BAB III
ANALISIS DAN PERANCANGAN

III.1. Analisis Masalah

Analisa sistem yang berjalan bertujuan untuk mengidentifikasi serta melakukan evaluasi terhadap sistem Keamanan Data SMS Dengan Menggunakan Kriptografi Vigenere Chipper Berbasis Android yang telah ada sebelumnya. Data SMS saat ini telah berkembang pesat terutama dibagian teknologi-teknologi dalam kebutuhan komunikasi modern, layanan SMS mulai dikembangkan untuk berbagai jaringan selain GSM seperti CDMA (*Code Division Multiple Access*) dan jaringan lain.

Seiring dengan perkembangan teknologi kemanan dalam teknologi merupakan hal yang sangat penting walaupun teknologi makin bekembang begitu cepat, tetapi layanan SMS tidak menjamin keamanan pesan yang akan disampaikan. Pesan yang bersifat personal atau rahasia tidak menjamin sampai ke penerima tanpa diketahui informasinya oleh pihak – pihak yang tidak bertanggung jawab.

Ada beberapa resiko yang dapat mengancam kemanan pesan yaitu SMS *Spoofing* dan SMS *Snoping*, sehingga para user harus mencari solusi agar pesan aman sampai kepada penerima. Salah satu cara mengamankan pesan adalah menggunakan metode algoritma vigenere cipher.

Hal ini dikarenakan algoritma vigenere cipher mudah diimplentasikan, algoritma vigenere chiper merupakan salah satu algoritma kriptografi klasik untuk menyandikan suatu plaintext dengan menggunakan teknik substitusi. Vigenere

cipher pada dasarnya cukup rumit untuk dipecahkan sehingga terbilang cukup aman dalam melakukan keamanan data terutama data sms yang akan dirancang penulis.

III.1.1. Strategi Pemecahan Masalah

Strategi dalam melakukan pemecahan masalah yang sedang dianalisa oleh penulis mengenai sistem sms menggunakan Kriptografi Vigenere Chipper adalah sebagai berikut :

1. Membuat aplikasi keamanan data SMS dalam jaringan yang dilengkapi keamanan data dengan algoritma Vigenere Cipher.
2. Meningkatkan jaminan keamanan dan privasi dalam proses keamanan data SMS saat pengguna melakukan komunikasi.
3. Mengetahui tingkat keamanan enkripsi data menggunakan algoritma Vigenere Chipper.
4. Mengetahui seberapa besar efektivitas enkripsi pada algoritma Vigenere Chipper.

III.1.2. Analisa Kebutuhan Fungsional

Kebutuhan fungsional yang dibutuhkan pada penggunaan sistem antara lain sebagai berikut :

1. User
    a. Melakukan percakapan melalui form sms yang telah disediakan oleh sistem.

III.1.3. Analisa Kebutuhan NonFungsional

Kebutuhan NonFungsional yang dibutuhkan dalam mengakses sistem adalah sebagai berikut :

1. Android,
2. intellij idea,
3. java sdk,
4. android sdk,
5. genymotion.

III.2. Penerapan Algoritma

Vigenere Chiper termasuk dalam cipher abjad majemuk (polyalphabetic substitution Chiper) yang dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigenere pada abad 16 (tahun 1586). Vigenere Chiper adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Vigenere Chiper menggunakan table, Vigenere Cipher dengan angka. dalam melakukan enkripsi. Teknik dari substitusi vigenere cipher bisadilakukan dengan dua cara yaitu angka dan huruf (Putu H. Arjana ; 2012 : 165).

III.2.1. Perhitungan Algoritma

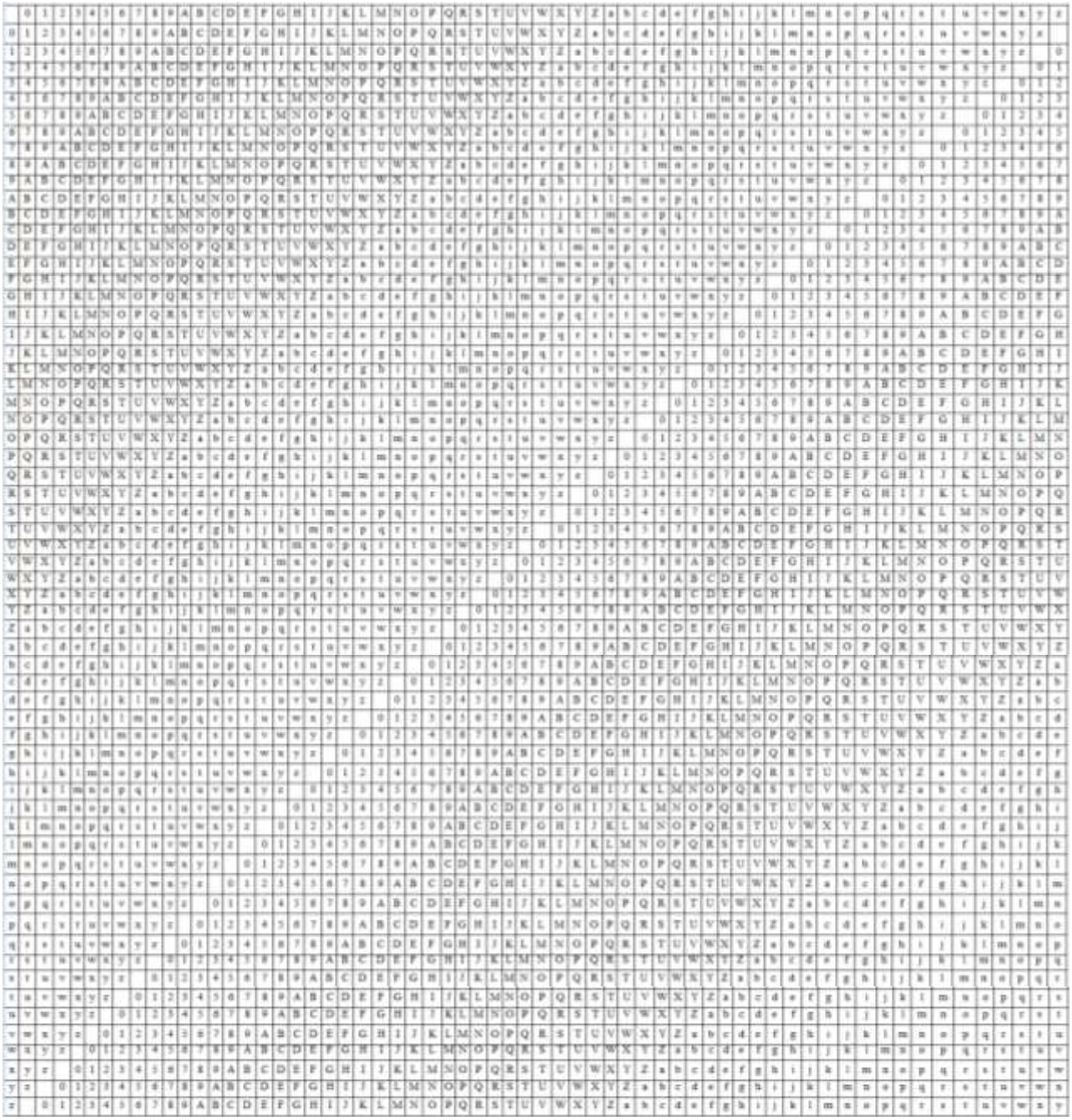
Berikut adalah perhitungan manual studi kasus dengan algoritma vigenere chipper, untuk lebih jelasnya maka akan dijabarkan seperti dibawah ini :

Pesan : **PIN ATM saya 188223**

Kunci: **R1T4ArDaNA**

Modulus : **63** (Jumlah Karakter Yang Didukung)

Tabel III.1. Tabel Vigenere



#PROSES ENKRIPSI

0. P->R (26+28) mod 63 = 54, Karakter(54) adalah r

1. I->1 (19+2) mod 63 = 21, Karakter(21) adalah K

2. N->T (24+30) mod 63 = 54, Karakter(54) adalah r

3. [spasi] ->4 (0+5) mod 63 = 5, Karakter(5) adalah 4

4. A->A (11+11) mod 63 = 22, Karakter(22) adalah L

5. T->r (30+54) mod 63 = 21, Karakter(21) adalah K

6. M->D (23+14) mod 63 = 37, Karakter(37) adalah a

7.[spasi] ->a (0+37) mod 63 = 37, Karakter(37) adalah a

8. s->N (55+24) mod 63 = 16, Karakter(16) adalah F

9. a->A (37+11) mod 63 = 48, Karakter(48) adalah l

10. y->R (61+28) mod 63 = 26, Karakter(26) adalah P

11. a->1 (37+2) mod 63 = 39, Karakter(39) adalah c

12. [spasi] ->T (0+30) mod 63 = 30, Karakter(30) adalah T

13. 1->4 (2+5) mod 63 = 7, Karakter(7) adalah 6

14. 8->A (9+11) mod 63 = 20, Karakter(20) adalah J

15. 8->r (9+54) mod 63 = 0, Karakter(0) adalah [spasi]

16. 2->D (3+14) mod 63 = 17, Karakter(17) adalah G

17. 2->a (3+37) mod 63 = 40, Karakter(40) adalah d

18. 3->N (4+24) mod 63 = 28, Karakter(28) adalah R

Pesan: PIN ATM saya 188223

Kunci: R1T4ArDaNAR1T4ArDaN

Chipper: rKr4LKaaFlPcT6J GdR

#PROSES DEKRIPSI

0. r->R (54-28) mod 63 = 26, Karakter(26) adalah P

1. K->1 (21-2) mod 63 = 19, Karakter(19) adalah I

2. r->T (54-30) mod 63 = 24, Karakter(24) adalah N

3. 4->4 (5-5) mod 63 = 0, Karakter(0) adalah [spasi]

4. L->A (22-11) mod 63 = 11, Karakter(11) adalah A

5. K->r (21-54) mod 63 = 30, Karakter(30) adalah T

6. a->D (37-14) mod 63 = 23, Karakter(23) adalah M

7. a->a (37-37) mod 63 = 0, Karakter(0) adalah [spasi]

8. F->N (16-24) mod 63 = 55, Karakter(55) adalah s

9. l->A (48-11) mod 63 = 37, Karakter(37) adalah a

10. P->R (26-28) mod 63 = 61, Karakter(61) adalah y

11. c->1 (39-2) mod 63 = 37, Karakter(37) adalah a

12. T->T (30-30) mod 63 = 0, Karakter(0) adalah [spasi]

13. 6->4 (7-5) mod 63 = 2, Karakter(2) adalah 1

14. J->A (20-11) mod 63 = 9, Karakter(9) adalah 8

15. [spasi] ->r (0-54) mod 63 = 9, Karakter(9) adalah 8

16. G->D (17-14) mod 63 = 3, Karakter(3) adalah 2

17. d->a (40-37) mod 63 = 3, Karakter(3) adalah 2

18. R->N (28-24) mod 63 = 4, Karakter(4) adalah 3

Chipper: rKr4LKaaFlPcT6J GdR

Kunci: R1T4ArDaNAR1T4ArDaN

Plain Text: PIN ATM saya 188223

III.3. Perancangan

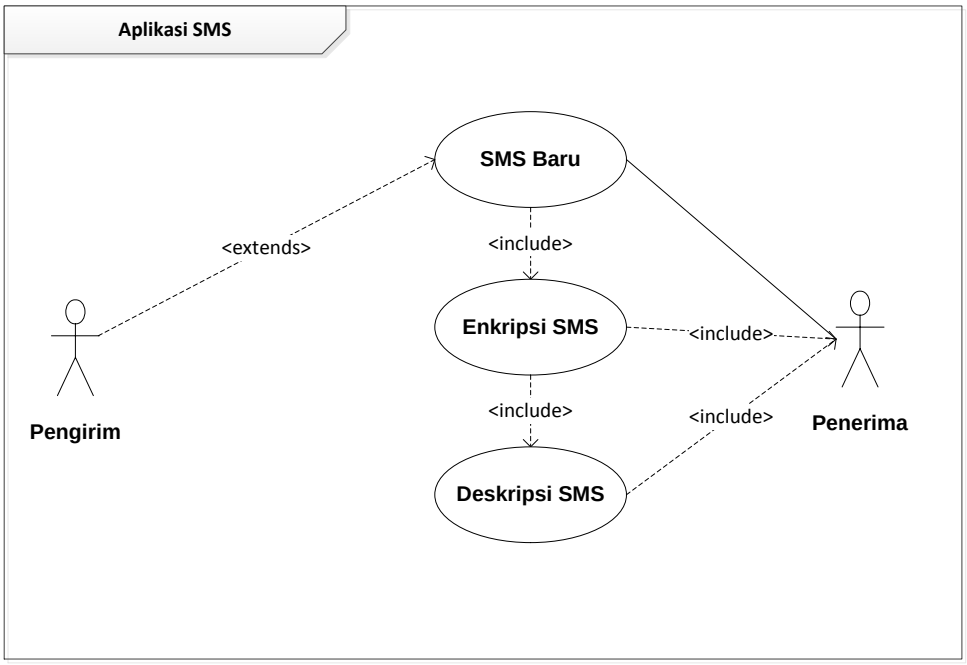
Desain sistem pada penelitian ini dibagi menjadi dua desain, yaitu desain sistem secara global untuk penggambaran model sistem secara garis besar dan desain sistem secara detail untuk membantu dalam pembuatan sistem.

III.3.1. Desain Sistem Secara Global

Desain sistem secara global menggunakan bahasa pemodelan UML yang terdiri dari *Usecase Diagram*, *Acitvity Diagram*, *Class Diagram*, dan *Sequence Diagram*.

III.3.1.1. *Usecase* Diagram

Secara garis besar, bisnis proses sistem yang akan dirancang digambarkan dengan *usecase diagram* yang terdapat pada Gambar III.1 :



Gambar III.1 *Use Case* Diagram Aplikasi Sms

Penjelasan :

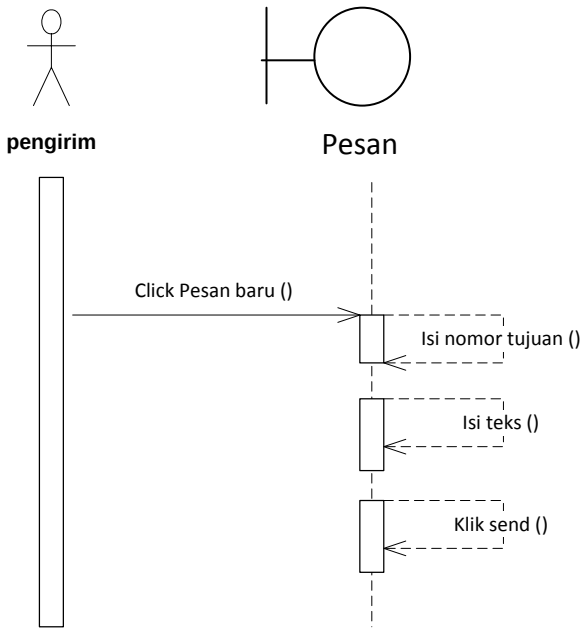
1. Pengirim membuat data sms baru.
2. Pada sms baru, pengirim mengisi data nomor tujuan dan data isi sms.
3. Saat melakukan pengiriman pesan, maka aplikasi akan memunculkan form enkripsi sms, pengirim mengisi *password* untuk enkripsi data sms.
4. Kemudian data dikirim.
5. Pada saat penerima menerima sms, maka penerima terlebih dahulu melakukan deskripsi sms dengan memasukkan *password* data sms untuk membaca pesan yang telah dikirim.

III.3.1.2. *Sequence* Diagram

Rangkaian kegiatan pada setiap terjadi *event* sistem digambarkan pada *sequence* diagram berikut:

1. *Sequence* Diagram Keamanan Data SMS

Aktifitas untuk keamanan data sms dengan menggunakan kriptografi vigenere terlihat seperti pada gambar III.2 berikut :



Gambar.III.2. *Sequence* Diagram Keamanan Data SMS

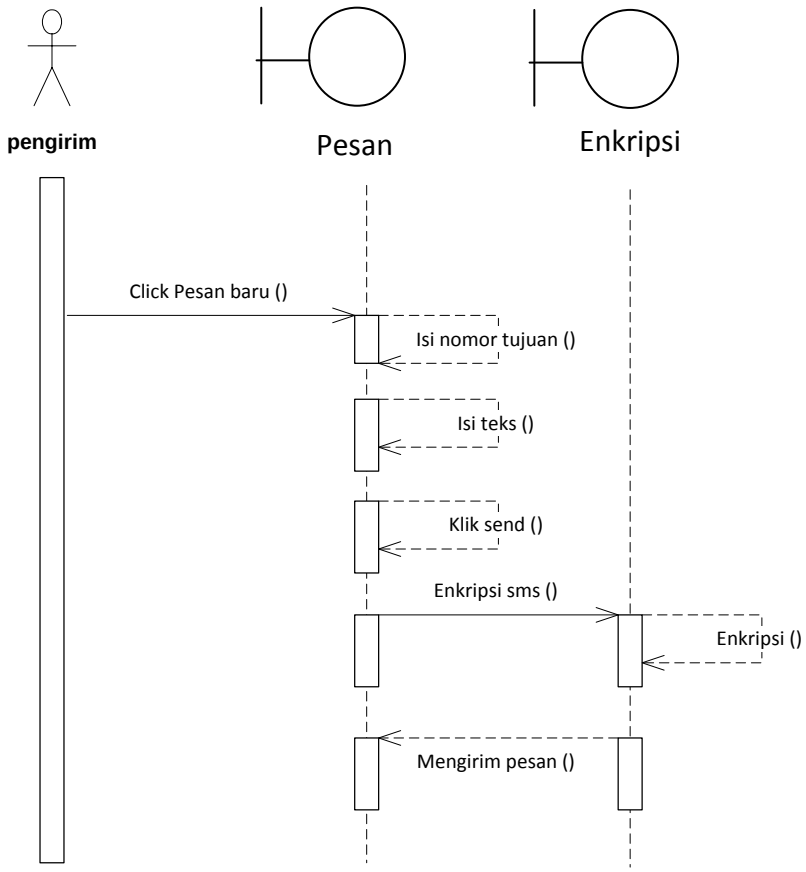
Penjelasan :

a. Pengirim membuat sms baru.

b. Pada sms baru, pengirim mengisi data nomor tujuan dan data isi sms kemudian mengirim data.

2. *Sequence* Diagram Enkripsi Data SMS

Aktifitas untuk enkripsi data sms dengan menggunakan kriptografi vigenere terlihat seperti pada gambar III.4 berikut :



Gambar.III.3. *Sequence* Diagram Enkripsi Data SMS

Penjelasan :

a. Pengirim membuat data sms baru.

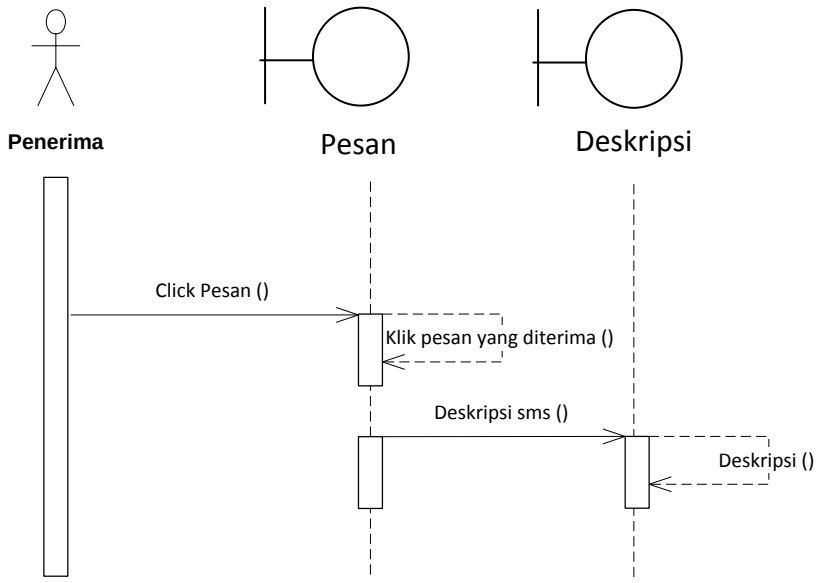
b. Pada sms baru, pengirim mengisi data nomor tujuan dan data isi sms.

c. Saat melakukan pengiriman pesan, maka aplikasi akan memunculkan form enkripsi sms, pengirim mengisi *password* untuk enkripsi data sms.

d. Kemudian data dikirim.

3. *Sequence* Diagram Deskripsi Data SMS

Aktifitas untuk deskripsi data sms dengan menggunakan kriptografi vigenere terlihat seperti pada gambar III.5 berikut :



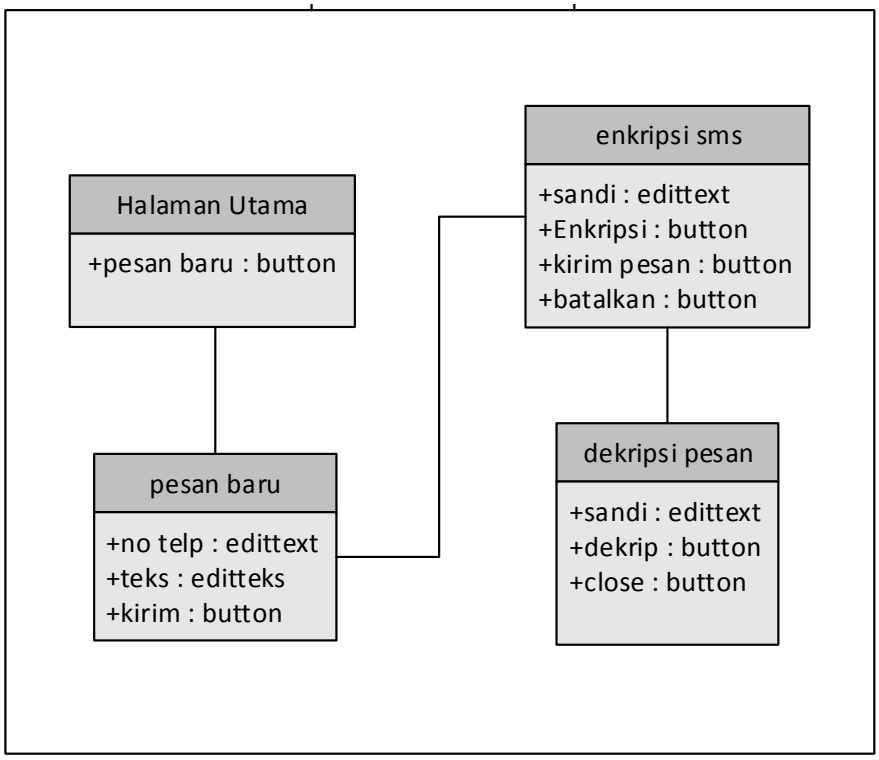
Gambar.III.4. *Sequence* Diagram Deskripsi Data SMS

Penjelasan :

a. Pada saat penerima menerima sms, maka penerima terlebih dahulu melakukan deskripsi sms dengan memasukkan *password* data sms untuk membaca pesan yang telah dikirim.

III.3.1.3. *Class* Diagram

Untuk mendapatkan hasil rancangan yang baik dan tersetruktur serta untuk menjelaskan hubbungan antara objek yang satu dengan objek yang lainnya dalam sistem yang diusulkan, maka penulis membuat sebuah class diagram. Pada class diagram ini akan mendekripsikan jenis – jenis objek dalam sistem dan berbagai macam hubungan statis yang terjadi serta akan menunjukkan propety dan operasi sebuah objek dan batasan yang terdapat dalam hubungan dengan objek lain.



Gambar.III.5. *Class* Diagram Keamanan Data SMS

Penjelasan :

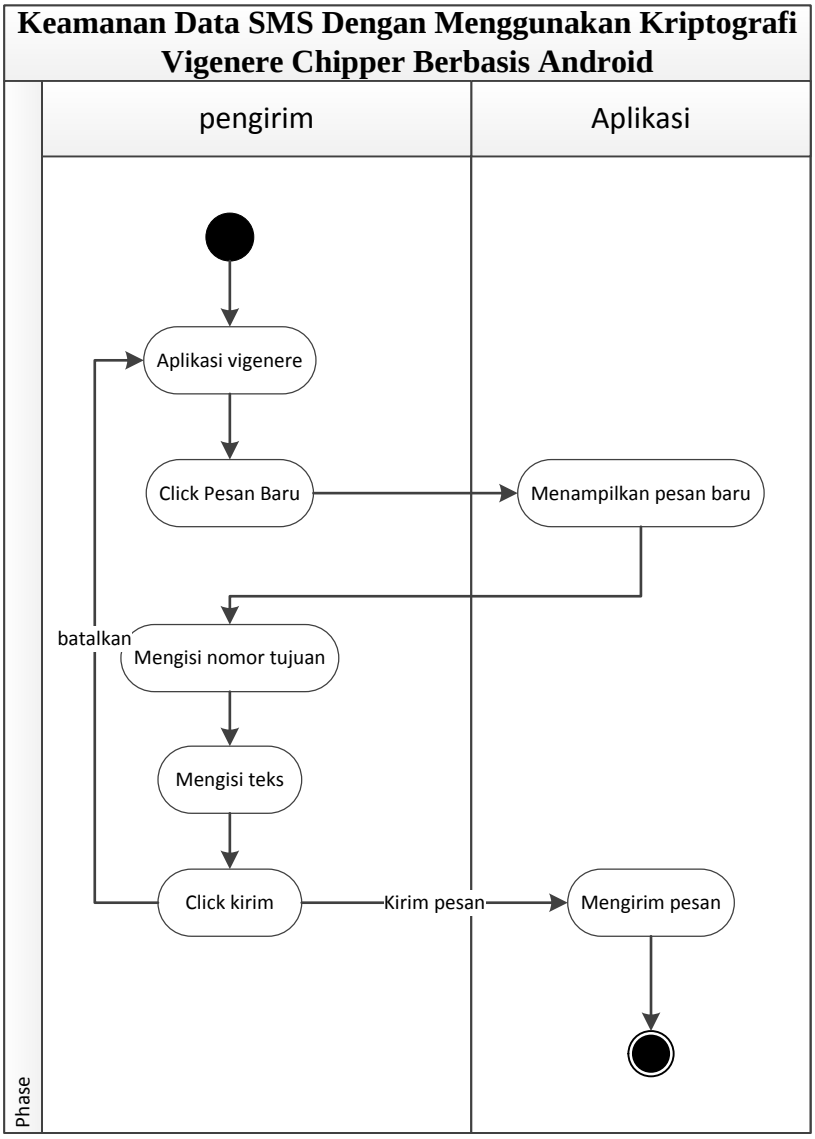
1. Pada form halaman utama, terdapat menu pesan baru.
2. Pada form pesan baru, terdapat menu untuk mengisi data telp dan data teks kemudian tombol kirim.
3. Pada form enkripsi, terdapat menu untuk mengisi data sandi dan tombol enkripsi, kirim pesan dan batalkan.
4. Pada form dekripsi pesan, terdapat menu untuk mengisi kata sandi, tombol dekrip dan tombol close.

III.3.1.4. *Acitvity* Diagram

Bisnis proses yang telah digambarkan pada *use case diagram* dijabarkan dengan *Acitvity diagram* :

1. Activity Diagram Keamanan Data SMS

Aktifitas untuk Keamanan Data SMS terlihat seperti pada gambar III.6 berikut :



Gambar.III.6. *Acitvity* Diagram Keamanan Data SMS

Penjelasan :

a. Pengirim membuka aplikasi vigenere.

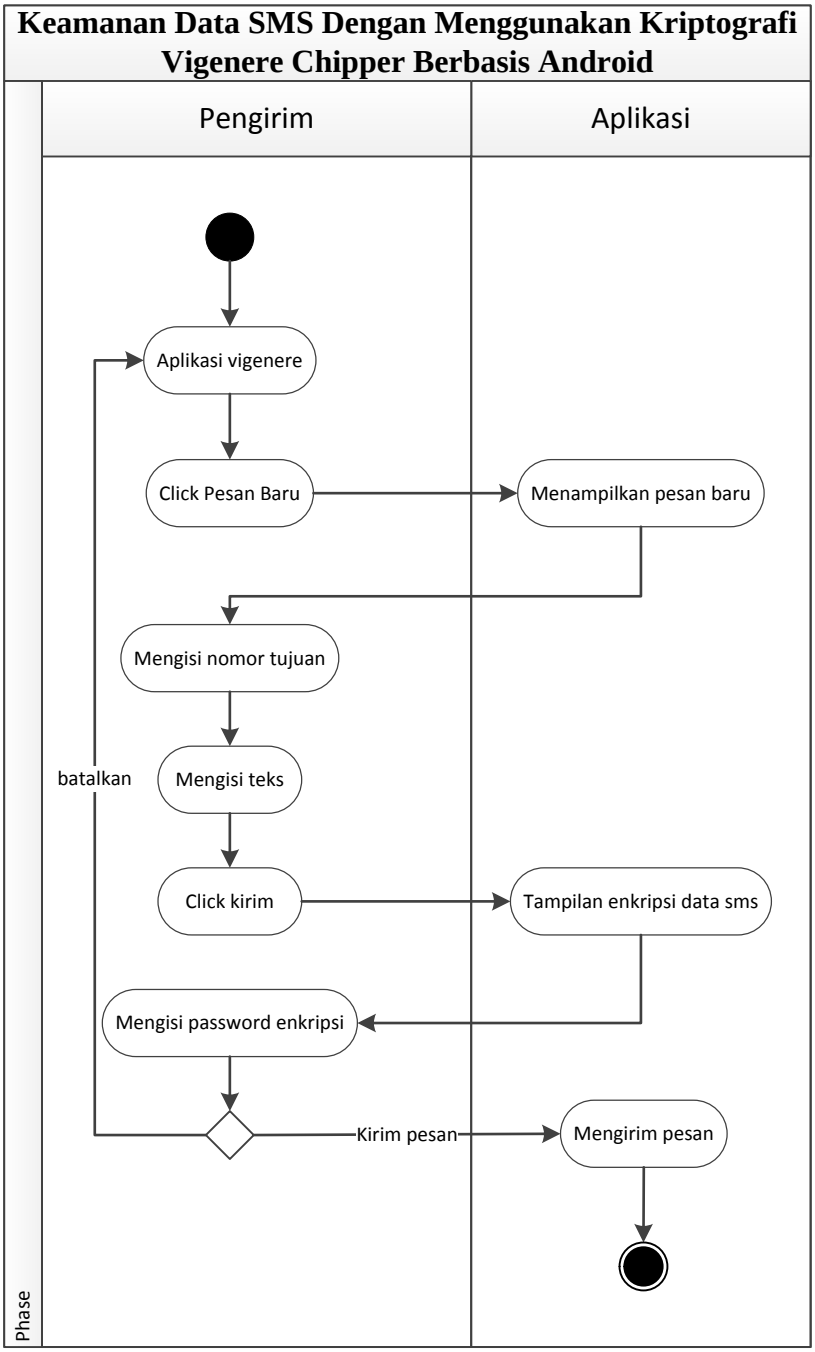
b. Kemudian mengklik pesan baru, aplikasi akan menampilkan pesan baru.

c. Pada sms baru, pengirim mengisi data nomor tujuan dan data isi sms.

d. Kemudian klik kirim, kemudian aplikasi akan mengirim pesan.

2. Activity Diagram Enkripsi Data SMS

Aktifitas untuk enkripsi Data SMS terlihat seperti pada gambar III.7 berikut :



Gambar.III.7. *Acitvity* Diagram Enkripsi Data SMS

Penjelasan :

a. Pengirim membuka aplikasi vigenere.

b. Kemudian mengklik pesan baru, aplikasi akan menampilkan pesan baru.

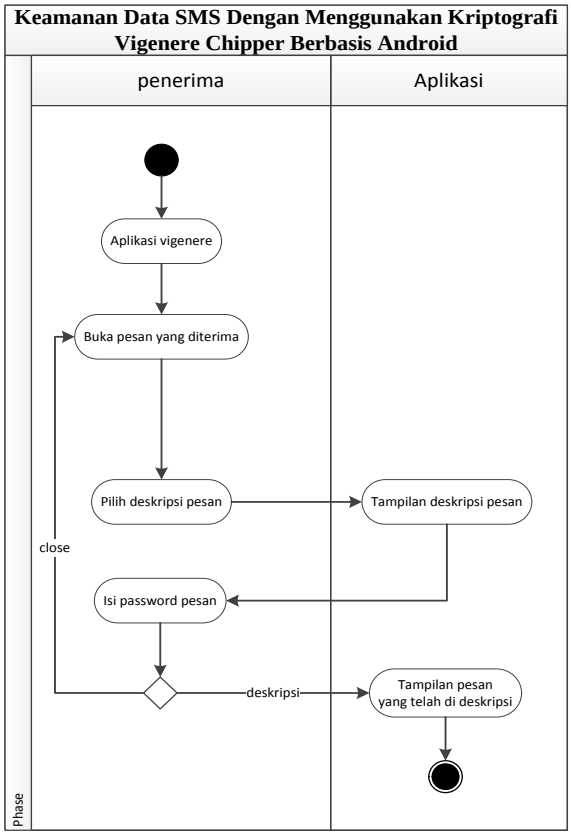
c. Pada sms baru, pengirim mengisi data nomor tujuan dan data isi sms.

d. Kemudian klik kirim, kemudian aplikasi akan menampilkan form enkripsi data sms.

e. Kemudian pengirim mengisi data password sms, kemudian aplikasi akan mengirim data sms.

3. Activity Diagram Deskripsi Data SMS

Aktifitas untuk deskripsi Data SMS terlihat seperti pada gambar III.8 berikut :



Gambar.III.8. *Acitvity* Diagram Deskripsi Data SMS

Penjelasan :

a. penerima membuka aplikasi vigenere.

b. Kemudian mengklik pesan yang diterima.

c. Kemudian penerima memilih deskripsi data sms dan mengisi password data sms untuk membaca pesan tersebut.

III.3.2. Desain Sistem Secara Detail

Berikut ini adalah rancangan tampilan desain sistem yang akan dihasilkan oleh sistem:

1. Desain Form Tampilan Awal Aplikasi Vigenere

Desain form tampilan awal aplikasi vigenere terlihat seperti pada gambar III.9 berikut :

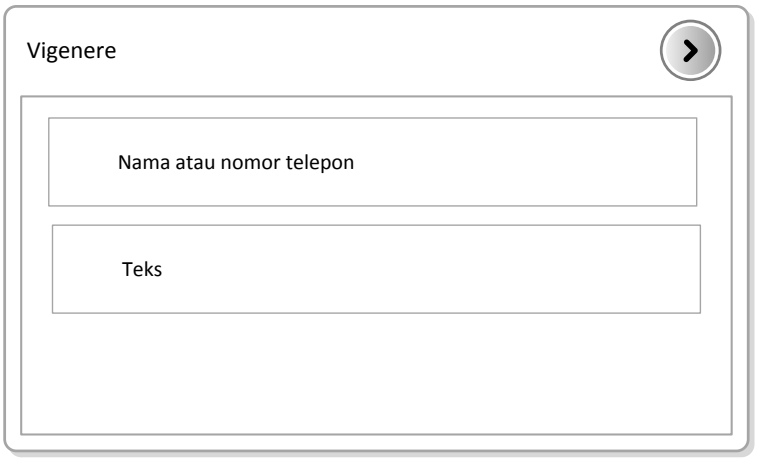
Gambar.III.9. Desain Tampilan Awal Aplikasi Vigenere

Penjelasan :

Form Tampilan Awal Aplikasi Vigenere berfungsi sebagai tampilan awal dari aplikasi keamanan data SMS yang telah dirancang oleh penulis.

2. Desain Form Pesan Baru

Desain form untuk membuat pesan baru terlihat seperti pada gambar III.10 berikut :



Gambar.III.10. Desain Form Pesan Baru

Penjelasan :

Form Pesan Baru berfungsi sebagai form untuk membuat pesan SMS baru yang dilakukan oleh pengirim.

3. Desain Form Enkripsi Pesan

Desain form untuk mengenkripsi pesan terlihat seperti pada gambar III.11 berikut :

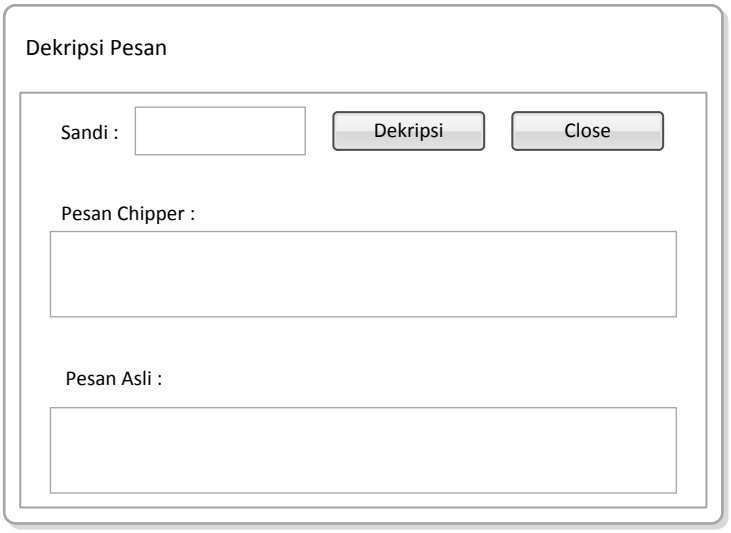
Gambar.III.11. Desain Form Enkripsi Pesan

Penjelasan :

Form enkripsi pesan berfungsi sebagai form untuk melakukan enkripsi data sms yaitu dengan memasukkan sandi atau password untuk mengunci data sms sebelum dikirim kemudian pengirim mengklik tombol enkripsi pesan dan mengirim pesan.

4. Desain Form Deskripsi Pesan

Desain form untuk deskripsi pesan terlihat seperti pada gambar III.12 berikut:



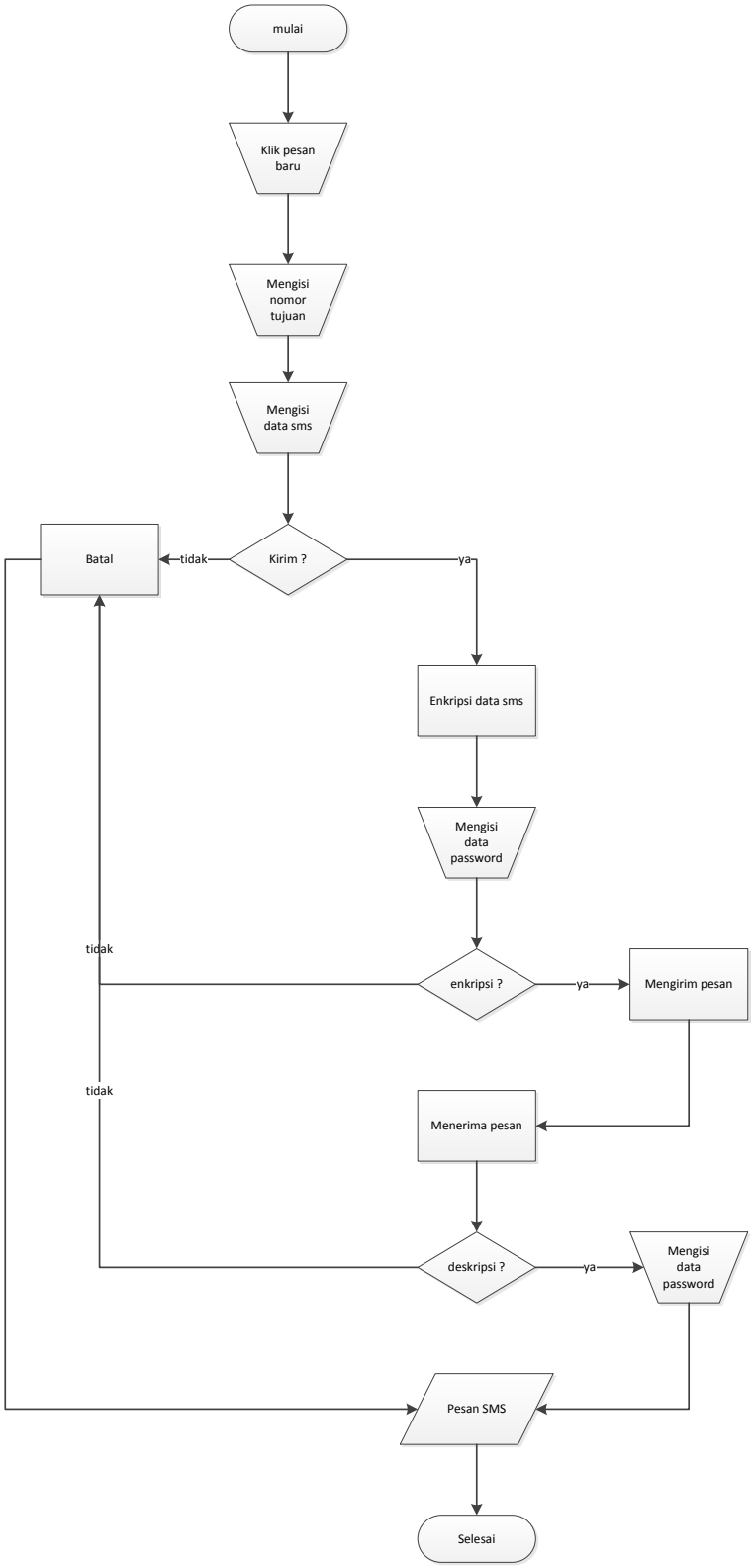
Gambar.III.12. Desain Form Deskripsi Pesan

Penjelasan :

Form deskripsi pesan berfungsi sebagai form untuk melakukan deskripsi data sms yaitu dengan memasukkan sandi atau password untuk mengunci data sms untuk membaca pesan tersebut.

III.4. *Flowchart* Keamanan Data SMS Vigenere Chipper

Flowchart adalah penggambaran secara grafik dari langkah-langkah dan urut-urutan prosedur dari suatu program. *Flowchart* menolong analis dan programmer untuk memecahkan masalah kedalah segmen-segmen yang lebih kecil dan menolong dalam menganalisis alternatif-alternatif lain dalam pengoperasian. Berikut adalah *flowchart* untuk keamanan data sms menggunakan algoritma vigenere :



Gambar III.13. *Flowchart* Keamanan Data SMS