

BAB III

ANALISIS DAN PERANCANGAN

III.1. Analisis Masalah

Kebanyakan orang menggunakan MySQL untuk penyimpanan data karena selain penggunaannya yang mudah dan gratis untuk digunakan, MySQL dapat menampung jumlah data yang sangat banyak. Data yang tersimpan pada MySQL umumnya tersimpan pada localhost dan data dalam MySQL juga dapat disimpan dalam bentuk *script*, sehingga pengguna dapat dengan mudah memindahkan data MySQL ke komputer lain. Namun akan menjadi masalah ketika orang yang berniat jahat mendapatkan *script* tersebut. Isi data yang berharga di dalam basis data MySQL dapat dicuri dan digunakan oleh pihak yang tidak diinginkan, sehingga merugikan pemilik isi basis data MySQL. Oleh karena itu dibutuhkan sebuah cara yang dapat diterapkan untuk keamanan pada isi sebuah basis data MySQL. Cara yang dapat digunakan yaitu menerapkan kriptografi pada isi sebuah basis data MySQL. Dalam penggunaan kriptografi diperlukan adanya metode yang dapat memproses sebuah pesan asli menjadi pesan rahasia. Oleh karena itu peneliti merekomendasikan metode *rail fence cipher*. Namun metode *rail fence cipher* tidak memiliki kunci yang baik seperti halnya pada metode kriptografi yang lain, sehingga keamanannya masih dapat diragukan. Oleh karena itu peneliti menambahkan metode ROT13 pada metode *rail fence cipher*. Dengan adanya penerapan metode *rail fence cipher* dan ROT13 maka *script* MySQL dapat diamankan.

III.2. Strategi Pemecahan Masalah

Strategi pemecahan masalah keamanan *script* MySQL adalah sebagai berikut :

1. Dengan menerapkan teknik kriptografi pada *script* MySQL maka dapat mengatasi masalah keamanan *script* MySQL..
2. Dengan menggunakan metode *rail fence cipher* dan ROT13 maka dapat mengubah isi *script* MySQL menjadi tidak diketahui oleh pencuri informasi.
3. Dengan menciptakan aplikasi yang dapat mengamankan *script* MySQL maka dapat menjadi solusi untuk masalah keamanan data.

III.3. Penerapan Metode

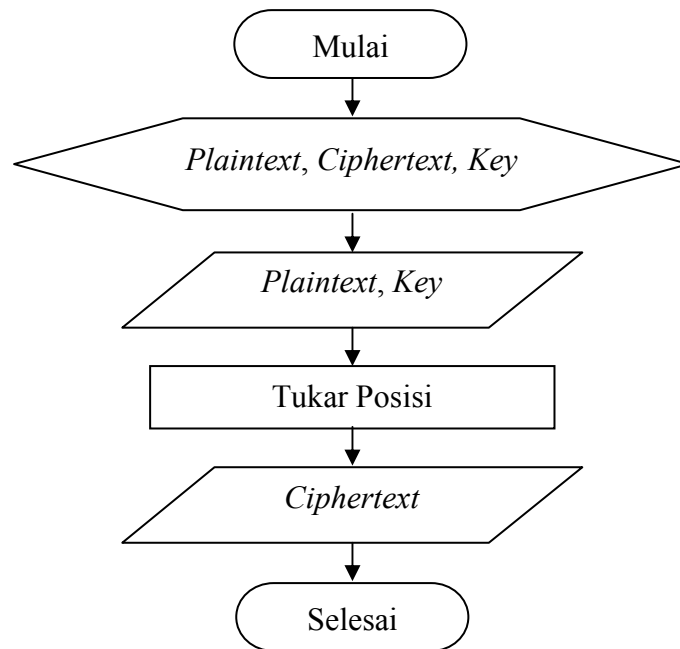
Berikut ini adalah rumus dan langkah dari metode *rail fence cipher* dan ROT13 beserta contoh perhitungannya :

III.3.1. Metode *Rail Fence Cipher*

Pada *Rail Fence Cipher*, plainteks dituliskan secara vertikal ke bawah sepanjang *n-rails*, dan menulis lagi ke kolom baruketika telah mencapai karakter ke-*n*. Cipherteks yang dihasilkan adalah urutan karakter yang dibaca secara horizontal.

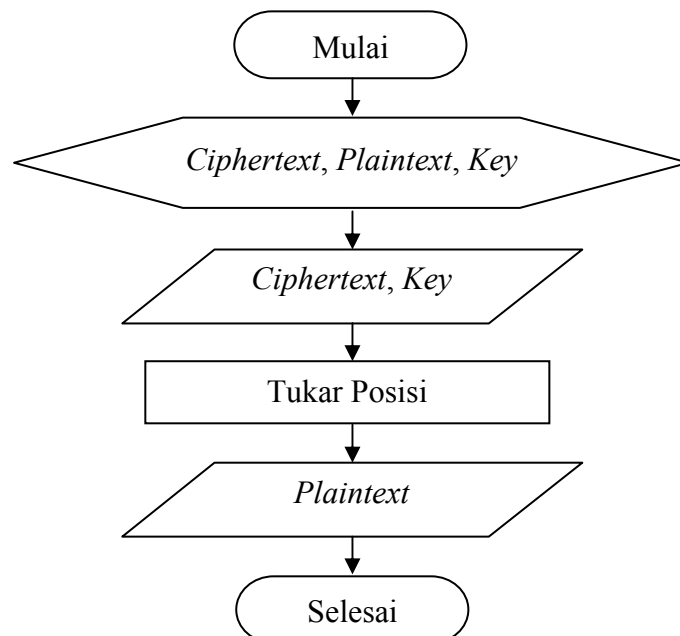
1. Flowchart Metode Railfence Cipher

a. Enkripsi



Gambar III.1. Flowchart Enkripsi Metode Railfence Cipher

b. Dekripsi



Gambar III.2. Flowchart Dekripsi Metode Railfence Cipher

2. Studi Kasus :

Berikut ini contoh enkripsi dari penerapan metode *rail fence cipher* :

Plaintext : MAAFLAHIRBATIN

Key : 3

| | | | | |
|---|---|---|---|---|
| M | F | H | B | I |
| A | L | I | A | N |
| A | A | R | T | |

Hasil enkripsi *Railfence Cipher*

Ciphertext :MFHBIALIANAART

Berikut ini contoh Dekripsi dari penerapan metode *rail fence cipher* :

Hitung Jumlah Karakter *Ciphertext*, selanjutnya Bagikan dengan Nilai Kunci Dekripsi, Maka hasilnya sebagai Kunci Dekripsi.

Ciphertext:

MFHBIALIANAART = 15

Key Lama : 3

Key Dekripsi : $15/3 = 5$

| | | |
|---|---|---|
| M | A | A |
| F | L | A |
| H | I | R |
| B | A | T |
| I | N | |

Plaintext :MAAFLAHIRBATIN

III.3.2. Metode ROT13

Enkrip metode ROT13 menggunakan penjumlahan *ASCII plaintext* dengan 13 sebagai berikut :

$$C_i = P_i + 13 \dots \dots \dots (1)$$

Keterangan :

C_i = *Ciphertext* hasil enkrip

P_i = *Plaintext* yang akan dienkrip

Dekrip metode ROT13 menggunakan pengurangan *ASCII ciphertext* dengan 13 sebagai berikut :

$$P_i = C_i - 13 \dots \dots \dots (2)$$

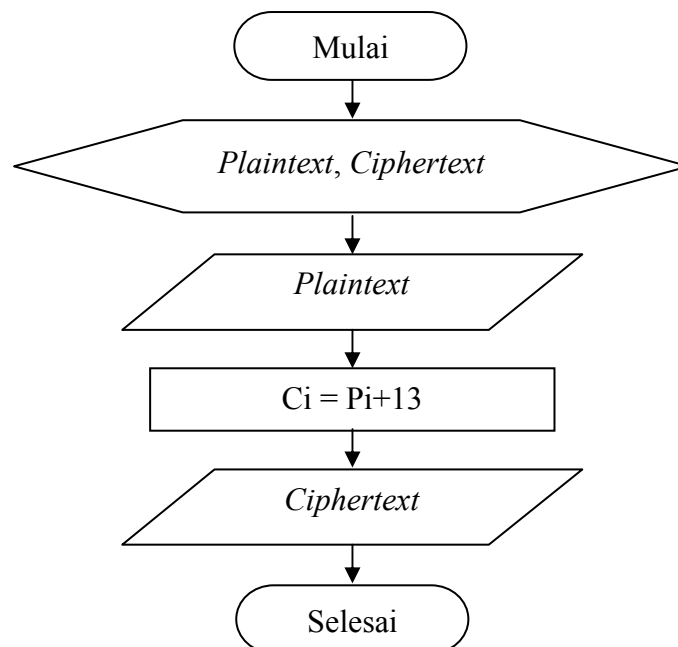
Keterangan :

C_i = *Ciphertext* yang akan didekrip

P_i = *Plaintext* hasil dekrip

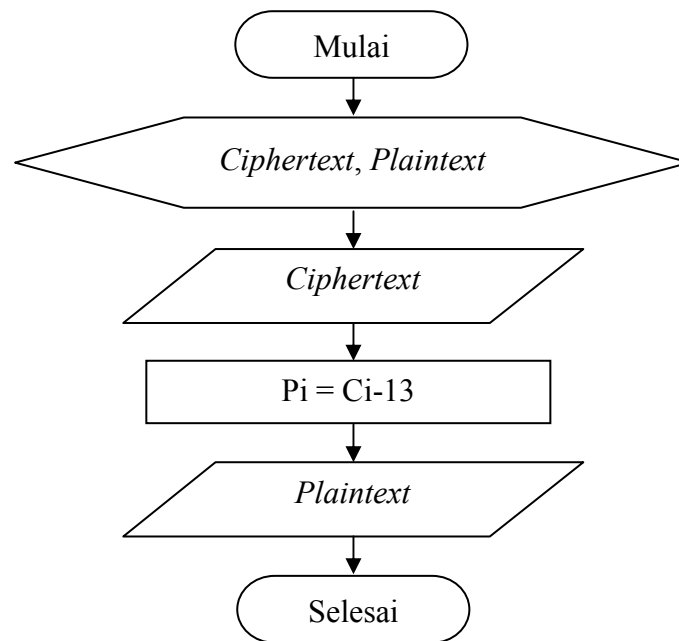
1. Flowchart Metode ROT13

a. Enkripsi



Gambar III.3. Flowchart Enkripsi Metode ROT13

b. Dekripsi



Gambar III.4. Flowchart Dekripsi Metode ROT13

Studi Kasus :

Contoh Proses Enkrip dari penerapan metode ROT13:

Plaintext : ABC

Solusi :

Ascii Plaintext :

$$A = 65$$

$$B = 66$$

$$C = 67$$

$$C1 = 65 + 13$$

$$= 78$$

$$C2 = 66 + 13$$

$$= 79$$

$$\begin{aligned}C3 &= 67 + 13 \\ &= 80\end{aligned}$$

Ascii Chipertext : NOQ

Contoh Proses Dekrip dari penerapan metode ROT13 :

Ascii Ciphertext :

$$N = 78$$

$$O = 79$$

$$Q = 80$$

$$\begin{aligned}C1 &= 78 - 13 \\ &= 65\end{aligned}$$

$$\begin{aligned}C2 &= 79 - 13 \\ &= 66\end{aligned}$$

$$\begin{aligned}C3 &= 80 - 13 \\ &= 66\end{aligned}$$

Plaintext: ABC

III.4. Desain Sistem

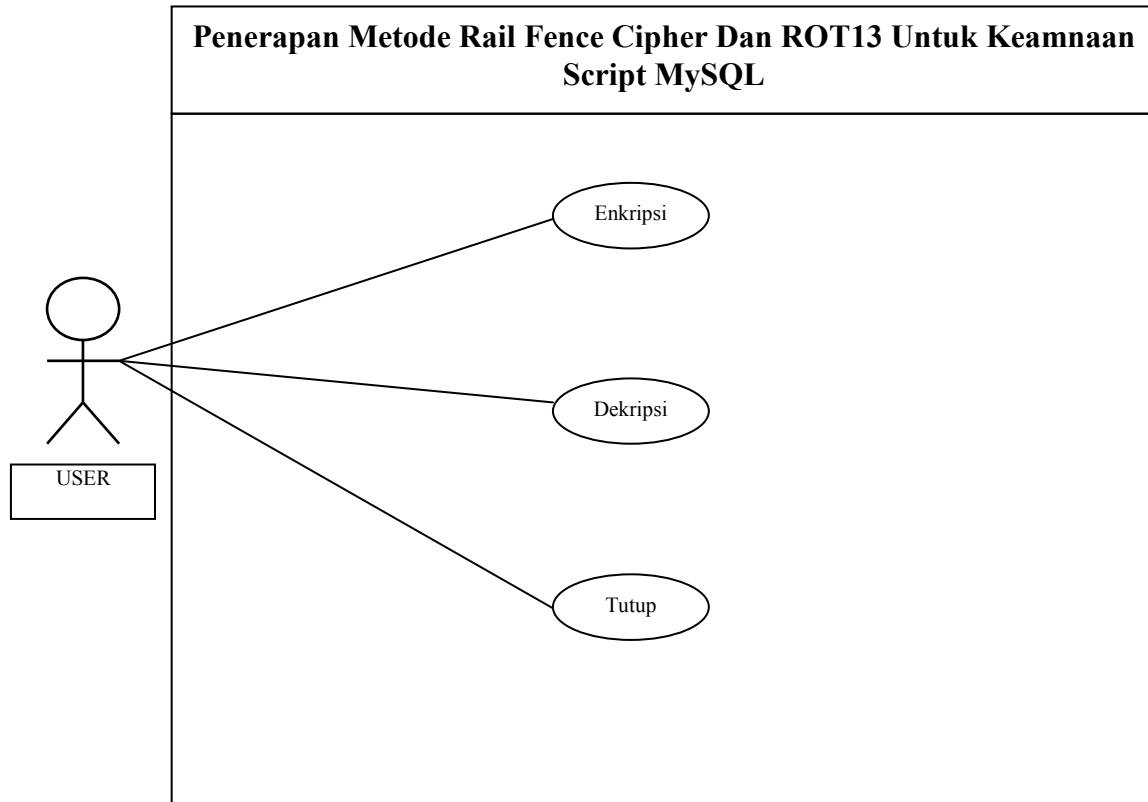
III.4.1. Desain Sistem Pemodelan UML

Bentuk rancangan sistem yang penulis buat menggunakan beberapa bentuk diagram dari *Unified Modeling Language* (UML) yaitu *Use Case Diagram*, *Class Diagram* dan *Activity Diagram*.

III.4.1.1. Use Case Diagram

Use case diagram Penerapan Metode Rail Fence Cipher Dan ROT13

Untuk Keamanan Script MySQL dapat dilihat pada gambar III.5 sebagai berikut :



Gambar III.5. Use Case Penerapan Metode Rail Fence Cipher Dan ROT13 Untuk Keamanan Script MySQL

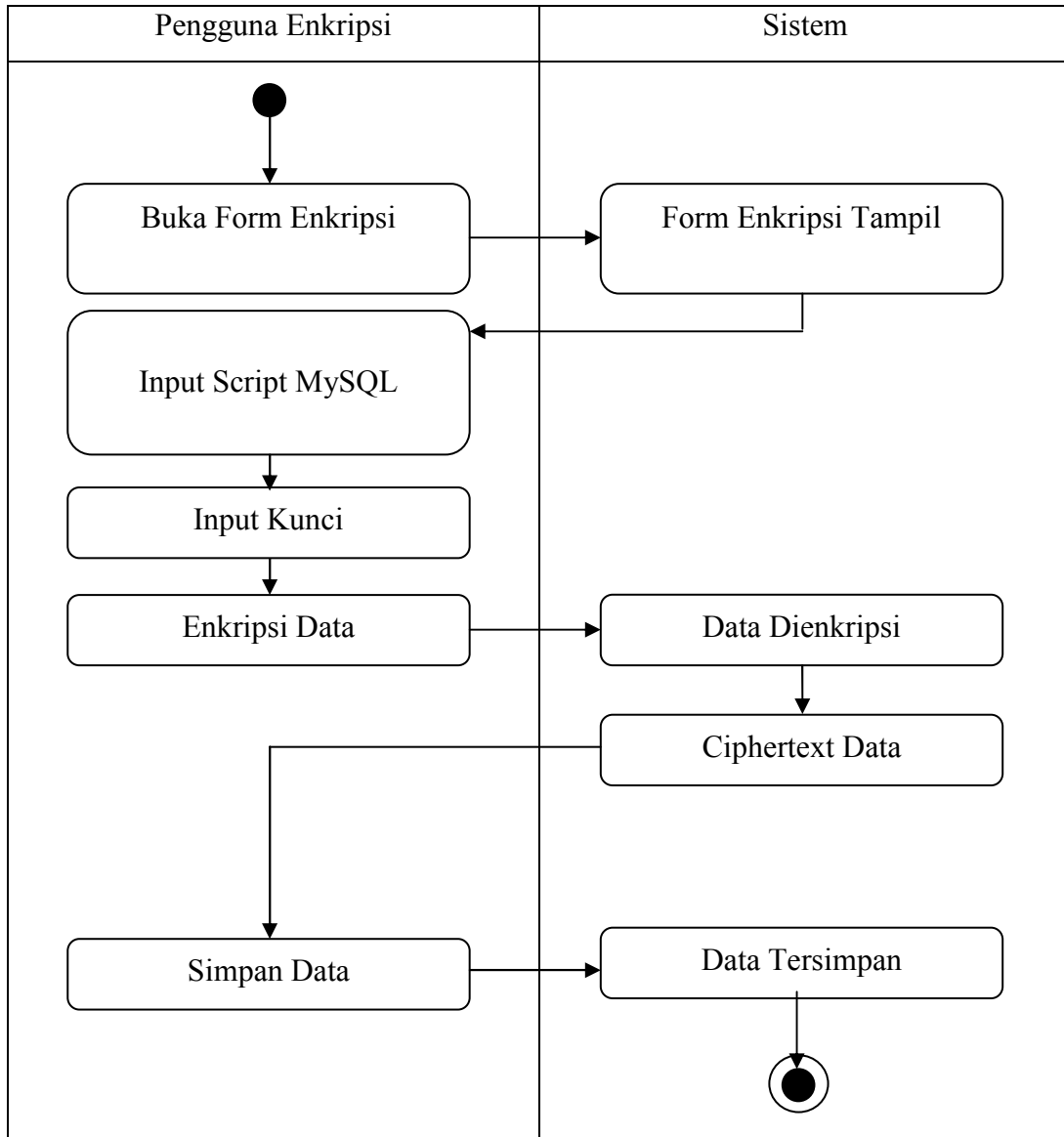
III.4.1.2. Activity Diagram

Activity diagram Penerapan Metode Rail Fence Cipher Dan ROT13

Untuk Keamanan Script MySQL dapat dilihat sebagai berikut :

1. Activity Diagram Enkripsi

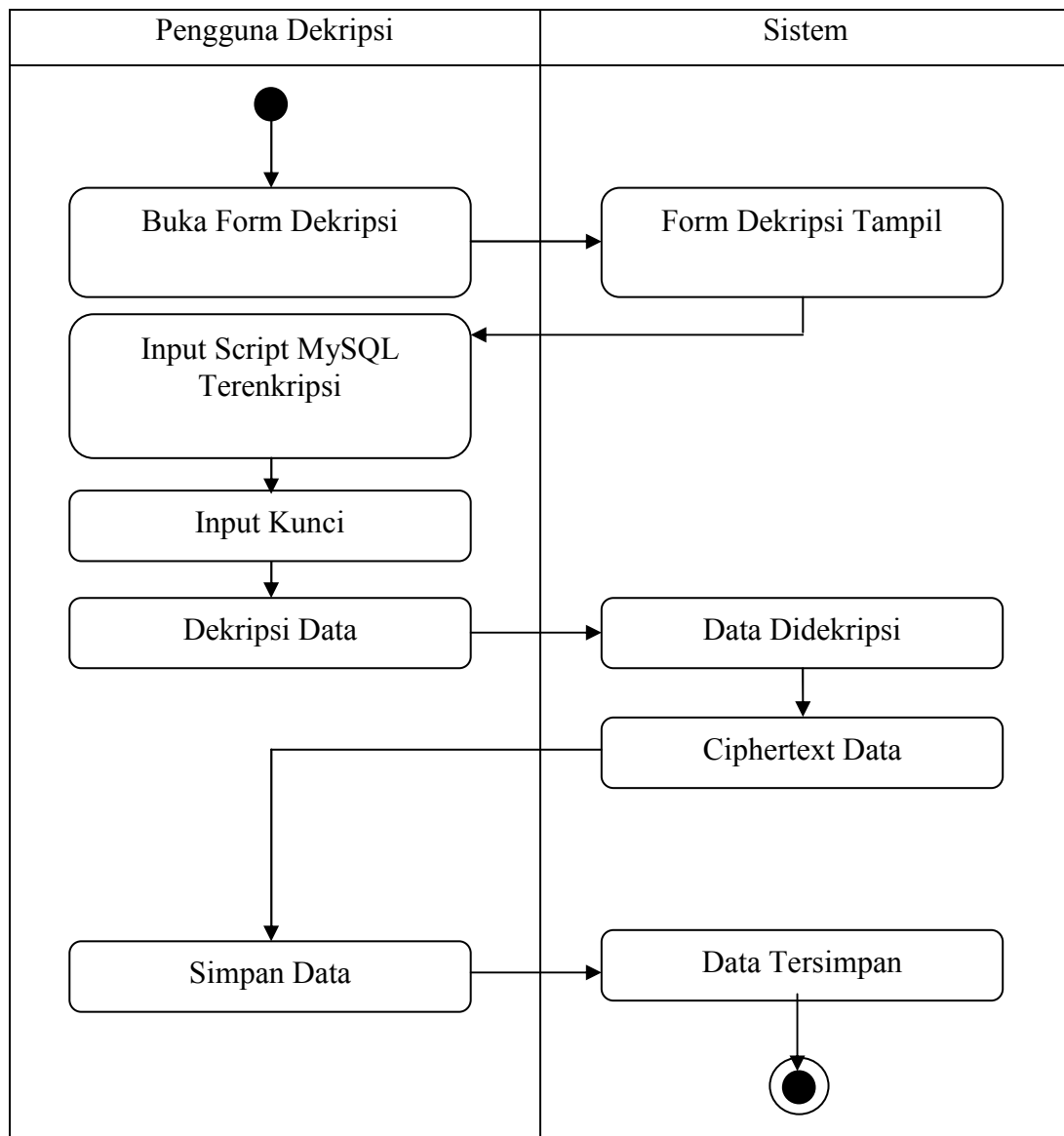
Activity Diagram dalam melakukan proses enkripsi dapat terlihat seperti pada gambar III.6 sebagai berikut :



Gambar III.6. Activity Diagram Enkripsi

2. Activity Diagram Dekripsi

Activity Diagram dalam melakukan proses dekripsi dapat terlihat seperti pada gambar III.7 sebagai berikut :



Gambar III.7. Activity Diagram Dekripsi

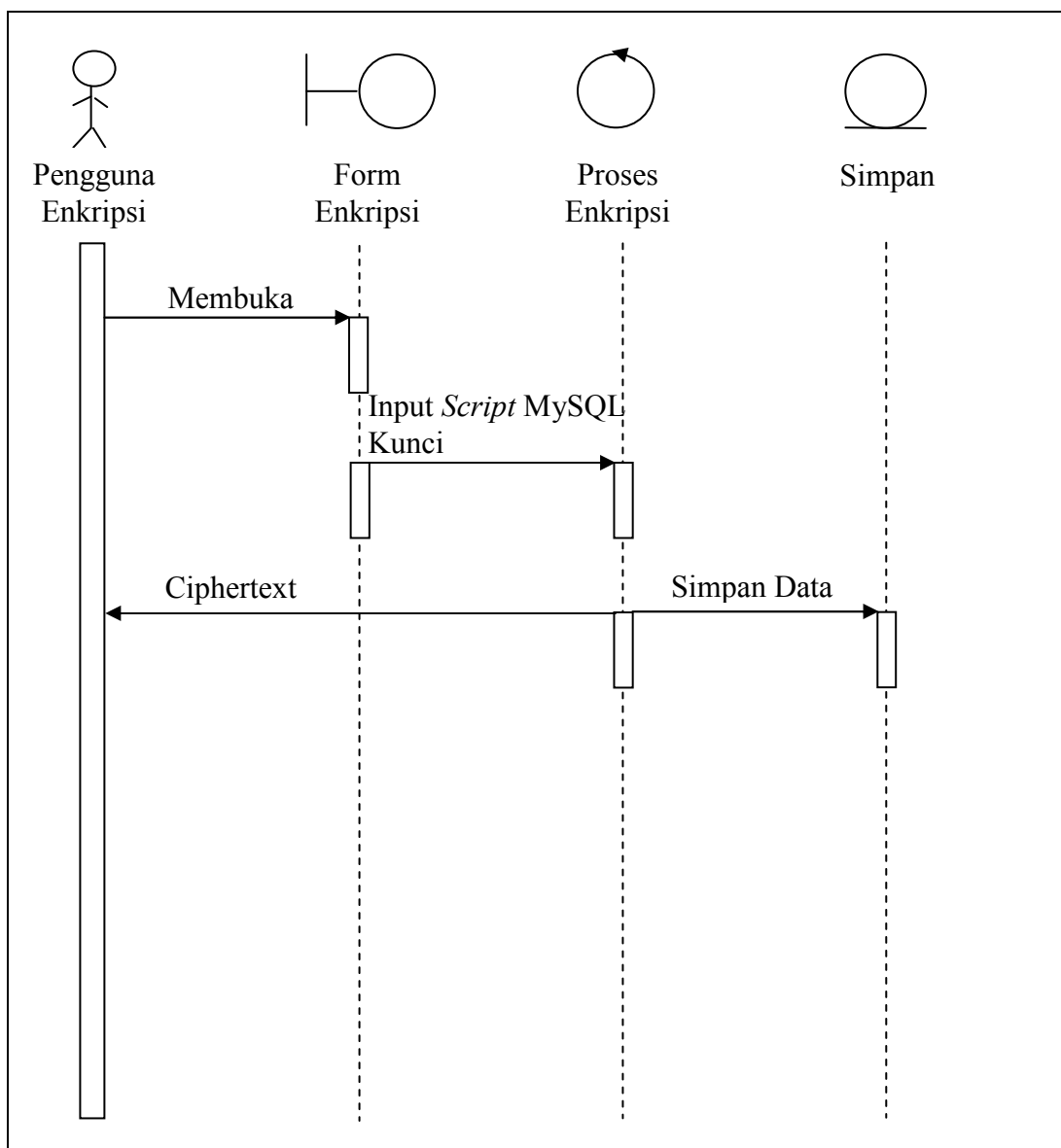
III.4.1.3. *Sequence Diagram*

Sequence diagram Penerapan Metode *Rail Fence Cipher* Dan ROT13

Untuk Keamanan *Script MySQL* sebagai berikut :

1. *Sequence Diagram* Enkripsi

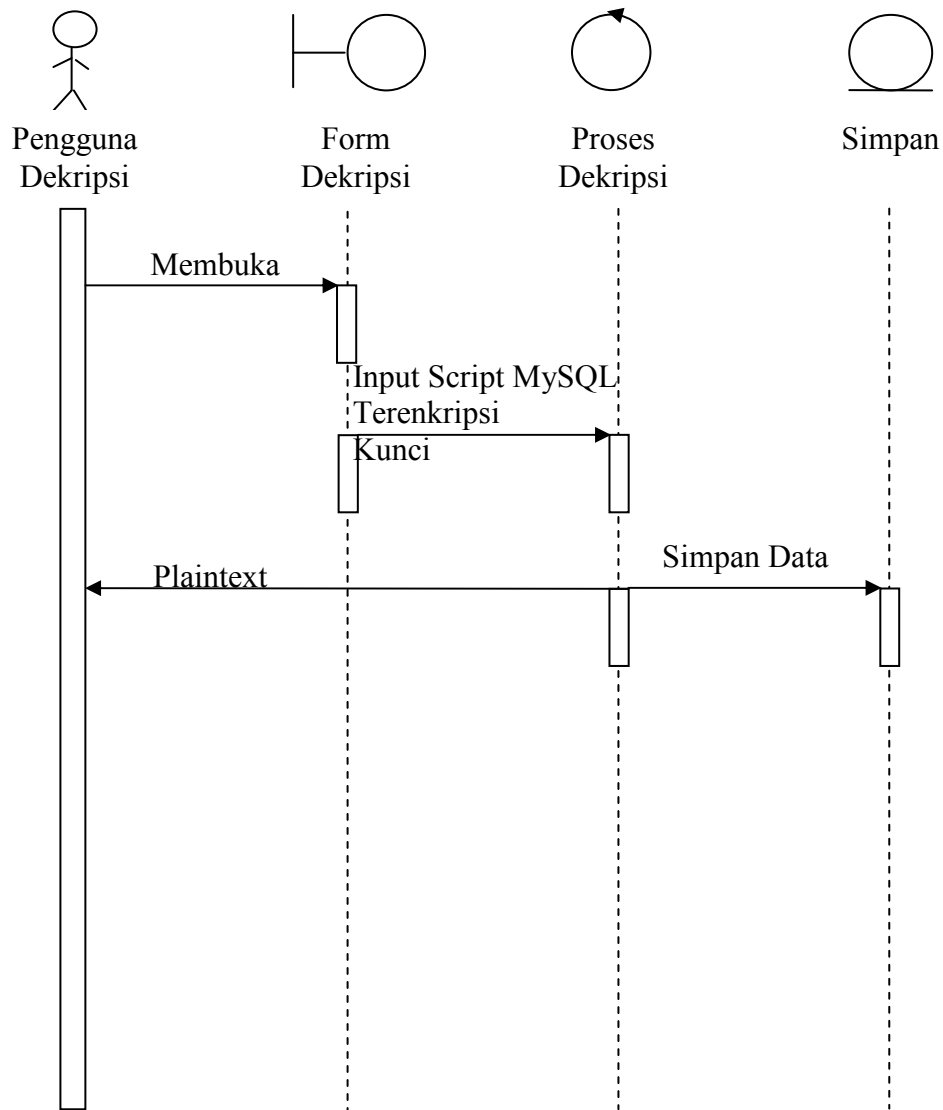
Sequence Diagram dalam melakukan proses enkripsi dapat terlihat seperti pada gambar III.8 sebagai berikut :



Gambar III.8. *Sequence Diagram* Enkripsi

2. *Sequence Diagram* Dekripsi

Sequence Diagram dalam melakukan proses dekripsi dapat terlihat seperti pada gambar III.9 sebagai berikut :



Gambar III.9. *Sequence Diagram* Dekripsi

III.4.2. Desain Sistem Aplikasi

Desain sistem aplikasi yang telah dibuat digambarkan dan dijabarkan sebagai berikut :

1. Desain Sistem *Form* Menu

Desain Sistem *Form* Menu Penerapan Metode *Rail Fence Cipher* Dan ROT13 Untuk Keamanan *Script* MySQL dapat dilihat pada gambar III.10 sebagai berikut :

| | | |
|--------|--------|-------|
| Menu | | |
| Enkrip | Dekrip | Tutup |
| | | |

Gambar III.10. Desain Sistem *Form* Menu

2. Desain Sistem *Form* Enkripsi

Desain Sistem *Form* Enkripsi Penerapan Metode *Rail Fence Cipher* Dan ROT13 Untuk Keamanan *Script* MySQL dapat dilihat pada gambar III.11 sebagai berikut :

Enkrip

Isi Script MySQL

Kunci Enkrip

Kunci Dekrip

Bersihkan Buka Simpan Simpan Baru Enkrip

Gambar III.11. Desain Sistem *Form* Enkripsi

3. Desain Sistem *Form* Dekripsi

Desain Sistem *Form* Penerapan Metode *Rail Fence Cipher* Dan ROT13

Untuk Keamanan *Script* MySQL dapat dilihat pada gambar III.12.

Dekrip

Isi Script MySQL

Kunci Enkrip

Bersihkan Buka Simpan Simpan Baru Dekrip

Gambar III.12. Desain Sistem *Form* Dekripsi