

BAB IV

PEMBAHASAN DAN HASIL

1.1 Pembahasan

Beberapa tahapan yang akan dibahas pada penelitian ini yaitu analisis data, representasi data, hasil analisis data dan perancangan sebagai berikut :

1.1.1 Analisis Data

Data yang dibutuhkan dalam penelitian ini adalah data berupa teks. Pada tahap analisis data dilakukan penginputan data teks serta perancangan tampilan. Kemudian mengimplementasikan kombinasi algoritma *Rail Fence Cipher* dan ROT13 pada aplikasi untuk melakukan enkripsi dan dekripsi. Ada beberapa langkah program yang dilakukan yaitu:

- a. Menginput data teks.
- b. Pembacaan data teks.
- c. Melakukan enkripsi dengan algoritma Rail Fence cipher dan ROT13.
- d. Menampilkan cipherteks hasil enkripsi.

1.1.2 Analisis Kebutuhan

Tahap kedua setelah mengidentifikasi penyebab masalah penelitian yaitu tahap analisis kebutuhan yang mempunyai tujuan yaitu mengumpulkan kebutuhan atau informasi yang harus dimiliki oleh sistem. Analisis kebutuhan terbagi menjadi dua, yaitu kebutuhan fungsional dan kebutuhan non-fungsional. Kebutuhan fungsional mendeskripsikan aktivitas yang dilakukan oleh suatu sistem, sedangkan kebutuhan non-fungsional mendeskripsikan fitur, karakteristik dan batasan lainnya. Adapun kebutuhan fungsional dari sistem yang dikembangkan adalah sebagai berikut:

1. Menerima input plainteks

Sistem menerima input plainteks dari pengguna secara manual. Sistem hanya membaca data berupa teks, tidak membaca gambar maupun tabel.

2. Mengenkripsi pesan

Sistem dapat mengenkripsi serta dekripsi teks sesuai dengan kombinasi algoritma kriptografi Rail Fence Cipher dan ROT13, kemudian mengirim hasil cipherteks ke user melalui aplikasi pihak ketiga dan setelah cipherteks diterima, maka user melakukan enkripsi dengan kunci yang telah ditentukan.

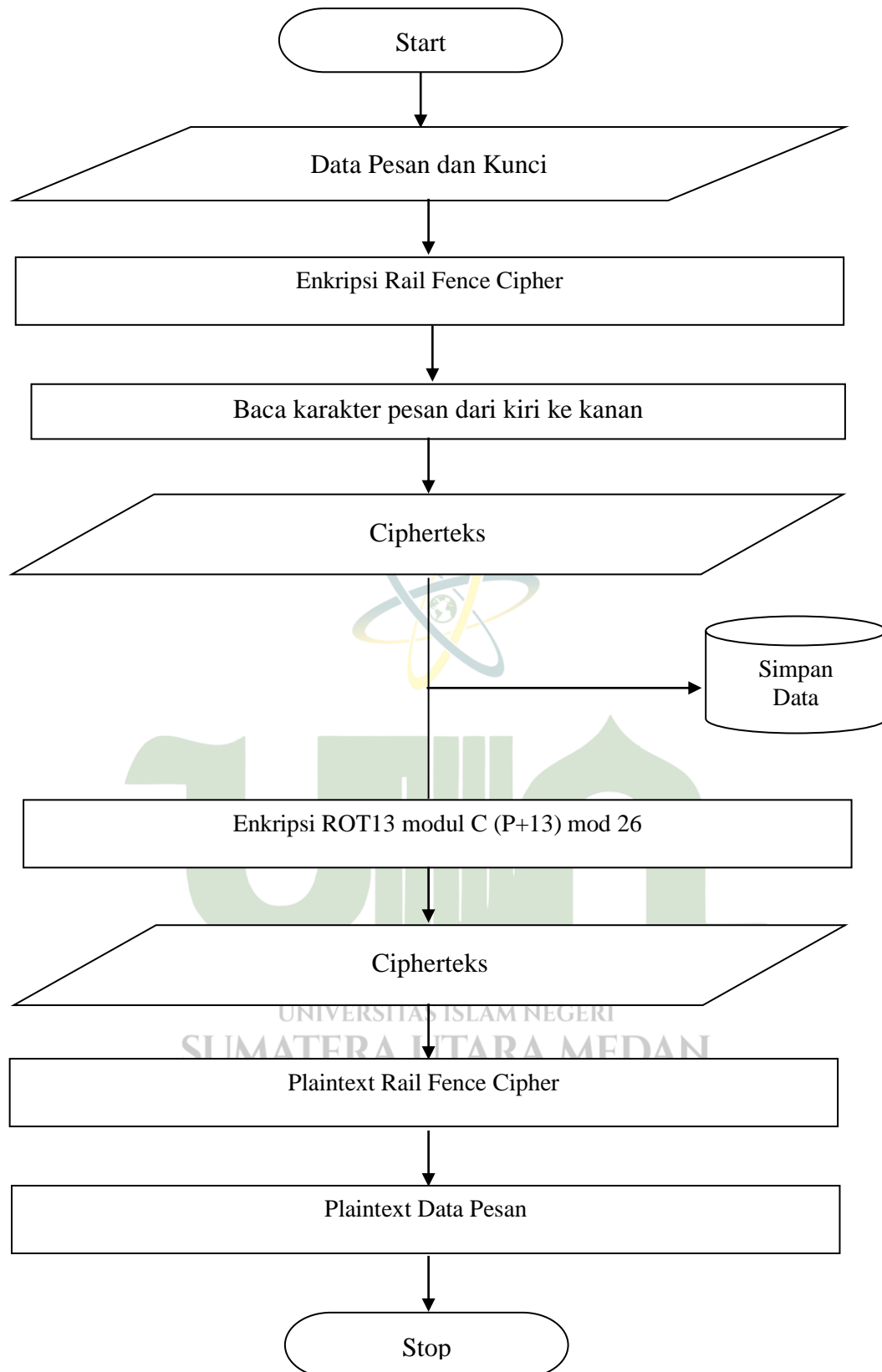
3. Mendekripsi pesan

Sistem dapat mengembalikan pesan ke bentuk semula dengan mendekripsi kembali cipherteks sesuai dengan kunci yang digunakan pada proses enkripsi.

1.1.3 *Flowchart* Enkripsi Algoritma Rail Fence Cipher

Enkripsi dengan kombinasi menggunakan algoritma kriptografi *Rail Fence Cipher* dengan ROT13 dimulai dengan enkripsi algoritma Rail Fence Cipher dengan dua jenis masukan yaitu untuk *input* file teks dan kunci. Pada gambar 4.1 dapat dilihat *flowchart* proses enkripsi *Rail Fence Cipher*.



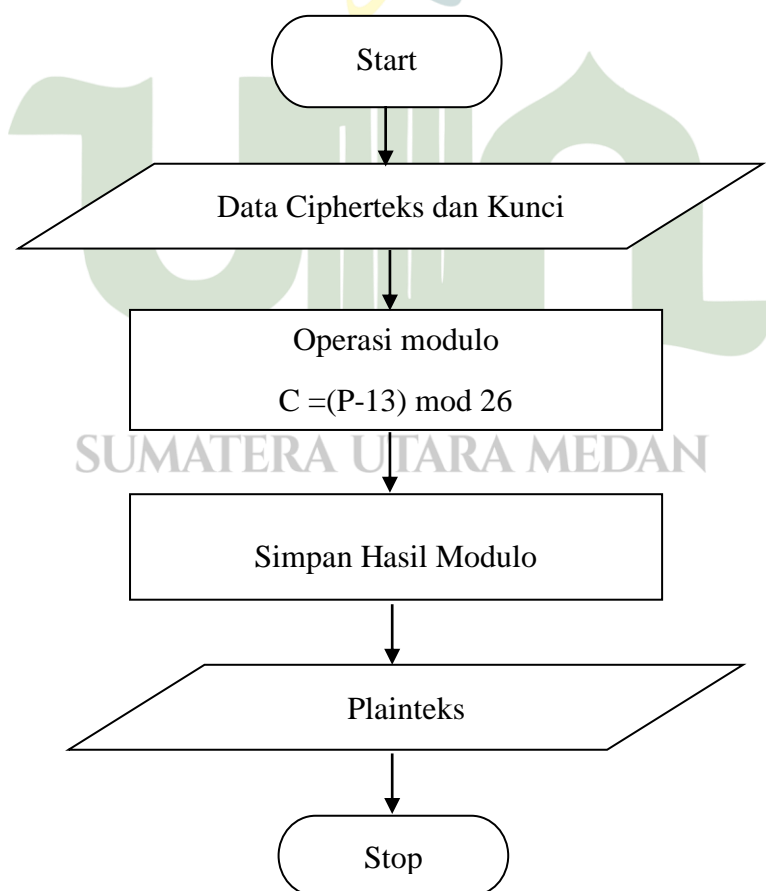


Gambar 4.1 Flowchart Hybrid Rail Fence Cipher dan ROT13

Pada gambar 4.1 menunjukkan proses enkripsi algoritma *Rail Fence Cipher* yang dimulai dengan memasukan sebuah pesan dan kunci kemudian karakter pesan pada baris disusun secara zig-zag sebanyak jumlah kunci selanjutnya karakter dibaca dari kiri ke kanan atau secara horizontal pada setiap baris maka diperoleh hasil dari cipherteks, enkripsi algoritma ROT13 yang dimulai dengan memasukan sebuah pesan dan kunci kemudian karakter pesan pada baris disusun secara zig-zag sebanyak jumlah kunci selanjutnya karakter dibaca dari kiri ke kanan atau secara horizontal pada setiap baris maka diperoleh hasil dari cipherteks.

1.1.4 Flowchart Dekripsi Algoritma Rail Fence Cipher dan ROT13

Proses dekripsi menggunakan algoritma kriptografi ROT13 mempunyai dua jenis masukan yaitu untuk *input* cipherteks dan kunci. Pada Gambar 4.1 dapat dilihat *flowchart* proses dekripsi ROT13.



Gambar 4.2 Flowchart Dekripsi Rail Fence Cipher dan ROT13

Pada gambar 4.2 menunjukkan proses dekripsi algoritma ROT13 yang dimulai dengan memasukan sebuah data cipherteks dan kunci kemudian karakter pesan pada baris disusun secara zig-zag sebanyak jumlah kunci selanjutnya karakter dibaca dari kiri ke kanan atau secara horizontal pada setiap baris maka diperoleh hasil dari cipherteks.

1.1.5 Proses Enkripsi Algoritma Rail Fence Cipher

Proses enkripsi teks dengan algoritma *Rail Fence Cipher* dilakukan dimana plainteks yang digunakan adalah "KRIPTOGRAFI DATA ADALAH SEBUAH CARA UNTUK MENYAMARKAN DATA" dan kunci yang digunakan adalah $n=4$. Langkah-langkah perhitungannya dapat dilihat sebagai berikut:

1. Enkripsi *plaintext* menggunakan fungsi enkripsi *Rail Fence Cipher* dengan kunci $n=4$. Proses enkripsi karakter dapat dilihat seperti pada tabel 4.1 sebagai berikut:

Tabel 4.1 Proses Enkripsi Rail Fence Cipher

N	Plainteks = KRIPTOGRAFI DATA ADALAH SEBUAH CARA UNTUK MENYAMARKAN DATA														
1	K	T	A	A	D	H	U	A	N	M	A	K	A		
2		R	O	F	T	A	S	A	R	T	E	M	A	T	
3			I	G	I	A	L	E	H	A	U	N	A	N	A
4				P	R	D	A	A	B	C	U	K	Y	R	D

Proses dekripsi adalah nilai kunci yang digunakan adalah dengan menghitung jumlah karakter *ciphertext*, selanjutnya bagikan dengan nilai kunci enkripsi, maka hasilnya sebagai kunci dekripsi.

Ciphertext = KTAADHUANMAKA ROFTASARTEMAT IGIALEHAUNANA
PRDAABCUKYRD

Kunci dekripsi = $51 / 4 = 12.75 \sim 13$

1.1.6 Proses Enkripsi Algoritma ROT13

Proses enkripsi dengan algoritma ROT13 dilakukan dimana plainteks yang digunakan adalah hasil enkripsi algoritma Rail Fence Cipher adalah sebagai berikut :

Tabel 4.2 Tabel Alfabet dan Indeks

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

Cara enkripsi K indeks = 10, maka cipherteks = $(10+13) \bmod 26 = 23$

D indeks = 3, maka cipherteks = $(3+13) \bmod 26 = 16$

Untuk plainteks selanjutnya dapat dilihat seperti pada tabel 4.3.

Tabel 4.3 Hasil Enkripsi ROT13

Plainteks	IdxP	Operasi Mod $(\text{IdxP}+13) \bmod 26$	IdxC	Cipherteks
K	10	$(10+13) \bmod 26$	23	X
T	19	$(19+13) \bmod 26$	6	G
A	0	$(0+13) \bmod 26$	13	N
A	0	$(0+13) \bmod 26$	13	N
D	3	$(3+13) \bmod 26$	16	Q
H	7	$(7+13) \bmod 26$	20	U
U	20	$(20+13) \bmod 26$	7	H
A	0	$(0+13) \bmod 26$	13	N
N	13	$(13+13) \bmod 26$	0	A
M	12	$(12+13) \bmod 26$	25	Z
A	0	$(0+13) \bmod 26$	13	N
K	10	$(10+13) \bmod 26$	23	X

Plainteks	IdxP	Operasi Mod (IdxP+13) mod 26	IdxC	Cipherteks
A	0	$(0+13) \bmod 26$	13	N
R	17	$(17+13) \bmod 26$	4	E
O	14	$(14+13) \bmod 26$	1	B
F	5	$(5+13) \bmod 26$	18	S
T	19	$(19+13) \bmod 26$	6	G
A	0	$(0+13) \bmod 26$	13	N
S	18	$(18+13) \bmod 26$	5	F
A	0	$(0+13) \bmod 26$	13	N
R	17	$(17+13) \bmod 26$	4	E
T	19	$(19+13) \bmod 26$	6	G
E	4	$(4+13) \bmod 26$	17	R
M	12	$(12+13) \bmod 26$	25	Z
A	0	$(0+13) \bmod 26$	13	N
T	19	$(19+13) \bmod 26$	6	G
I	8	$(8+13) \bmod 26$	21	V
G	6	$(6+13) \bmod 26$	19	T
I	8	$(8+13) \bmod 26$	21	V
A	0	$(0+13) \bmod 26$	13	N
L	11	$(11+13) \bmod 26$	24	Y
E	4	$(4+13) \bmod 26$	17	R
H	7	$(7+13) \bmod 26$	20	U
A	0	$(0+13) \bmod 26$	13	N
U	20	$(20+13) \bmod 26$	7	H
N	13	$(13+13) \bmod 26$	0	A
A	0	$(0+13) \bmod 26$	13	N
N	13	$(13+13) \bmod 26$	0	A

Plainteks	IdxP	Operasi Mod (IdxP+13) mod 26	IdxC	Cipherteks
A	0	(0+13) mod 26	13	N
P	15	(15+13) mod 26	2	C
R	17	(17+13) mod 26	4	E
D	3	(3+13) mod 26	16	Q
A	0	(0+13) mod 26	13	N
A	0	(0+13) mod 26	13	N
B	1	(1+13) mod 26	14	O
C	2	(2+13) mod 26	15	P
U	20	(20+13) mod 26	7	H
K	10	(10+13) mod 26	23	X
Y	24	(24+13) mod 26	11	L
R	17	(17+13) mod 26	4	E
D	3	(3+13) mod 26	16	Q

Hasil enkripsinya Rail Fence Cipher teks :

“KTAADHUANMAKA ROFTASARTEMAT IGIALEHAUNANA
PRDAABCUKYRD”

Hasil enkripsinya ROT13 teks :

“XGNNQUHNAZNXN EBSGNFNEGRZNG VTVNYRUNHANAN
CEQNNOPHXLEQ”

1.1.7 Proses Dekripsi Algoritma ROT13

Proses dekripsi dengan algoritma ROT13 dilakukan dimana cipherteks yang digunakan adalah hasil enkripsi algoritma ROT13 adalah sebagai berikut:

Cara dekripsi Indeks cipherteks X = 23, maka Plainteks = $(23+13) \bmod 26 = 10$

Indeks cipherteks Q = 16, maka Plainteks = $(16+13) \bmod 26 = 3$

Indeks cipherteks H = 7, maka Plainteks = $(7+13) \bmod 26 = 20$

Untuk plainteks selanjutnya dapat dilihat seperti pada tabel 4.4.

Tabel 4.4 Hasil Dekripsi ROT13

Cipherteks	IdxC	Operasi Mod (IdxC+13) mod 26	IdxP	Plainteks
X	23	$(23+13) \bmod 26$	10	K
G	6	$(6+13) \bmod 26$	19	T
N	13	$(13+13) \bmod 26$	0	A
N	13	$(13+13) \bmod 26$	0	A
Q	16	$(16+13) \bmod 26$	3	D
U	20	$(20+13) \bmod 26$	7	H
H	7	$(7+13) \bmod 26$	20	U
N	13	$(13+13) \bmod 26$	0	A
A	0	$(0+13) \bmod 26$	13	N
Z	25	$(25+13) \bmod 26$	12	M
N	13	$(13+13) \bmod 26$	0	A
X	23	$(23+13) \bmod 26$	10	K
N	13	$(13+13) \bmod 26$	0	A
E	4	$(4+13) \bmod 26$	17	R
B	1	$(1+13) \bmod 26$	14	O
S	18	$(18+13) \bmod 26$	5	F
G	6	$(6+13) \bmod 26$	19	T
N	13	$(13+13) \bmod 26$	0	A
F	5	$(5+13) \bmod 26$	18	S
N	13	$(13+13) \bmod 26$	0	A
E	4	$(4+13) \bmod 26$	17	R
G	6	$(6+13) \bmod 26$	19	T
R	17	$(17+13) \bmod 26$	4	E
Z	25	$(25+13) \bmod 26$	12	M
N	13	$(13+13) \bmod 26$	0	A
G	6	$(6+13) \bmod 26$	19	T

Cipherteks	IdxC	Operasi Mod (IdxC+13) mod 26	IdxP	Plainteks
V	21	$(21+13) \bmod 26$	8	I
T	19	$(19+13) \bmod 26$	6	G
V	21	$(21+13) \bmod 26$	8	I
N	13	$(13+13) \bmod 26$	0	A
Y	24	$(24+13) \bmod 26$	11	L
R	17	$(17+13) \bmod 26$	4	E
U	20	$(20+13) \bmod 26$	7	H
N	13	$(13+13) \bmod 26$	0	A
H	7	$(7+13) \bmod 26$	20	U
A	0	$(0+13) \bmod 26$	13	N
N	13	$(13+13) \bmod 26$	0	A
A	0	$(0+13) \bmod 26$	13	N
N	13	$(13+13) \bmod 26$	0	A
C	2	$(2+13) \bmod 26$	15	P
E	4	$(4+13) \bmod 26$	17	R
Q	16	$(16+13) \bmod 26$	3	D
N	13	$(13+13) \bmod 26$	0	A
N	13	$(13+13) \bmod 26$	0	A
O	14	$(14+13) \bmod 26$	1	B
P	15	$(15+13) \bmod 26$	2	C
H	7	$(7+13) \bmod 26$	20	U
X	23	$(23+13) \bmod 26$	10	K
L	11	$(11+13) \bmod 26$	0	Y
E	4	$(4+13) \bmod 26$	17	R
Q	16	$(16+13) \bmod 26$	3	D

Hasil dekripsinya adalah “KTAADHUANMAKA ROFTASARTEMAT IGIALEHAUNANA PRDAABCUKYRD”

1.1.8 Proses Dekripsi Algoritma Rail Fence Cipher

Untuk mengembalikan *ciphertext* ke data plainteks aslinya maka dilakukan dekripsi *Rail Fence Cipher* dimana *ciphertext* dapat ditulis secara horizontal dengan kunci sebanyak $n=4$, kemudian *plaintext* dapat dibaca secara vertikal yang dapat dilihat pada tabel 4.5 sebagai berikut:

Tabel 4.5 Proses Dekripsi Rail Fence Cipher

N	Chiperteks = KTAADHUANMAKA ROFTASARTEMAT IGIALEHAUNANA PRDAABCUKYRD													
1	K	T	A	A	D	H	U	A	N	M	A	K	A	
2		R	O	F	T	A	S	A	R	T	E	M	A	T
3			I	G	I	A	L	E	H	A	U	N	A	N
4				P	R	D	A	A	B	C	U	K	Y	R

Proses dekripsi nilai kunci yang digunakan adalah dengan menghitung jumlah karakter *ciphertext*, selanjutnya bagikan dengan nilai kunci enkripsi, maka hasilnya sebagai kunci dekripsi.

Ciphertext = KTAADHUANMAKA ROFTASARTEMAT IGIALEHAUNANA
PRDAABCUKYRD

Kunci dekripsi = $51 / 4 = 12.75 \sim 13$

Selanjutnya, menentukan nilai plainteks dengan cara membaca karakter secara baris, seperti pada gambar berikut ini :

Tabel 4.6 Hasil Dekripsi Rail Fence Cipher

Baris-1	K	R	I	P
Baris-2	T	O	G	R
Baris-3	A	F	I	D
Baris-4	A	T	A	A
Baris-5	D	A	L	A
Baris-6	H	S	E	B
Baris-7	U	A	H	C
Baris-8	A	R	A	U
Baris-9	N	T	U	K
Baris-10	M	E	N	Y
Baris-11	A	M	A	R
Baris-12	K	A	N	D
Baris-13	A	T	A	

Hasil Dekripsi Rail Fence Cipher :

Plainteks = **KRIPTOGRAFI DATA ADALAH SEBUAH CARA UNTUK
MENYAMARKAN DATA**

Pada tabel 4.6 setelah dilakukan fungsi dekripsi *Rail Fence Cipher* maka diperoleh pesan asli atau plainteks yaitu "**KRIPTOGRAFI DATA ADALAH SEBUAH CARA UNTUK MENYAMARKAN DATA**". Dari perhitungan diatas dapat disimpulkan bahwa *plaintext* yang telah dienkripsi akan kembali seperti semula setelah dilakukannya proses dekripsi.

Setelah menganalisis data diatas, maka dapat diketahui proses pembentukan hasil enkripsi teks pesan dengan kombinasi algoritma dengan ROT13 yaitu pada algoritma Rail Fence Cipher dengan penulisan pesan secara zigzag dan pembentukan cipherteksnya secara pembacaan horizontal dan dengan algoritma ROT13 yaitu dengan melakukan operasi modulo dari nilai indeks huruf plainteks maupun cipherteksnya yang ditambah dengan angka 13.

1.1.9 Perancangan Antarmuka

Rancangan antar muka bagi pengguna untuk melakukan enkripsi dan dekripsi dengan kombinasi algoritma Rail Fence Cipher dan ROT13 dapat dilihat seperti pada gambar 4.3.

a. Rancangan form Enkripsi dan Dekripsi

Data teks	Cipherteks1	Cipherteks2	Plainteks1	Plainteks2
-----------	-------------	-------------	------------	------------

File	Enkripsi	Dekripsi	Simpan	Bersih	Keluar
------	----------	----------	--------	--------	--------

Nama File	XX
Jumlah Karakter	XXXXX
Key	XXXXX
Lama Proses	XXXXX

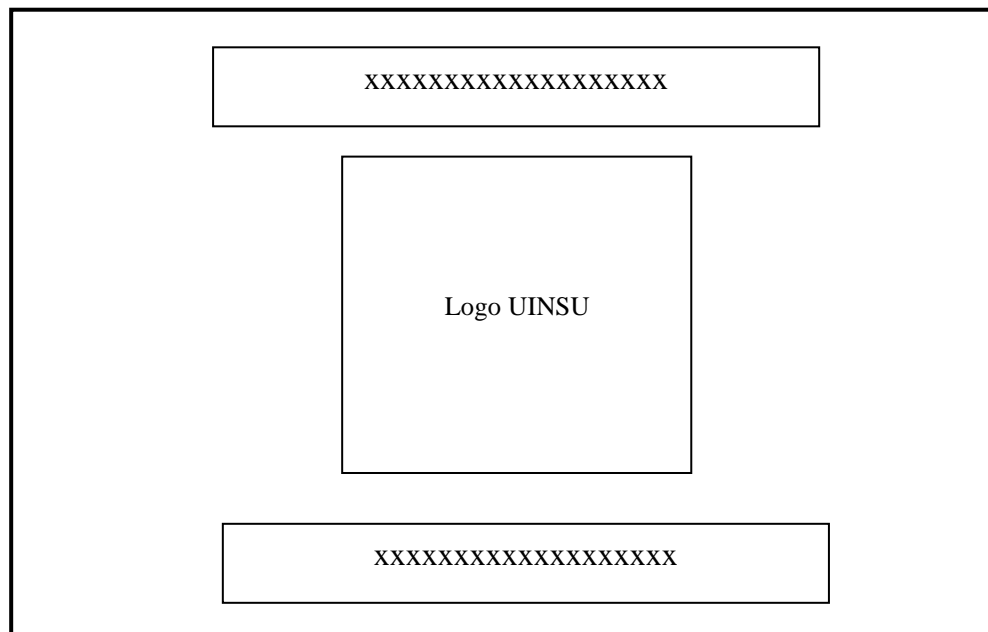
Gambar 4.3 Rancangan Form Enkripsi dan Dekripsi

Gambar diatas merupakan gambar perancangan dialog akan gambaran program yang akan dibuat dengan menerapkan kombinasi algoritma Rail Fence Cipher dengan ROT13 dalam melakukan enkripsi dan dekripsi file teks. Dimulai dari memasukkan file pesan teks yang akan diproses dengan cara menekan *button* “File” dan diikuti dengan pemasukan Key. Setelah dilakukan pemilihan file pesan, maka pada data pesan teks akan muncul huruf-huruf pesan yang akan dienkripsi, kemudian tekan *button* “Enkripsi”, yang dimana hasilnya pada *textBox* Cipherteks akan uncul hasil enkripsi dan selanjutnya pilih tombol “Dekripsi” untuk melakukan dekripsi data cipherteks dan jika memilih tombol Simpan, maka data hasil enkripsi yaitu cipherteks akan disimpan dengan memasukkan folder dan nama filenya. Untuk melakukan pembersihan hasil proses, maka pilih tombol “Bersih” untuk membersihkan hasil proses enkripsi atau dekripsi yang telah

dilakukan atau jika ingin mengulangi dengan proses berikutnya, tekan button “*Bersih*” dan untuk menutup halaman Dialog, maka pilih tombol “*Keluar*”.

b. Menu Utama

Menu Utama digunakan untuk menampilkan *form* induk dari sistem yang didalamnya terdapat integrasi dengan program enkripsi dan dekripsi menggunakan kombinasi algoritma Rail Fence Cipher dengan ROT13. Adapun perancangan Menu Utama dapat dilihat pada gambar 4.4.



Gambar 4.4 Rancangan Form Menu

Pada tampilan form Menu diatas terdapat judul penelitian, logo UINSU serta informasi program studi mahasiswa.

1.1.10 Gambar Tampilan

a. Tampilan *Form* Menu

Form menu digunakan untuk menampilkan *form* induk dari sistem yang didalamnya terdapat integrasi antar *form* yang terhubung kedalam *form* utama. Tampilan *form* Menu berisi 2 menu yaitu File dan Keluar. Pada menu File terdapat sub menu file program Enkripsi. Tampilan form Menu dapat dilihat pada gambar 4.5.

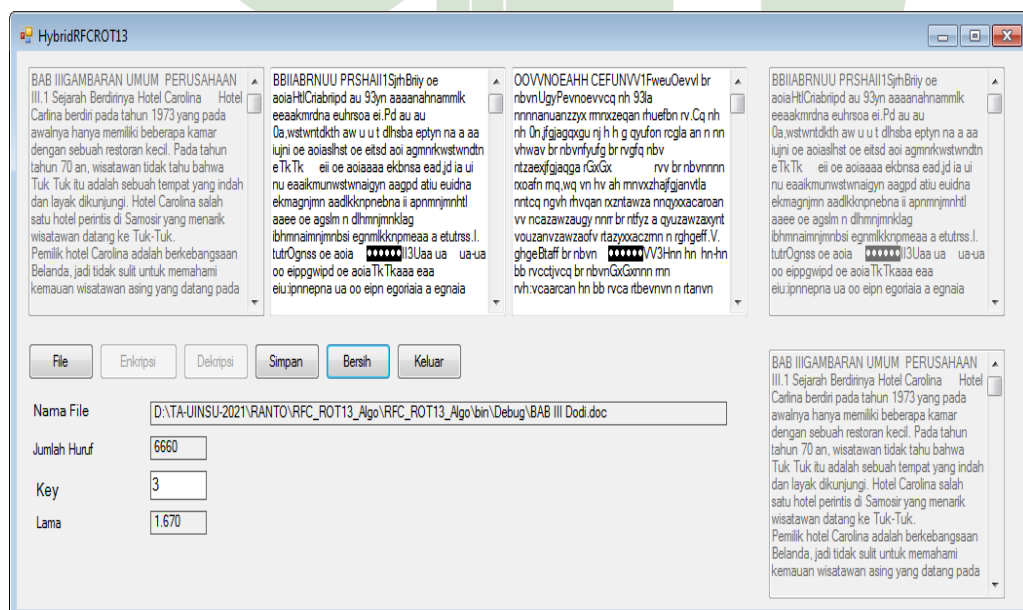


Gambar 4.5 Tampilan Form Menu

Pada tampilan form Menu diatas terdapat judul penelitian, logo UINSU serta informasi program studi mahasiswa.

b. Tampilan *Form* Enkripsi

Form Enkripsi berfungsi untuk melakukan enkripsi dan dekripsi file teks dengan kombinasi algoritma Rail Fence Cipher dengan ROT13. Tampilan *form* Enkripsi dapat dilihat pada Gambar 4.6.



Gambar 4.6 Tampilan Form Enkripsi

Pada tampilan Form Enkripsi terdapat tombol File yang berfungsi untuk memilih file teks yang akan di enkripsi. Selanjutnya isi file teks tersebut akan ditampilkan pada *text box* dan dilakukan enkripsi dengan pemilihan tombol. Enkripsi dan hasilnya adalah cipherteks ditampilkan pada *text box* disebelahnya. Selanjutnya atas hasil enkripsi yaitu cipherteks tersebut dilakukan dekripsi dengan memilih tombol Dekripsi. Hasil enkripsi juga dapat disimpan dalam file berformat .hyb.

1.2 Hasil Pengujian

Pada tahap ini akan dilakukan pengujian enkripsi dan dekripsi masing-masing algoritma terhadap data teks dengan jumlah karakter yang bervariasi anatar 10 sampai 100 karakter serta output yang akan ditampilkan adalah hasil enkripsi berupa file cipherteks serta waktu proses (running time). Hasil pengujian enkripsi file pesan dengan 10 karakter sampai dengan 100 karakter adalah seperti pada tabel 4.6.

a. Hasil Pengujian

Tabel 4.7 Hasil Pengujian Enkripsi

No	Nama File Pesan	Plainteks	Cipherteks	Running time (s)
1	Pesan-10	KRIPTOGRAF	XVGTNECBES	0.0006
2	Pesan-20	KRIPTOGRAFI DATA ADA	XVGTNVQG QECBES NNNN	0.0007
3	Pesan-30	KRIPTOGRAFI DATA ADALAH SEBUAH	XVGTNVQG QYUFONECBES NNNNN RHU	0.006
4	Pesan-40	MENJAGA KERAHASIAAN FILE DENGAN MENGGUNA	ZANNXEUFNASY RTAZATARWT RNNVN VRQAN RTHN	0.008
5	Pesan-50	MENJAGA KERAHASIAAN FILE DENGAN MENGGUNAKAN METODE	ZANNXEUFNASY RTAZATAZGQRWT RNNVN VRQAN RTHNN RBR	0.008

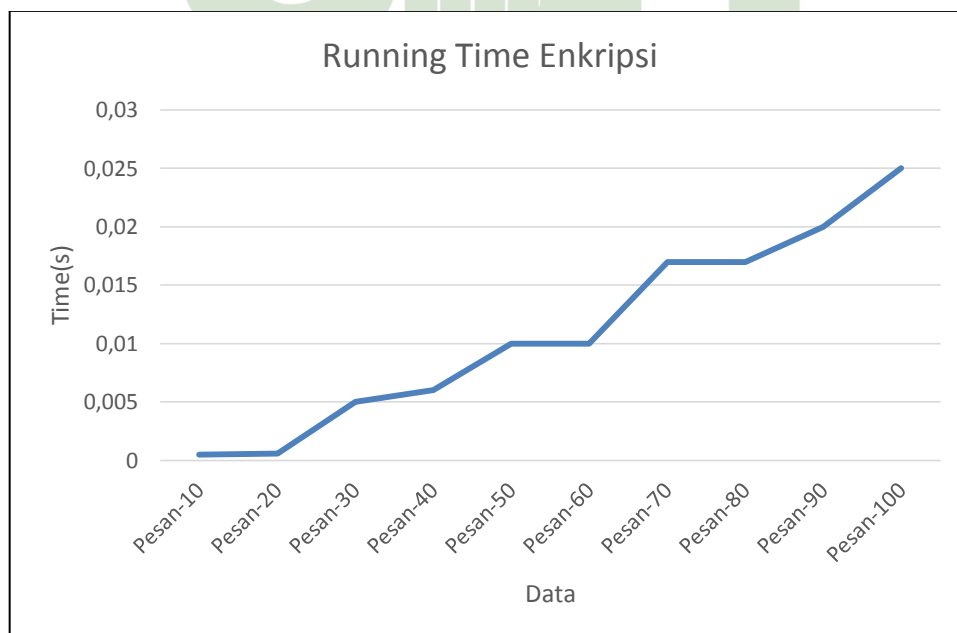
No	Nama File Pesan	Plainteks	Cipherteks	Running time (s)
6	Pesan-60	MENJAGA KERAHASIAAN FILE DENGAN MENGUNAKAN METODE RAIL FENCE	ZANNXEUFNASY RTAZATAXAZGQ NYRPRWT RNNVN VRQAN RTHNN RBREVSAR	0.009
7	Pesan-70	MENJAGA KERAHASIAAN FILE DENGAN MENGUNAKAN METODE RAIL FENCE CIPHER DAN	ZANNXEUFNASY RTAZATAXAZGQ NYRP VUEQARWT RNNVN VRQAN RTHNN RBREVSARPCR N	0.009
8	Pesan-80	MENJAGA KERAHASIAAN FILE DENGAN MENGUNAKAN METODE RAIL FENCE CIPHER DAN ROT13 PE	ZANNXEUFNASY RTAZATAXAZGQ NYRP VUEQAEG3CRWT RNNVN VRQAN RTHNN RBREVSARPCR N B1 R	0.012
9	Pesan-90	MENJAGA KERAHASIAAN FILE DENGAN MENGUNAKAN METODE RAILFENCE CIPHER DAN ROT13 PERKEMBANGAN	ZANNXEUFNASY RTAZATAXAZGQ NYRP VUEQAEG3CEROANRWT RNNVN VRQAN RTHNN RBREVSARPCR N B1 RXZNTA	0.012
10	Pesan-100	MENJAGA KERAHASIAAN FILE DENGAN MENGUNAKAN METODE RAILFENCE CIPHER DAN ROT13 PERKEMBANGAN TEKNOLOGI	ZANNXEUFNASY RTAZATAXAZGQ NYRP VUEQAEG3CEROAN RAYTRWT RNNVN VRQAN RTHNN RBREVSARPCR N B1 RXZNTAGXBBV	0.015

b. Waktu Proses Enkripsi

Tabel 4.8 Waktu Proses Enkripsi

No	Nama File	Running Time (s)
1	Pesan-10	0.0005
2	Pesan-20	0.0006
3	Pesan-30	0.005
4	Pesan-40	0.006
5	Pesan-50	0.010
6	Pesan-60	0.010
7	Pesan-70	0.017
8	Pesan-80	0.017
9	Pesan-90	0.020
10	Pesan-100	0.025

Dari data pada tabel 4.8 diatas dapat dibuatkan Grafik Running Time Enkripsi seperti pada gambar 4.7.

**Gambar 4.7** Tampilan Running Time Enkripsi