flowchart* sistem. Selain itu juga akan dijelaskan rancangan antarmuka sistem (*system interface*) yang akan dibangun. *Interface* yang akan dirancang pada sistem ini memiliki lima bagian utama, yaitu halaman utama (*home*), halaman enkripsi, halaman dekripsi, halaman *help*, dan halaman *about*.

3.3.4.1 *Flowchart* Sistem

Flowchart sistem dapat dijelaskan sebagai bagan yang menunjukkan arus pekerjaan secara keseluruhan dari sistem. Bagan ini menjelaskan urutan-urutan dari prosedur-prosedur yang ada di dalam sistem. Bagan alir sistem menunjukkan apa yang dikerjakan di sistem kriptografi super enkripsi dengan memanfaatkan algoritma simetris *Beaufort Cipher* dan algoritma asimetris RSA.

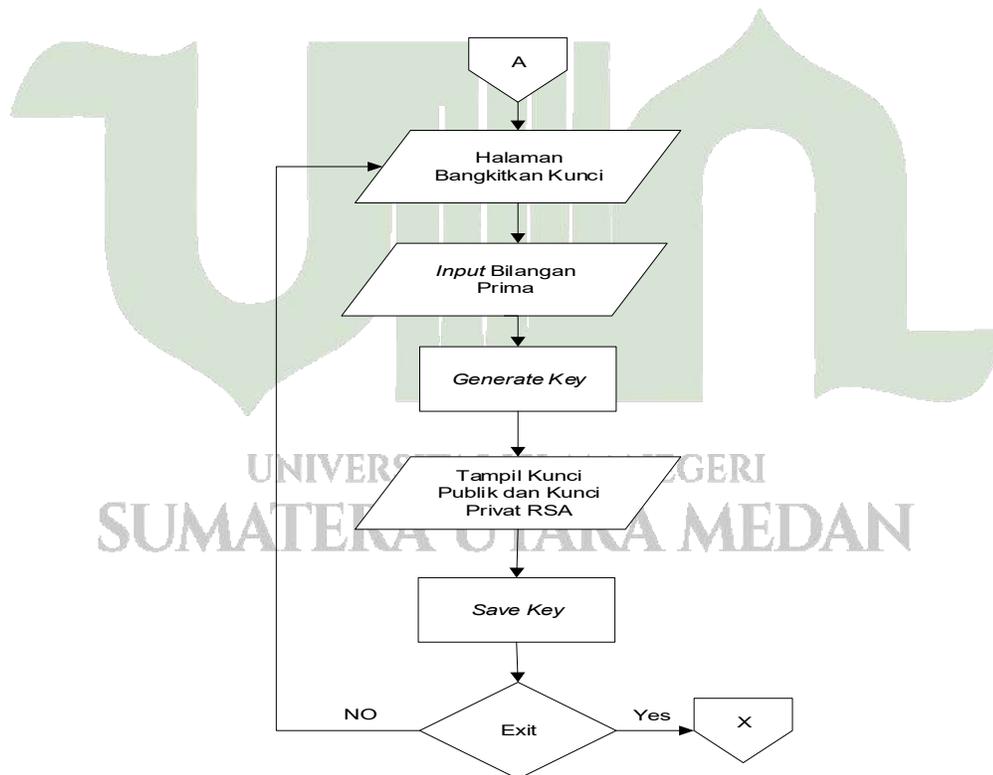
Flowchart sistem dimulai dengan menampilkan halaman utama yang dapat dijelaskan pada gambar 3.3.



Gambar 3.3 *Flowchart* Sistem Halaman Utama

Flowchart sistem pada gambar 3.3 dimulai dengan menampilkan halaman utama sistem. Pada halaman utama terdapat sejumlah menu yang dapat diakses oleh *User*, jika memilih menu *home* maka sistem akan menampilkan informasi mengenai aplikasi, jika memilih menu bangkitkan kunci maka sistem akan menampilkan halaman bangkitkan kunci, jika memilih menu enkripsi maka sistem akan menampilkan halaman enkripsi, jika memilih menu dekripsi maka sistem akan menampilkan halaman dekripsi, jika memilih menu *help* maka sistem akan menampilkan informasi panduan cara menggunakan aplikasi, jika memilih menu *about* maka sistem akan menampilkan informasi mengenai aplikasi, jika memilih menu *exit* maka akan keluar dari sistem.

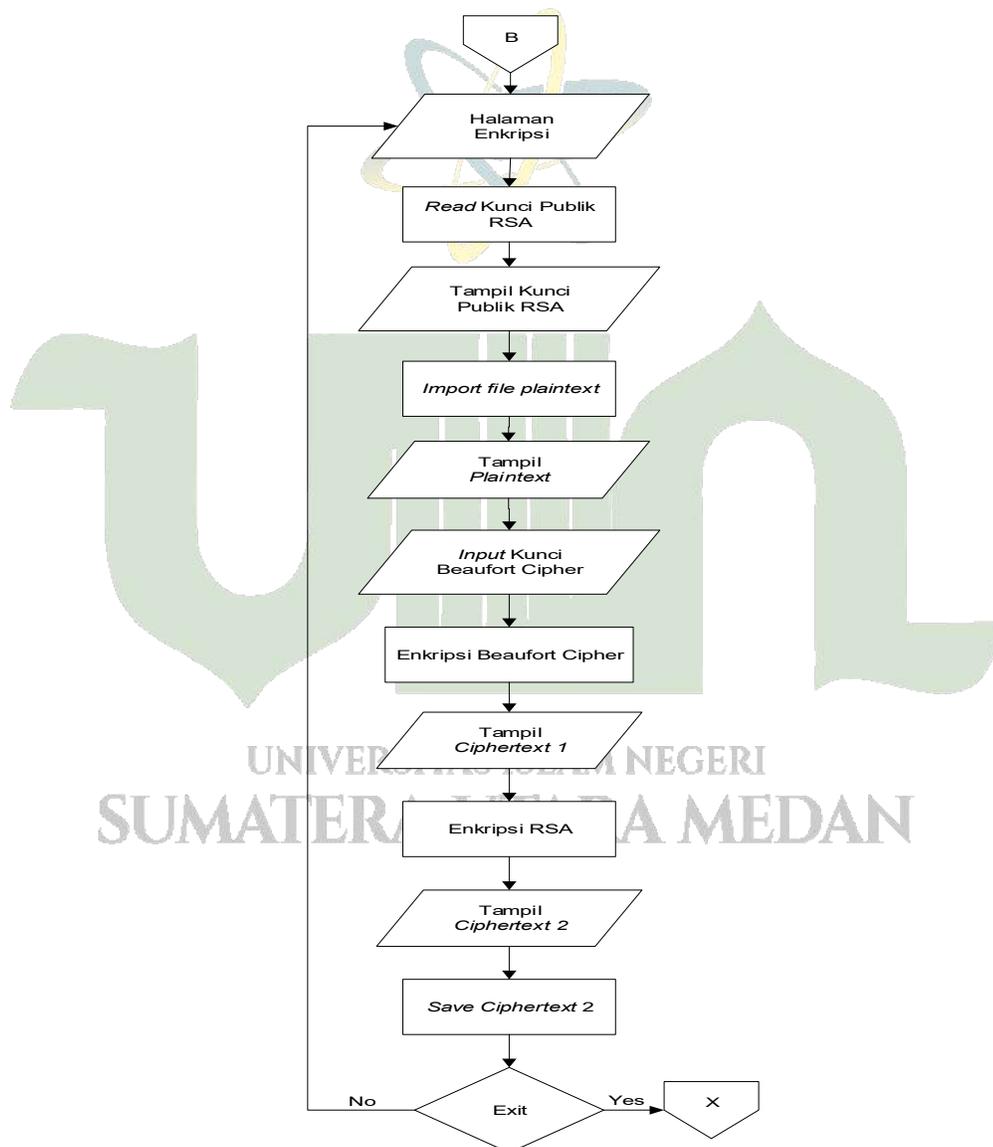
Adapun *flowchart* sistem pada halaman bangkitkan kunci publik (*public key*) dan kunci privat (*private key*) dari algoritma asimetris RSA dapat dijelaskan pada gambar 3.4.



Gambar 3.4 *Flowchart* Sistem Halaman Bangkitkan Kunci

Flowchart sistem pada gambar 3.4 dimulai dengan menampilkan halaman bangkitkan kunci. Pada halaman ini pilih tombol *generate key* untuk membangkitkan kunci publik dan kunci privat algoritma RSA. Selanjutnya pilih tombol *save key* untuk menyimpan kunci yang nantinya akan digunakan untuk proses enkripsi dan dekripsi.

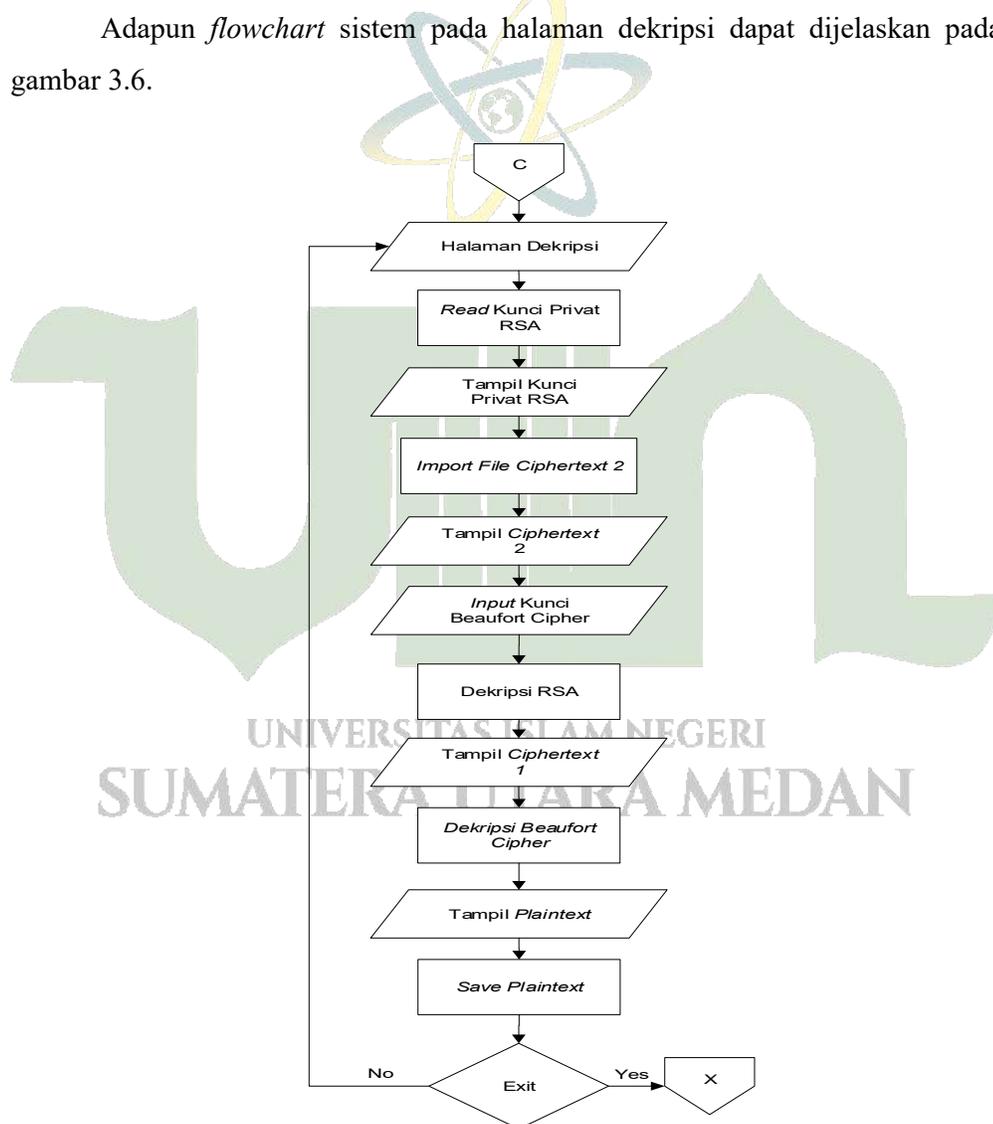
Adapun *flowchart* sistem pada halaman enkripsi dapat dijelaskan pada gambar 3.5.



Gambar 3.5 *Flowchart* Sistem Halaman Enkripsi

Flowchart sistem pada gambar 3.5 dimulai dengan menampilkan halaman enkripsi. Pada halaman ini pilih tombol *input file* untuk menginputkan pesan yang akan di enkripsi, lalu masukkan kunci algoritma *Beaufort Cipher* serta dilanjutkan dengan meng*import* kunci publik dari algoritma RSA yang telah dibangkitkan sebelumnya. Selanjutnya pilih tombol enkripsi untuk melakukan proses enkripsi dengan menggunakan algoritma *Beaufort Cipher* dan algoritma RSA dan sistem akan menampilkan hasil enkripsi (*ciphertext*). Setelah itu simpan *ciphertext* untuk proses selanjutnya pada saat melakukan dekripsi.

Adapun *flowchart* sistem pada halaman dekripsi dapat dijelaskan pada gambar 3.6.



Gambar 3.6 *Flowchart* Sistem Halaman Dekripsi

Flowchart sistem pada gambar 3.6 dimulai dengan menampilkan halaman dekripsi. Pada halaman ini pilih tombol *import file* untuk menginputkan *ciphertext* yang akan di dekripsi, lalu mengimport kunci privat dari algoritma RSA yang telah dibangkitkan sebelumnya dan masukkan kunci *Beaufort cipher*. Selanjutnya pilih tombol dekripsi untuk melakukan proses dekripsi dengan menggunakan algoritma *Beaufort Cipher* dan algoritma RSA dan sistem akan menampilkan hasil dekripsi (*plaintext*).

3.3.4.2 Rancangan *Interface* Sistem

Proses perancangan *interface* sistem (antarmuka sistem) merupakan hal yang sangat penting karena berpengaruh pada saat pengguna menggunakan sistem atau berkomunikasi dengan sistem. Apabila suatu sistem menggunakan perancangan antarmuka yang sulit untuk dimengerti pengguna, maka pengguna akan melakukan kesalahan pada saat menjalankan sistem tersebut. Sehingga diperlukan perancangan yang sederhana dan efisien agar pengguna tidak sulit pada saat menjalankan sistem.

Sistem dibangun berbasis *web* dengan menggunakan *PHP* sebagai bahasa pemrograman. *Interface* yang akan dirancang pada sistem ini memiliki enam bagian utama, yaitu halaman *home* atau halaman utama, halaman bangkitkan kunci, halaman enkripsi, halaman dekripsi, halaman *help*, dan halaman *about*. Berikut ini dijelaskan mengenai rancangan antarmuka pada sistem yang akan dibangun, yaitu sebagai berikut:

1. Rancangan Halaman Utama

Halaman utama (*home*) berfungsi sebagai tampilan awal pada saat aplikasi dijalankan. Pada halaman utama terdapat lima buah menu yang dapat diakses oleh *user*, yaitu menu *home*, menu bangkitkan kunci, menu enkripsi, menu dekripsi, menu *help*, dan menu *about*.

2. Rancangan Halaman Bangkitkan Kunci

Halaman bangkitkan kunci dirancang untuk membangkitkan kunci publik (*public key*) dan kunci privat (*private key*) dari algoritma RSA. Kunci publik digunakan untuk mengenkripsi pesan (*plaintext*) yang terdapat dalam *file* teks

dengan format *.txt*, sedangkan kunci privat digunakan untuk mendekripsi pesan (*ciphertext*) yang terdapat dalam *file* teks dengan format *.txt*.

3. Rancangan Halaman Enkripsi

Halaman enkripsi dirancang untuk melakukan proses enkripsi pesan (*plaintext*) yang terdapat dalam *file* teks dengan format *.txt* menggunakan kombinasi algoritma kriptografi *Beaufort Cipher* dan algoritma RSA dalam skema super enkripsi.

4. Rancangan Halaman Dekripsi

Halaman dekripsi dirancang untuk melakukan proses dekripsi pesan (*ciphertext*) yang terdapat dalam *file* teks dengan format *.txt* menggunakan kombinasi algoritma kriptografi *Beaufort Cipher* dan algoritma RSA dalam skema super enkripsi.

5. Rancangan Halaman *Help*

Halaman *help* dirancang untuk menampilkan informasi panduan kepada *user* mengenai proses membangkitkan kunci, proses enkripsi dan proses dekripsi yang terdapat pada aplikasi yang dibuat.

6. Rancangan Halaman *About*

Halaman *about* dirancang untuk menampilkan informasi mengenai *profile* pembuat aplikasi yang berisi mengenai nama, nim, dan prodi.

3.3.5 Pengujian

Tahap pengujian dilakukan dengan tujuan untuk menjamin sistem yang dibuat sesuai dengan hasil analisis dan perancangan serta menghasilkan satu kesimpulan apakah sistem tersebut sesuai dengan yang diharapkan. Untuk itu dibutuhkan sebuah metode pengujian yang menjadi ukuran atau parameter sehingga dapat ditarik kesimpulan bahwa sistem memang telah berjalan sesuai dengan tujuan. Pengujian sistem pada penelitian ini dilakukan dengan menggunakan metode pengujian *black box* (*black box testing*).

Pengujian *black box* adalah salah satu metode pengujian aplikasi atau perangkat lunak yang berfokus pada sisi fungsionalitas, khususnya pada *input* dan

output aplikasi (apakah sudah sesuai dengan apa yang diharapkan atau belum). Pengujian dengan metode *black box* dilakukan dengan cara memberikan sejumlah *input* pada program kemudian diproses sesuai dengan kebutuhan fungsionalnya untuk melihat apakah program aplikasi dapat menghasilkan *output* yang sesuai dengan yang diinginkan dan sesuai pula dengan fungsi dasar dari program tersebut. Jika dari *input* yang diberikan dapat menghasilkan *output* yang sesuai dengan kebutuhan fungsionalnya, maka program yang dibuat sudah benar, tetapi apabila *output* yang dihasilkan tidak sesuai, maka masih terdapat kesalahan pada program tersebut, dan selanjutnya dilakukan penelusuran perbaikan untuk memperbaiki kesalahan yang terjadi.

Berikut dijelaskan beberapa tahapan pengujian yang akan dilakukan yaitu mencakup pengujian *interface*, pengujian fungsi dasar sistem, dan pengujian validasi.

1. Pengujian *Interface*

Pengujian *interface* ini bertujuan untuk mengetahui fungsionalitas dari elemen-elemen *interface* yang terdapat pada tiap *form* dalam aplikasi yang dibangun. Adapun rencana kasus uji pada pengujian *interface* mencakup menu bangkitkan kunci, menu enkripsi, menu dekripsi, menu *help*, dan menu *about*.

2. Pengujian Fungsi Dasar Sistem

Pengujian fungsi dasar sistem bertujuan untuk mengetahui fungsi-fungsi dasar yang ada di dalam aplikasi. Adapun rencana kasus uji pada pengujian fungsi dasar sistem ini mencakup menu bangkitkan kunci pada tombol *generate key* dan tombol *save key*. Menu enkripsi pada tombol *import file* teks, tombol *import* kunci publik RSA, tombol enkripsi *file* teks, dan tombol simpan *ciphertext*. Menu dekripsi pada tombol *import* kunci privat RSA, tombol *import ciphertext*, tombol dekripsi *ciphertext*, dan tombol simpan *plaintext*.

3. Pengujian Validasi

Pengujian ini bertujuan untuk mengetahui apakah validasi-validasi yang ada didalam sistem sudah berjalan dengan baik. Adapun rencana kasus uji pada pengujian validasi ini mencakup validasi *import file* teks, validasi *import file* kunci, validasi enkripsi, validasi dekripsi, dan validasi simpan *file*.