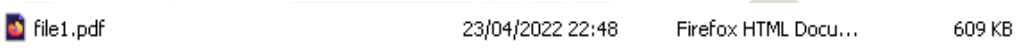
BAB IV
HASIL DAN PEMBAHASAN

4.1.Pembahasan

Adapun Beberapa tahapan yang akan dibahas dalam penelitian ini yaitu analisis data, representasi data, hasil analisis data dan perancangan sebagai berikut.

4.1.1. Analisis Data

Proses penyandian data dengan teknik cryptografi memerlukan sebuah objek, pada penelitian ini data objek yang digunakan adalah pdf dengan format pdf. Adapun dokumen pdf yang digunakan adalah pdf sampel dengan nama file.pdf seperti pada gambar di bawah ini :



Gambar 4.1 File PDF Sampel

Berdasarkan pada gambar 4.1, didapati sebuah objek dokumen pdf yang akan dienkripsi agar isi dalam sebuah dokumen tidak bisa dibaca. Selanjutnya adalah menentukan kunci yang akan dibuat agar bisa di dekripsi kembali pada objek dokumen pdf. Adapun contoh kunci yang akan dibuat pada proses penerapan manual adalah dengan character ASCII “‼ 4Wy¼ ß ñ”.

4.1.2. Representasi Data

Berdasarkan pada analisis data, didapatkan objek dokumen pdf sebagai media yang akan dienkripsi. Selanjutnya penulis menggunkan CRC32 untuk bertujuan dimana mengubah file untuk menjadi karakter, dalam hal ini karakter yang di dapat adalah ⊤ x G>” yang nanti nya berfungsi untuk keperluan hitungan manual, untuk proses enkripsi dengan metode DES.

1. Data Pdf Sample

Berdasarkan pada gambar 4.1, diambil nilai pdf dalam bentuk ASCII yaitu "^⊤ xG>" dan dirubah kedalam bentuk biner seperti pada gambar di bawah ini:

Dec	Hex	Name	Char	Ctrl-char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	0	Null	NUL	CTRL-@	32	20	Space	64	40	@	96	60	`
1	1	Start of heading	SOH	CTRL-A	33	21	!	65	41	A	97	61	a
2	2	Start of text	STX	CTRL-B	34	22	"	66	42	B	98	62	b
3	3	End of text	ETX	CTRL-C	35	23	#	67	43	C	99	63	c
4	4	End of xmit	EOT	CTRL-D	36	24	$	68	44	D	100	64	d
5	5	Enquiry	ENQ	CTRL-E	37	25	%	69	45	E	101	65	e
6	6	Acknowledge	ACK	CTRL-F	38	26	&	70	46	F	102	66	f
7	7	Bell	BEL	CTRL-G	39	27	'	71	47	G	103	67	g
8	8	Backspace	BS	CTRL-H	40	28	(	72	48	H	104	68	h
9	9	Horizontal tab	HT	CTRL-I	41	29	)	73	49	I	105	69	i
10	0A	Line feed	LF	CTRL-J	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	VT	CTRL-K	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	FF	CTRL-L	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage feed	CR	CTRL-M	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	SO	CTRL-N	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	SI	CTRL-O	47	2F	/	79	4F	O	111	6F	o
16	10	Data line escape	DLE	CTRL-P	48	30	0	80	50	P	112	70	p
17	11	Device control 1	DC1	CTRL-Q	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	DC2	CTRL-R	50	32	2	82	52	R	114	72	r
19	13	Device control 3	DC3	CTRL-S	51	33	3	83	53	S	115	73	s
20	14	Device control 4	DC4	CTRL-T	52	34	4	84	54	T	116	74	t
21	15	Neg acknowledge	NAK	CTRL-U	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	SYN	CTRL-V	54	36	6	86	56	V	118	76	v
23	17	End of xmit block	ETB	CTRL-W	55	37	7	87	57	W	119	77	w
24	18	Cancel	CAN	CTRL-X	56	38	8	88	58	X	120	78	x
25	19	End of medium	EM	CTRL-Y	57	39	9	89	59	Y	121	79	y
26	1A	Substitute	SUB	CTRL-Z	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	ESC	CTRL-[	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	FS	CTRL-\	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	GS	CTRL-]	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	RS	CTRL-^	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	US	CTRL-_	63	3F	?	95	5F	_	127	7F	DEL

Gambar 4.3 Tabel Ascii 0-127 Nguyen(2021)

Adapun ASCII pdf yang telah didapatkan sebagai berikut:

2. Data dan kunci

Sebelum proses enkripsi, terlebih dahulu setiap karakter dirubah kedalam bentuk biner, proses perubahan karakter kedalam bentuk biner dapat menggunakan tabel ASCII. Adapun nilai biner dari key adalah sebagai berikut :

Tabel 4.1 Biner Data IV Pdf

No.	Karakter	Heksadesimal	Biner	Jumlah bit
1.	^	5e	01011110	8
2.	□	Af	10101111	8
3.	⊤	16	00010110	8
4.	X	78	01111000	8
5.	□	9b	10011011	8
6.	□	e1	11100001	8
7.	G	47	01000111	8
8.	>	3e	00111110	8
Total bit				64

Tabel 4.2 Biner Kunci

No.	Karakter	Heksadesimal	Biner	Jumlah bit
1.	‼	13	00010011	8
2.	4	34	00110100	8
3.	W	57	01010111	8
4.	Y	79	01111001	8
5.	□	9B	10011011	8
6.	¼	BC	10111100	8
7.	ß	DF	11011111	8
8.	Ñ	F1	11110001	8
Total bit				64

Berdasarkan tabel di atas, didapati data biner dari data kunci yang akan dienkripsi

4.1.3. Hasil Analisis Data

1. Proses Enkripsi DES

Setelah nilai object file pdf didapati dan key didapati, selanjutnya adalah melakukan proses pengekripsian dengan metode DES. Pada proses pengekripsian, enkripsi membutuhkan sebuah kunci sebagai penanda awal serta penanda akhir sebagai pembatas dalam pengambilan bit biner pada object pdf. Adapun penanda yang digunakan adalah karakter "::", sedangkan kunci yang digunakan dalam proses hitungan manual ini adalah string "‼ 4Wy¿ ¼ ß ñ". sebagai berikut :

a. Mengubah Plaintext dan kunci ke biner.

1. Plaintext (x) : ^¿⊤ x¿¿G>

Hex = 5EAF 16 78 9BE1 47 3E

Binary = 01011110 10101111 00010110 01111000 10011011 11100001 01000111 00111110

2. Kunci (k) : ‼ 4Wy¿ ¼ ß ñ

Hex = 13 34 57 799B BC DFF1

Binary = 00010011 0011010001010111011110011001101110111100110111111111110001

b. Initial Permutasi Plaintext

Lakukan Initial Permutation (IP) pada bit plaintext menggunakan tabel IP berikut:

Tabel 4.3 Initial Permutasi

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Urutan bit pada plaintext urutan ke 58 ditaruh diposisi 1,
Urutan bit pada plaintext urutan ke 50 ditaruh di posisi 2,
Urutan bit pada plaintext urutan ke 42 ditaruh di posisi 3, dst

Sehingga hasil outputnya adalah:

Pecah bit pada IP(x) menjadi 2 bagian yaitu:
L_0 : 01101001 10011101 11000111 01110010
R_0 : 00110010 10101010 10011011 11010111

c. Generate Kunci dengan table PC-1

Generate kunci yang akan digunakanuntuk mengenkripsi plaintext dengan menggunakan tabel permutasi PC-1, pada langkah ini terjadi kompresi dengan membuang 1 bit masing-masing blok kunci dari 64 bit menjadi 56 bit.

Tabel 4.4 Tabel PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	45	38	30	22

14	6	61	53	45	37	29
21	13	5	28	20	12	4

Dapat kita lihat pada tabel diatas, tidak terdapat urutan bit 8,16,24,32,40,48,56,64 karena telah dikompress. Berikut hasil outpunya :

CD(k) : 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

Pecah CD(k) menjadi dua bagian kiri dan kanan, sehingga menjadi

C_0 : 1111000 0110011 0010101 0101111

D_0 : 0101010 1011001 1001111 0001111

d. Lakukan 16 kali putaran pada permutasi kompresi key

Lakukan pergeseran kiri (Left Shift) pada C_0 dan D_0, sebanyak 1 atau 2 kali berdasarkan kali putaran yang ada pada tabel putaran sebagai berikut:

Tabel 4.5 Tabel Left Shift

Putaran ke – i	Jumlah Pergeseran(Left Shift)
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Untuk putaran ke 1, dilakukan pegeseran 1 bit ke kiri

Untuk putaran ke 2, dilakukan pergeseran 1 bit kekiri

Untuk putaran ke 3, dilakukan pergeseran 2 bit kekiri, dst

Berikut hasil outputnya:

C_0 : 1111000 0110011 0010101 0101111

D_0 : 0101010 1011001 1001111 0001111

1). Digeser 1 bit ke kiri

C_1 : 1110000 1100110 0101010 1011111

D_1 : 1010101 0110011 0011110 0011110

2). Digeser 1 bit ke kiri

C_2 : 1100001 1001100 1010101 0111111

D_2 : 0101010 1100110 0111100 0111101

3). Digeser 2 bit ke kiri

C_3 : 0000110 0110010 1010101 1111111

D_3 : 0101011 0011001 1110001 1110101

4). Digeser 2 bit ke kiri

C_4 : 0011001 1001010 1010111 1111100

D_4 : 0101100 1100111 1000111 1010101

5). Digeser 2 bit ke kiri

C_5 : 1100110 0101010 1011111 1110000

D_5 : 0110011 0011110 0011110 1010101

6).Digeser 2 bit ke kiri

C_6 : 0011001 0101010 1111111 1000011

D_6 : 1001100 1111000 1111010 1010101

7). Digeser 2 bit ke kiri

C_7 : 1100101 0101011 1111110 0001100

D_7 : 0110011 1100011 1101010 1010110

8). Digeser 2 bit ke kiri

C_8 : 0010101 0101111 1111000 0110011

D_8 : 1001111 0001111 0101010 1011001

9). Digeser 1 bit ke kiri

C_9 : 0101010 1011111 1110000 1100110

D_9 : 0011110 0011110 1010101 0110011

10). Digeser 2 bit ke kiri

C_{10} : 0101010 1111111 1000011 0011001

D_{10} : 1111000 1111010 1010101 1001100

11).Digeser 2 bit ke kiri

C_{11} : 0101011 1111110 0001100 1100101

D_{11} : 1100011 1101010 1010110 0110011

12). Digeser 2 bit ke kiri

C_{12} : 0101111 1111000 0110011 0010101

D_{12} : 0001111 0101010 1011001 1001111

13). Digeser 2 bit ke kiri

C_{13} : 0111111 1100001 1001100 1010101

D_{13} : 0111101 0101010 1100110 0111100

14). Digeser 2 bit ke kiri

C_{14} : 1111111 0000110 0110010 1010101

D_{14} : 1110101 0101011 0011001 1110001

15). Digeser 2 bit ke kiri

C_{15} : 1111100 0011001 1001010 1010111

D_{15} : 1010101 0101100 1100111 1000111

16).Digeser 1 bit ke kiri

C_{16} : 1111000 0110011 0010101 0101111

D_{16} : 0101010 1011001 1001111 0001111

Setiap hasil putaran digabungkan kembali menjadi C_iD_i dan diinput kedalam tabel Permutation Compression 2 (PC-2) dan terjadi kompresi data C_iD_i 56 bit menjadi CiDi 48 bit.

Tabel 4.6 Tabel PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	12	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Berikut hasil outputnya:

1). C_1D_1 = 1110000 1100110 0101010 1011111 1010101 0110011 0011110 0011110

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

2). C_2D_2 = 1100001 1001100 1010101 0111111 0101010 1100110 0111100 0111101

K_2 = 011110 011010 111011 011001 110110 111100 100111 100101

3). C_3D_3 = 0000110 0110010 1010101 1111111 0101011 0011001 1110001 1110101

K_3 = 010101 011111 110010 001010 010000 101100 111110 011001

4). C_4D_4 = 0011001 1001010 1010111 1111100 0101100 1100111 1000111 1010101

K_4 = 011100 101010 110111 010110 110110 110011 010100 011101

5). C_5D_5 = 1100110 0101010 1011111 1110000 0110011 0011110 0011110 1010101

K_5 = 011111 001110 110000 000111 111010 110101 001110 101000

6). C_6D_6 = 0011001 0101010 1111111 1000011 1001100 1111000 1111010 1010101

K_6 = 011000 111010 010100 111110 010100 000111 101100 101111

7). C_7D_7 = 1100101 0101011 1111110 0001100 0110011 1100011 1101010 1010110

K_7 = 111011 001000 010010 110111 111101 100001 100010 111100

8). C_8D_8 = 0010101 0101111 1111000 0110011 1001111 0001111 0101010 1011001

K_8 = 111101 111000 101000 111010 110000 010011 101111 111011

9). C_9D_9 = 0101010 1011111 1110000 1100110 0011110 0011110 1010101 0110011

K_9 = 111000 001101 101111 101011 111011 011110 011110 000001

10). $C_{10}D_{10}$ = 0101010 1111111 1000011 0011001 1111000 1111010 1010101 1001100

K_{10} = 101100 011111 001101 000111 101110 100100 011001 001111

11). $C_{11}D_{11}$ = 0101011 1111110 0001100 1100101 1100011 1101010 1010110

0110011

K_{11} = 001000 010101 111111 010011 110111 101101 001110 000110

12). $C_{12}D_{12}$ = 0101111 1111000 0110011 0010101 0001111 0101010 1011001 1001111

K_{12} = 011101 010111 000111 110101 100101 000110 011111 101001

13).$C_{13}D_{13}$ = 0111111 1100001 1001100 1010101 0111101 0101010 1100110 0111100

K_{13} = 100101 111100 010111 010001 111110 101011 101001 000001

14). $C_{14}D_{14}$ = 1111111 0000110 0110010 1010101 1110101 0101011 0011001 1110001

K_{14} = 010111 110100 001110 110111 111100 101110 011100 111010

15). $C_{15}D_{15}$ = 1111100 0011001 1001010 1010111 1010101 0101100 1100111 1000111

K_{15} = 101111 111001 000110 001101 001111 010011 111100 001010

16). $C_{16}D_{16}$ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

K_{16} = 110010 110011 110110 001011 000011 100001 011111 110101

e. Ekspansi dan Iterasi data sebanyak 16 kali

Pada langkah ini, kita akan meng-ekspansi data R_{i-1} 32 bit menjadi R_i 48 bit sebanyak 16 kali putaran dengan nilai perputaran 1<= i <=16 menggunakan Tabel Ekspansi (E).

Pada langkah ini, kita akan meng-ekspansi data R_{i-1} 32 bit menjadi R_i 48 bit sebanyak 16 kali putaran dengan nilai perputaran

Tabel 4.7 Tabel Ekspansi

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Hasil E(Ri-1) kemudian di XOR dengan Ki dan menghasilkan Vektor Matriks Ai. hasil XOR antara E(R(1)-1) dengan K1 dan menghasilkan A1, maka proses berikutnya dimana A1 akan dimasukan ke dalam S-Box dan menghasilkan output B1. B1 kemudian akan dipermutasikan lagi dengan tabel P-Box dan menghasilkan nilai PB1 yang kemudian di XOR-kan dengan L0 dan menghasilkan nilai R1. Nilai R1 ini digunakan untuk melanjutkan iterasi ke-2.

R_0

0 (1) 0 (2) 1 (3) 1 (4) 0 (5) 0 (6) 1 (7) 0 (8)

1 (9) 0 (10) 1 (11) 0 (12) 1 (13) 0 (14) 1 (15) 0 (16)

1 (17) 0 (18) 0 (19) 1 (20) 1 (21) 0 (22) 1 (23) 1 (24)

1 (25) 1 (26) 0 (27) 1 (28) 0 (29) 1 (30) 1 (31) 1 (32)

E (R_0) = 100110 100101 010101 010101 010011 110111 111010 101110

Berikut hasil outputnya:

1). Iterasi 1

E(R_0) = 100110 100101 010101 010101 010011 110111 111010 101110

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

---------- XOR

A_1 = 100000010101 011110111010101100110000111011011100

A_1Dibagi menjadi 8 blok

S_1=100000
S_2= 010101
S_3= 011110
S_4 = 111010
S_5 = 101100
S_6 = 110000
S_7 = 111011
S_8 = 011100

Lalu Masing masing di subtitusikan ke tabel S-Box.Cara menentukan baris ambil 1 digit awal dan 1 digit akhir dari S. Cara menentukan kolom yaitu diambil dari digit 2 sampai digit 5 dari S.

S1 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

100000
Baris = 10
Kolom = 0000
S_1 = 4 = 0100

S2 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
01	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
10	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
11	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

010101
Baris = 01
Kolom = 1010
S_2 = 1 = 0001

S3 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
01	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
10	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
11	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

011110
Baris = 00
Kolom = 1111
S_3= 8 = 1000

S4 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
01	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
11	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

111010
Baris = 10
Kolom = 1101
S_4 = 2 = 0010

S5 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
01	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	15
10	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

101100
Baris = 10
Kolom = 0110
S_5 = 7 = 0111

S6 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
01	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
10	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
11	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

110000
Baris = 10
Kolom = 1000
S_6 = 7 = 0111

S7 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
01	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
10	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
11	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

111011
Baris = 11
Kolom = 1101
S_7 = 2 = 0010

S8 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
01	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
10	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8

1 1	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

011100
Baris = 00
Kolom = 1110
S_8 = 12 = 1100

$B_1 = S_1S_2S_3S_4S_5S_6S_7S_8$

B_1 = 0100 0001 1000 0010 0111 0111 0010 1100

Setelah didapatkan nilai vektor B_i, langkah selanjutnya adalah memutasikan bit vektor B_i menggunakan tabel P-Box, kemudian dikelompokkan menjadi 4 blok dimana tiap-tiap blok memiliki 32 bit data.

Tabel 4.8 Tabel P-Box

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Sehingga hasil yang didapat adalah sebagai berikut:

B_1 = 0100 0001 1000 0010 0111 0111 0010 1100

$0_{(1)}\ 1_{(2)}\ 0_{(3)}\ 0_{(4)}\ 0_{(5)}\ 0_{(6)}\ 0_{(7)}\ 1_{(8)}$
$1_{(9)}\ 0_{(10)}\ 0_{(11)}\ 0_{(12)}\ 0_{(13)}\ 0_{(14)}\ 1_{(15)}\ 0_{(16)}$
$0_{(17)}\ 1_{(18)}\ 1_{(19)}\ 1_{(20)}\ 0_{(21)}\ 1_{(22)}\ 1_{(23)}\ 1_{(24)}$
$0_{(25)}\ 0_{(26)}\ 1_{(27)}\ 0_{(28)}\ 1_{(29)}\ 1_{(30)}\ 0_{(31)}\ 0_{(32)}$

$P(B_1)$= 00101000 01100100 11100101 10101000
L_0 = 01101001 10011101 11000111 01110010
----------XOR
R_1 = 0100000111111001 0010001011011010

Lalu lakukan Iterasi selanjutnya seperti yang dilakukan sebelumnya dimulai dari tabel ekspansi sampai hal yang sama sampai ke R_{16}.

R_1
0 (1) 1 (2) 0 (3) 0 (4) 0 (5) 0(6) 0(7) 1 (8)
1 (9) 0(10) 0 (11) 0 (12) 0 (13) 0(14)1(15)0 (16)
0 (17) 1(18) 1(19) 1(20) 0(21) 1(22)1(23)1(24)
0 (25) 0(26) 1 (27) 0(28) 1 (29) 1 (30)0 (31)0 (32)

2). Iterasi 2
E (R_1) =001000 000011 111111 110010 100100 000101 011011 110100
K_2 = 011110 011010 111011 011001 110110 111100 100111 100101
---------- XOR
A_2= 010110 011001 000100 101011 010010 111001 111100 010001

S1 :010110
Baris = 00
Kolom = 1011
S_1 = 12 = 1100

S2 :011001
Baris = 01
Kolom = 1100
S_2 = 6 = 0110

S3 :000100
Baris = 00
Kolom = 0010
S_3= 9 = 1001

S4 : 101011
Baris = 11
Kolom = 0101
S_4 = 1 = 0001

S5 : 010010
Baris = 00
Kolom = 1001
S_5 = 5 = 0101

S6 : 111001
Baris = 11
Kolom = 1100
S_6 = 6 = 0110

S7 : 111100
Baris = 10

Kolom = 1110
S_7 = 9 = 1001

S8 : 010001
Baris = 01
Kolom = 1000
S_8 = 12 = 1100

B_2= 1100 0110 1001 0001 0101 0110 1001 1100

Permutasi dengan tabel P-Box

$1_{(1)}$ $1_{(2)}$ $0_{(3)}$ $0_{(4)}$ $0_{(5)}$ $1_{(6)}$$1_{(7)}$$0_{(8)}$
$1_{(9)}$ $0_{(10)}$$0_{(11)}$ $1_{(12)}$ $0_{(13)}$ $0_{(14)}$ $0_{(15)}$ $1_{(16)}$
$0_{(17)}$ $1_{(18)}$$0_{(19)}$ $1_{(20)}$ $0_{(21)}$ $1_{(22)}$ $1_{(23)}$ $0_{(24)}$
$1_{(25)}$ $0_{(26)}$$0_{(27)}$ $1_{(28)}$ $1_{(29)}$ $1_{(30)}$ $0_{(31)}$ $0_{(32)}$

P(B_2) = 11101110 10100100 10000001 00111001
L_1= R_0= 00110010 10101010 10011011 11010111
----------XOR
R_2 = 11011100 00001110 00011010 11101110

R_2
$1_{(1)}$ $1_{(2)}$ $0_{(3)}$ $1_{(4)}$ $1_{(5)}$ $1_{(6)}$ $0_{(7)}$ $0_{(8)}$
$0_{(9)}$ $0_{(10)}$$0_{(11)}$ $0_{(12)}$$1_{(13)}$$1_{(14)}$$1_{(15)}$$0_{(16)}$
$0_{(17)}$ $0_{(18)}$$0_{(19)}$ $1_{(20)}$ $1_{(21)}$ $0_{(22)}$$1_{(23)}$$0_{(24)}$
$1_{(25)}$ $1_{(26)}$$1_{(27)}$ $0_{(28)}$$1_{(29)}$ $1_{(30)}$$1_{(31)}$$0_{(32)}$

3). Iterasi 3
E (R_2) = 011011 111000 000001 011100 000011 110101 011101
011101
K_3 = 010101 011111 110010 001010 010000 101100 111110 011001
----------XOR
A_3= 001110 100111 110011 010110 010011 011001 100011 000100

S1 : 001110
Baris = 00
Kolom = 0111
S_1 = 8 = 1000

S2 : 100111
Baris = 11
Kolom = 0011
S_2 = 1 = 0001

S3 : 110011
Baris = 11
Kolom = 1001
S_3 = 15 = 1111

S4 : 010110
Baris = 00
Kolom = 1011
S_4 = 5 = 0101

S5 : 010011
Baris = 01
Kolom = 1001
S_5 = 0 = 0000

S6 : 011001
Baris = 01
Kolom = 1100
S_6 = 0 = 0000

S7 : 100011
Baris = 11
Kolom = 0001
S_7 = 11 = 1011

S8 : 000100
Baris = 00
Kolom = 0010
S_8 = 8 = 1000

B_3=1000 0001 1111 0101 0000 0000 1011 1000

Permutasi dengan tabel P-Box

$1_{(1)}$ $0_{(2)}$ $0_{(3)}$ $0_{(4)}$ $0_{(5)}$ $0_{(6)}$$0_{(7)}$ $1_{(8)}$
$1_{(9)}$ $1_{(10)}$ $1_{(11)}$ $1_{(12)}$ $0_{(13)}$ $1_{(14)}$$0_{(15)}$$1_{(16)}$
$0_{(17)}$ $0_{(18)}$ $0_{(19)}$ $0_{(20)}$ $0_{(21)}$ $0_{(22)}$$0_{(23)}$$0_{(24)}$
$1_{(25)}$ $0_{(26)}$ $1_{(27)}$ $1_{(28)}$ $1_{(29)}$ $0_{(30)}$ $0_{(31)}$ $0_{(32)}$

$P(B_3)$ = 10001110 10000001 01010101 00000101
L_2= R_1= 01000001 11111001 00100010 11011010
----------XOR
R_3 = 11001111 01111000 01110111 11011111

R_3
1 (1) 1 (2) 0 (3) 0 (4) 1 (5) 1(6) 1(7) 1 (8)
0 (9) 1(10) 1 (11) 1 (12) 1 (13) 0(14) 0(15) 0 (16)
0 (17) 1(18) 1(19) 1(20) 0(21) 1(22)1(23)1(24)
1 (25) 1(26) 0 (27) 1(28) 1 (29) 1 (30)1 (31)1 (32)

4). Iterasi 4
E (R_3) = 111001 011110 101111 110000 001110 101111 111011 111111

K_4 = 011100 101010 110111 010110 110110 110011 010100 011101
----------XOR
A_4= 100101 110100 011000 100110 111000 011100 101111 100010

S1 : 100101
Baris = 11
Kolom = 0010
S_1 = 8 = 1000

S2 : 110100
Baris = 10
Kolom = 1010
S_2 = 12 = 1100

S3 : 011000
Baris = 00
Kolom = 1100
S_3 = 11 = 1011

S4 : 100110
Baris = 10
Kolom = 0011
S_4 = 0 = 0000

S5 : 111000
Baris = 10
Kolom = 1100
S_5 = 6 = 0110

S6 : 011100
Baris = 00
Kolom = 1110
S_6 = 5 = 0101

S7 : 101111
Baris = 11
Kolom = 0111
S_7 = 7 = 0111

S8 : 100010
Baris = 10
Kolom = 0001
S_8 = 1 = 1011

B_4= 1000 1100 1011 0000 0110 0101 0111 1011

Permutasi dengan tabel P-Box

$1_{(1)}$ $0_{(2)}$ $0_{(3)}$ $0_{(4)}$ $1_{(5)}$ $1_{(6)}$ $0_{(7)}$ $0_{(8)}$
$1_{(9)}$ $0_{(10)}$ $1_{(11)}$ $1_{(12)}$ $0_{(13)}$ $0_{(14)}$ $0_{(15)}$ $0_{(16)}$
$0_{(17)}$ $1_{(18)}$ $1_{(19)}$ $0_{(20)}$ $0_{(21)}$ $1_{(22)}$ $0_{(23)}$ $1_{(24)}$
$0_{(25)}$ $1_{(26)}$ $1_{(27)}$ $1_{(28)}$ $1_{(29)}$ $0_{(30)}$ $1_{(31)}$ $1_{(32)}$

P(B_4) = 00001110 10011110 00101101 10011100
L_3= R_2= 11011100 00001110 00011010 11101110
----------XOR
R_4 = 11010010 10010000 00110111 01110010

R_4
$1_{(1)}$ $1_{(2)}$ $0_{(3)}$ $1_{(4)}$ $0_{(5)}$ $0_{(6)}$ $1_{(7)}$ $0_{(8)}$
$1_{(9)}$ $0_{(10)}$ $0_{(11)}$ $1_{(12)}$ $0_{(13)}$ $0_{(14)}$ $0_{(15)}$ $0_{(16)}$
$0_{(17)}$ $0_{(18)}$ $1_{(19)}$ $1_{(20)}$ $0_{(21)}$ $1_{(22)}$ $1_{(23)}$ $1_{(24)}$
$0_{(25)}$ $1_{(26)}$ $1_{(27)}$ $1_{(28)}$ $0_{(29)}$ $0_{(30)}$ $1_{(31)}$ $0_{(32)}$

5). Iterasi 5
E (R_4) = 011010 100101 010010 100000 000110 101110 101110 100101
K_5 = 011111 001110 110000 000111 111010 110101 001110 101000
---------- XOR
A_5= 000101 101011 100010 100111 111100 011011 100000 001101

S1 : 000101
Baris = 01
Kolom = 0010
S_1 = 7 = 0111

S2 : 101011
Baris = 11
Kolom = 0101
S_2 = 15 = 1111

S3 : 100010
Baris = 10
Kolom = 0001
S_3 = 6 = 0110

S4 : 100111
Baris = 11
Kolom = 0011
S_4 = 6 = 0110

S5 : 111100
Baris = 10
Kolom = 1110
S_5 = 0 = 0000

S6 : 011011
Baris = 01
Kolom = 1101
S_6 = 11 = 1011

S7 : 100000
Baris = 10
Kolom = 00
S_7 = 1 = 0001

S8 : 001101
Baris = 01
Kolom = 0110
S_8 = 0 = 0111

B_5= 0111 1111 0110 0110 0000 1011 0001 0111

Permutasi dengan tabel P-Box

$0_{(1)}$ $1_{(2)}$ $1_{(3)}$ $1_{(4)}$ $1_{(5)}$ $1_{(6)}$ $1_{(7)}$ $1_{(8)}$
$0_{(9)}$ $1_{(10)}$ $1_{(11)}$ $0_{(12)}$ $0_{(13)}$ $1_{(14)}$ $1_{(15)}$ $0_{(16)}$
$0_{(17)}$ $0_{(18)}$ $0_{(19)}$ $0_{(20)}$ $1_{(21)}$ $0_{(22)}$ $1_{(23)}$ $1_{(24)}$
$0_{(25)}$ $0_{(26)}$ $0_{(27)}$ $1_{(28)}$ $0_{(29)}$ $1_{(30)}$ $1_{(31)}$ $1_{(32)}$

$P(B_5)$ = 01010010 01101011 11111010 00110110
$L_4 = R_3$ = 11001111 01111000 01110111 11011111
----------XOR
R_5 = 10011101 00010011 10001101 11101001

R_5
1 (1) 0 (2) 0 (3) 1 (4) 1 (5) 1 (6) 0 (7) 1 (8)
0 (9) 0 (10) 0 (11) 1 (12) 0 (13) 0 (14) 1 (15) 1 (16)
1 (17) 0 (18) 0 (19) 0 (20) 1 (21) 1 (22) 0 (23) 1 (24)
1 (25) 1 (26) 1 (27) 0 (28) 1 (29) 0 (30) 0 (31) 1 (32)

6). Iterasi 6
E (R_5) = 110011 111010 100010 100111 110001 011011 111101 010011
K_6 = 011000 111010 010100 111110 010100 000111 101100 101111
---------- XOR
A_6= 101011 000000 110110 011001 100101 011100 010001 111100

S1 : 101011
Baris = 11
Kolom = 0101
S_1 = 9 = 1001

S2 : 000000
Baris = 00
Kolom = 0000
S_2 = 15 = 1111

S3 : 110110
Baris = 10
Kolom = 1011
S_3 = 12 = 1100

S4 : 011001
Baris = 01
Kolom = 1100
S_4 = 1 = 0001

S5 : 100101
Baris = 11
Kolom = 0010
S_5 = 12 = 1100

S6 : 011100
Baris = 00
Kolom = 1110
S_6 = 5 = 0101

S7 : 010001
Baris = 01
Kolom = 1000
S_7 = 14 = 1110

S8 : 111100
Baris = 10
Kolom = 1110
S_8 = 8 = 0101

B_6= 1001 1111 1100 0001 1100 0101 1110 0101

Permutasi dengan tabel P-Box

$1_{(1)}$ $0_{(2)}$ $0_{(3)}$ $1_{(4)}$ $1_{(5)}$ $1_{(6)}1_{(7)}$ $1_{(8)}$
$1_{(9)}$ $1_{(10)}0_{(11)}$ $0_{(12)}0_{(13)}0_{(14)}0_{(15)}1_{(16)}$
$1_{(17)}1_{(18)}0_{(19)}$ $0_{(20)}$ $0_{(21)}$ $1_{(22)}0_{(23)}$ $1_{(24)}$
$1_{(25)}1_{(26)}1_{(27)}0_{(28)}0_{(29)}1_{(30)}$ $0_{(31)}$ $1_{(32)}$

$P(B_6)$ = 11000001 10011101 01101101 00111011
L_5= R_4= 11010010 10010000 00110111 01110010
----------XOR
R_6 = 00010011 00001101 01011010 01001001

R_6
$0_{(1)}$ $0_{(2)}$ $0_{(3)}$ $1_{(4)}$ $0_{(5)}$ $0_{(6)}$ $1_{(7)}$ $1_{(8)}$
$0_{(9)}$ $0_{(10)}$ $0_{(11)}$ $0_{(12)}$ $1_{(13)}$ $1_{(14)}0_{(15)}$ $1_{(16)}$
$0_{(17)}$ $1_{(18)}0_{(19)}$ $1_{(20)}$ $1_{(21)}$ $0_{(22)}1_{(23)}0_{(24)}$
$0_{(25)}1_{(26)}0_{(27)}0_{(28)}1_{(29)}$ $0_{(30)}$ $0_{(31)}$ $1_{(32)}$

7). Iterasi 7
E (R_6) = 100010 100110 100001 011010 101011 110100 001001 010010
K_7 = 111011 001000 010010 110111 111101 100001 100010 111100
---------- XOR
A_7= 011001 101110 110011 101101 010110 010101 101011 101110

S1 : 011001
Baris = 01
Kolom = 1100
S_1 = 9 = 1001

S2 : 101110
Baris = 10
Kolom = 0111
S_2 = 1 = 0001

S3 : 110011
Baris = 11
Kolom = 1001
S_3 = 15 = 1111

S4 : 101101
Baris = 11
Kolom =0110
S_4 = 11 = 1101

S5 : 010110
Baris = 00
Kolom = 1011
S_5 = 12 = 1111

S6 : 010101
Baris = 01
Kolom = 1010
S_6 = 13 = 1101

S7 : 101011
Baris = 11
Kolom = 0101
S_7 = 4 = 0100

S8 : 101110
Baris = 10
Kolom = 0111
S_8 = 2 = 0010

B_7= 1001 0001 1111 1101 1111 1101 0100 0010

Permutasi dengan tabel P-Box

$1_{(1)}$ $0_{(2)}$ $0_{(3)}$ $1_{(4)}$ $0_{(5)}$ $0_{(6)}$ $0_{(7)}$ $1_{(8)}$
$1_{(9)}$ $1_{(10)}$ $1_{(11)}$ $1_{(12)}$ $1_{(13)}$ $1_{(14)}$ $0_{(15)}$ $1_{(16)}$
$1_{(17)}$ $1_{(18)}$ $1_{(19)}$ $1_{(20)}$ $1_{(21)}$ $1_{(22)}$ $0_{(23)}$ $1_{(24)}$
$0_{(25)}$ $1_{(26)}$ $0_{(27)}$ $0_{(28)}$ $0_{(29)}$ $0_{(30)}$ $1_{(31)}$ $0_{(32)}$

$P(B_7)$ = 10110101 10010111 01110001 11001110
$L_6 = R_5$= 10011101 00010011 10001101 11101001
----------XOR
R_7 = 00101000 10000100 11111100 00100111

R_7
0 (1) 0 (2) 1 (3) 0 (4) 1 (5) 0(6) 0(7) 0 (8)
1 (9) 0(10) 0 (11) 0 (12) 0(13) 1(14) 0(15) 0 (16)
1 (17) 1(18) 1(19) 1(20) 1(21) 1(22) 0(23) 0(24)
0 (25) 0(26) 1 (27) 0(28) 0 (29) 1 (30) 1 (31) 1 (32)

8). Iterasi 8
E (R_7) = 100101 010001 010000 001001 011111 111000 000100 001110
K_8 = 111101 111000 101000 111010 110000 010011 101111 111011
----------XOR
A_8= 011000 101001 111000 110011 101111 101011 101011 110101

S1 : 011000
Baris = 00
Kolom = 1100
S_1 = 5 = 0101

S2 : 101001
Baris = 11
Kolom = 0100
S_2 = 3 = 0011

S3 : 111000
Baris = 10
Kolom = 1100
S_3 = 5 = 0101

S4 : 110011
Baris = 11
Kolom =1001
S_4 = 4 = 0100

S5 : 101111
Baris = 11
Kolom = 0111
S_5 = 13 = 1101

S6 : 101011
Baris = 11
Kolom = 0101

S_6 = 5 = 0101

S7 : 101011
Baris = 11
Kolom = 0101
S_7 = 4 = 0100

S8 : 110101
Baris = 11
Kolom = 1010
S_8 = 9 = 1001

B_8= 0101 0011 0101 0100 1101 0101 0100 1001

Permutasi dengan tabel P-Box

$0_{(1)}$ $1_{(2)}$ $0_{(3)}$ $1_{(4)}$ $0_{(5)}$ $0_{(6)}$ $1_{(7)}$ $1_{(8)}$
$0_{(9)}$ $1_{(10)}$ $0_{(11)}$ $1_{(12)}$ $0_{(13)}$ $1_{(14)}$ $0_{(15)}$ $0_{(16)}$
$1_{(17)}$ $1_{(18)}$ $0_{(19)}$ $1_{(20)}$ $0_{(21)}$ $1_{(22)}$ $0_{(23)}$ $1_{(24)}$
$0_{(25)}$ $1_{(26)}$ $0_{(27)}$ $0_{(28)}$ $1_{(29)}$ $0_{(30)}$ $0_{(31)}$ $1_{(32)}$

$P(B_8)$ = 01101101 00010101 11111000 00001010
L_7= R_6= 00010011 00001101 01011010 01001001
----------XOR
R_8 = 01111110 00011000 10100010 01000011

R_8
$1_{(1)}$ $1_{(2)}$ $1_{(3)}$ $1_{(4)}$ $1_{(5)}$ $1_{(6)}$ $1_{(7)}$ $0_{(8)}$
$0_{(9)}$ $0_{(10)}$ $0_{(11)}$ $1_{(12)}$ $1_{(13)}$ $0_{(14)}$ $0_{(15)}$ $0_{(16)}$
$1_{(17)}$ $0_{(18)}$ $1_{(19)}$ $0_{(20)}$ $0_{(21)}$ $0_{(22)}$ $1_{(23)}$ $0_{(24)}$
$0_{(25)}$ $1_{(26)}$ $0_{(27)}$ $0_{(28)}$ $0_{(29)}$ $0_{(30)}$ $1_{(31)}$ $1_{(32)}$

9). Iterasi 9
E (R_8) = 101111 111100 000011 110001 010100 000100 001000 000110
K_9 = 111000 001101 101111 101011 111011 011110 011110 000001
----------XOR
A_9= 010111 110001 101100 011010 101111 011010 010110 000111

S1 : 010111
Baris = 01
Kolom = 1011
S_1 = 11 = 1011

S2 : 110001
Baris = 11
Kolom = 1000
S_2 = 11 = 1011

S3 : 101100
Baris = 10
Kolom = 0110
S_3 = 3 = 0011

S4 : 011010
Baris = 00
Kolom =1101
S_4 = 12 = 1100

S5 : 101111
Baris = 11
Kolom = 0111
S_5 = 13 = 1101

S6 : 011010
Baris = 00
Kolom = 1101
S_6 = 7 = 0111

S7 : 010110
Baris = 00
Kolom = 0111
S_7 = 7 = 0111

S8 : 000111
Baris = 01
Kolom = 0011
S_8 = 8 = 1000

B_9= 1011 1011 0011 1100 1101 0111 0111 1000

Permutasi dengan tabel P-Box

1(1) 0(2) 1(3) 1(4) 1(5) 0(6) 1(7) 1(8)
0(9) 0(10) 1(11) 1(12) 1(13) 1(14) 0(15) 1(16)
0(17) 1(18) 1(19) 1(20) 0(21) 1(22) 1(23) 1(24)
0(25) 1(26) 1(27) 1(28) 1(29) 0(30) 0(31) 0(32)

$P(B_9)$ = 01101111 10111100 01110110 01001110
$L_8 = R_7$= 00101000 10000100 11111100 00100111
----------XOR
R_9 = 01000111 00111000 10001010 01101001

R_9
0 (1) 1 (2) 0 (3) 0 (4) 0 (5) 1(6) 1(7) 1 (8)
0 (9) 0(10) 1 (11) 1 (12) 1(13) 0(14) 0(15) 0 (16)
1 (17) 0(18) 0(19) 0(20) 1(21) 0(22)1(23)0(24)
0 (25) 1(26) 1 (27) 0(28) 1 (29) 0(30)0 (31) 1 (32)

10). Iterasi 10
E (R_9) = 101000 001110 100111 110001 010001 010100 001101 010010
K_{10} = 101100 011111 001101 000111 101110 100100 011001 001111
---------- XOR
A_{10}= 000100 010001 101010 110110 111111 110000 010100 011101

S1 : 000100
Baris = 00
Kolom = 0010
S_1 = 13 = 0100

S2 :010001
Baris = 11
Kolom = 0100
S_2 = 14 = 1100

S3 : 101010
Baris = 10
Kolom = 0101
S_3 = 15 = 0001

S4 : 110110
Baris = 10
Kolom =1011
S_4 = 14 = 1001

S5 : 111111
Baris = 11
Kolom = 1111
S_5 = 3 =0011

S6 : 110000
Baris = 10
Kolom = 1000

S_6 = 7 = 0111

S7 : 010100
Baris = 00
Kolom = 1010
S_7 = 9 = 0011

S8 : 011101
Baris = 01
Kolom = 1110
S_8 = 9 = 1000

B_{10}= 1101 1100 1111 1110 0011 0111 1001 1001

Permutasi dengan tabel P-Box
$1_{(1)}$ $1_{(2)}$ $0_{(3)}$ $1_{(4)}$ $1_{(5)}$ $1_{(6)}$ $0_{(7)}$ $0_{(8)}$
$1_{(9)}$ $1_{(10)}$ $1_{(11)}$ $1_{(12)}$ $1_{(13)}$ $1_{(14)}$ $1_{(15)}$ $0_{(16)}$
$0_{(17)}$ $0_{(18)}$ $1_{(19)}$ $1_{(20)}$ $0_{(21)}$ $1_{(22)}$ $1_{(23)}$ $1_{(24)}$
$1_{(25)}$ $0_{(26)}$ $0_{(27)}$ $1_{(28)}$ $1_{(29)}$ $0_{(30)}$ $0_{(31)}$ $1_{(32)}$

$P(B_{10})$ = 00101110 11101001 10111001 11011111
L_9= R_8= 01111110 00011000 10100010 01000011
----------XOR
R_{10} = 01010000 11110001 00011011 10011100

R_{10}
$0_{(1)}$ $1_{(2)}$ $0_{(3)}$ $1_{(4)}$ $0_{(5)}$ $0_{(6)}$ $0_{(7)}$ $0_{(8)}$
$1_{(9)}$ $1_{(10)}$ $1_{(11)}$ $1_{(12)}$ $0_{(13)}$ $0_{(14)}$ $0_{(15)}$ $1_{(16)}$
$0_{(17)}$ $0_{(18)}$ $0_{(19)}$ $1_{(20)}$ $1_{(21)}$ $0_{(22)}$ $1_{(23)}$ $1_{(24)}$
$1_{(25)}$ $0_{(26)}$ $0_{(27)}$ $1_{(28)}$ $1_{(29)}$ $1_{(30)}$ $0_{(31)}$ $0_{(32)}$

11). Iterasi 11
E (R_{10}) = 001010 100001 011110 100010 100011 110111 110011 111000
K_{11} = 001000 010101 111111 010011 110111 101101 001110 000110
---------- XOR
A_{11}=000010 110100 100001 110001 010100 011010 111101 111110

S1 : 000010
Baris = 00
Kolom = 0001
S_1 = 4 = 0100

S2 : 110100
Baris = 10
Kolom = 1010

S_2 = 12 = 1100

S3 : 100001
Baris = 11
Kolom = 0000
S_3 = 1 = 0001

S4 : 110001
Baris = 11
Kolom =1000
S_4 = 9 = 1001

S5 : 010100
Baris = 00
Kolom = 1010
S_5 = 3 = 0011

S6 : 011010
Baris = 00
Kolom = 1101
S_6 = 7 = 0111

S7 : 111101
Baris = 11
Kolom = 1110
S_7 = 3 = 0011

S8 :0111110
Baris = 00
Kolom = 1111
S_8 = 8 = 1000

B_{11}= 0100 1100 0001 1001 0011 0111 0011 1000

Permutasi dengan tabel P-Box

$0_{(1)}$ $1_{(2)}$ $0_{(3)}$ $0_{(4)}$ $1_{(5)}$ $1_{(6)}$ $0_{(7)}$ $0_{(8)}$
$0_{(9)}$ $0_{(10)}$ $0_{(11)}$ $1_{(12)}$ $0_{(13)}$ $0_{(14)}$ $1_{(15)}$ $1_{(16)}$
$0_{(17)}$ $0_{(18)}$ $1_{(19)}$ $1_{(20)}$ $0_{(21)}$ $1_{(22)}$ $1_{(23)}$ $1_{(24)}$
$0_{(25)}$ $0_{(26)}$ $1_{(27)}$ $1_{(28)}$ $1_{(29)}$ $0_{(30)}$ $0_{(31)}$ $0_{(32)}$

$P(B_{11})$ = 10101110 00101000 10100100 11011000
L_{10}= R_9= 01000111 00111000 10001010 01101001
----------XOR
R_{11} = 11101001 00010000 00101110 10110001

R_{11}
1 (1) 1 (2) 1(3) 0 (4) 1 (5) 0(6) 0(7) 1 (8)
0 (9) 0(10) 0 (11) 1 (12) 1(13) 0(14)0(15) 0 (16)
0 (17) 0(18) 1(19) 0(20) 1(21) 1(22)1(23)0(24)
1 (25) 0(26) 1 (27) 1(28) 0 (29) 0(30)1 (31)1 (32)

12). Iterasi 12
E (R_{11}) = 111101 010010 100010 100000 000101 011101 010110 100011
K_{12} = 011101 010111 000111 110101 100101 000110 011111 101001
----------XOR
A_{12}= 100000 000101 100101 010101 100000 011011 001001 001010

S1 : 100000
Baris = 10
Kolom = 0000
S_1 = 4 = 0100

S2 :1000101
Baris = 11
Kolom = 0010
S_2 = 4 = 0100

S3 : 100101
Baris = 11
Kolom = 0010
S_3 = 13 =1101

S4 : 010101
Baris = 01
Kolom =1010
S_4 = 2 = 0010

S5 : 100000
Baris = 10
Kolom = 0000
S_5 = 4 = 0100

S6 : 011011
Baris = 01
Kolom = 1101
S_6 = 11 = 1011

S7 : 001001
Baris = 01
Kolom = 0100
S_7 = 4 =0100

S8 : 001010
Baris = 00
Kolom = 0101
S_8 = 15 = 1111

B_{12}= 0100 0100 1101 0010 0100 1011 0100 1111

Permutasi dengan tabel P-Box

$0_{(1)}$ $1_{(2)}$ $0_{(3)}$ $0_{(4)}$ $0_{(5)}$ $1_{(6)}0_{(7)}$ $0_{(8)}$
$1_{(9)}$ $1_{(10)}0_{(11)}$ $1_{(12)}0_{(13)}1_{(14)}0_{(15)}0_{(16)}$
$0_{(17)}1_{(18)}0_{(19)}$ $0_{(20)}$ $1_{(21)}$ $0_{(22)}1_{(23)}1_{(24)}$
$0_{(25)}1_{(26)}0_{(27)}0_{(28)}1_{(29)}$ $1_{(30)}1_{(31)}1_{(32)}$

$P(B_{12})$ = 00011100 01110111 10101001 00110000
$L_{11}= R_{10}$= 01010000 11110001 00011011 10011100
----------XOR
R_{12} = 01001100 10000110 10110010 10101100

R_{12}
$0_{(1)}$ $1_{(2)}$ $0_{(3)}$ $0_{(4)}$ $1_{(5)}$ $1_{(6)}$ $0_{(7)}$ $0_{(8)}$
$1_{(9)}$ $0_{(10)}0_{(11)}$ $0_{(12)}0_{(13)}1_{(14)}$ $1_{(15)}$ $0_{(16)}$
$1_{(17)}0_{(18)}1_{(19)}$ $1_{(20)}$ $0_{(21)}$ $0_{(22)}1_{(23)}0_{(24)}$
$1_{(25)}0_{(26)}1_{(27)}0_{(28)}1_{(29)}$ $1_{(30)}0_{(31)}0_{(32)}$

13). Iterasi 13
E (R_{12}) = 001001 011001 010000 001101 010110 100101 010101 011000
K_{13} = 100101 111100 010111 010001 111110 101011 101001 000001
----------XOR
A_{13}= 101100 100101 000111 011100 101000 001110 111100 011001

S1 :1101100
Baris = 10
Kolom = 1011
S_1 = 2 = 0010

S2 : 100101
Baris = 11
Kolom = 0010
S_2 = 11 = 1010

S3 : 000111
Baris = 01
Kolom = 0011
S_3 = 9 = 1001

S4 : 011100
Baris = 00
Kolom =1110
S_4 = 4 = 0100

S5 : 101000
Baris = 10
Kolom = 0100
S_5 = 11 = 1010

S6 : 001110
Baris = 00
Kolom = 0111
S_6 = 8 = 1000

S7 : 111100
Baris = 10
Kolom = 1110
S_7 = 9 = 1001

S8: 011001
Baris = 01
Kolom = 1100
S_8 = 0 = 0000

B_{13}= 0010 1010 1001 0100 1010 1000 1001 0000

Permutasi dengan tabel P-Box

$0_{(1)}$ $0_{(2)}$ $1_{(3)}$ $0_{(4)}$ $1_{(5)}$ $0_{(6)}$$1_{(7)}$$0_{(8)}$
$1_{(9)}$ $0_{(10)}$$0_{(11)}$ $1_{(12)}$$0_{(13)}$$1_{(14)}$ $0_{(15)}$ $0_{(16)}$
$1_{(17)}$$0_{(18)}$$1_{(19)}$ $0_{(20)}$ $1_{(21)}$ $0_{(22)}$$0_{(23)}$ $0_{(24)}$
$1_{(25)}$$0_{(26)}$$0_{(27)}$$1_{(28)}$$0_{(29)}$ $0_{(30)}$$0_{(31)}$ $0_{(32)}$

P(B_{13}) = 01010111 00001000 00010011 10000001
L_{12}= R_{11}= 11101001 00010000 00101110 10110001
----------XOR
R_{13} = 10111110 00011000 00111101 00110000

R_{13}
1 (1) 0 (2) 1(3) 1 (4) 1 (5) 1(6) 1(7) 0 (8)
0 (9) 0(10) 0 (11) 1 (12) 1(13) 0(14) 0(15) 0 (16)
0 (17) 0(18) 1(19) 1(20) 1(21) 1(22)0(23)1(24)
0 (25) 0(26) 1 (27) 1(28) 0 (29) 0(30)0 (31)0 (32)

14). Iterasi 14
E (R_{13}) = 010111 111100 000011 110000 000111 111010 100110 100001
K_{14}= 010111 110100 001110 110111 111100 101110 011100 111010
----------XOR
A_{14}= = 000000 001000 001101 000111 111011 010100 111010 011011

S1 : 000000
Baris = 00
Kolom = 0000
S_1 = 14 = 1110

S2 : 001000
Baris = 00
Kolom = 0100
S_2 = 6 = 0110

S3 : 001101
Baris = 01
Kolom = 0110
S_3 = 6 = 0110

S4 : 000111
Baris = 01
Kolom = 001
S_4 = 5 = 0101

S5 : 111011
Baris = 11
Kolom = 1101
S_5 = 4 = 0100

S6 : 010100
Baris = 00
Kolom = 1010
S_6 = 3 = 0011

S7 : 111010
Baris = 10
Kolom = 1101
S_7 = 5 =0101

S8 : 011011
Baris = 01
Kolom = 1101
S_8 = 14 = 1110

B_{14}= 1110 0110 0110 0101 0100 0011 0101 1110

Permutasi dengan tabel P-Box

$1_{(1)}$ $1_{(2)}$ $1_{(3)}$ $0_{(4)}$ $0_{(5)}$ $1_{(6)}$$1_{(7)}$$0_{(8)}$
$0_{(9)}$ $1_{(10)}$ $1_{(11)}$ $0_{(12)}$ $0_{(13)}$ $1_{(14)}$ $0_{(15)}$ $1_{(16)}$
$0_{(17)}$ $1_{(18)}$ $0_{(19)}$ $0_{(20)}$ $0_{(21)}$ $0_{(22)}$ $1_{(23)}$ $1_{(24)}$
$0_{(25)}$ $1_{(26)}$ $0_{(27)}$ $1_{(28)}$ $1_{(29)}$ $1_{(30)}$ $1_{(31)}$ $0_{(32)}$

P(B_{14}) = 11001010 10110111 10110010 00110100
L_{13}= R_{12}= 01001100 10000110 10110010 10101100
----------XOR
R_{14}= 10000110 00110001 00000000 10011000

R_{14}
$1_{(1)}$ $0_{(2)}$ $0_{(3)}$ $0_{(4)}$ $0_{(5)}$ $1_{(6)}$$1_{(7)}$ $0_{(8)}$
$0_{(9)}$ $0_{(10)}$ $1_{(11)}$ $1_{(12)}$ $0_{(13)}$ $0_{(14)}$$0_{(15)}$ $1_{(16)}$
$0_{(17)}$ $0_{(18)}$ $0_{(19)}$ $0_{(20)}$ $0_{(21)}$ $0_{(22)}$ $0_{(23)}$ $0_{(24)}$
$1_{(25)}$ $0_{(26)}$ $0_{(27)}$ $1_{(28)}$ $1_{(29)}$ $0_{(30)}$$0_{(31)}$$0_{(32)}$

15). Iterasi 15
E (R_{14}) = 010000 001100 000110 100010 100000 000001 010011 110001
K_{15}= 101111 111001 000110 001101 001111 010011 111100 001010
----------XOR
A_{15}= 111111 110101 000000 101111 101111 010010 101111 111011

S1 : 111111
Baris = 11
Kolom = 1111
S_1 = 1 =1101

S2 : 110101
Baris = 11
Kolom = 1010
S_2 =10 = 0111

S3 : 000000
Baris = 00
Kolom = 0000
S_3 = 9 = 1010

S4 : 101111
Baris = 11
Kolom =0111
S_4 = 15 = 1000

S5 : 101111
Baris = 11
Kolom = 0111
S_5 = 3 = 1101

S6 : 010010
Baris = 00
Kolom = 1001
S_6 = 2 = 1101

S7 : 101111
Baris = 11
Kolom = 0111
S_7 = 7 = 0111

S8 : 111011
Baris = 11
Kolom = 1101
S_8 = 0 = 0101

B_{15}=1101 0111 1010 1000 1101 1101 0111 0101

Permutasi dengan tabel P-Box

$1_{(1)}$ $1_{(2)}$ $0_{(3)}$ $1_{(4)}$ $0_{(5)}$ $1_{(6)}$$1_{(7)}$$1_{(8)}$
$1_{(9)}$ $0_{(10)}$$1_{(11)}$ $0_{(12)}$$1_{(13)}$$0_{(14)}$$0_{(15)}$$0_{(16)}$
$1_{(17)}$$1_{(18)}$$0_{(19)}$ $1_{(20)}$ $0_{(21)}$ $1_{(22)}$$1_{(23)}$$1_{(24)}$
$0_{(25)}$$1_{(26)}$$1_{(27)}$$1_{(28)}$$0_{(29)}$ $1_{(30)}$$0_{(31)}$$1_{(32)}$

$P(B_{15})$ = 01110011 10010100 11101101 01111110
L_{14}= R_{13}= 10111110 00011000 00111101 00110000
----------XOR
R_{15}= 11001101 10001100 11010000 01001110

R_{15}
1 (1) 1 (2) 0(3) 0 (4) 1 (5) 1(6) 0(7) 1 (8)
1 (9) 0(10) 0 (11) 0 (12) 1(13) 1(14) 0(15) 0 (16)
1 (17) 1(18) 0(19) 1(20) 0(21) 0(22)0(23)0(24)
0 (25) 1(26) 0 (27) 0(28) 1 (29) 1(30)1 (31)0 (32)

16). Iterasi 16
E (R_{15}) = 011001 011011 110001 011001 011010 100000 001001 011101
K_{16}= 110010 110011 110110 001011 000011 100001 011111 110101
---------- XOR
A_{16}=101011 101000 000111 010010 011001 000001 010110 101000

S1 : 101011
Baris = 11
Kolom = 0101
S_1 = 9 = 1001

S2 : 101000
Baris = 10
Kolom = 0100
S_2 =10 = 1010

S3 : 000111
Baris = 01
Kolom = 0011
S_3 = 9 = 1001

S4 : 010010
Baris = 00
Kolom =1001
S_4 = 2 = 0010

S5 : 011001
Baris = 01
Kolom = 1100
S_5 = 3 = 0011

S6 : 000001
Baris = 01
Kolom = 0000
S_6 = 10 = 1010

S7 : 010110
Baris = 00
Kolom = 1011
S_7 =7 = 0111

S8 : 101000
Baris = 10
Kolom = 0100
S_8 = 9 = 1001

B_{16}=1001 1010 1001 0010 0011 1010 0111 1001

Permutasi dengan tabel P-Box

$1_{(1)}$ $0_{(2)}$ $0_{(3)}$ $1_{(4)}$ $1_{(5)}$ $0_{(6)}$ $1_{(7)}$ $0_{(8)}$
$1_{(9)}$ $0_{(10)}$ $1_{(11)}$ $0_{(12)}$ $0_{(13)}$ $0_{(14)}$ $1_{(15)}$ $0_{(16)}$
$0_{(17)}$ $0_{(18)}$ $1_{(19)}$ $1_{(20)}$ $1_{(21)}$ $0_{(22)}$ $1_{(23)}$ $0_{(24)}$
$0_{(25)}$ $1_{(26)}$ $1_{(27)}$ $1_{(28)}$ $1_{(29)}$ $0_{(30)}$ $0_{(31)}$ $1_{(32)}$

$P(B_{16})$ = 01111110 11111000 00001101 10000010
L_{15}= R_{14}= 10000110 00110001 00000000 10011000
----------XOR
R_{16}= 11111000 11001001 00001101 00011010

L_{16} = R_{15} =11001101 10001100 11010000 01001110

f. Permutasi R_{16} dengan L_{16}dengan tabel ip-1

Tabel 4.9 Tabel IP - 1

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Input :
$R_{16}L_{16}$ = 11111000 11001001 00001101 00011010 11001101 10001100 11010000 01001110

$1_{(1)}$ $1_{(2)}$ $1_{(3)}$ $1_{(4)}$ $1_{(5)}$ $0_{(6)}$ $0_{(7)}$ $0_{(8)}$
$1_{(9)}$ $1_{(10)}$ $0_{(11)}$ $0_{(12)}$ $1_{(13)}$ $0_{(14)}$ $0_{(15)}$ $1_{(16)}$
$0_{(17)}$ $0_{(18)}$ $0_{(19)}$ $0_{(20)}$ $1_{(21)}$ $1_{(22)}$ $0_{(23)}$ $1_{(24)}$
$0_{(25)}$ $0_{(26)}$ $0_{(27)}$ $1_{(28)}$ $1_{(29)}$ $0_{(30)}$ $1_{(31)}$ $0_{(32)}$

$1_{(33)}\,1_{(34)}0_{(35)}\;0_{(36)}\;1_{(37)}\;1_{(38)}0_{(39)}1_{(40)}$
$1_{(41)}\,0_{(42)}\,0_{(43)}\,0_{(44)}\,1_{(45)}\,1_{(46)}0_{(47)}0_{(48)}$
$1_{(49)}\,1_{(50)}\,0_{(51)}\;1_{(52)}\;0_{(53)}\;0_{(54)}0_{(55)}0_{(56)}$
$0_{(57)}1_{(58)}0_{(59)}\,0_{(60)}\,1_{(61)}\;1_{(62)}1_{(63)}0_{(64)}$

Output akhir adalah sebagai berikut:
Cipher dalam biner = 10010100
00000011101001101111011101001001010000001101101011111000
Chiper dalam heksadesimal = 9403A6F74940DAF8

g. Proses Deskripsi dari chipertext ke plaintext

Untuk mendekripsikan Chiper teks, hanya melakukan sedikit perubahan dimana membalikkan urutan kunci di putaran kunci pada point (d.) yaitu, kunci 16 menjadi kunci 1, Setelah mendapatkan K_1 sampai dengan K_{16} dilakukan Ekspansi dan Iterasi data sebanyak 16 kali setelah itu dilakukan pemutasian akhir dengan menggunakan tabel ip-1

Berikut hasil outputnya:

1) C_1D_1 = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

K_1= 110010 110011 110110 001011 000011 100001 011111 110101

2.) C_2D_2 = 1111100 0011001 1001010 1010111 1010101 0101100 1100111 1000111

K_2 = 101111 111001 000110 001101 001111 010011 111100 001010

3.) C_3D_3 = 1111111 0000110 0110010 1010101 1110101 0101011 0011001 1 110001

K_{14} = 010111 110100 001110 110111 111100 101110 011100 111010

4.) C_4D_4 = 0111111 1100001 1001100 1010101 0111101 0101010 1100110 0111100

K_4 = 100101 111100 010111 010001 111110 101011 101001 000001

5.) C_5D_5 = 0101111 1111000 0110011 0010101 0001111 0101010 1011001 1001111

K_5 = 011101 010111 000111 110101 100101 000110 011111 101001

6.) C_6D_6 = 0101011 1111110 0001100 1100101 1100011 1101010 1010110 0110011

K_6 = 001000 010101 111111 010011 110111 101101 001110 000110

7.) C_7D_7 = 0101010 1111111 1000011 0011001 1111000 1111010 1010101 1001100

K_7 = 101100 011111 001101 000111 101110 100100 011001 001111

8.) C_8D_8 = 0101010 1011111 1110000 1100110 0011110 0011110 1010101 0110011

K_8 = 111000 001101 101111 101011 111011 011110 011110 000001

9.) C_9D_9 = 0010101 0101111 1111000 0110011 1001111 0001111 0101010 1011001

K_9 = 111101 111000 101000 111010 110000 010011 101111 111011

10.)$C_{10}D_{10}$ = 1100101 0101011 1111110 0001100 0110011 1100011 1101010 1010110

K_{10} = 111011 001000 010010 110111 111101 100001 100010 111100

11.) $C_{11}D_{11}$ = 0011001 0101010 1111111 1000011 1001100 1111000 1111010 1010101

K_{11} = 011000 111010 010100 111110 010100 000111 101100 101111

12.) $C_{12}D_{12}$ = 1100110 0101010 1011111 1110000 0110011 0011110 0011110 1010101

K_{12} = 011111 001110 110000 000111 111010 110101 001110 101000

13.) $C_{13}D_{13}$ = 0011001 1001010 1010111 1111100 0101100 1100111 1000111 1010101

K_{13} = 011100 101010 110111 010110 110110 110011 010100 011101

14.) $C_{14}D_{14}$ = 0000110 0110010 1010101 1111111 0101011 0011001 1110001 1110101

K_{14} = 010101 011111 110010 001010 010000 101100 111110 011001

15.) $C_{15}D_{15}$ = 1100001 1001100 1010101 0111111 0101010 1100110 0111100 0111101

K_{15} = 011110 011010 111011 011001 110110 111100 100111 100101

16.) $C_{16}D_{16}$ = 1110000 1100110 0101010 1011111 1010101 0110011 0011110 0011110

K_{16} = 000110 110000 001011 101111 111111 000111 000001 110010

Berikut output Ekspansi dan Iterasi data sebanyak 16 kali :

Chiper = 1001010000000011101001101111011101001001010000
001101101011111000
chiperIP = 1111100011001001000011010001101011001101100011
1001101000001001110

L0 = 11111000110010010000110100011010
R0 = 11001101100011001101000001001110

1). Iterasi 1

$E(R_0)$ = 011001011011110001011001011010100000001001011101

K_1 = 110010110011110110001011000011100001011111111010

---------- XOR

A_1 = 101011 101000 000111 010010 011001 000001 010110 101000

B_1 100110101001001000111010011110 01

$P(B_1)$= 01111110 11111000 00001101 10000010

L_0 = 11111000 11001001 00001101 00011010
----------XOR
R_1 = 10000110 00110001 00000000 10011000

2). Iterasi 2
E (R_1) =010000011000001101000101000000000010100111100 01
K_2 = 101111111001000110001101001111010011111100001010
---------- XOR
A_2= 111111 110101 000000 101111 101111 010010 101111 111011
B_2 110101111010100011011101011101 01

$P(B_2)$ = 01110011 10010100 11101101 01111110

L_1= R_0= 11001101 10001100 11010000 01001110

----------XOR

R_2 = 10111110 00011000 00111101 00110000

3). Iterasi 3

E (R_2) = 010111111100000011110000000111111010100110100001

K_3 = 010111110100001110110111111100101110011100111010
----------XOR
A_3= 000000001000001101000111111011010100111010011011

$B_3$111001100110010101000011010111 10

$P(B_3)$ = 11001010 10110111 10110010 00110100

L_2= R_1= 10000110 0011000 1 00000000 10011000
----------XOR

R_3 = 01001100 10000110 10110010 10101100

4). Iterasi 4

E (R_3) = 001001 011001 010000 001101 010110 100101 010101 011000

K_4 = 100101111100010111010001111110101011101001000001
----------XOR
A_4= 101100100101000111011100101000011101111000 11001

B_4 00101010100101001010100010010000

$P(B_4)$ = 01010111000010000001001110000001

L_3= R_2= 10111110 00011000 00111101 00110000

----------XOR

R_4 = 11101001000100000010111010110001

5). Iterasi 5

E (R_4) = 11110101001010001010000000010101110101011010011

K_5 = 01110101011100011111010110010100011001111110100 1

---------- XOR

A_5= 100000 000101 100101 010101 100000 011011 001001 001010

B_5 0100 0100 1101 0010 0100 1011 0100 1111

$P(B_5)$ 00011100011101111010100100110000

L_4= R_3= 01001100 10000110 10110010 10101100

----------XOR

R_5 = 01010000111100010001101110011100

6). Iterasi 6

E (R_5) = 00101010000101111010001010001111011111001111 1000

K_6 = 00100001010111111101001111011110110100111000011 0

---------- XOR

A_6= 00001011010010000111000101010001101011110111111 0

B_6 01001100000110010011011100111000

$P(B_6)$ = 101011100010100010100100110110000

$L_5 = R_4$ = 111010010001000000101110101100001

----------XOR

R_6 = 010001110011100010001010011010001

7). Iterasi 7

E (R_6) = 101000001110100111110001010001010100001101010010

K_7 = 101100011111001101000111101110100100011001001111

---------- XOR

A_7= 000100010001101010110110111111110000010100011101

B_4 110111001111111000110111100110001

$P(B_7)$ = 001011101110100110111001110111111

$L_6 = R_5$= 010100001111000100011011100111100

----------XOR

R_7 = 011111100001100010100010010000011

8). Iterasi 8

E (R_7) = 101111111100000011110001010100000100001000000110

K_8 = 111000001101101111101011111011011110011110000001

----------XOR

A_8= 010111110001101100011010101111011010010110000111

B_8 101110110011110011010111011110000

$P(B_8)$ = 011011111011110001110110010011110

$L_7 = R_6$= 010001110011100010001010011010001

----------XOR

R_8 = 001010001000010011111100001001111

9). Iterasi 9

$E(R_8)$ = 10010101000101000000100101111111100000010000111 0

K_9 = 11110111100010100011101011000001001110111111101 1

----------XOR

A_9= 01100010100111100011001110111110101110101111010 1

B_9 0101 0011 0101 0100 1101 0101 0100 1001

$P(B_9)$ = 01101101000101011111100000001010

L_8= R_7= 01111110000110001010001001000011

----------XOR

R_9 = 00010011000011010101101001001001

10). Iterasi 10

$E(R_9)$ = 10001010011010000101101010101111010000100101001 0

K_{10} = 11101100100001001011011111111011000011000101111 00

---------- XOR

A_{10}= 01100110111011001110110101011001010110101110111 10

B_{10} 00100011111110111111101010000 10

$P(B_{10})$ = 10110101100101110111000111001110

L_9= R_8= 00101000100001001111110000100111

----------XOR

R_{10} = 10011101000100111000110111101001

11). Iterasi 11

$E(R_{10})$ = 11001111101010001010011111000101101111110101001 1

K_{11} = 01100011101001010011111001010000011110110010111 1

---------- XOR

A_{11}=10101100000011011001100110010101110001000111110 0

B_{11} 100111111100000111000101111100101

$P(B_{11})$ = 110000011001110101101101001110 11

$L_{10}= R_9$= 00010011000011010101101001001001

----------XOR

R_{11} = 11010010100100000011011101110010

12). Iterasi 12

E (R_{11}) = 011010100101010010100000000110101110101110100101

K_{12} = 011111001110110000000111111010110101001110101000

----------XOR

A_{12}= 000101101011100010100111111100011011100000001101

B_{12} 011111110110011000001011000 10111

$P(B_{12})$ = 010100100110101111111010001 10110

$L_{11}= R_{10}$= 100111010001001110001101111 01001

----------XOR

R_{12} = 110011110111100001110111110111 11

13). Iterasi 13

E (R_{12}) = 111001011110101111110000001110101111111011111111

K_{13} = 011100101010110111010110110110110011010100011101

----------XOR

A_{13}= 100101 110100 011000 100110 111000 011100 101111 100010

B_{13} 1000 1100 1011 0000 0110 0101 0111 1011

$P(B_{13})$ = 000011101001111000101101100 11100

$L_{12}= R_{11}$= 11010010100100000011011101110010

----------XOR

R_{13} = 110111000000111000011010111011 10

14). Iterasi 14

E (R_{13}) = 011011111000000001011100000011110101011101011101

K_{14}= 010101011111110010001010010000101100111110011001

----------XOR

A_{14}= = 001110100111110011010110010011011001100011000100

B_{14} 100000011111010100000000010111000

P(B_{14}) = 010000011111100100100001011011010

L_{13}= R_{12}= 110011110111100001110111111011111

----------XOR

R_{14}= 010000011111100100100001011011010

15). Iterasi 15

E (R_{14}) = 001000000011111111110010100100000101011011110100

K_{15}= 011110011010111011011001110110111100100111100101

----------XOR

A_{15}= 010110011001000100101011010010111001111100010001

B_{15}110001101001000101010110100111 00

P(B_{15}) = 111011101010010010000000100111001

L_{14}= R_{13}= 110111000000111000011010111011 10

----------XOR

R_{15}= 001100101010101010011011111010111

16). Iterasi 16

E (R_{15}) = 100110100101010101010101010011111011111101010111 0

K_{16}= 000110110000000101110111111111100011100000111001 0

---------- XOR

A_{16}=100000 010101 011110 111010 101100 110000 111011 011100

B_{16} 010000011000001001110111001011 00

$P(B_{16})$ = 00101000011001001110010110101000
$L_{15}= R_{14}$= 01000001111110010010001011011010
----------XOR
R_{16}= 01101001100111011100011101110010

$L_{16}= R_{15}$ = 00110010101010101001101111010111

$R_{16}L_{16}$

01101001100111011100011101110010001100101010101010011011110101111

Permutasian Akhir Sebagai Beriku :

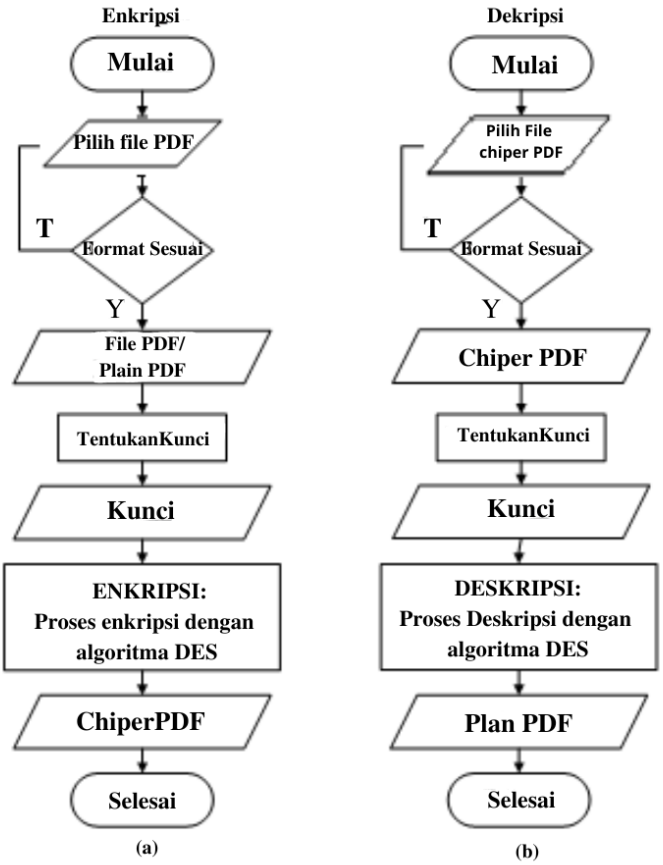
Cipher dalam biner = 01011110 10101111 00010110 01111000 10011011 11100001 01000111 00111110

Chiper dalam heksadesimal = 5EAF16789BE1473E

4.1.4. Flowchart Sistem

Flowchart sistem berfungsi untuk menunjukan alur proses dari sistem yang akan di bangun.Adapun flowchart sistem terdiri 3 bagian yaitu : flowchart Menu utama, flowcart enkripsi dan flowchart deskripsi.Berikut adalah flowchart sistem yang akan di bangun:

a. Flowchart Enkripsi & Deskrispi

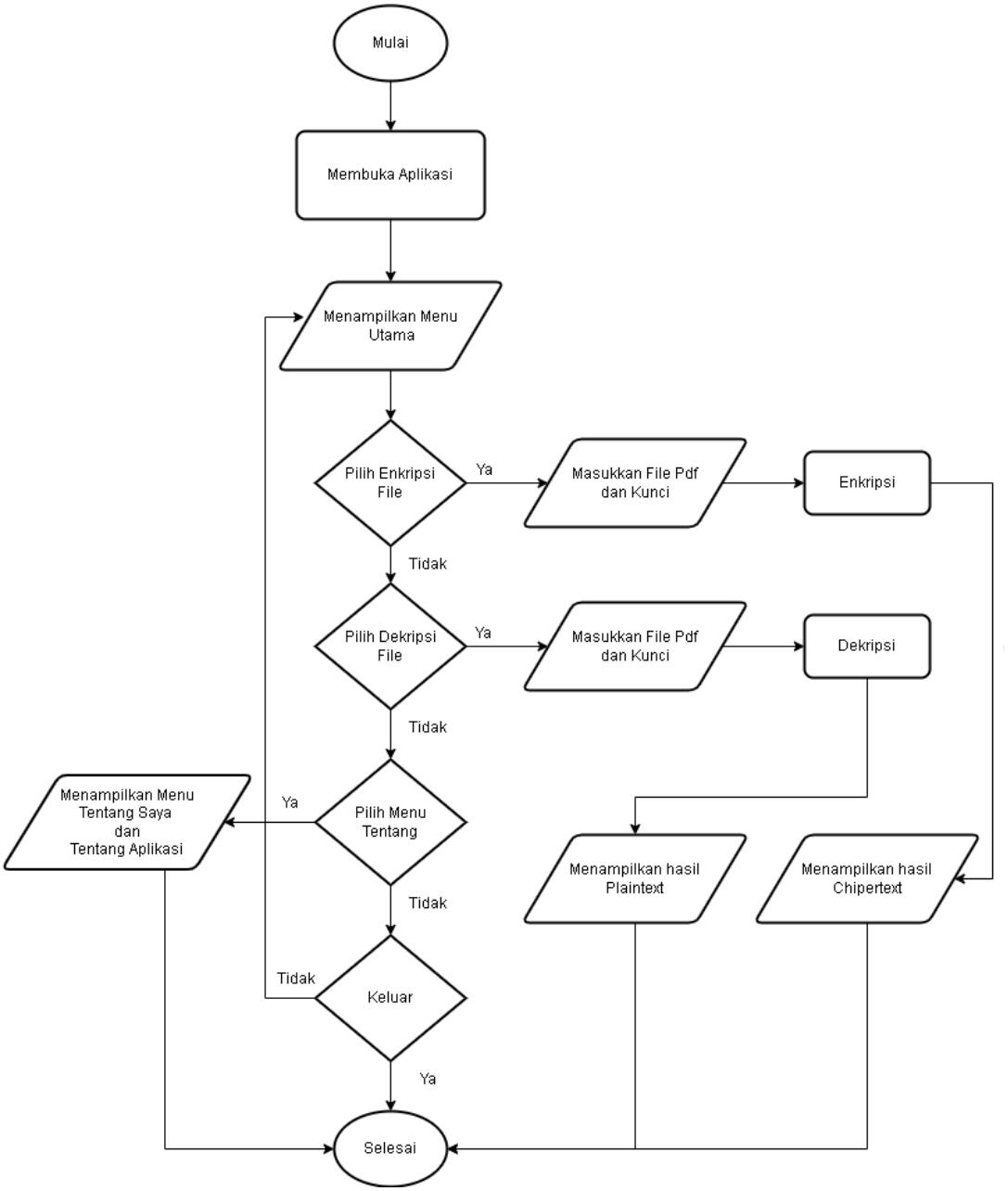


Gambar 4.4. *Flowchart* enkripsi &deskripsi

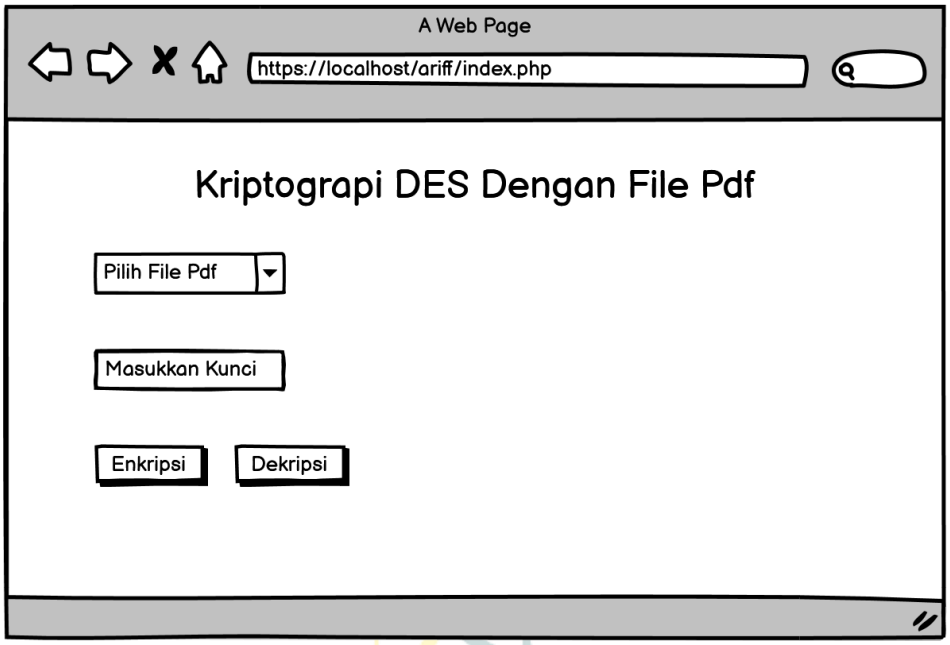
Gambar diatas adalah *flowchart* Enkripsi & Deksripsi dalam mengimplementasikan *Cryptography DES* dalam mengenkripsi file pdf dengan kunci.Dimulai dari menginput file pdf dan kunci kemudian terjadilah proses enkripsi.Proses dekripsi dilakukan sesuai dengan kunci yang pernah dipakai dalam menenkripsi file sebelumny, jika kunci tidak sesuai maka proses tidak akan dilakukan dan data akan kosong.

b. Flowchart Antar Muka

Sistem ini dirancang,,/ menggunakan pemrograman Web(PHP). Perancangan ini bertujuan untuk memudahkan pemakai (user) dalam menggunakan sistem yang telah dibuat. desain *interface* ini akan mempengaruhi spesifikasi komputer yang digunakan, agar dapat berjalan dengan baik, spesifikasi *hardware* harus sesuai. Bentuk perancangan antarmuka ini digunakan untuk menginput file pdf



Gambar 4.4 *Flowchart* Antar Muka



Gambar 4.5 Perancangan Antar Muka Masukan.

4.1.5. Pengujian

Sesuai dengan hasil perancangan aplikasi dan proses perhitungan manual dengan melakukan enkripsi file pdf menggunakan algoritma DES, dilakukan pengujian sesuai dengan tabel sebagai berikut.

Tabel 4.10. Pengujian Sistem

No.	Pengujian Sistem	Berhasil	Tidak Berhasil
1	Pengujian Sistem Input File Pdf	☑	☒
2	PengujianSistem Input Kunci	☑	☒
3	Menghasilkan File Enkripsi Dengan Menggunakan Algoritma DES	☑	☒
4	File Pdf dan Kunci Sesuai Dengan Proses Enkripsi dan Dekripsi	☑	☒
5	Menghasilkan File Dekripsi Dengan Menggunakan Algoritma DES	☑	☒

4.1.6. Implementasi

Setelah merancang dan membuat sistem, selanjutnya dilakukan pengujian. Pengujian bertujuan untuk melihat sejauh mana sistem yang telah dibangun sesuai dengan yang diharapkan, contoh hasil penerapan *Cryptography DES* dalam mengenkripsi file pdf menggunakan kunci dengan algoritma DES, dapat dilihat sebagai berikut ini :

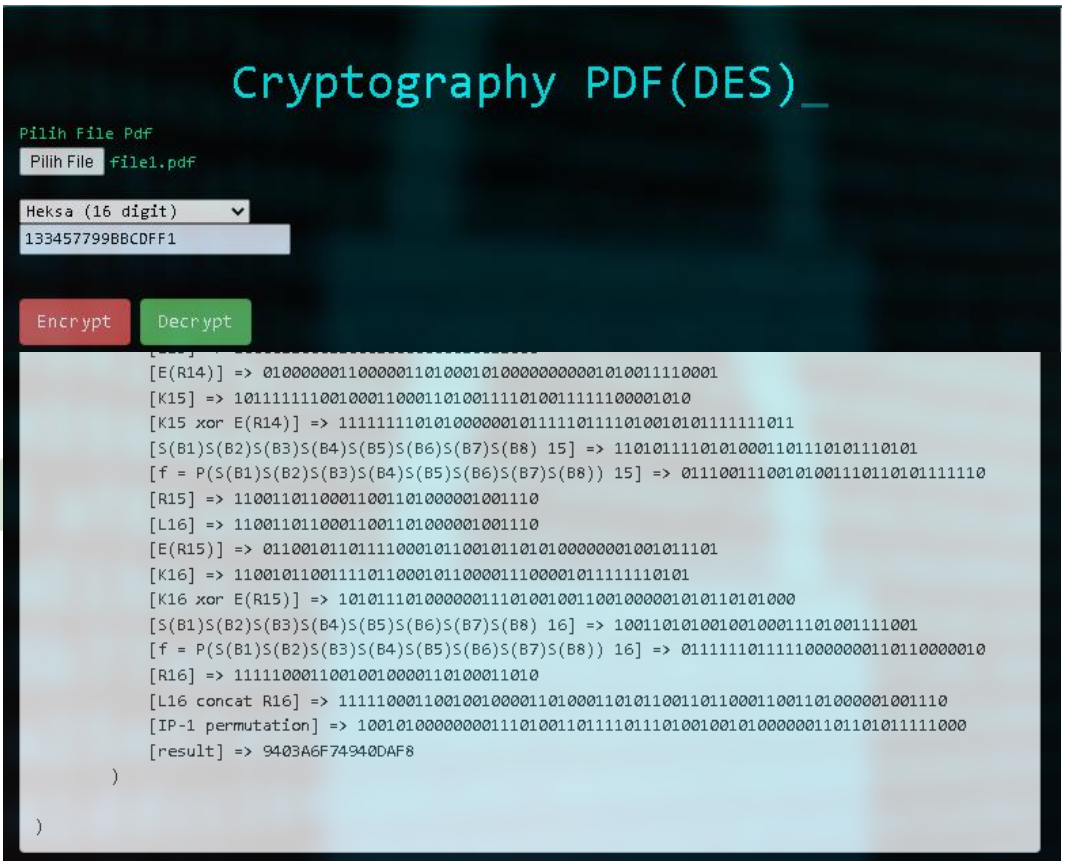
1. Tampilan awal aplikasi

Setelah merancang dan membuat sistem, selanjutnya dilakukan pengujian. Pengujian Tampilan dibawah ini adalah tampilan aplikasi penerapan *Cryptography DES* dalam mengenkripsi file pdf menggunakan kunci .

Gambar 4.6 Tampilan Aplikasi

2. Tampilan input file,kunci dan output

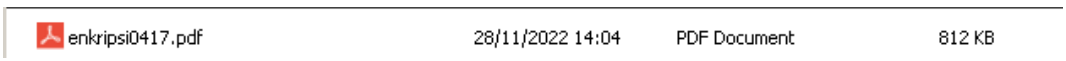
Setelah itu masukkan file pdf dan kunci lalu pilih jenis kunci hexa sesuai dengan standard yang ditentukan dan lakukan proses enkripsi lalu setalah itu muncul untuk mengeluaran nya bertujuan untuk membuktikan hasil manual sama dengan hasil di dalam program tersebut , seperti gambar dibawah ini:



Gambar 4.7 Tampilan Input File Pdf dan Kunci

3. Tampilan file pdf setelah dienkripsi

Setelah mengklik button proses enkripsi,file pdf akan disimpan di directory yang sudah ditentukan dan akan membuat file baru , seperti gambar dibawah ini:



Gambar 4.8 Tampilan File Pdf Setelah Dienkripsi

-

Gambar 4.9 Tampilan Isi File Pdf Setelah Dienkripsi

Berdaskan pada gambar diatas berikut ini adalah isi file yang telah di enkripsi dengan kunci sesuai dengan standard yang ditentukan dan dilakukan proses enkripsi.

4. Tampilan hasil dari file pdf setelah didekripsi dengan kunci yang salah

Setelah mengklik button proses dekripsi dengan kunci yang salah,file pdf akan disimpan di directory yang sudah ditentukan dan akan membuat file baru , seperti gambar dibawah ini:

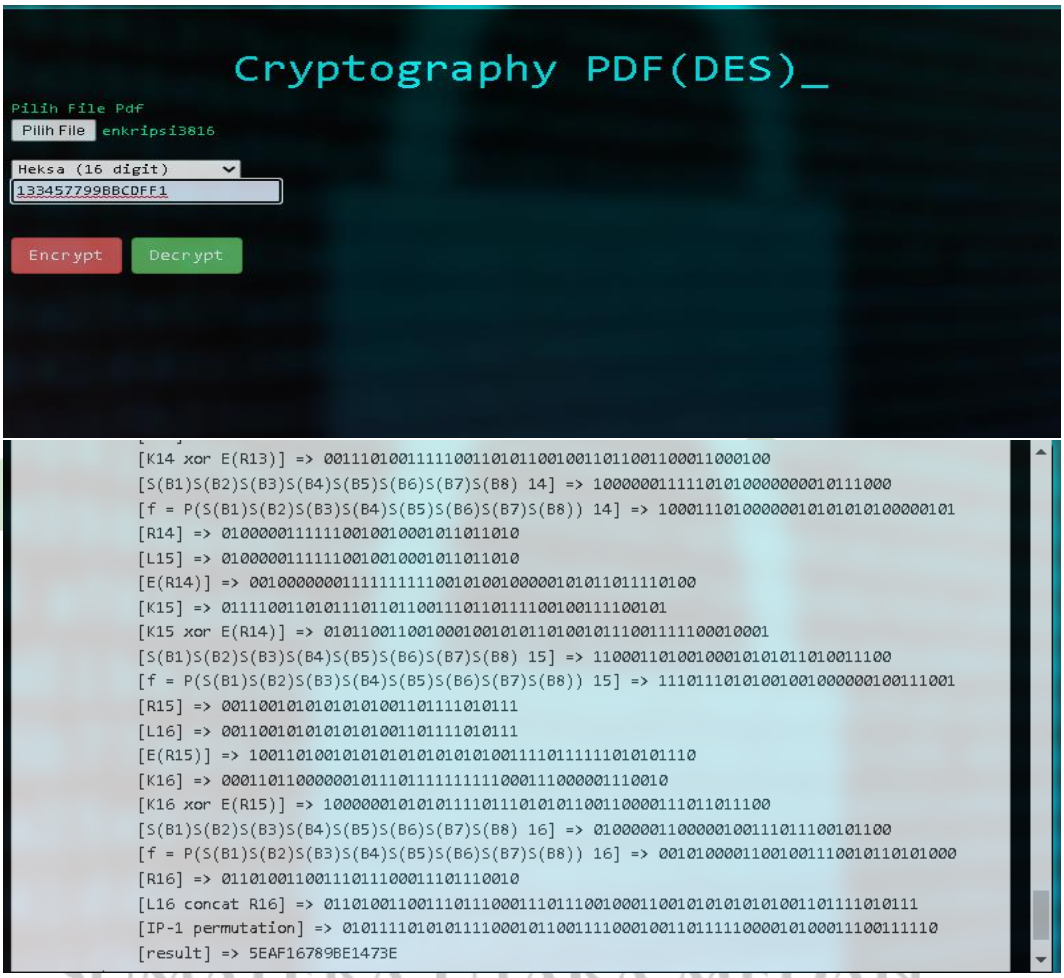
Gambar 4.11 Tampilan Input File Pdf Dengan Kunci Yang Salah

Gambar 4.12 Tampilan File Pdf Setelah Didekripsi Dengan Kunci Yang Salah

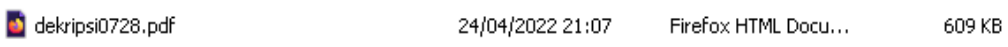
Bedasarkan pada gambar diatas, proses Dekripsi dengan kunci yang salah akan membuat file pdf kosong dan tidak melakukan prosesnya dengan benar.

5. Tampilan hasil dari file pdf setelah didekripsi dengan kunci yang benar

Setelah mengklik button proses dekripsi dengan kunci yang benar,file pdf akan disimpan di directory yang sudah ditentukan dan akan membuat file baru setalah itu muncul untuk mengeluaran nya bertujuan untuk membuktikan hasil manual sama dengan hasil di dalam program tersebut , seperti gambar dibawah ini:



Gambar 4.13 Tampilan Input File Pdf Dengan Kunci Yang Benar



Gambar 4.14 Tampilan File Pdf Setelah Didekripsi Dengan Kunci Yang Benar

Bedasarkan pada gambar diatas, proses Dekripsi dengan kunci yang benar akan membuat file pdf kembali seperti file sebelumnya.

6. Hasil Pengujian kunci enkripsi dan deskripsi

Berdasarkan uji cryptografi pada aplikasi, ditemukan bahwa file pdf yang menjadi objek file data untuk melakukan Algoritma DES, Hal ini tentunya membuat data file pdf tidak akan rusak, karena tidak ada pengubahan data object asli dikarenakan diencoding ke base64 agar file pdf tidak berubah sedikitpun sebelum dilakukan enkripsi. Oleh karena itu, kerahasiaan file pdf yang enkripsi tidak akan bocor dikarenakan kunci hanya bisa disimpan oleh si pembuat. Hasil pengujian dengan 3 sampel pdf dan kunci adalah sebagai berikut:

Tabel 4.11. Hasil Uji Sistem

No	Nama File Pdf			Ukuran Data Pdf			Kunci	Keterangan
	Original	Enkripsi	Dekripsi	Original	Enkripsi	Dekripsi		
1	file1.pdf	enk1.pdf	dek1.pdf	609KB	812KB	609 KB	133457799BBCDFF1	Berhasil
2	file2.pdf	Enk2.pdf	Dek2.pdf	430KB	574KB	430KB	5EAF57799BBCDFe1	Berhasil
3	File3.pdf	Enk3.pdf	Dek3.pdf	20KB	26KB	20KB	COMPUTER	Berhasil

Berdasarkan pada tabel 4.11, Pdf yang dienkripsi dengan kunci, file berubah dari segi ukuran maupun isi. Data file pdf yang didekripsi kembali seperti semula baik dari segi ukuran maupun banyaknya byte dalam file.