

BAB III

ANALISIS DAN DESAIN SISTEM

III.1. Analisis Masalah

Analisis masalah yang bertujuan untuk mengidentifikasi serta melakukan evaluasi pada Pemanfaatan Algoritma Beaufort Sebagai Pengamanan Pesan pada Aplikasi *Chatting* Dengan Koneksi *WiFi Direct* Berbasis Android.

adapun masalah yang penulis identifikasi adalah sebagai berikut :

1. Belum adanya aplikasi *chatting* yang bersifat *offline*
2. Dibutuhkan aplikasi *chatting* yang dapat digunakan tanpa akses *point* maupun koneksi *internet*.
3. Dibutuhkan sebuah aplikasi *chatting* yang dapat menjaga privasi antara pengguna dengan memanfaatkan algoritma Beaufort.

III.2. Strategi Pemecahan Masalah

Beberapa strategi pemecahan masalah dalam perancangan pemanfaatan algoritma Beaufort sebagai pengamanan pesan pada aplikasi *chatting* dengan koneksi *Wifi Direct* berbasis Android ini adalah sebagai berikut:

1. Aplikasi ini akan dibangun menggunakan perangkat lunak android studio dan akan digunakan pada *smartphone* android.

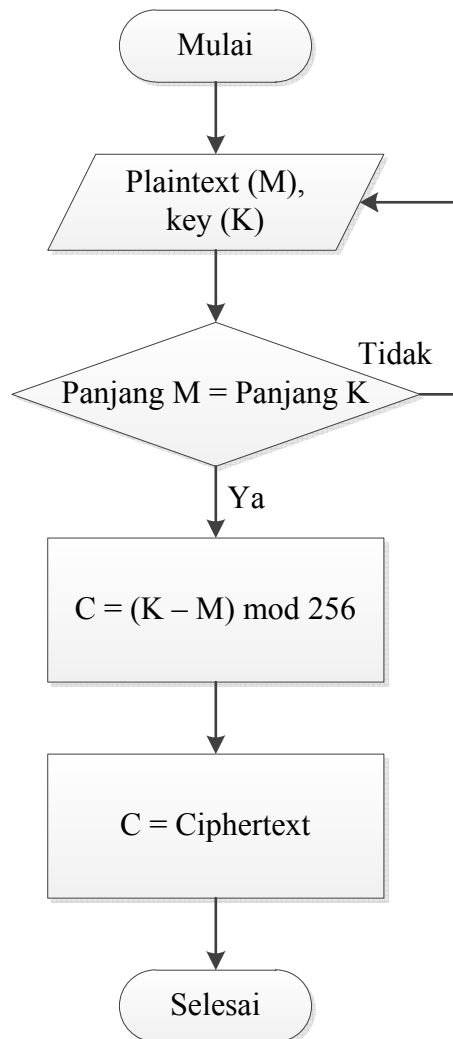
2. Aplikasi ini digunakan untuk kegiatan *chatting* pada *smartphone* android yang dihubungkan dengan koneksi *Wifi Direct*.
3. Pesan yang akan dikirimkan dapat diamankan menggunakan algoritma beaufort.
4. Pesan yang diterima juga dapat dikembalikan ke dalam bentuk aslinya menggunakan algoritma beaufort.

III.3. Penerapan Algoritma Beaufort

Pada penelitian ini akan diterapkan algoritma Beaufort untuk proses enkripsi dan dekripsi pesan pada kegiatan *chatting* menggunakan koneksi *Wifi Direct*. Untuk proses enkripsi dapat dilihat pada flowchart gambar III.1 dan III.2.

III.3.1. Flowchart Enkripsi Algoritma Beaufort

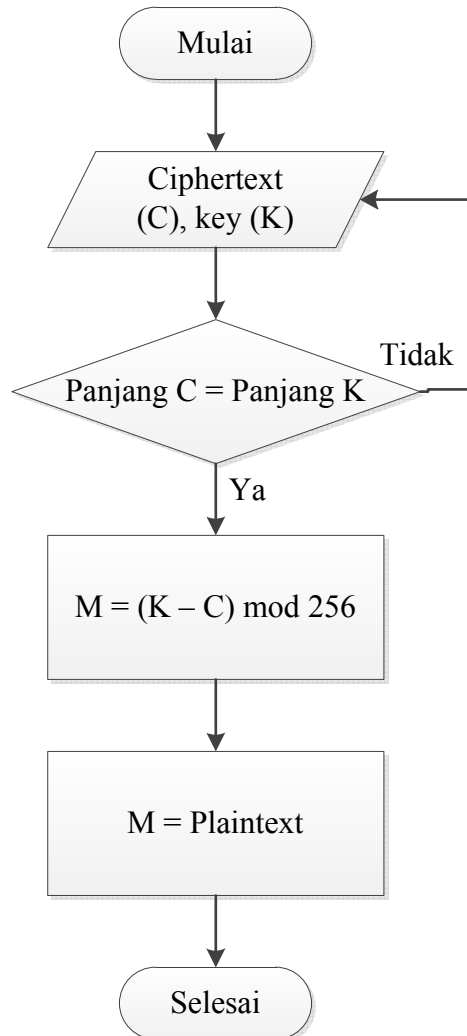
Flowchart yang menjelaskan proses enkripsi menggunakan algoritma Beaufort dapat dilihat pada Gambar III.1.



Gambar III.1. Flowchart Enkripsi Algoritma Beaufort

III.3.2. Flowchart Dekripsi Algoritma Beaufort

Flowchart yang menjelaskan proses dekripsi menggunakan algoritma Beaufort dapat dilihat pada Gambar III.2.



Gambar III.2. Flowchart Dekripsi Algoritma Beaufort

III.3.4. Studi Kasus Algoritma Beaufort

III.3.4.1. Proses Enkripsi

Pada proses enkripsi menggunakan algoritma Beaufort menggunakan persamaan II.1.

Untuk proses enkripsinya menggunakan *plaintext* dan kunci sebagai berikut :

Pi (*Plaintext*) = **POTENSI**

Ki (Kunci) = **1234567**

Maka perhatikan langkahnya seperti di bawah ini :

1. Konversikan *plaintext* dan kunci kedalam bentuk ASCII desimal.
2. Kurangi nilai desimal dari setiap karakter kunci dengan *plaintext* dimulai dari yang paling kiri hingga ke kanan.
3. Cari hasil sisa pembagian dari penjumlahan setiap karakter.

$$\begin{aligned}
 \text{Contoh : } Ciphertext &= (1 - P) \text{ mod } 256 \\
 &= (49 - 80) \text{ mod } 256 \\
 &= (-31) \text{ mod } 256 \\
 &= 225
 \end{aligned}$$

4. Konversikan kembali nilai desimal yang di dapat kedalam bentuk karakter.

Contoh : 225 = á (*Ciphertext* yang dihasilkan adalah á)

Untuk perhitungan keseluruhan dapat dilihat sebagai berikut :

Kunci	49(1)	50(2)	51(3)	52(4)	53(5)	54(6)	55(7)
<i>Plaintext</i>	80(P)	79(O)	84(T)	69(E)	78(N)	83(S)	73(I)

Hasil <i>mod</i> 256	225	227	223	239	231	227	238
Ci (<i>Ciphertext</i>)	á	ã	ß	ï	ç	ã	î

Jadi *ciphertext* yang di hasilkan, yaitu : **áãßïçãî**

III.3.4.2. Proses Dekripsi

Setelah mendapatkan *ciphertext* dari hasil enkripsi selanjutnya penulis akan menjabarkan proses dekripsi agar menghasilkan *plaintext* dari *ciphertext* yang telah diketahui. Dalam proses dekripsi dapat digunakan persamaan II.2.

Untuk proses dekripsinya adalah sebagai berikut :

C_i (*ciphertext*) = **áãßîçâî**

K_i (Kunci) = **1234567**

Maka perhatikan langkahnya seperti di bawah ini :

1. Konversikan *ciphertext* dan kunci kedalam bentuk ASCII desimal.
2. Kurangi nilai karakter *ciphertext* menggunakan nilai karakter kunci dimulai dari yang paling kiri hingga ke kanan.
3. Cari hasil sisa pembagian dari pengurangan setiap karakter.

$$\begin{aligned}
 \text{Contoh : } \quad \textit{Plaintext} &= (1 - \acute{a}) \bmod 256 \\
 &= (49 - 225) \bmod 256 \\
 &= (-179) \bmod 256 \\
 &= 80
 \end{aligned}$$

4. Konversikan kembali nilai desimal yang didapat kedalam bentuk karakter.

Contoh : 80 = P (*Plaintext* yang dihasilkan adalah P)

Untuk perhitungan keseluruhan dapat dilihat sebagai berikut :

Kunci	49(1)	50(2)	51(3)	52(4)	53(5)	54(6)	55(7)
<i>Chipertext</i>	225(á)	227(ã)	223(ß)	239(ï)	231(ç)	227(ã)	238(î)

Hasil <i>mod</i> 256	80	79	84	69	78	83	73
<i>Plaintext</i>	P	O	T	E	N	S	I

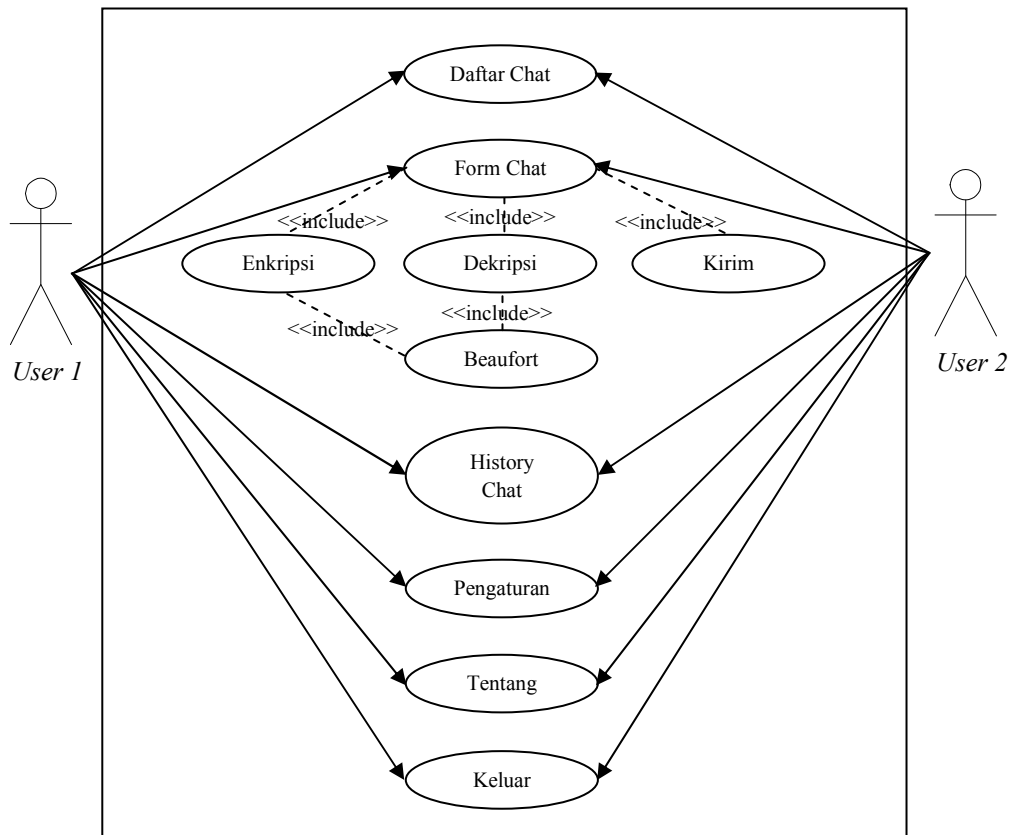
Jadi *Plaintext* yang dihasilkan, yaitu : **POTENSI**

III.4. Desain Sistem

Aplikasi pemanfaatan algoritma Beaufort sebagai pengamanan pesan pada aplikasi chatting dengan koneksi *Wifi Direct* berbasis Android dirancang dengan menggunakan perangkat lunak Android Studio. Perancangan sistem yang dirancang terdiri dari *use case*, *activity diagram*, *sequence diagram* serta desain dan penjelasan dari sistem yang dirancang. Berikut adalah perancangannya :

III.4.1. Use Case Diagram

Use case mendiskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem yang akan dibuat. *Use case* digunakan untuk mengetahui fungsi yang ada didalam sistem informasi tersebut. Berikut adalah *use case diagram* dari sistem yang dirancang :



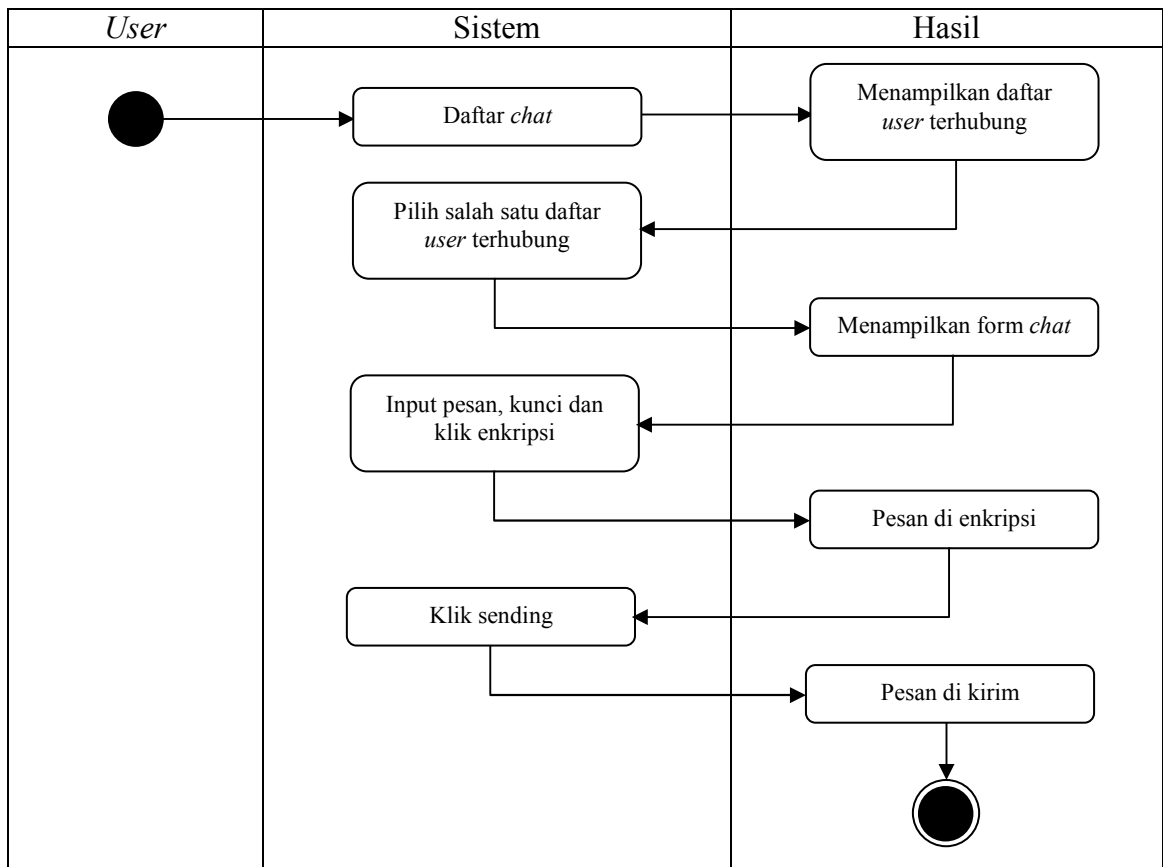
Gambar III.1. Use Case Diagram Aplikasi Wifi Direct Chatting

III.3.2. Activity Diagram

Activity diagram menggambarkan berbagai alir aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir. *Activity diagram* yang terdapat pada aplikasi yaitu sebagai berikut :

III.3.2.1. Activity Diagram Daftar Chat

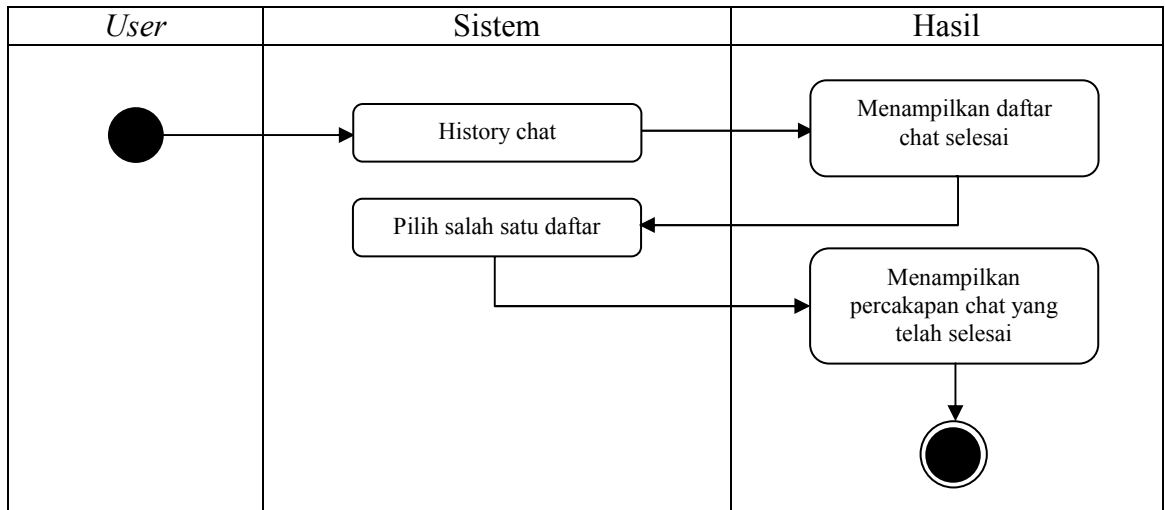
Activity diagram daftar chat menggambarkan alir aktifitas dalam interface daftar chat. Activity diagram daftar chat dapat dilihat pada gambar III.2.



Gambar III.2. Activity Diagram Daftar Chat

III.3.2.2. Activity Diagram History Chat

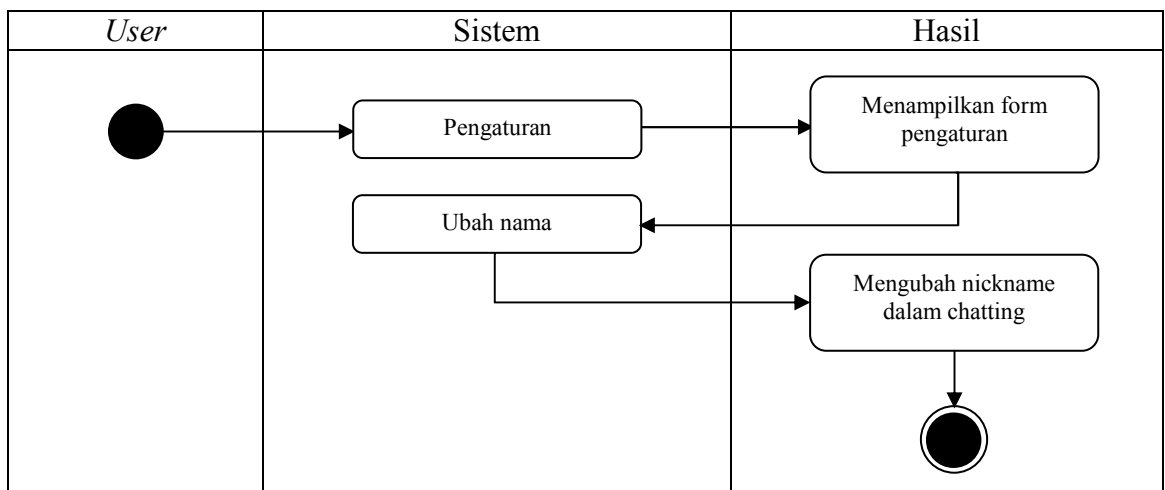
Activity diagram history chat menggambarkan alir aktifitas dalam interface history chat. Activity diagram history chat dapat dilihat pada gambar III.3.



Gambar III.3. Activity Diagram History Chat

III.3.2.3. Activity Diagram Pengaturan

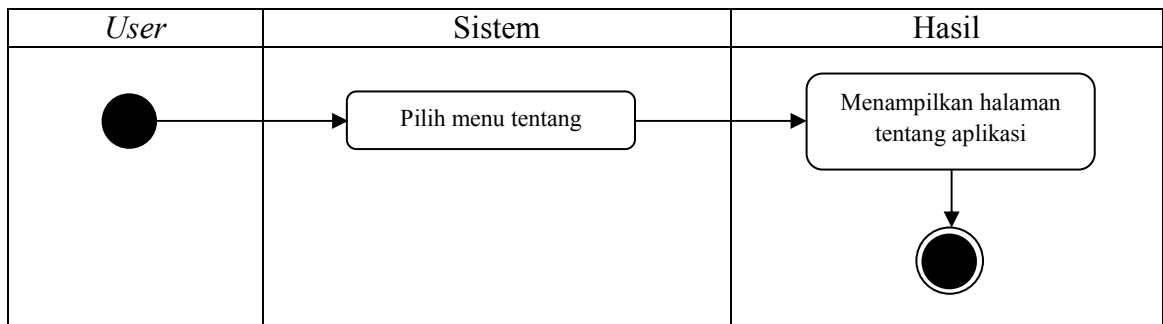
Activity diagram pengaturan menggambarkan alir aktifitas dalam memilih menu pengaturan pada aplikasi. *Activity diagram* pengaturan dapat dilihat pada gambar III.4.



Gambar III.4. Activity Diagram Pengaturan

III.3.2.4. Activity Diagram Tentang

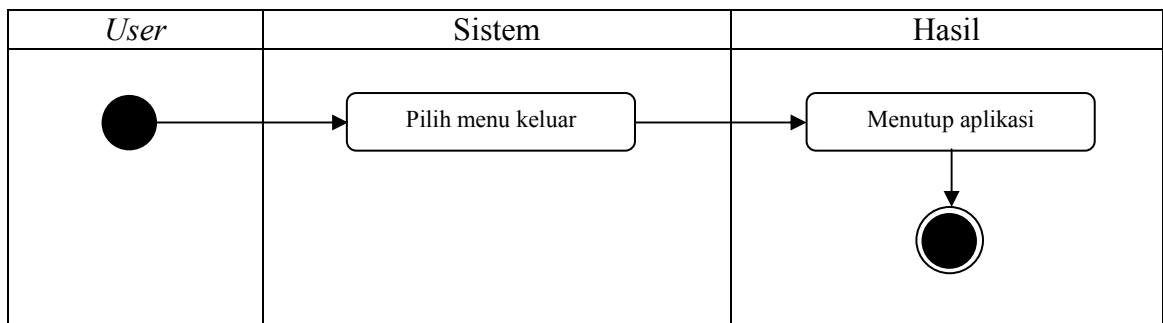
Activity diagram tentang digunakan untuk menampilkan informasi tentang aplikasi yang dibuat. *Activity diagram* tentang dapat dilihat pada gambar III.5.



Gambar III.5. Activity Diagram Tentang

III.3.2.5. Activity Diagram Keluar

Activity diagram keluar digunakan untuk menutup aplikasi. *Activity diagram* keluar dapat dilihat pada gambar III.6.



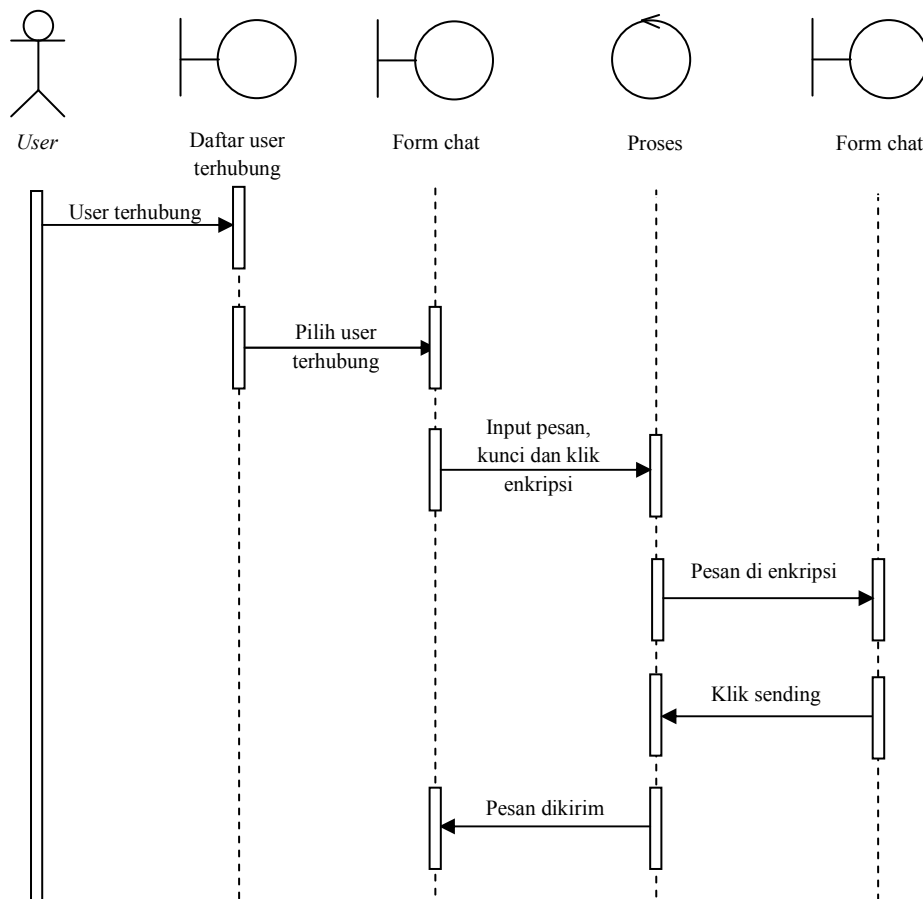
Gambar III.6. Activity Diagram Keluar

III.3.3. Sequence Diagram

Sequence diagram pada aplikasi yang akan dibuat yaitu : *Sequence diagram* user terhubung, *history chat*, pengaturan, tentang dan keluar.

III.3.3.1. Sequence Diagram User Terhubung

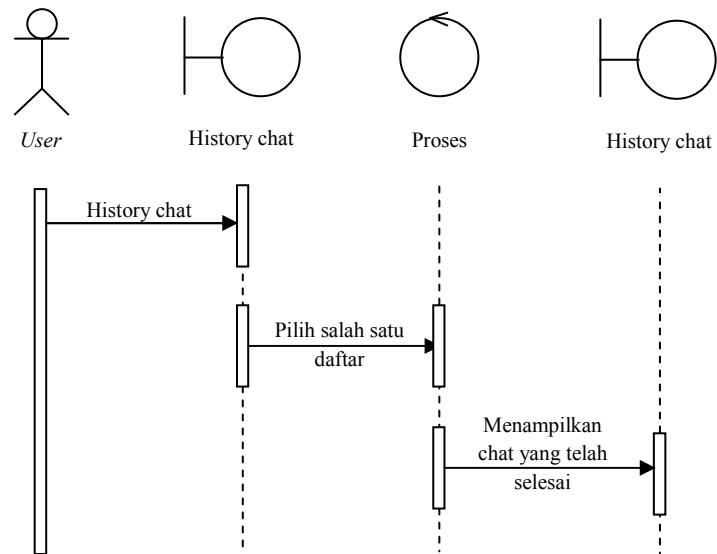
Sequence diagram daftar chat menggambarkan interaksi yang terjadi pada halaman daftar chat. *Sequence diagram* daftar chat ditunjukkan pada gambar III.7.



Gambar III.7. Sequence Diagram Daftar Chat

III.3.3.2. Sequence Diagram History Chat

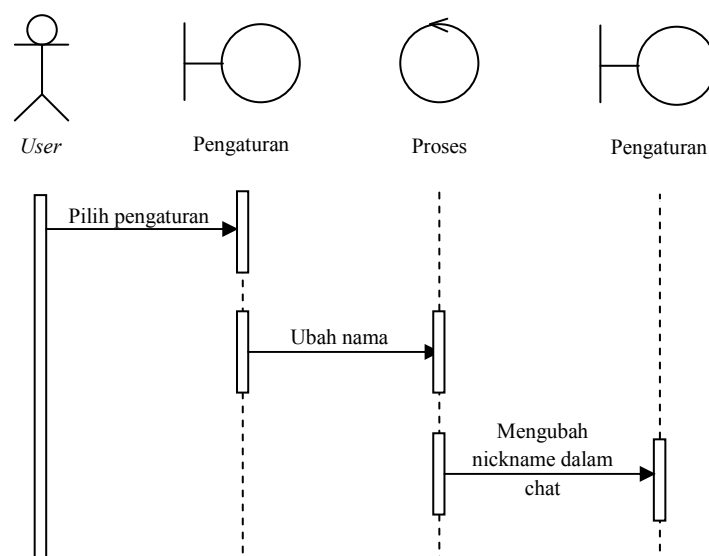
Sequence diagram history chat menggambarkan interaksi yang terjadi pada halaman *history chat*. *Sequence diagram history chat* ditunjukkan pada gambar III.8.



Gambar III.8. Sequence Diagram History Chat

III.3.3.3. Sequence Diagram Pengaturan

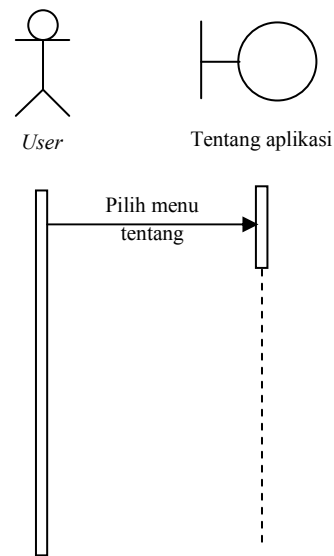
Sequence diagram pengaturan menggambarkan interaksi yang terjadi pada saat memilih menu pengaturan. *Sequence diagram* pengaturan ditunjukkan pada gambar III.9.



Gambar III.9. Sequence Diagram Pengaturan

III.3.3.4. *Sequence Diagram* Tentang

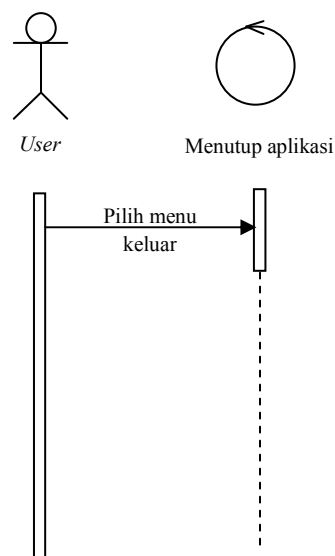
Sequence diagram tentang menggambarkan interaksi yang terjadi pada saat memilih menu tentang pada aplikasi yang akan menampilkan informasi tentang aplikasi yang dibangun. *Sequence diagram* tentang ditunjukkan pada gambar III.10.



Gambar III.10. *Sequence Diagram* Tentang

III.3.3.5. *Sequence Diagram* Keluar

Sequence diagram keluar menggambarkan interaksi yang terjadi pada saat memilih *menu* keluar pada aplikasi yang akan menutup aplikasi. *Sequence diagram* keluar ditunjukkan pada gambar III.11.



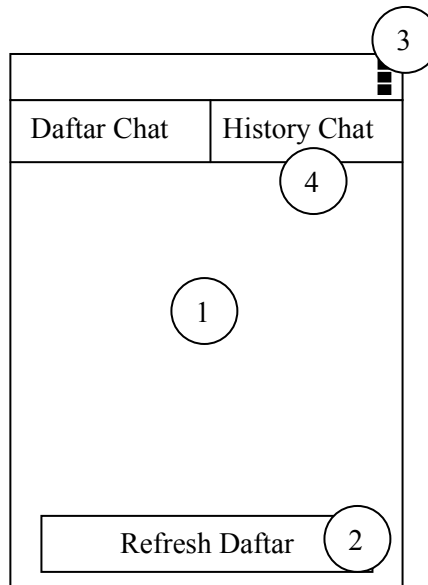
Gambar III.11. Sequence Diagram Menu Keluar

III.4. Desain *User Interface*

Antarmuka peamakai (*user interface*) adalah tampilan program yang dapat dilihat atau dipersepsikan oleh pengguna dan perintah-perintah atau mekanisme yang digunakan pemakai untuk mengendalikan operasi dan memasukkan data. Berikut ini merupakan perancangan antarmuka dari aplikasi pemanfaatan algoritma Beaufort sebagai pengamanan pesan pada aplikasi *chatting* dengan koneksi *Wifi Direct* berbasis Android, yaitu :

1. Desain Halaman Daftar *Chat*

Rancangan desain halaman daftar chat pada aplikasi dapat dilihat pada gambar III.12.



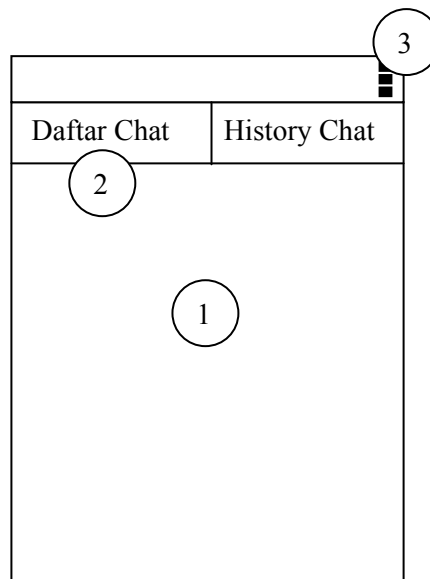
Gambar III.12. Desain Halaman Daftar *Chat*

Keterangan tampilan desain halaman daftar chat, yaitu :

- 1) Menampilkan daftar *chat/user* yang aktif atau terkoneksi.
- 2) Tombol untuk melakukan refresh terhadap daftar *chat/user* yang aktif atau terkoneksi.
- 3) Tombol untuk menampilkan pengaturan aplikasi.
- 4) Tab untuk menampilkan halaman *history chat*.

2. Desain Halaman *History Chat*

Rancangan desain halaman history chat dapat dilihat pada gambar III.13.



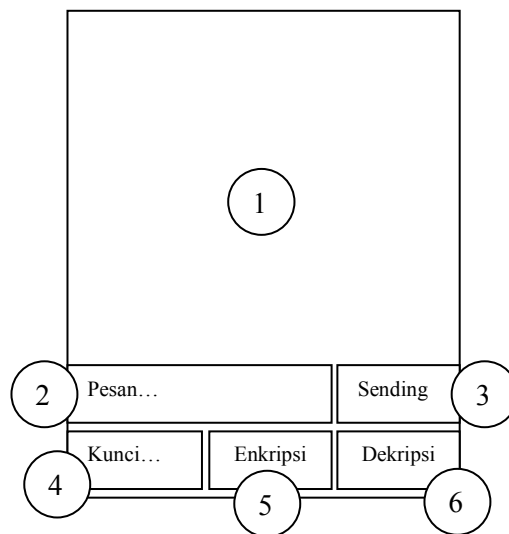
Gambar III.13. Desain Halaman *History Chat*

Adapun keterangannya sebagai berikut :

- 1) Menampilkan daftar *chat* yang telah selesai.
- 2) Tab untuk menampilkan halaman daftar *chat*.
- 3) Tombol untuk menampilkan pengaturan aplikasi.

3. Desain *Form Chatting*

Rancangan desain dari form chatting yang terdapat pada aplikasi ini dapat dilihat pada gambar III.14.



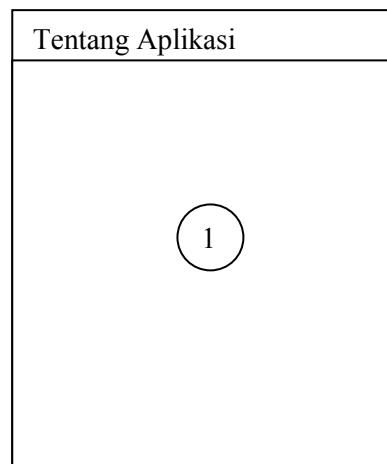
Gambar III.14. Desain *Form Chatting*

Adapun keterangan tampilan *form chatting* adalah sabagai berikut :

- 1) Halaman untuk menampilkan pesan *chatting*.
- 2) *Edittext* untuk input pesan *chatting*.
- 3) Tombol untuk mengirim pesan.
- 4) *Edittext* untuk input kunci.
- 5) Tombol untuk melakukan enkripsi pesan.
- 6) Tombol untuk melakukan dekripsi pesan.

4. Desain Halaman Tentang

Adapun rancangan desain halaman tentang dapat dilihat pada gambar III.15.



Gambar III.15. Desain Halaman Tentang

Adapun keterangannya sebagai berikut :

- 1) Menampilkan informasi dari aplikasi pemanfaatan algoritma Beaufort sebagai pengamanan pesan pada aplikasi *chatting* dengan koneksi *Wifi Direct* berbasis Android.