BAB III

ANALISA DAN DESAIN SISTEM

III.1. Analisis Masalah

Umumnya basis data hanya mengandalkan sandi login untuk akses ke dalam isi basis data. Akan tetapi isi basis data masih dapat terbaca oleh pihak yang tidak diinginkan yang mengetahui sandi login basis data. Masalah yang terjadi adalah kecurian isi dari basis data yang digunakan, sehingga merugikan pemilik basis data dan menguntungkan pencuri basis data untuk kepentingan pribadinya. Oleh karena itu dibutuhkan sebuah teknik yang dapat merahasiakan isi teks basis data dari pencuri informasi.

Strategi pemecahan masalah:

1. Menggunakan basis data MySQL sebagai objek kerahasiaan data
2. Menggunakan perangkat *android* untuk enkrip dan dekrip isi basis data
3. Menggunakan konsep kriptografi dalam merahasiakan isi basis data
4. Menggunakan modifikasi metode *porta cipher* dan *diffie hellman* untuk merahasiakan isi teks basis data.

III.2. Penerapan Metode

Metode yang digunakan untuk kerahasiaan isi teks basis data adalah *Porta Cipher* Dan *Diffie Hellman*. Sebelum melakukan enkrip dan dekrip pada sebuah teks maka langkah pertama adalah membentuk kunci menggunakan metode *Diffie Hellman* sebagai berikut:

Algoritma Pertukaran kunci *Diffie Hellman* (DH), diusulkan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976, adalah skema algoritma asimetris yang pertama kali diterbitkan dalam literatur terbuka. penemuan ini juga dipengaruhi oleh karya Ralph Merkle. pertukaran kunci ini memberikan solusi praktis untuk masalah distribusi kunci, yaitu, memungkinkan dua pihak untuk mendapatkan kunci rahasia dengan berkomunikasi melalui saluran tidak aman. Kita dapat memberikan *public key* ke manapun tujuan yang kita inginkan, melalui telepon, internet, *keyserver*, dan sebagainya. Kunci rahasia yang telah didistribusikan kemudian digunakan untuk enkripsi dan Fungsi algoritma ini sendiri terbatas pada pertukaran nilai rahasia. (Alam, dkk, 2019: 201).

Contoh:

Pengguna enkrip dan pengguna dekrip menyepakati P = 97 dan G = 5 (G < P)

a. Pengguna enkrip memilih X1 = 36 dan menghitung

   $A = G^{x1} \bmod P = 5^{36} \bmod 97 = 50$

   Pengguna enkrip mengirimkan A kepada pengguna dekrip.

b. Pengguna dekrip memilih X2 = 58 dan menghitung

   $B = G^{x2} \bmod P = 5^{58} \bmod 97 = 44$

   Pengguna dekrip mengirimkan B kepada pengguna enkrip.

c. Pengguna enkrip menghitung kunci simetri K,

   $K = B^{X1} \bmod P = 44^{36} \bmod 97 = 75$

d. Pengguna dekrip menghitung kunci simetri K,

   $K = A^{X2} \bmod P = 50^{58} \bmod 97 = 75$

Jadi, Pengguna enkrip dan pengguna dekrip sekarang sudah mempunyai kunci enkripsi simetri yang sama, yaitu K = 75.

Porta adalah sandi substitusi polialfabetik. Dulu ditemukan oleh Giovanni Battista della Porta. Ini menggunakan 13 huruf secara timbal balik dan penyandiannya sama dengan menguraikan. Ini cukup kuat. Sandi Porta bisa menjadi rusak dengan cara yang sama seperti *Vigenere Cipher*. Dia diakui oleh ACA. (Biswas, dkk, 2019: 509).

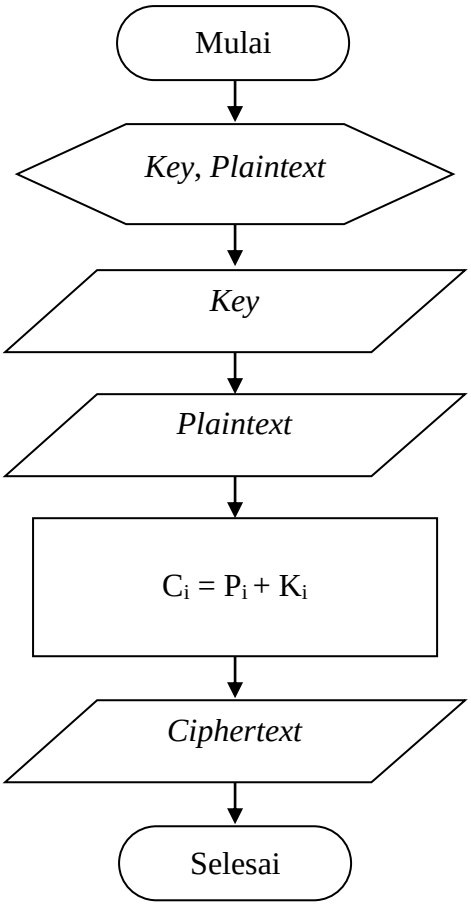
Langkah-langkah metode *Porta Cipher* untuk enkrip dapat dilihat sebagai berikut:

1. Buat pesan untuk di enkrip.
2. Buat kunci untuk proses enkrip.
3. Ubah pesan perkarakter dan kunci ke dalam kode ASCII.
4. Lakukan proses + ASCII kunci terhadap ASCII pesan pada tiap karakter.

Berikut ini adalah rumus enkrip dari metode *Porta Cipher*:

Ci = (Pi + Ki) mod 256

Flowchart metode enkrip *Porta Cipher* dapat dilihat sebagai berikut:



Gambar III.1. *Flowchart* Enkrip Metode *Porta Cipher*

Langkah-langkah metode *Porta Cipher* untuk dekrip dapat dilihat sebagai berikut:

1. Masukkan *ciphertext* untuk di dekrip.
2. Masukkan kunci dekrip *ciphertext.*
3. Ubah pesan per karakter dan kunci ke dalam kode ASCII.
4. Lakukan proses penjumlahan ASCII pesan terhadap ASCII kunci pada tiap karakter.

Contoh Proses Enkrip:

Terdapat isi basis data dengan teks sebagai berikut:

Tabel III.1. Isi Basis Data

No.	Nama	Kampus
1.	Agus Rahmadani D	POTENSI
2.	Deni Anggara	POTENSI

Plaintext : POTENSI

Kunci : 75

Solusi:

Ascii Plaintext:

P = 80

O = 79

T = 84

E = 69

N = 78

S = 83

I = 73

Key:

7 = 55

5 = 53

C1 = (P + k1) mod 256

= (80 + 55) mod 256

= 135 mod 256

= 135 = ‡

C2 = (O + k2) mod 256

= (79 + 53) mod 256

= 132 mod 256

= 132 = „

C3 = (T + k3) mod 256

= (84 + 55) mod 256

= 139 mod 256

= 139 = ‹

C4 = (E + k4) mod 256

= (69 + 53) mod 256

= 122 mod 256

= 122 = z

C5 = (N + k5) mod 256

= (78 + 55) mod 256

= 133 mod 256

= 133 = …

C6 = (S + k6) mod 256

= (83 + 53) mod 256

= 136 mod 256

= 136 = ˆ

C7 = (I + k7) mod 256

= (73 + 55) mod 256

= 128 mod 256

= 128 = €

Chipertext: ‡„‹z…ˆ€

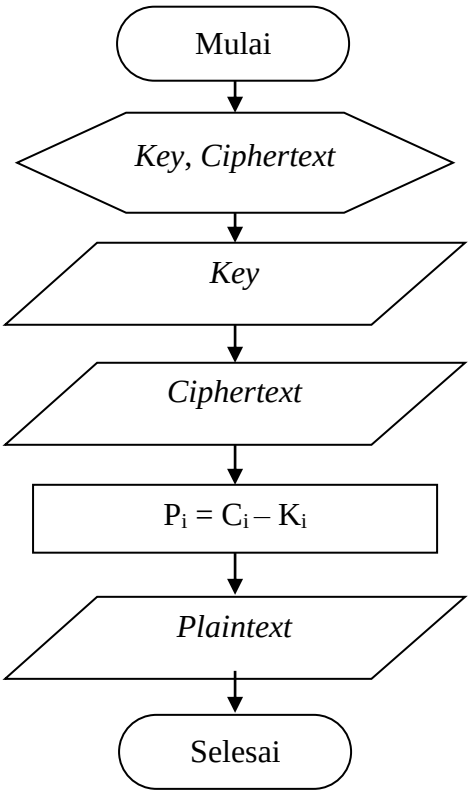
Tabel III.2. Isi Basis Data Terenkripsi

No.	Nama	Kampus
1.	Agus Rahmadani D	‡„‹z…ˆ€
2.	Deni Anggara	‡„‹z…ˆ€

Berikut ini adalah rumus dekrip dari metode *Porta Cipher*:

Pi = (Ci - Ki) mod 256

Flowchart metode dekrip *Porta Cipher* dapat dilihat sebagai berikut:



Gambar III.2. *Flowchart* Dekrip Metode *Porta Cipher*

Contoh proses dekrip:

Terdapat isi basis data dengan teks sebagai berikut:

Tabel III.3. Isi Basis Data Terenkripsi

No.	Nama	Kampus
1.	Agus Rahmadani D	‡„‹z…ˆ€
2.	Deni Anggara	‡„‹z…ˆ€

Chipertext: ‡„‹z…ˆ€

Kunci: 75

Ascii Plaintext:

‡ = 135

„ = 132

‹ = 139

Z = 122

… = 133

ˆ = 136

€ = 128

Key:

7 = 55

5 = 53

P1 = (‡- k1) mod 256

= (135 - 55) mod 256

= 80 mod 256

= 80 = P

P2 = („ - k2) mod 256

= (132 - 53) mod 256

= 79 mod 256

= 79 = O

P3 = (‹ - k3) mod 256

= (139 - 55) mod 256

= 84 mod 256

= 84 = T

P4 = (Z - k4) mod 256

= (122 - 53) mod 256

= 69 mod 256

= 69 = E

P5 = (… - k5) mod 256

= (133 - 55) mod 256

= 78 mod 256

= 78 = N

P6 = (ˆ - k6) mod 256

= (136 - 53) mod 256

= 83 mod 256

= 83 = S

P7 = (€ + k7) mod 256

= (128 - 55) mod 256

= 73 mod 256

= 73 = I

Plaintext: POTENSI

Tabel III.4. Isi Basis Data Terdekripsi

No.	Nama	Kampus
1.	Agus Rahmadani D	POTENSI
2.	Deni Anggara	POTENSI

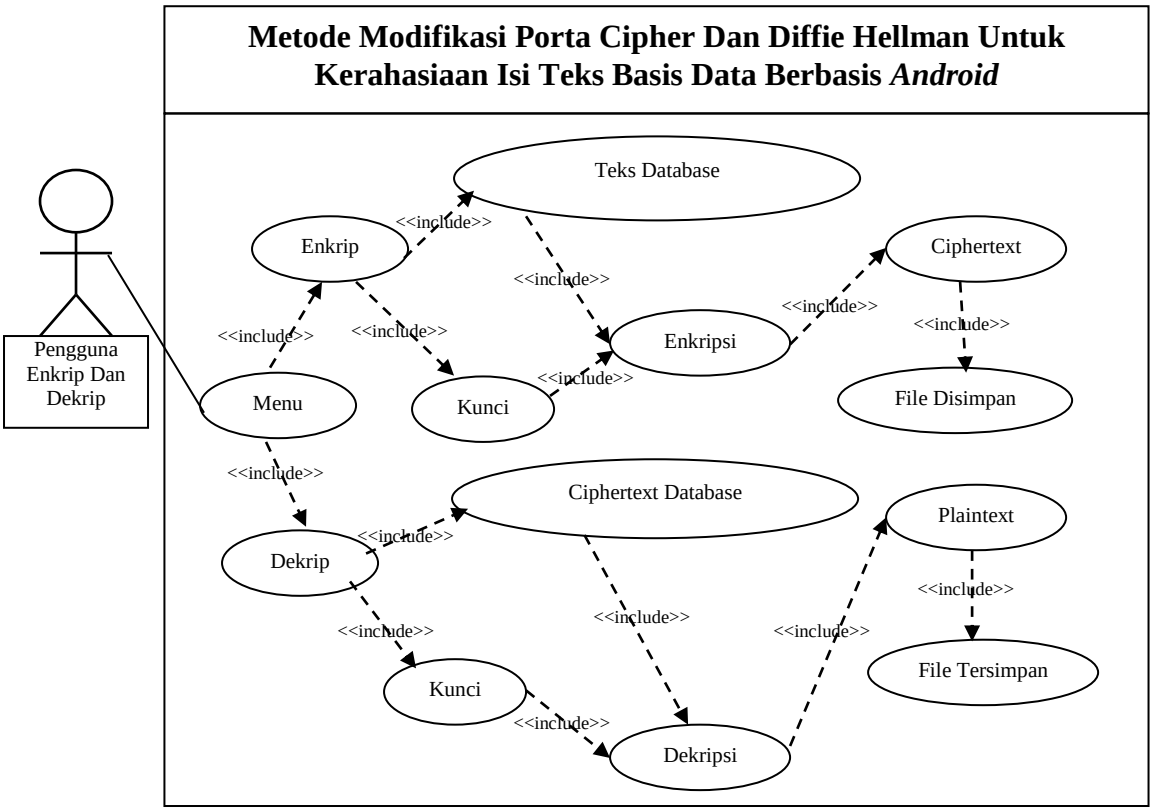
III.3. Desain Sistem

III.3.1. Desain Sistem Secara Global

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

III.3.1.1 *Use Case Diagram*

Use case diagram Metode *Porta Cipher* Dan *Diffie Hellman* Untuk Kerahasiaan Isi Teks Basis Data Berbasis *Android* dapat dilihat pada gambar III.3.



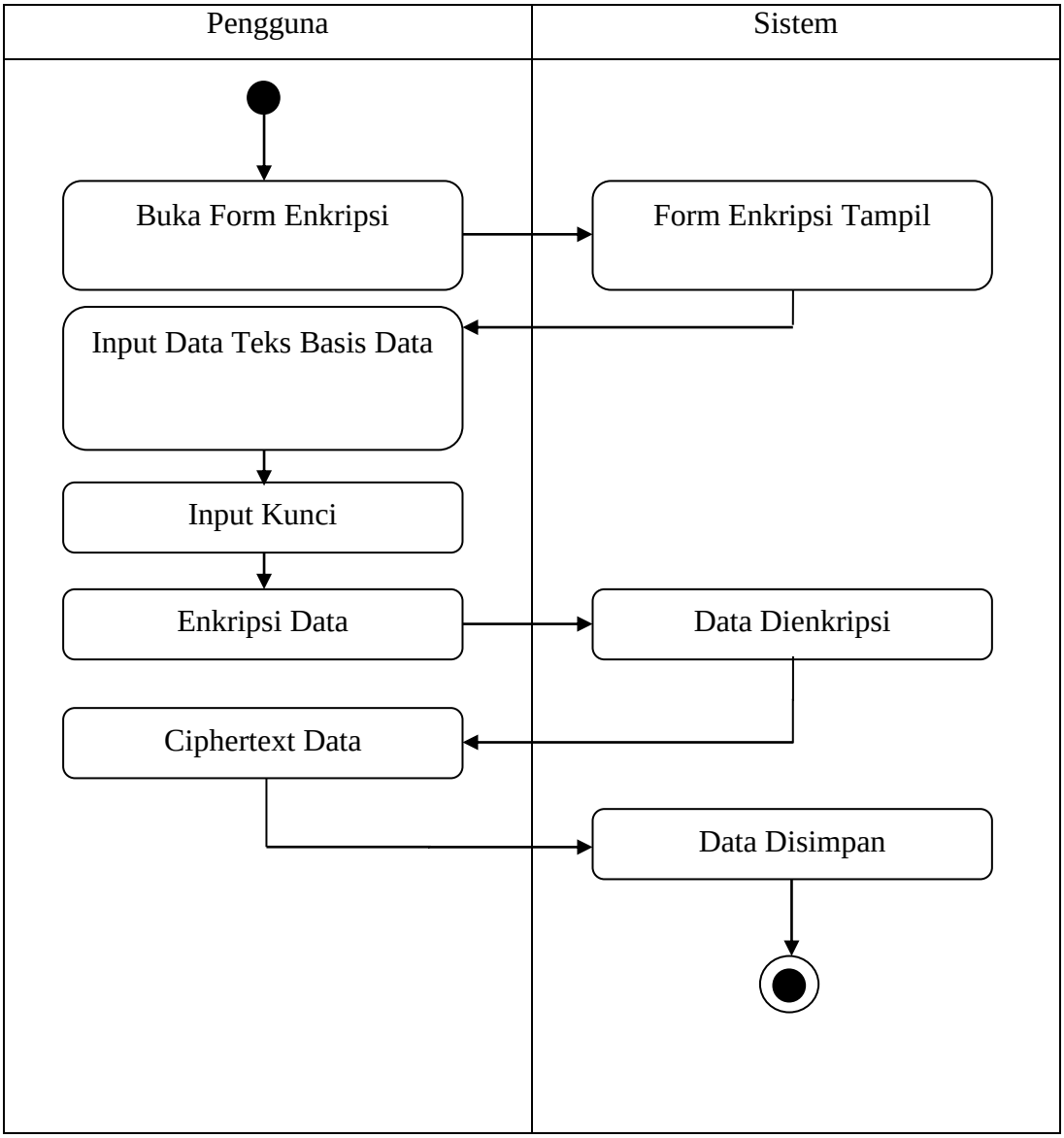
Gambar III.3. *Use Case Diagram* Metode Modifikasi *Porta Cipher* Dan *Diffie Hellman* Untuk Kerahasiaan Isi Teks Basis Data Berbasis *Android*

III.3.1.2. *Activity Diagram*

Activity diagram Metode Modifikasi *Porta Cipher* Dan *Diffie Hellman* Untuk Kerahasiaan Isi Teks Basis Data Berbasis *Android* dapat dilihat sebagai berikut:

1. *Activity Diagram* Enkripsi

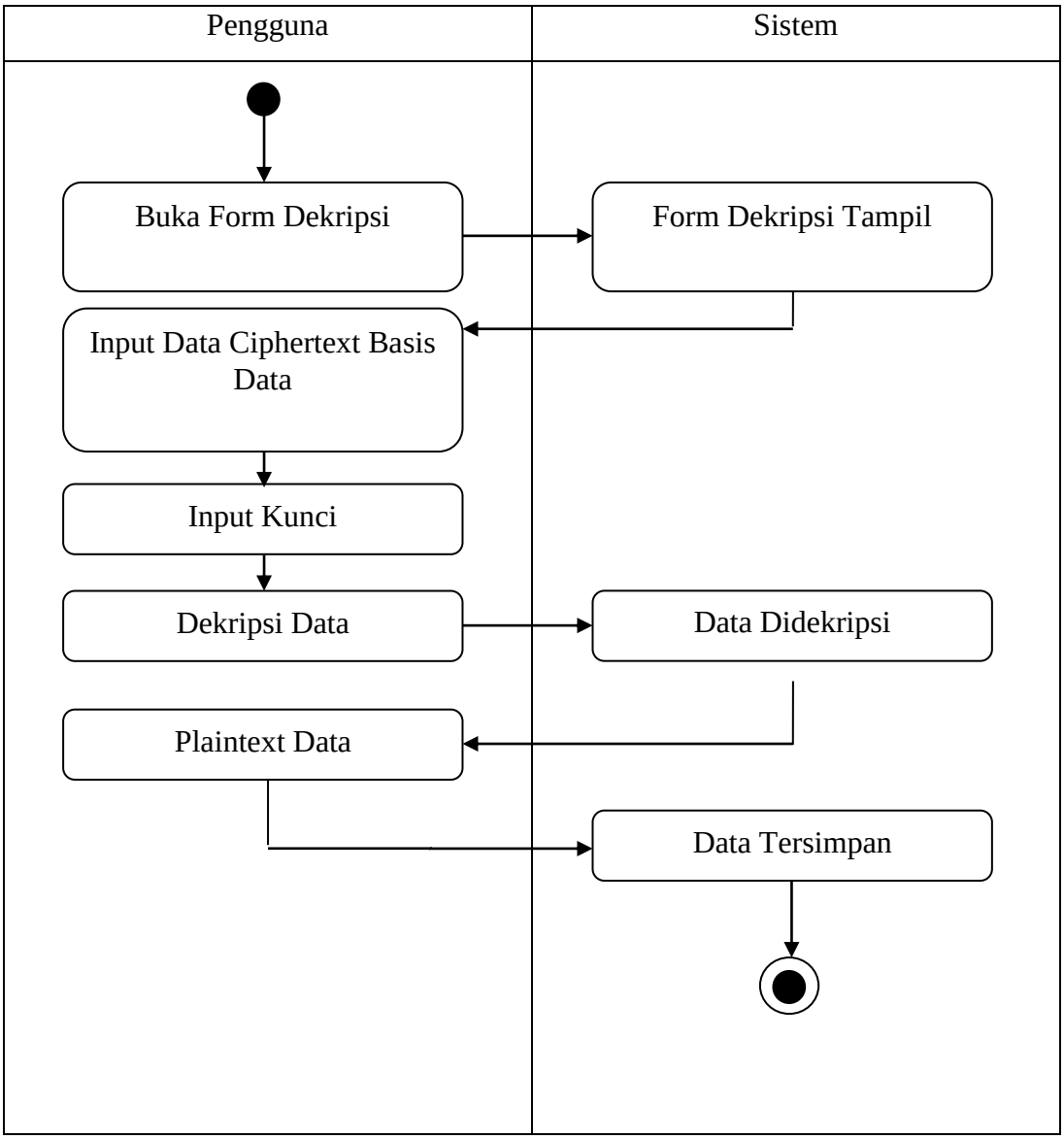
Activity Diagram dalam melakukan proses enkripsi dapat terlihat seperti pada gambar III.4 berikut:



Gambar III.4. *Activity Diagram* Enkripsi

2. *Activity Diagram* Dekripsi

Activity Diagram dalam melakukan proses dekripsi dapat terlihat seperti pada gambar III.5 berikut:



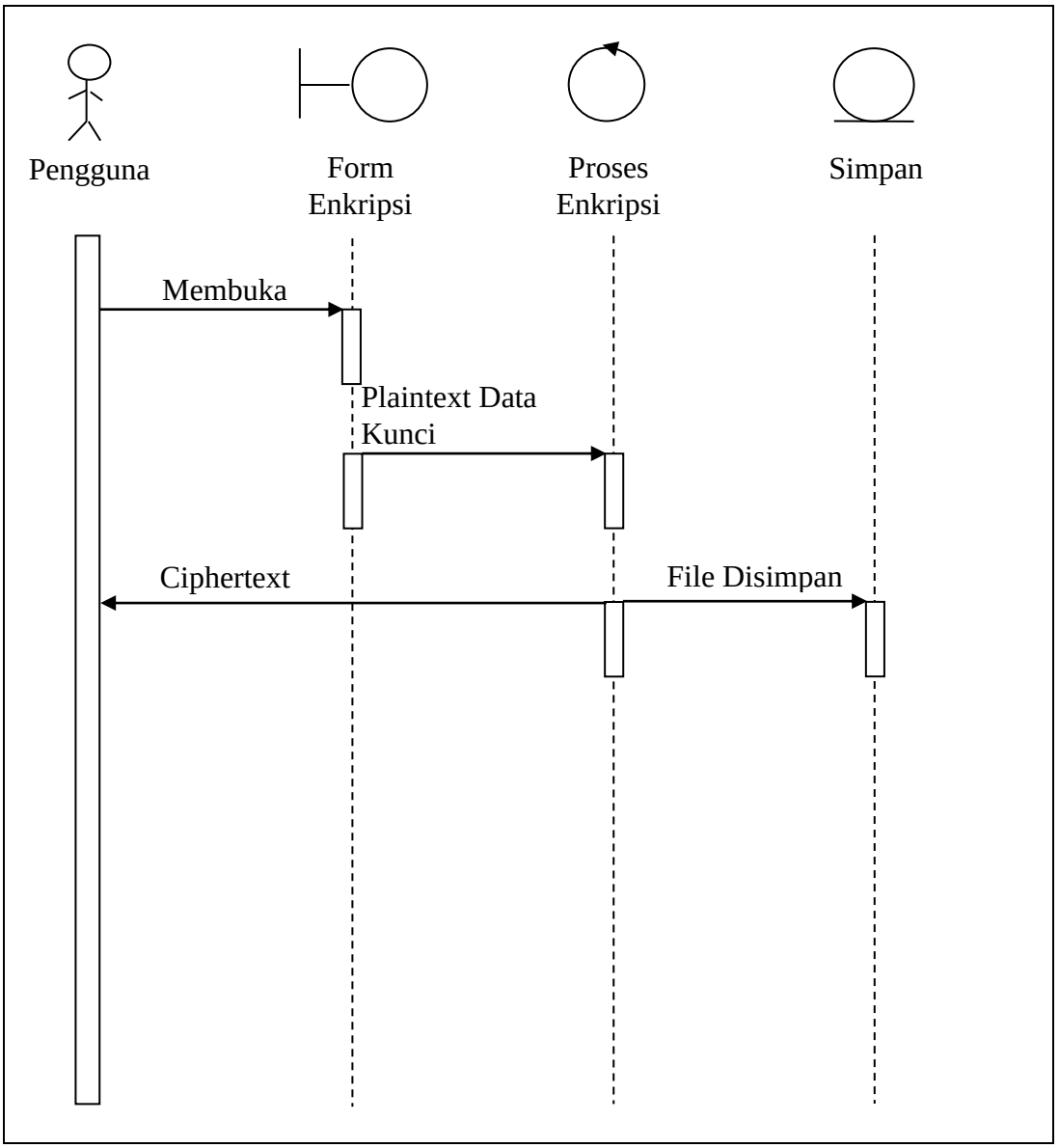
Gambar III.5. *Activity Diagram* Dekripsi

III.3.1.3. *Sequence Diagram*

Sequence diagram Metode Modifikasi *Porta Cipher* Dan *Diffie Hellman* Untuk Kerahasiaan Isi Teks Basis Data Berbasis *Android* sebagai berikut:

1. *Sequence Diagram* Enkripsi

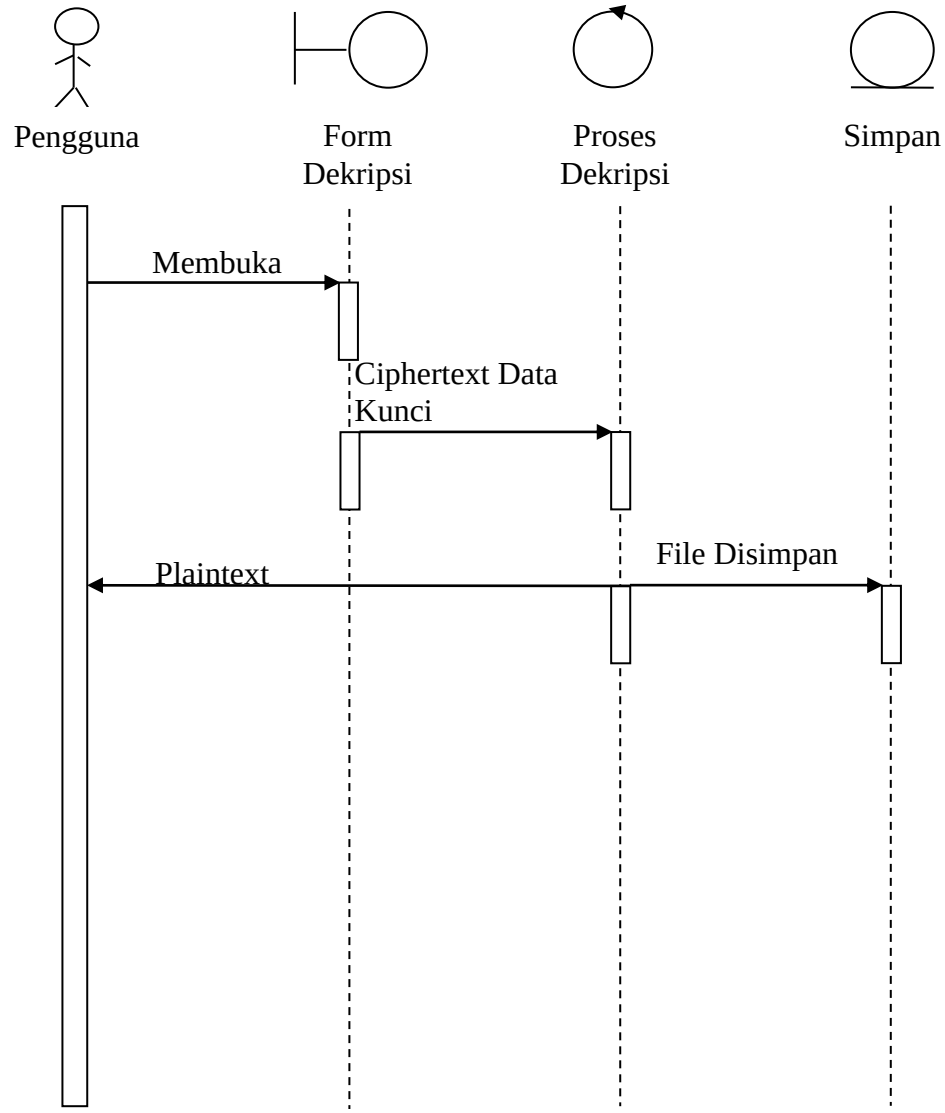
Sequence Diagram dalam melakukan proses enkripsi dapat terlihat seperti pada gambar III.6 berikut:



Gambar III.6. *Sequence Diagram* Enkripsi

2. *Sequence Diagram* Dekripsi

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

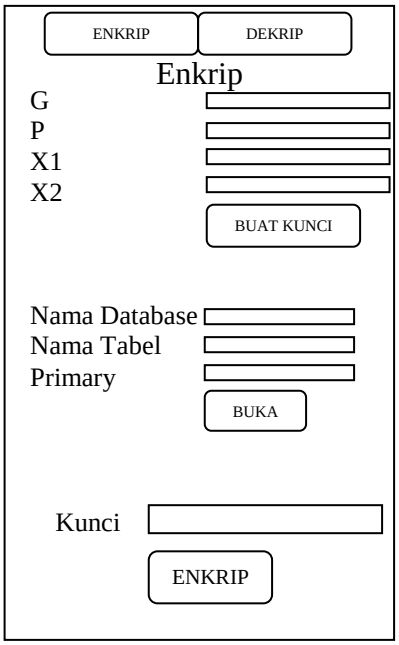


Gambar III.7. *Sequence Diagram* Dekripsi

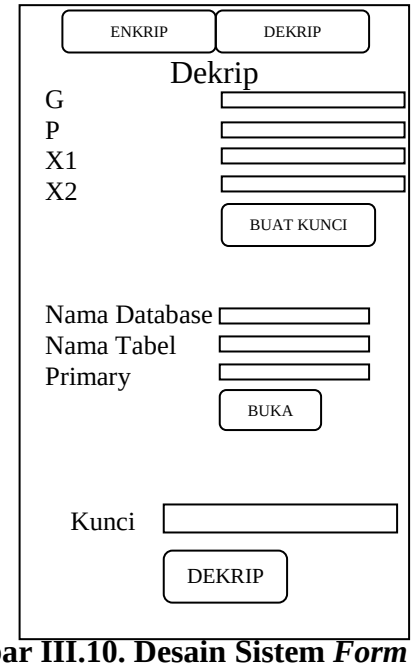
III.3.2. Desain Sistem Aplikasi

Desain sistem aplikasi yang telah dibuat digambarkan dan dijabarkan dapat dilihat pada gambar III.8.

Gambar III.8. Desain Sistem *Form* Menu



Gambar III.9. Desain Sistem *Form* Enkrip



Gambar III.10. Desain Sistem *Form* Dekrip

Gambar III.11. Desain Sistem Keterangan