

BAB III

ANALISA DAN DESAIN SISTEM

III.1. Analisis Masalah

Penerapan keamanan pada basis data biasanya hanya menggunakan sandi *login* untuk melindungi isi di basis data. Akan tetapi jika basis data dicuri, maka pencuri dapat membuka isi datanya secara langsung menggunakan aplikasi basis data yang lain, sehingga pencuri dapat membaca isi dari basis data yang dicuri. Oleh karena itu perlunya diterapkan keamanan dalam sebuah basis data sehingga para pencuri informasi tidak dapat mencuri data yang terdapat di dalam basis data dengan cara mengubah isi dari teks yang tersimpan di dalam basis data menjadi teks rahasia. Penelitian ini menggunakan metode *Zig-Zag Cipher* dan ROT13 untuk menutupi beberapa kelemahan yaitu dengan menggunakan metode *Zig-Zag Cipher* dan ROT13 tidak memberatkan proses enkripsi dan dekripsi dan metode *Zig-Zag Cipher* dan ROT13 memiliki kunci yang dapat menggunakan seluruh abjad. Dengan adanya metode *Zig-Zag Cipher* dan ROT13 maka basis data mendapatkan kerahasiaan isi teks yang lebih baik.

III.2. Penerapan Metode

Metode yang digunakan untuk isi teks basis data yaitu *zig-zag cipher* dan ROT13.

III.2.1. Metode Zig-Zag Cipher

Metode *zig-zag cipher* merupakan salah satu algoritma kriptografi klasik dengan teknik transposisi. Teknik transposisi menggunakan permutasi karakter, yang mana dengan menggunakan teknik ini pesan yang asli tidak dapat dibaca kecuali orang yang memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula.

III.2.2. Metode ROT13

ROT13 (Rotate 13) adalah enkripsi substitution cipher yang umum digunakan di sistem operasi UNIX. Pada sistem enkripsi ROT13 sebuah huruf digantikan dengan huruf yang letaknya di atas 13 posisi darinya. Enkrip metode ROT13 menggunakan penjumlahan *ascii plaintext* dengan *ascii* kunci 13 sebagai berikut :

$$C_i = P_i + 13$$

Keterangan :

C_i = *Ciphertext* hasil enkrip

P_i = *Plaintext* yang akan dienkrip

Dekrip metode ROT13 menggunakan pengurangan *ascii Ciphertext* dengan *ascii* kunci 13 sebagai berikut :

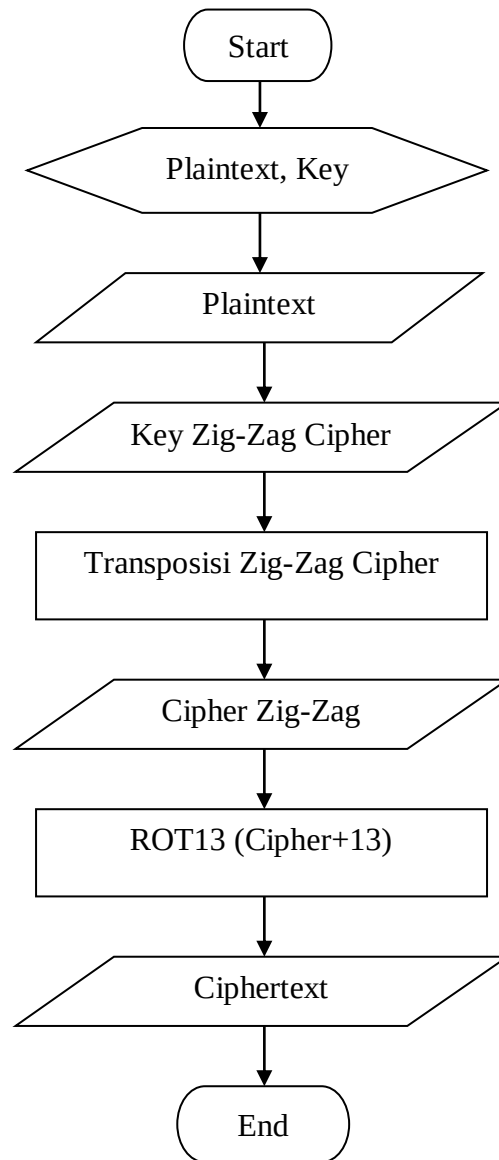
$$P_i = C_i - 13$$

Keterangan :

C_i = *Ciphertext* yang akan didekrip

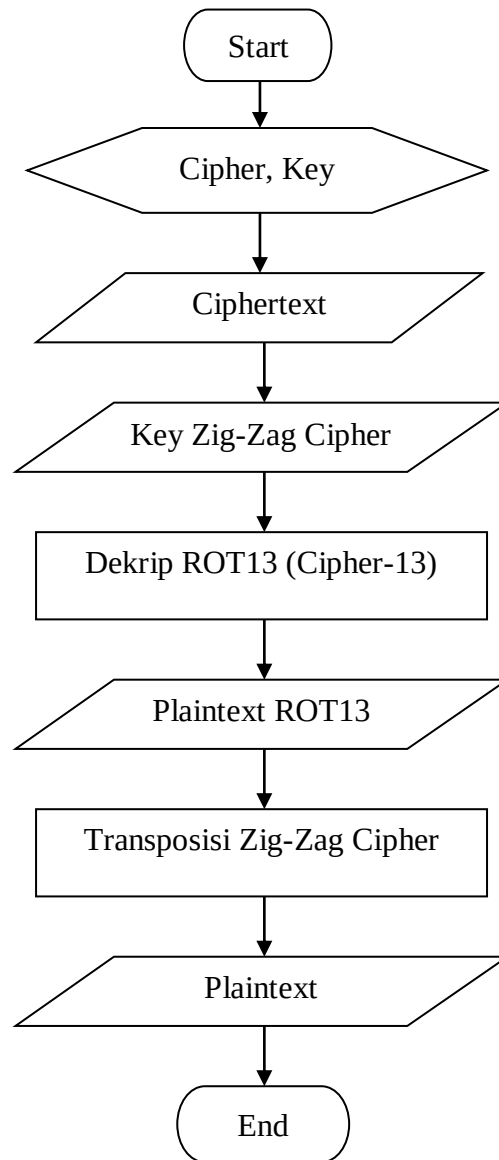
P_i = *Plaintext* hasil dekrip. (Yazid dan Haryanto, 2021 : 68).

Flowchart enkripsi kombinasi metode *zig-zag cipher* dan ROT13 :



Gambar III.1. Flowchart Enkripsi Kombinasi Ziig-Zag Cipher Dan ROT13

Flowchart dekripsi kombinasi metode *zig-zag cipher* dan ROT13 :



Gambar III.2. Flowchart Dekripsi Kombinasi Ziig-Zag Cipher Dan ROT13

Berikut ini akan diuraikan contoh enkripsi berdasarkan algoritma *zig-zag cipher* dan ROT13.

Tabel III.1. Data Login Portal Mahasiswa Universitas Potensi Utama

No.	Username	Password
1.	1812000427	12345deni

2.	1812000428	73840ucan
3.	1812000429	IO1234567
4.	1812000430	xyz123490
5.	1812000431	abcde1234

1. Enkrip

Kunci Zig-zag = 3 dan offset = 0

a. Username 1812000427

Plaintext : 12345deni

Di enkripsi dengan metode *zig zag cipher* sebagai berikut :

1				5				i
	2		4		d		n	
		3				e		

Ciphertext : 15i24dn3e

Di enkripsi dengan metode ROT13 sebagai berikut :

$$1 = 49 + 13 = 62 = >$$

$$5 = 53 + 13 = 66 = B$$

$$i = 105 + 13 = 118 = v$$

$$2 = 50 + 13 = 63 = ?$$

$$4 = 52 + 13 = 65 = A$$

$$d = 100 + 13 = 113 = q$$

$$n = 110 + 13 = 123 = \{$$

$$3 = 51 + 13 = 64 = @$$

$$e = 101 + 13 = 114 = r$$

Ciphertext : >Bv?Aq{@r

b. Username 1812000428

Plaintext : 73840ucan

Di enkripsi dengan metode *zig zag cipher* sebagai berikut :

7				0				n
	3		4		u		a	
		8				c		

Ciphertext : 70n34ua8c

Di enkripsi dengan metode ROT13 sebagai berikut :

$$7 = 55 + 13 = 68 = D$$

$$0 = 48 + 13 = 61 =$$

$$n = 110 + 13 = 123 = \{$$

$$3 = 51 + 13 = 64 = @$$

$$4 = 52 + 13 = 65 = A$$

$$u = 117 + 13 = 130 = ,$$

$$a = 97 + 13 = 110 = n$$

$$8 = 56 + 13 = 69 = E$$

$$c = 99 + 13 = 112 = p$$

Ciphertext : D={@A,nEp**c. Username 1812000429**

Plaintext : IO1234567

Di enkripsi dengan metode *zig zag cipher* sebagai berikut :

I				3				7
	O		2		4		6	
		1				5		

Ciphertext : I37O24615

Di enkripsi dengan metode ROT13 sebagai berikut :

$$I = 73 + 13 = 86 = V$$

$$3 = 51 + 13 = 64 = @$$

$$7 = 55 + 13 = 68 = D$$

$$O = 79 + 13 = 92 = \backslash$$

$$2 = 50 + 13 = 63 = ?$$

$$4 = 52 + 13 = 65 = A$$

$$6 = 54 + 13 = 67 = C$$

$$1 = 49 + 13 = 62 = >$$

$$5 = 53 + 13 = 66 = B$$

Ciphertext : V@D\?AC>B

d. Username 1812000430

Plaintext : xyz123490

Di enkripsi dengan metode *zig zag cipher* sebagai berikut :

x				2				0
	Y		1		3		9	
		Z				4		

Ciphertext : x20y139z4

Di enkripsi dengan metode ROT13 sebagai berikut :

$$x = 120 + 13 = 133 = _$$

$$2 = 50 + 13 = 63 = ?$$

$$0 = 48 + 13 = 61 = =$$

$$y = 121 + 13 = 134 = †$$

$$1 = 49 + 13 = 62 = >$$

$$3 = 51 + 13 = 64 = @$$

$$9 = 57 + 13 = 70 = F$$

$$z = 122 + 13 = 135 = \ddagger$$

$$4 = 52 + 13 = 65 = A$$

Ciphertext : _?=†>@F‡A

e. Username 1812000431

Plaintext : abcde1234

Di enkripsi dengan metode *zig zag cipher* sebagai berikut :

A				e				4
	B		D		1		3	
		c				2		

Ciphertext : ae4bd13c2

Di enkripsi dengan metode ROT13 sebagai berikut :

$$a = 97 + 13 = 110 = n$$

$$e = 101 + 13 = 114 = r$$

$$4 = 52 + 13 = 65 = A$$

$$b = 98 + 13 = 111 = o$$

$$d = 100 + 13 = 113 = q$$

$$1 = 49 + 13 = 62 = >$$

$$3 = 51 + 13 = 64 = @$$

$$c = 99 + 13 = 112 = p$$

$$2 = 50 + 13 = 63 = ?$$

Ciphertext : nrAoq>@p?

Berikut ini adalah hasil enkripsi yang telah dilakukan :

Tabel III.2. Data Login Portal Mahasiswa Terenkripsi

No.	Username	Password
1.	1812000427	>Bv?Aq{@r
2.	1812000428	D={@A,nEp
3.	1812000429	V@D\?AC>B
4.	1812000430	_?=†>@F‡A
5.	1812000431	nrAoq>@p?

2. Dekrip

Berikut ini akan diuraikan contoh dekrip berdasarkan algoritma *zig-zag cipher*.

Kunci Zig-zag = 3 dan offset = 0 dan jumlah cipher = 9

x				x				x
	X		x		x		x	
		x				x		

a. Username 1812000427

Ciphertext : >Bv?Aq{@r

Di dekripsi dengan metode ROT13 sebagai berikut :

$$> = 62 - 13 = 49 = 1$$

$$B = 66 - 13 = 53 = 5$$

$$v = 118 - 13 = 105 = i$$

$$? = 63 - 13 = 50 = 2$$

$$A = 65 - 13 = 52 = 4$$

$$q = 113 - 13 = 100 = d$$

$$\{ = 123 - 13 = 110 = n$$

$$@ = 64 - 13 = 51 = 3$$

$$r = 114 - 13 = 101 = e$$

Ciphertext : 15i24dn3e

Di dekripsi dengan metode *zig zag cipher* sebagai berikut :

1				5				i
	2		4		d		n	
		3				e		

Plaintext : 12345deni

b. Username 1812000428

Ciphertext : D={@A,nEp

Di dekripsi dengan metode ROT13 sebagai berikut :

$$D = 68 - 13 = 55 = 7$$

$$= = 61 - 13 = 48 = 0$$

$$\{ = 123 - 13 = 110 = n$$

$$@ = 64 - 13 = 51 = 3$$

$$A = 65 - 13 = 52 = 4$$

$$, = 130 - 13 = 117 = u$$

$$n = 110 - 13 = 97 = a$$

$$E = 69 - 13 = 56 = 8$$

$$p = 112 - 13 = 99 = c$$

Ciphertext : 70n34ua8c

Di dekripsi dengan metode *zig zag cipher* sebagai berikut :

7				0				n
	3		4		u		a	
		8				c		

Plaintext : 73840ucan

c. Username 1812000429

Ciphertext : V@D\?AC>B

Di dekripsi dengan metode ROT13 sebagai berikut :

$$V = 86 - 13 = 73 = I$$

$$@ = 64 - 13 = 51 = 3$$

$$D = 68 - 13 = 55 = 7$$

$$\backslash = 92 - 13 = 79 = O$$

$$? = 63 - 13 = 50 = 2$$

$$A = 65 - 13 = 52 = 4$$

$$C = 67 - 13 = 54 = 6$$

$$> = 62 - 13 = 49 = 1$$

$$B = 66 - 13 = 53 = 5$$

Ciphertext : I37O24615

Di dekripsi dengan metode *zig zag cipher* sebagai berikut :

I				3				7
	O		2		4		6	
		1				5		

Plaintext : IO1234567

d. Username 1812000430

Ciphertext : _?=†>@F‡A

Di dekripsi dengan metode ROT13 sebagai berikut :

$$_ = 133 - 13 = 120 = x$$

$$? = 63 - 13 = 50 = 2$$

$$= = 61 - 13 = 48 = 0$$

$$† = 134 - 13 = 121 = y$$

$$> = 62 - 13 = 49 = 1$$

$$@ = 64 - 13 = 51 = 3$$

$$F = 70 - 13 = 57 = 9$$

$$\ddagger = 135 - 13 = 122 = z$$

$$A = 65 - 13 = 52 = 4$$

Ciphertext : x20y139z4

Di dekripsi dengan metode *zig zag cipher* sebagai berikut :

x				2				0
	y		1		3		9	
		z				4		

Plaintext : xyz123490

e. Username 1812000431

Ciphertext : nrAoq>@p?

Di dekripsi dengan metode ROT13 sebagai berikut :

$$n = 100 - 13 = 97 = a$$

$$r = 114 - 13 = 101 = e$$

$$A = 65 - 13 = 52 = 4$$

$$o = 111 - 13 = 98 = b$$

$$q = 113 - 13 = 100 = d$$

$$> = 62 - 13 = 49 = 1$$

$$@ = 64 - 13 = 51 = 3$$

$$p = 112 - 13 = 99 = c$$

$$? = 63 - 13 = 50 = 2$$

Ciphertext : ae4bd13c2

Di dekripsi dengan metode *zig zag cipher* sebagai berikut :

a				E				4
	b		d		1		3	
		c				2		

Plaintext : abcde1234

Tabel III.3. Data Login Portal Mahasiswa Terdekripsi

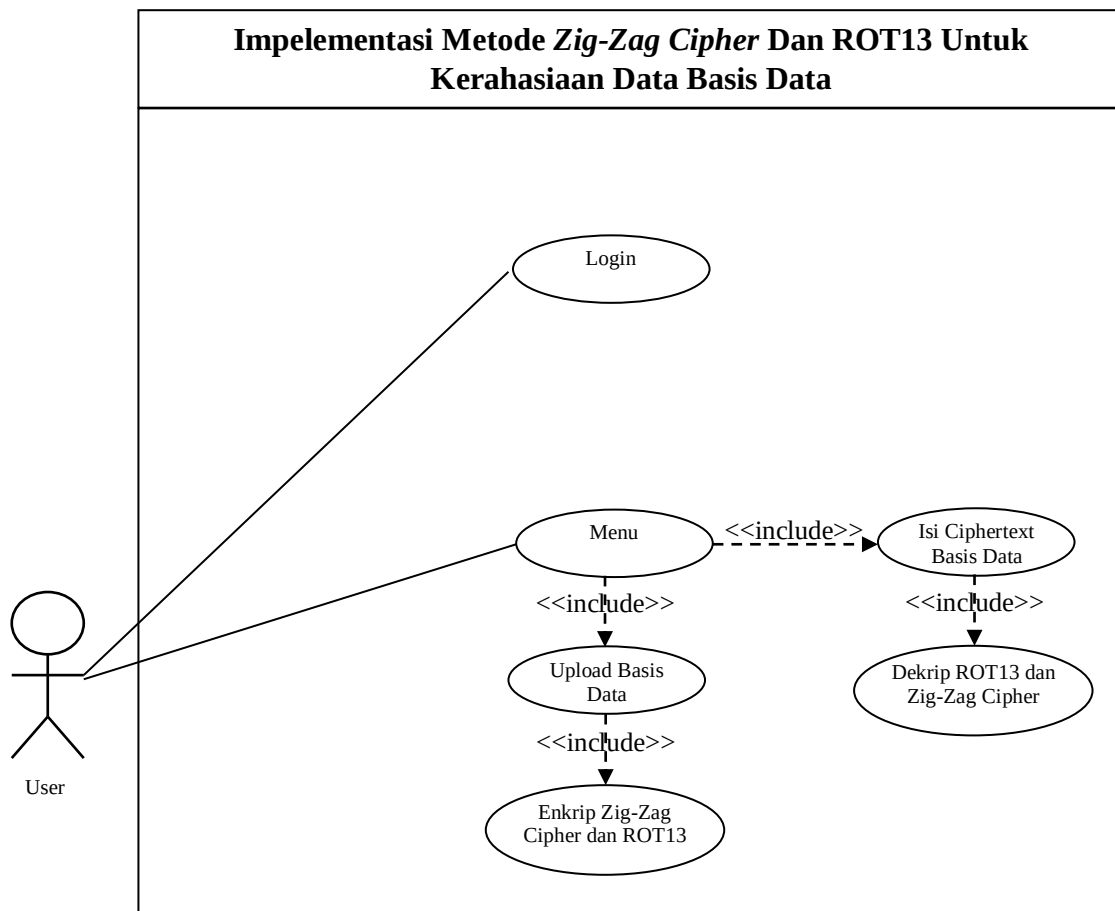
No.	Username	Password
1.	1812000427	12345deni
2.	1812000428	73840ucan
3.	1812000429	IO1234567
4.	1812000430	xyz123490
5.	1812000431	abcde1234

III.3. Desain Sistem

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.3.1. Use Case Diagram

Perancangan dimulai dari identifikasi aktor dan bagaimana hubungan antara aktor dan use case didalam sistem. Perancangan *Use Case Diagram* dapat dilihat pada gambar III.1 sebagai berikut :



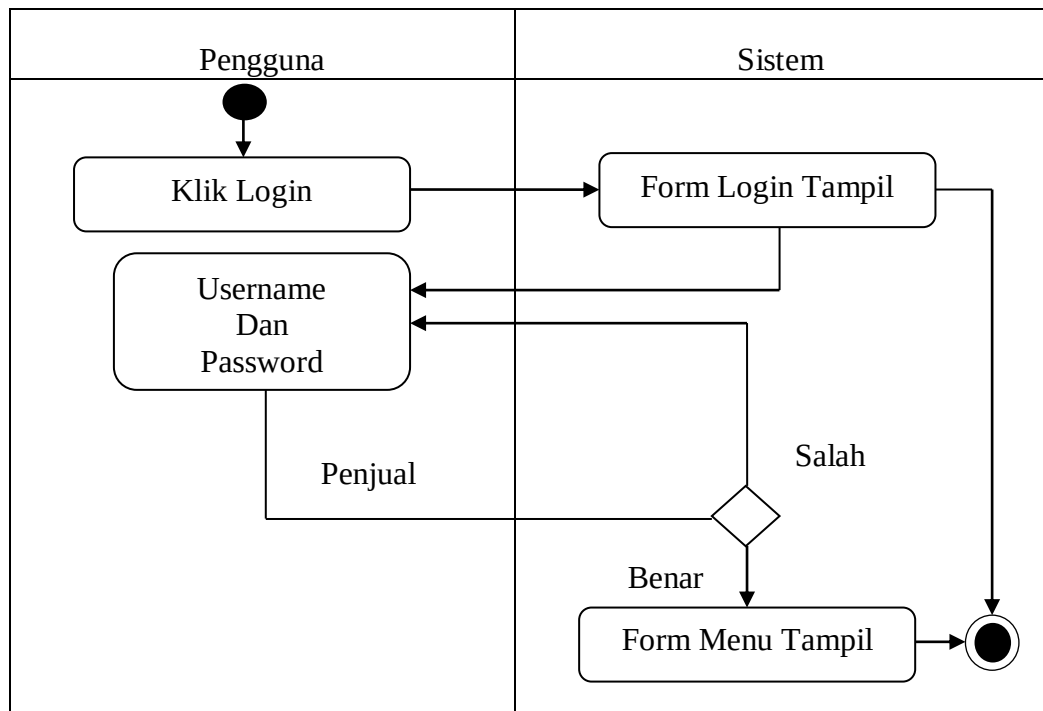
Gambar III.3. Use Case Implementasi Metode Zig-Zag Cipher Dan ROT13 Untuk Kerahasiaan Data Basis Data

III.3.2. Activity Diagram

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

1. Activity Diagram Login

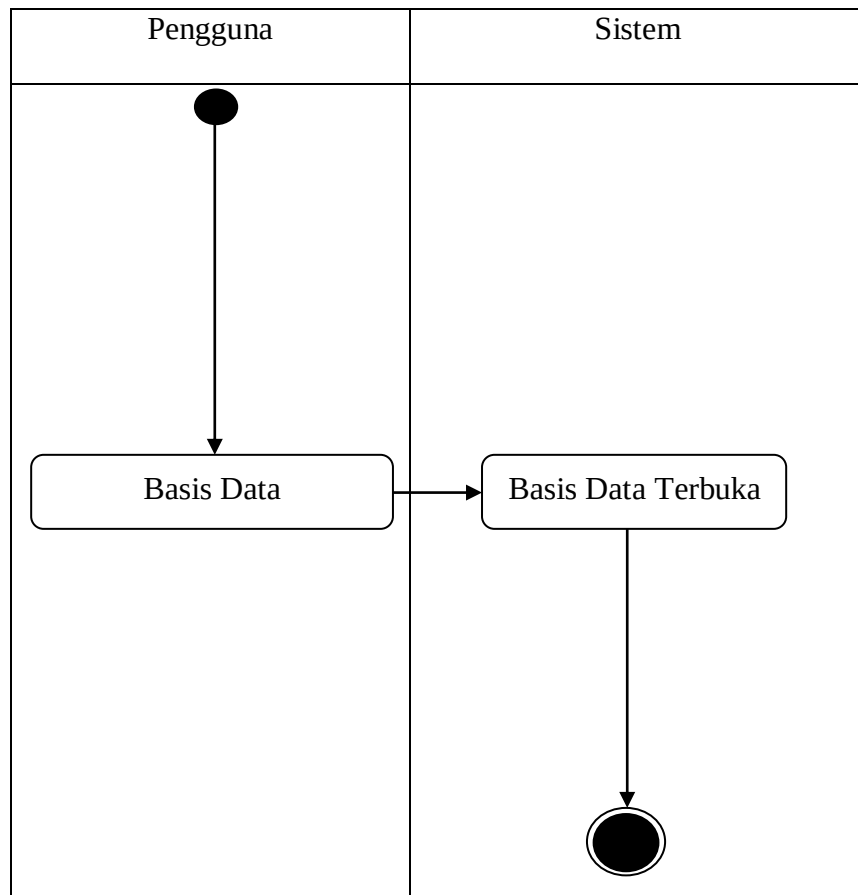
Serangkaian kerja melakukan *login* dapat terlihat seperti pada gambar III.4 berikut :



Gambar III.4. Activity Diagram Login

2. Activity Diagram Upload Basis Data

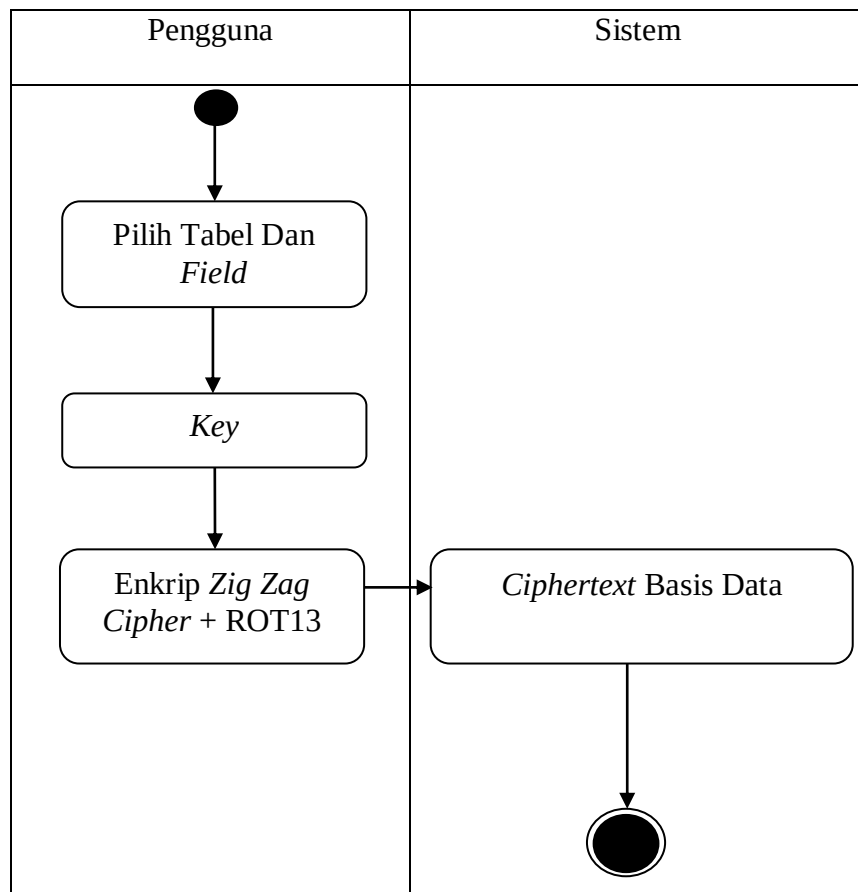
Serangkaian kerja melakukan upload Basis Data dapat terlihat seperti pada gambar III.5 berikut :



Gambar III.5. Activity Diagram Upload Basis Data

3. Activity Diagram Enkrip

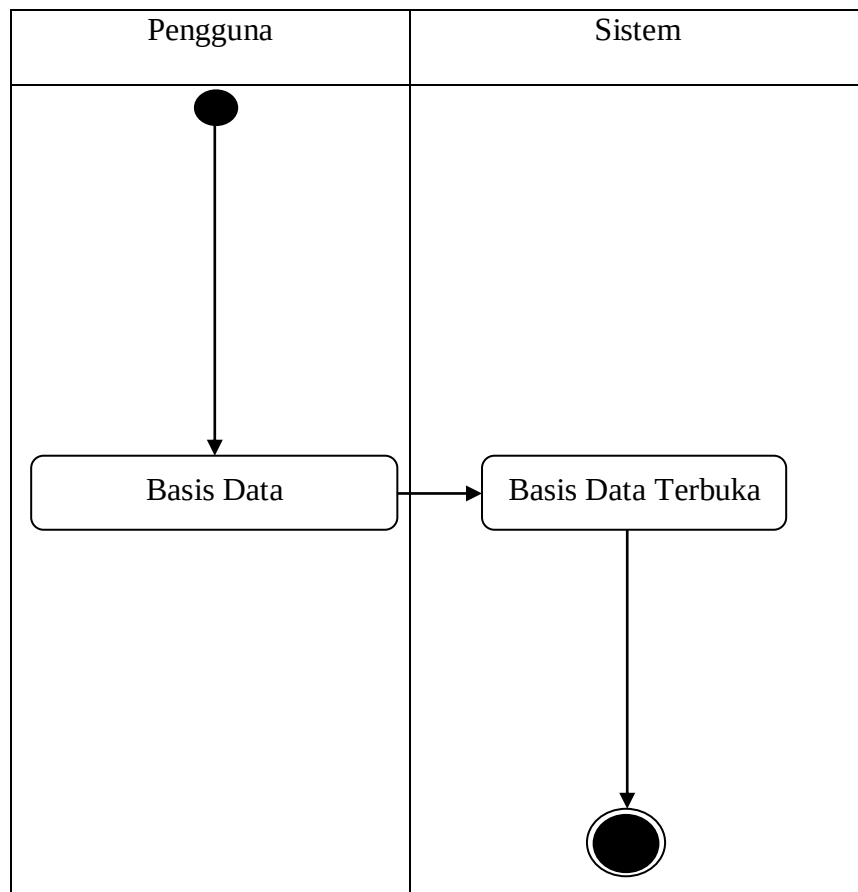
Serangkaian kerja melakukan enkrip dapat terlihat seperti pada gambar III.6 berikut :



Gambar III.6. Activity Diagram Enkrip

4. *Activity Diagram Ciphertext Basis Data*

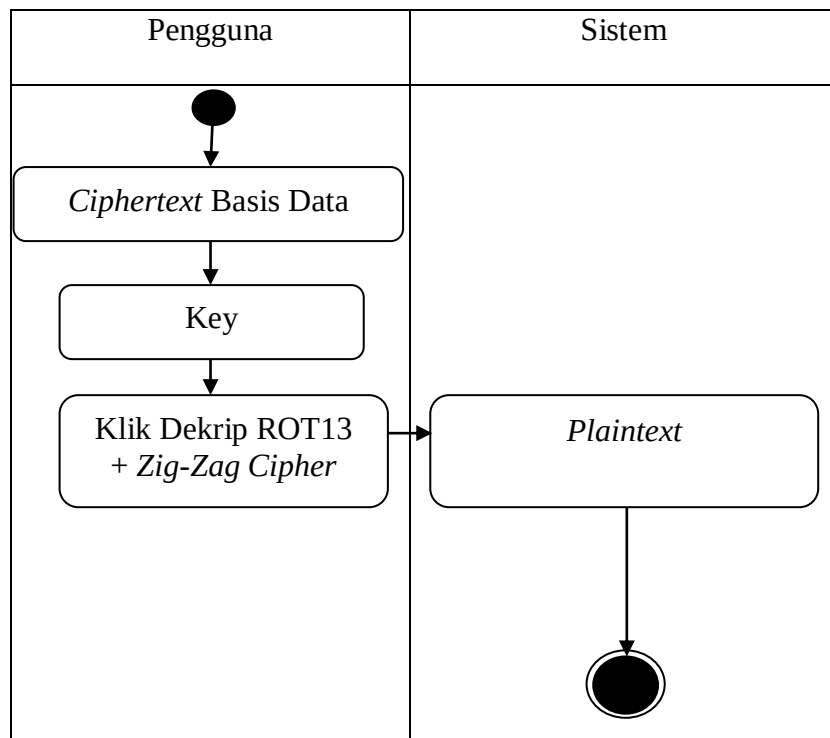
Serangkaian kerja melakukan upload ciphertext Basis Data dapat terlihat seperti pada gambar III.7 berikut :



Gambar III.7. Activity Diagram Ciphertext

5. Activity Diagram Dekrip

Serangkaian kerja melakukan Dekrip dapat terlihat seperti pada gambar III.8 berikut :



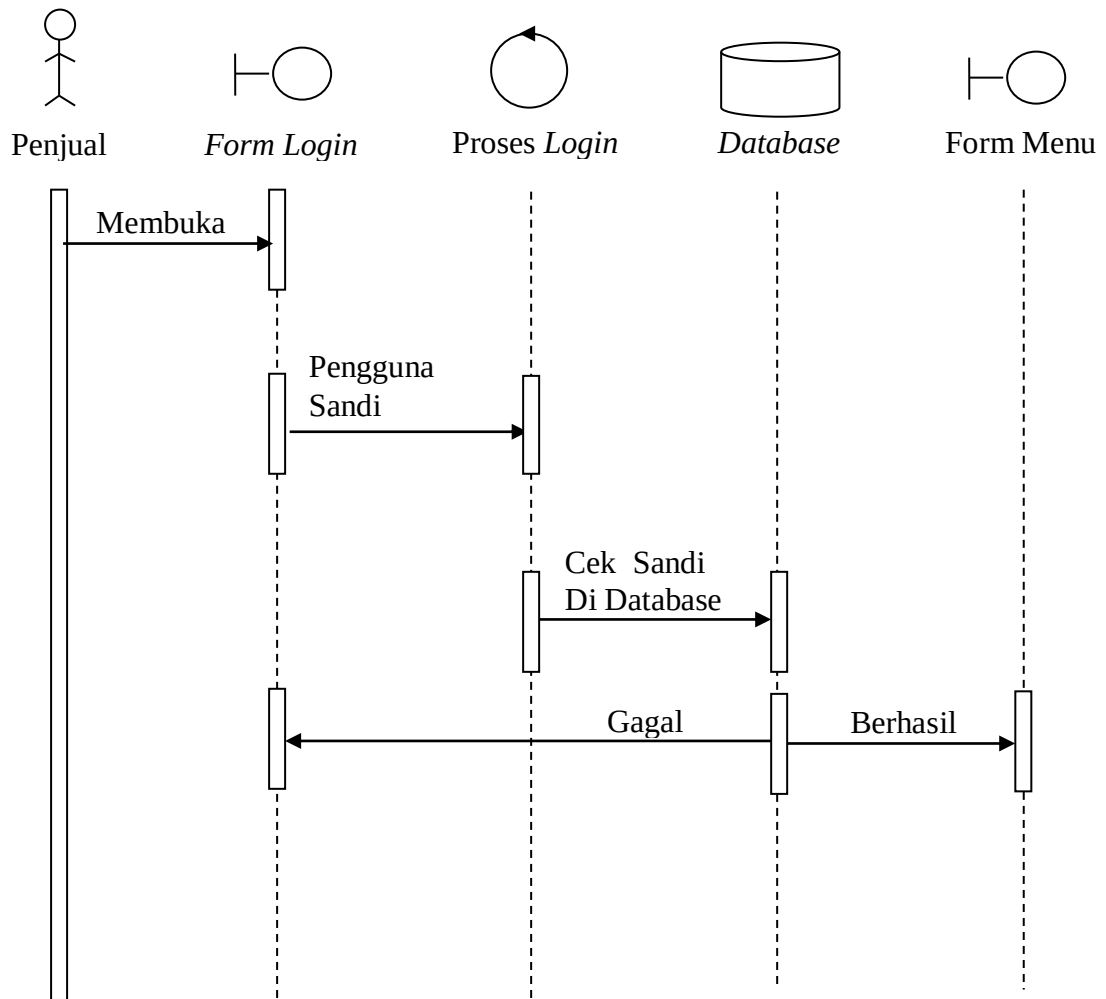
Gambar III.8. Activity Diagram Dekrip

III.3.3. Sequence Diagram Enkrip

Pada proses ini kita akan membuat alur dari sistem yang dirancang yaitu *sequence diagram*. Berikut adalah *sequence diagram* sistem yang dirancang.

1. Sequence Diagram Login

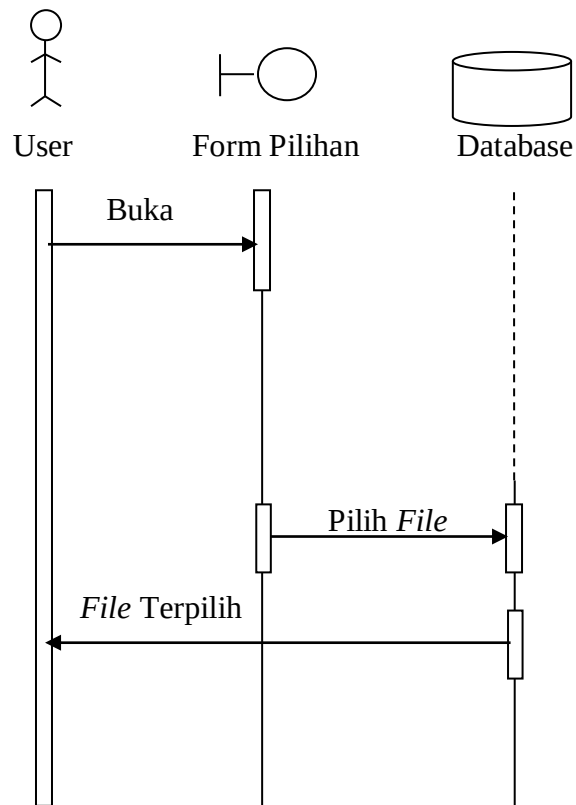
Aktivitas yang dilakukan untuk melakukan *login* dapat dilihat seperti pada gambar III.9 berikut :



Gambar III.9. Sequence Diagram Login

1. Sequence Diagram Upload Basis Data

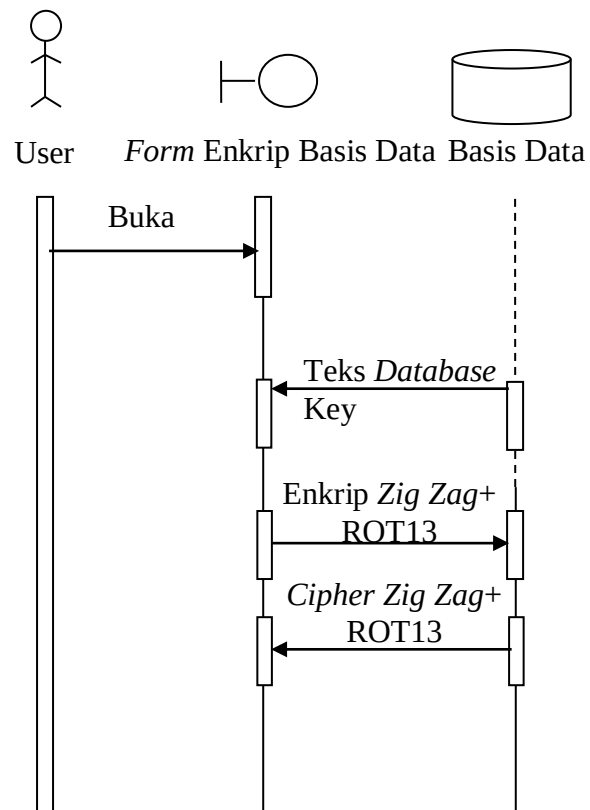
Aktivitas yang dilakukan untuk melakukan upload basis data dapat dilihat seperti pada gambar III.10 berikut :



Gambar III.10. Sequence Diagram Upload Basis Data

2. Sequence Diagram Enkrip

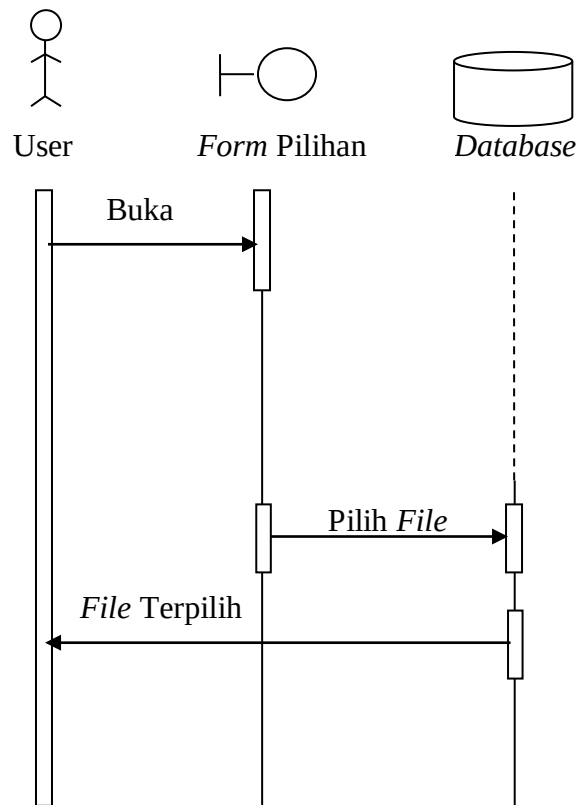
Aktivitas yang dilakukan untuk melakukan Enkrip dapat dilihat seperti pada gambar III.11 berikut :



Gambar III.11. Sequence Diagram Enkrip

3. Sequence Diagram *Ciphertext* Basis Data

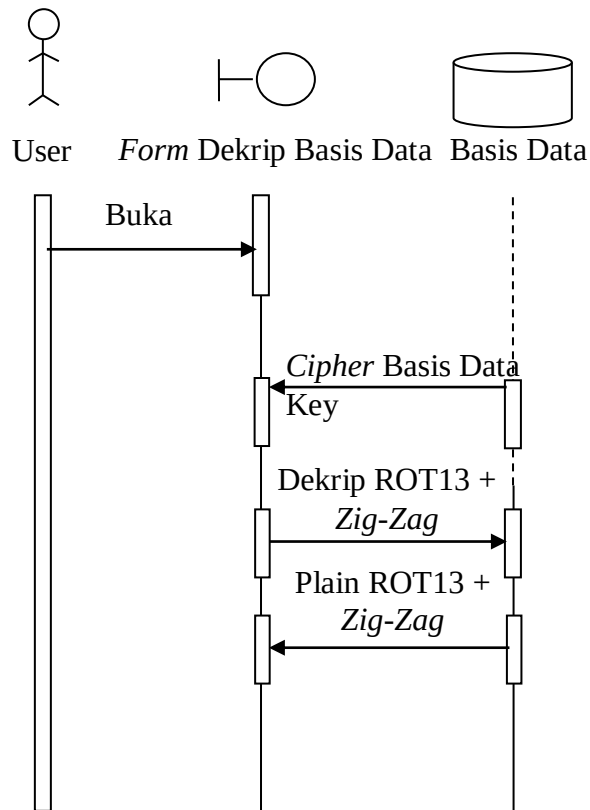
Aktivitas yang dilakukan untuk upload *ciphertext* basis data dapat dilihat seperti pada gambar III.12 berikut :



Gambar III.12. Sequence Diagram Upload Ciphertext Basis Data

4. Sequence Diagram Dekrip

Aktivitas yang dilakukan untuk melakukan Dekrip dapat dilihat seperti pada gambar III.13 berikut :



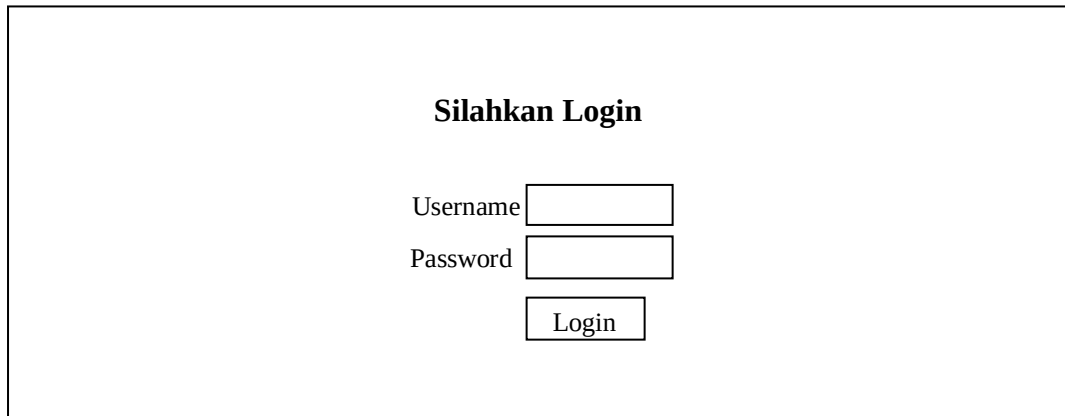
Gambar III.13. Sequence Diagram Dekrip

III.3.4. Desain Sistem

Perancangan *User Interface* merupakan masukan yang penulis rancang guna lebih memudahkan dalam *entry data*. *Entry data* yang dirancang akan lebih mudah dan cepat dan meminimalisir kesalahan penulisan dan memudahkan perubahan. Adapun bentuk rancangan *output* dari aplikasi penyandian isi *Basis Data* ini adalah sebagai berikut :

1. Rancangan *Output Form Login*

Rancangan *Output Form Login* berfungsi menampilkan *form login*. Adapun rancangan *Output Form Login* dapat dilihat pada Gambar III.14. sebagai berikut :

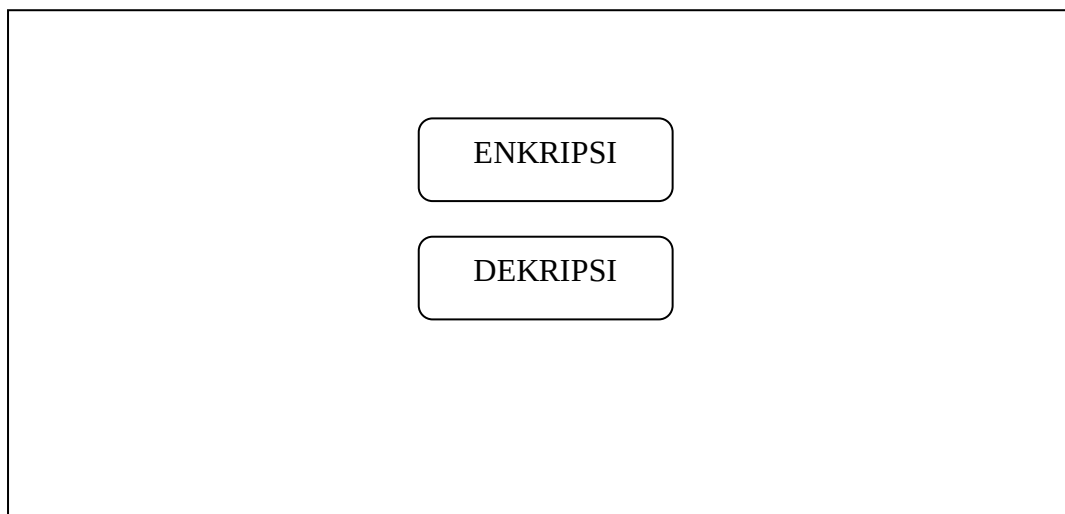


The image shows a login form layout. At the top center, the text "Silahkan Login" is displayed. Below this, there are two input fields: "Username" and "Password". Each label is positioned to the left of its corresponding input box. Below the "Password" field, there is a "Login" button.

Gambar III.14. Rancangan *Output Form Login*

2. Rancangan *Output Form Menu*

Rancangan *Output Form Menu* berfungsi menampilkan *form menu*. Adapun rancangan *Output Form Login* dapat dilihat pada Gambar III.15. sebagai berikut :



The image shows a menu form layout. It contains two buttons stacked vertically in the center. The top button is labeled "ENKRIPSI" and the bottom button is labeled "DEKRIPSI". Both buttons have rounded corners and a thin border.

Gambar III.15. Rancangan *Output Form Menu*

3. Rancangan *Output Form* Enkripsi

Rancangan *Output Form* Enkripsi berfungsi menampilkan *form* enkripsi. Adapun rancangan *Output Form* Enkripsi dapat dilihat pada Gambar III.16. sebagai berikut :

Isi Tabel Basis Data			
Teks Asli		Masukkan Data:	
Kunci Enkrip		Primary Key Name	
Teks Rahasia		Database	
	Enkrip	Nama Tabel	
			Cari Data

Gambar III.16. Rancangan *Output Form* Enkripsi

Keterangan :

Gambar III.16 merupakan tampilan *form* enkripsi dan untuk menggunakannya terlebih dahulu pengguna menuliskan nama basis data pada kotak teks Nama Basis Data dan menuliskan nama tabel pada kotak teks Nama Tabel kemudian mengklik tombol Tampilkan Basis Data. Setelah diklik maka akan tampil seluruh isi basis data meliputi nama-nama *field* dan isi setiap *field* tabel dari basis data yang ditampilkan. Kemudian pengguna menuliskan kunci pada kotak teks Kunci Zig Zag Cipher lalu memilih isi teks yang akan di enkrip dan mengklik tombol Enkrip, maka isi teks basis data akan menjadi teks rahasia.

4. Rancangan *Output Form* Dekripsi

Rancangan *Output Form* Dekripsi berfungsi menampilkan *form* enkripsi. Adapun rancangan *Output Form* Dekripsi dapat dilihat pada Gambar III.17. sebagai berikut :

Isi Tabel Basis Data			
Teks Rahasia Kunci Dekrip Teks Asli	 	Dekrip	Masukkan Data: Primary Key Name Database Nama Tabel
		Cari Data	

Gambar III.17. Rancangan *Output Form* Dekripsi

Keterangan :

Gambar III.17 merupakan tampilan *form* dekripsi dan untuk menggunakannya terlebih dahulu pengguna menuliskan nama basis data pada kotak teks Nama Basis Data dan menuliskan nama tabel pada kotak teks Nama Tabel kemudian mengklik tombol Tampilkan Basis Data. Setelah diklik maka akan tampil seluruh isi basis data meliputi nama-nama *field* dan isi setiap *field* tabel dari basis data yang ditampilkan. Kemudian pengguna menuliskan kunci pada kotak teks Kunci Zig Zag Cipher lalu memilih isi teks yang akan di dekrip dan mengklik tombol Dekrip, maka isi teks basis data akan menjadi teks asli.