Sains dan Komputer (SAINTIKOM)
Vol., No., September 2020, pp
ISSN:

Implementasi Kriptografi Keamanan Data Transaksi Biaya Sewa Angkutan Truk Di PTPN II Dengan Mennggunakan Metode DES (Data Encryption Standard)

Dela Oktami*, Nurcahyo Budi Nugroho, S.Kom., M.Kom.,Sri Murniyanti,S.S., M.M.**
***Program Studi Sistem Informasi, STMIK Triguna Dharma
****Program Studi Sistem Informasi Dosen Pembimbing, STMIK Triguna Dharma

Article Info
Article history:
-

Keyword:
Implementasi Kriptografi Keamanan Data Transaksi Biaya Sewa Angkutan Truk Di PTPN II Dengan Menggunakan Metode DES (Data Encyption Standard)

ABSTRACT
Kegiatan transportasi dan logistik memiliki peranan dalam pembiayaan perusahaan. Meningkatnya permintaan membuat perusahaan mengalami overload dalam melakukan pengangkutan buah Tbs (Tandan Buah Segar) ke PKS (Pabrik Kelapa Sawit) sehingga pihak perusahaan perlu melakukan tambahan angkutan truk sewa juga biaya sewa yang bertambah setiap bulannya untuk meminialisirkan terjadinya penumpukkan buah TBS di perkebunan tersebut.
Untuk itu pihak dari perusahaan PTPN II sangatlah membutuhkan aplikasi keamanan untuk meindungi data transaksi biaya sewa angkutan truk sebagai alat transportasi dari pihak perusahaan PTPN II. Kriptografi merupakan aspek kemanan data yang berbasis komputer yang menghasilkan berbagai alternatif keamanan data dan membantu pihak keuangan sdm dalam menjaga kerahasiaan data keuangan biaya sewa angkutan di PTPN II.
Untuk meningkatkan keamanan kerahasiaan data transaksi biaya sewa angkutan di PTPN II dibutuhkan sistem keamanan. Sistem keamanan yang dimaksud adalah Implementasi keamanan data transaksi biaya sewa angkutan truk di PTPN II dengan menggunakan metode DES (Data Encryption Standard).

Kata kunci : Keamana Data, Kriptografi, DES (Data Encryption Standard).

First Author
Nama : Dela Oktami
Kampus : STMIK Triguna Dharma
Program Studi : Sistem Informasi
E-Mail : delaoktami10@gmail.com

1. PENDAHULUAN

Aspek keamanan data telah menjadi aspek yang sangat penting dari suatu Sistem informasi. Kepedulian karyawan PTPN II terhadap data -data kantor dan kurangnya informasi tentang keamanan data, membuat mereka menginginkan sebuah aplikasi yang mudah untuk digunakan dan dapat membantu mereka dalam mengamankan data – data penting, seperti Data transaksi biaya sewa angkutan truk. Salah satu keamanan data dan kerahasiaan data tersebut yaitu dengan digunakannya algoritma kriptografi untuk melakukan penyandian data. Informasi dan komunikasi pada saat ini merupakan kebutuhan manusia yang sangat penting. Dengan kemajuan teknologi dan komunikasi (TIK) orang dapat melakukan komunikasi dan transaksi tanpa batas, salah satu hal terpenting dalam teknologi informasi adalah nilai dari informasi sendiri. Nilai dari sebuah informasi sangatlah penting untuk diketahui oleh orang yang tidak berhak melihatnya. Seiring dengan tuntutan keamanan data terhadap kerahasiaan informasi yang saling diperlukan. Data transaksi biaya sewa angkutan truk adalah salah satu dokumen yang sifatnya rahasia sehingga diperlukan tingkat keamanan data untuk mengunci data transaksi biaya sewa angkutan PTPN II. Berdasarkan masalah tersebut pengamanan data sangat penting dilakukan ada beberapa algoritma enkripsi yang telah dipublikasikan, salah satunya adalah algoritma enkripsi Data Encryption Standard.

Dari pembahasan penelitian ini maka dibuatlah sebuah teknik unruk mengamankan informasi yang terdapat dalam *data transaksi biaya sewa angkutan*, dengan cara melakukan enkripsi pada isi dokumen tersebut untuk dapat dibaca kecuali dengan algoritma yang digunakan dalam enkripsi data yang dimaksud. Dan berdasarkan uraian diatas, maka di angkatlah judul **" Implementasi Kriptografi Keamanan Data Transaksi Biaya Sewa Angkutan Truk Di PTPN II Menggunakan Metode Des (Data Encryption Standard)"**

2. KAJIAN PUSTAKA

2.1 Kriptografi

Kriptografi adalah ilmu dan teknik dalam pengamanan data dari pihak ketiga. Pada kriptografi terdapat istilah enkripsi dan dekripsi. Enkripsi adalah mengubah text awal (*plain text*) menjadi text ter-enkripsi (*cipher text*) menggunakan sebuah kunci.

Sedangkan Dekripsi adalah mengubah text ter-enkripsi (*cipher text*) kembali menjadi text awal (*plain text*) dengan menggunakan kunci yang sama, dalam hal ini jika menggunakan *symmetric-key cryptography*[1].

2.1.1 Sejarah Kriptorafi

Kriptografi (*Cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan sedangkan *graphia* artinya tulisan.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi [1].

2.2 Jenis – Jenis Kriptografi

Kriptografi memiliki dua jenis yaitu kriptografi berdasarkan perkembangan dan kriptografi berdasarkan kunci simetris. Sebagai beikut :

2.2.1 Kriptografi berdasarkan perkembangan

1. Kriptografi Klasik (*chiper*)

Algoritma kriptografi yang termasuk ke dalam jenis kriptografi klasik ini digunakan pada masa sebelum berlakunya komputarisasi dengan komputer, algoritma kriptografi ini rata-rata masih menggunakan kunci simetris dan menyandikan pesan dengan teknik subtitusi atau transposisi.

Salah satu algoritma klasik adalah *Caesar chipper*. Dalam kriptografi klasik, secara umum dapat dikelompokkan dalam dua model yaitu menggunakan tekik substitusi dan transposisi [6].

2. Kriptografi Modern

Algoritma kriptografi yang termasuk ke dalam jenis kriptografi modern ini memiliki tingkat kesulitan yang lebih tinggi dan kompleks serta menggunakan pengetahuan matematika dalam penerapan kuncinya. Pada kriptografi modern, kunci yang digunakan untuk menyandikan pesan sudah berupa kunci asimetris.

2.2.2 Jenis Kriptografi Berdasarkan Kunci

Algoritma kriptografi dapat dikelompokkan menjadi dua jenis berdasarkan kuncinya, yaitu :

1. Kriptografi Kunci-Simetris

Kriptografi kunci-simetrik mengarah kepada metode enkripsi yang mana baik pengirim maupun yang dikirim saling memiliki kunci yang sama(walaupun kebanyakan kunci yang ada sedikit berbeda namun masih berhubungan dalam hal kemudahan perhitungan). Sistem ini sering juga disebut dengan algoritma kunci tunggal atau algoritma satu kunci. Bila E adalah fungsi enkripsi (encryption), K adalah kunci rahasia (*key*), sedangkan M adalah pesan orisinil yang akan dikirimkan (*message*) dan C adalah pesan sandinya (*cipher*), maka *system* simetris dapat diformulasikan sebagai berikut:

Ek(M)=C dan Dk(C)=M

Dalam aplikasinya antara pengirim dan penerima harus ada persetujuan atau sinkronisasi kunci agar saling berkomunikasi. Jadi, keamanan algoritma sistem simetris terletak pada kunci. Siapapun yang memperoleh kunci, akan dapat membuka pesan yang dikomunikasikan. Karena itu selama proses komunikasi bersifat rahasia, maka kunci harus tetap dirahasiakan.

Algoritma memakai kunci simetis diantaranya, yaitu :

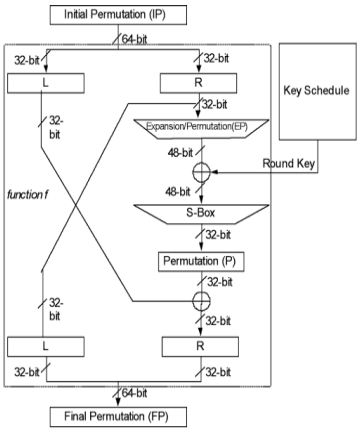
a. *Data Encrypion Standard*(DES)
b. *One Time Pad*(OTP)
c. *International Data Encryption Algorithm*(IDEA)
d. RC2, RC4, RC5, RC6

2. Kriptografi Kunci-Publik/Asimetris

Sistem sandi asimetris atau dikenal juga sebagai sistem sandi kunci publik adalah sistem sandi yang metode menyandi dan membuka sandinya menggunakan kunci yang berbeda. Tidak seperti sistem sandi simetris, sistem sandi ini relatif masih baru. Algoritma sandi jenis ini yang telah terkenal diantaranya RSA (Rivest-Shamir-Adleman), ElGamal, dan Diffie-Hellman.

2.3 Algoritma DES (*Data Encrytion Standard)*

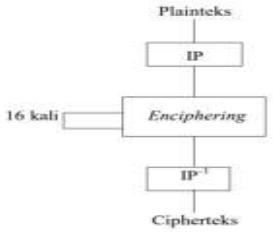
Algoritma DES merupakan algoritma enkripsi yang paling banyak digunakan di dunia yang diadopsi oleh NIST (*National Institue of Standards and Technology*) sebagai standar pengolah informasi Federal AS. Data *plaintext* dienkrip dalam blok-blok 64 bit menjadi 64 bit data *ciphertext* menggunakan kunci 56 bit kunci internal (*internal key*). DES mentransformasikan *input* 64 bit dalam beberapa tahap enkripsi ke dalam *output* 64 bit. Dengan demikian, DES termasuk *block cipher*. Dengan tahapan dan kunci yang sama, DES digunakan untuk membalik enkripsi. Kunci internal pada algoritma DES dibangkitkan dari kunci eksternal (*external key*) 64 bit. Skema global dari proses algoritma DES dapat dilihat pada gambar 2.1



Gambar 2.1 Skema Global Algoritma DES (M. Yuli Andri, 2009)

2.3.1 Skema global dari algoritma DES (*Data Encryption Standard)*

DES (Data Encryption Standard) termasuk ke dalam algoritma kunci-simetris, dimana kunci yang sama digunakan untuk enkripsi dan dekripsi. DES termasuk ke dalam blok *cipher*, dimana data tergabung dalam blok berukuran masing-masing 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (*internal key*) atau sub-kunci (*subkey*). Kunci internal dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit. Skema global dari algoritma DES adalah sebagai berikut:



Gambar 2.2 Skema Global Algoritma DES (Munir, 2004)

2.3.2 Struktur Kunci Internal

Enkripsi dan dekripsi DES memiliki 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah, yaitu *K*1,*K*2,…,*K*16. Kunci-kunci internal ini dapat dibangkitkan sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter.

Kemudian untuk struktur pembentukan kunci internal terdapat beberapa cara, yaitu:

1. Mengubah kunci menjadi blok lalu permutasikan dengan table PC-1, dan hasil permutasinya disimpan dalam bentuk C0 dan D0.

Tabel 2.2 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	10	12	4

2. C0 dan D0 melakukan pergeseran kunci (*left shift*) dengan aturansebanyak 16 kali perulangan sehingga menghasilkan C16 dan D16.

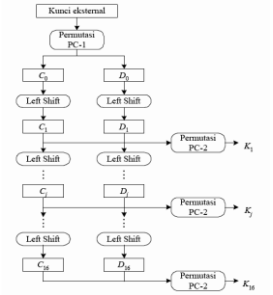
Putaran *Key*	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Jumlah Pergeseran	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

3. Lalu setelah melakukan pergeseran kunci sebanyak 16 kali perulangan lalu setiap Cj dan Dj (C1 dan D1, C2 dan D2, … C16 dan D16) melakukan permutasi dengan table PC-2 sehingga menghasilkan Kj.

Tabel 2.4 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	13	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

4. Kunci internal atau Kj (K1, K2, K3, … , K16) ini digunakan untuk proses enkripsi dan deskripsi dengan sesuai aturan skema global DES yang diproses sampai 16 kali perulangan.
   Dan untuk struktur pembentukan kunci internal sebagai beikut :



Gambar 2.3 Penurunan kunci DES (Rinaldi Munir, 2006)

2.3.3 Enkripsi dan Dekripsi

Plainteks sehingga urutan bit-bit di dalamnya berubah. Pengacakan dilakukan dengan menggunakan Proses enkripsi pada DES dilakukan setelah permutasi awal (IP). Tujuan permutasi awal adalah mengacak matriks permutasi awal berikut:

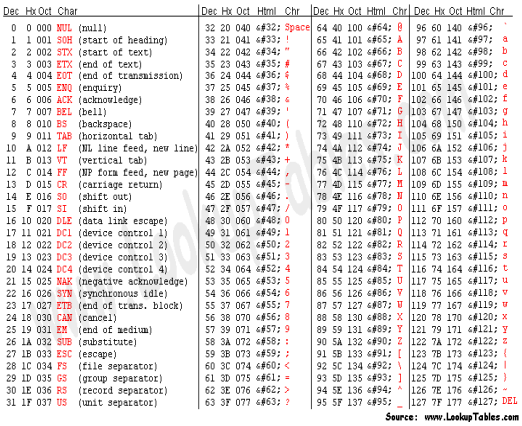
Tabel 2.5 Tabel Permutasi Awal (IP)

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

Setiap blok plainteks mengalami 16 kali putaran enkripsi. Setiap putaran enkripsi merupakan jaringan Feistel yang secara matematis dinyatakan sebagai :

$$\mathbf{Li = Ri–1}$$
$$\mathbf{Ri = Li – 1 \oplus f(Ri – 1, Ki)}$$

Dimana:
L = Literasi / perulangan
i = Alternatif / variabel
R = Round (putaran)
K = Key (kunci)



Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Gambar 2.5 ASCII

3. AN.ALISIS DAN HASIL

3.1 Metode Penelitian

Metode penelitian adalah langkah-langkah yang digunakan untuk mengumpulkan informasi atau data yang dapat diperoleh dari seorang narasumber sebagai gambaran rancangan penelitian yang akan dibuat. Didalam melakukan penelitian terdapat beberapa cara yaitu sebagai berikut :

1. *Data Collecting*

Teknik *data collecting* adalah proses pengumpulan data yang berguna untuk memastikan informasi yang didapat oleh peneliti. Dengan tujuan mengevaluasihasil atau mengumpulkan wawasan yang dapat ditindak lanjuti. Dalam teknik pengumpulan data, dilakukan dengan wawancara secara langsung dengan Pegawai PTPN II Limau Mungkur.Wawancara digunakan untuk memperoleh data-data yang berkaitan dengan data Biaya Sewa Angkutan pada PTPN 2 Limau Mungkur. Dalam proses wawancara ini peneliti menanyakan upaya apa yang telah dilakukan pihak perusahaan selama ini dalam mengamankan data biaya sewa angkutan. Tujuannya dikarenakan data tersebut merupakan data yang sangat penting dalam proses pengelolahan hasil kebun yang selama ini dilakukan oleh pegawai PTPN II, sehingga peneliti tertarik untuk melakukan pengamanan terhadap data biaya sewa angkutanagar dapat menghindari manipulatif ataupun kebocorandata yang dilakukan oleh pihak yang tidak bertanggung jawab.

No	Tanggal	No. Delivery Order (DO)	No. Polisi	Jenis Kendaraan	Nama Produk	Nama Perusahaan Pengangkutan	Harga Sewa Angkutan/Mobil
1	1 Januari 2020	202298	BK 8386 GM	Truck Bak Kayu	Kernel	PT. Tanindo Sejati	Rp 4,000,000
2	1 Januari 2020	2022988	BK 8720 XC	Truck Tanki	CPO	PT. Indostar Cargo	Rp 5,000,000
3	3 Januari 2020	2022989	BK 8478 XB	Dump Truck	Cangkang	PT. Sinar Raya	Rp 3,500,000
4	3 Januari 2020	2022990	BK 9865 CT	Dump Truck	Noten	PT. Indostar Cargo	Rp 4,500,000
5	6 Januari 2020	2022991	BK 9981 DA	Truck Bak Kayu	Kernel	PT. Tanindo Sejati	Rp 4,000,000
6	6 Januari 2020	2022992	BK 6687 CD	Truck Bak Kayu	Tebu	PT. Indostar Cargo	Rp 4,000,000
7	6 Januari 2020	2022993	BK 5467 DD	Truck Bak Kayu	Kernel	PT. Tanindo Sejati	Rp 4,000,000
8	9 Januari 2020	2022994	BK 8386 GM	Truck Bak Kayu	Kernel	PT. Tanindo Sejati	Rp 4,000,000
9	9 Januari 2020	2022995	BK 9865 CT	Dump Truck	Noten	PT. Indostar Cargo	Rp 4,500,000
10	14 Januari 2020	2022996	BK 5712 AB	Dump Truck	Noten	PT. Indostar Cargo	Rp 4,500,000
11	14 Januari 2020	2022997	BK 8720 XC	Truck Tanki	CPO	PT. Indostar Cargo	Rp 5,000,000
12	17 Januari 2020	2022998	BK 8478 XB	Dump Truck	Cangkang	PT. Sinar Raya	Rp 3,500,000
13	17 Januari 2020	2022999	BK 8478 XB	Dump Truck	Cangkang	PT. Sinar Raya	Rp 3,500,000
14	20 Januari 2020	2023000	BK 8720 XC	Truck Tanki	CPO	PT. Indostar Cargo	Rp 5,000,000
15	20 Januari 2020	2023001	BK 8720 XC	Truck Tanki	CPO	PT. Indostar Cargo	Rp 5,000,000
16	18 Januari 2020	2023002	BK 6687 CD	Truck Bak Kayu	Tebu	PT. Indostar Cargo	Rp 4,000,000
17	28 Januari 2020	2023003	BK 6687 CD	Truck Bak Kayu	Tebu	PT. Indostar Cargo	Rp 4,000,000

Tabel 3.1 Data Transaksi Biaya Sewa Angkutan Truk

2. StudiLiteratur

Untuk memperoleh informasi dengan mempelajari buku-buku literatur atau karya lainnya yang membahas tentang kriptografi atau untuk menunjang pembuatan perangkat lunak yang berhubungan dengan materi penulisan skripsi. Diharapkan dengan literatur tersebut dapat membantu peneliti dalam menyelesaikan permasalahan yang terjadi.

3.3 Algoritma Sistem

Untuk menganalisa algoritma yang digunakan ada beberapa tahapan yang akan dilakukan yaitu dengan membuat suatu skenario algoritma *Data Encryption Standart* (DES) yang akan dijelaskan dengan rancangan aplikasi yang akan dikerjakan serta fitur yang akan dipakai maupun pemodelan lainnya yang akan mendukung aplikasi tersebut.Objek dari penelitian ini yaitu salah satu dari data biaya transaksi angkutan karena sesuai dengan analisa permasalahan, maka bahan contoh sebagai plainteks yang akan di enkripsikan adalah **Trukkayu** salah satu dari data biaya sewa angkutan dan untuk key (K) yaitu Drumtruk maka langkah pertama yang harus dilakukan adalah mengubah plainteks kedalam bentuk biner.

3.3.1 Proses Enkripsi

Proses enkripsi adalah menyandikan data plainteks menjadi cipherteks. Dalam proses enkripsi terdapat beberapa langkah-langkah sebagai berikut :

1. Mengubah plainteks dan kunci menjadi bilangan biner

Ubahlah setiap karakter plainteks kedalam bentuk hexa dan biner berdasarkan table ASCII. Bahan contoh sebagai plainteks yang akan di enkripsikan adanya **TRUKKAYU** dan salah satu biaya biaya transaksi dan untuk key (k) yaitu **CANGKANG** maka langkah pertama yang harus dilakukan adalah mengubah plainteks kedalam bentuk biner.

Tabel 3.4 Plaintex

Char	Hexa	Biner							
T	54	0	1	0	1	0	1	0	0
R	52	0	1	0	1	0	0	1	0
U	55	0	1	0	1	0	1	0	1
K	48	0	1	0	0	1	0	1	1
K	48	0	1	0	0	1	0	1	1
A	41	0	1	0	0	0	0	0	1
Y	59	0	1	0	1	1	0	0	1
U	55	0	1	0	1	0	1	0	1

Ubah Kunci (Key) kedalam bentuk biner berdasarkan table ASCII

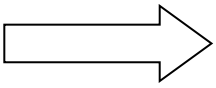
Tabel 3.5 Kunci

Char	Hexa	Biner							
C	43	0	1	0	0	0	0	1	1
A	41	0	1	0	0	1	1	1	0
N	4E	0	1	0	0	1	1	1	0
G	47	0	1	0	0	0	1	1	1
K	4B	0	1	0	0	1	0	1	1
A	41	0	1	0	0	0	0	1	1
N	4E	0	1	0	0	1	1	1	0
G	47	0	1	0	0	0	1	1	1

1. *Initial Permutation* (IP) Pada Plainteks

Tabel 3.6 Initial Permutation (ip)

Plaintext (X)							
0	1	0	1	0	1	0	0
0	1	0	1	0	0	1	0
0	1	0	1	0	1	0	1
0	1	0	0	1	0	1	1
0	1	0	0	1	0	1	1
0	1	0	0	0	0	0	1
0	1	0	1	1	0	0	1
0	1	0	1	0	1	0	1



Tabel IP							
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	34	31	23	15	7

2. Melakukan permutasi kompresi PC-1

Tabel 3.7 Kunci

Kunci							
0	1	0	0	0	0	0	1
0	1	0	0	0	0	1	1
0	1	0	0	1	1	1	0
0	1	0	0	0	1	1	1
0	1	0	0	1	0	1	1
0	1	0	0	0	0	1	1
0	1	0	0	1	1	1	0
0	1	0	0	0	1	1	1

Hasil Initial Permutation (IP)

Tabel 3.9*Initial Permutation* (IP)

0	0	0	0	0	0	0
0	1	1	1	1	1	1
1	1	0	0	0	0	0
0	0	0	0	0	0	0
1	1	1	1	1	1	1
0	1	1	0	0	1	1
0	0	0	0	0	1	0
1	0	0	0	0	0	0

Sehingga hasil keluarannya yang bias di tuliskan adalah :
IP (X) : 0000000 0111111 1100000 0000000 1111111 0110011 0000010 1000000
Selanjutnya bit pada output dipecah menjadi 2 bagian yaitu Co dan Do sehigga hasilnya sebagai berikut:
Co : 0000000 0111111 1100000 0000000
Do : 1111111 0110011 0000010 1000000

4. Melakukan Pergeseran Kiri (*Left Shift Operation)*

Tabel 3.10 *(Left Shift Operation)*

Putaran 1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Jumlah Pergerakan	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Keterangan :
Berikut hasil putaran putaran dari Left Shift
Perputaran ke 1 di geser 1 bit ke bit ke kiri

Tabel 3.11Hasil Putaran Dari Left Shift

Putaran Ke	Left Shift	Hasil
1	1	C1 : 0000000 1111111 1000000 0000000 D1 : 1111110 1100110 0000101 0000001
2	1	C2 : 0000001 1111111 0000000 0000000 D2 : 1111101 1001100 0001010 0000011
3	2	C3 : 0000011 1111110 0000000 0000000 .D3 : 1111011 0011000 0010100 0000111
4	2	C4 : 0000111 1111100 0000000 0000000 D4 : 1110110 01100001 0101000 0001111
5	2	C5 : 0001111 1111000 0000000 0000000 D5 : 1101100 1100000 0101000 0001111
6	2	C6 : 00111111 1110000 0000000 0000000 D6 : 1011001 1000001 0100000 0111111
7	2	C7 : 0111111 1100000 0000000 0000000 D7 : 0110011 0000010 1000000 1111111
8	2	C8 : 1111111 1000000 0000000 0000000 D8 : 1100110 0000101 0000001 1111110
9	1	C9 : 1111111 0000000 0000000 0000001 D9 : 1001100 0001010 0000011 1111101
10	2	C10 : 1111110 0000000 0000000 0000011 D10 : 0011000 0010100 0000111 1111011
11	2	C11 : 1111100 0000000 0000000 0000111

		D11 : 0110000 0101000 0001111 1110110
12	2	C12 : 1111000 0000000 0000000 0011111 D12 : 1100000 1010000 0001111 1110110
13	2	C13 : 1110000 0000000 0000000 0011111 D13 : 1000001 0100000 0111111 0011111
14	2	C14 : 1100000 0000000 0000000 0111111 D14 : 0000010 1000000 1111111 0110011
15	2	C15 : 1000000 0000000 0000000 1111111 D15 : 0000101 0000001 1111110 1100110
16	1	C16 : 0000000 0000000 0000001 1111111 D16 : 0001010 0000011 1111101 1001100

Langkah 4

Tabel 3.12 *Permutasi Kompresi 2 (PC-2)*

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	13	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 *output*nya:

Hasil
C1 : 0000000 1111111 1000000 0000000 D1 : 1111110 1100110 0000101 0000001 K1 : 101000 001001 001001 000010 101100 110010 010110 000111
C2 : 0000001 1111111 0000000 0000000 D2 : 1111101 1001100 0001010 0000011 K2 : 101000 000001 001001 010010 001001 110011 001100 101111
C3 : 0000011 1111110 0000000 0000000 D3 : 1111011 0011000 0010100 0000111 K3 : 001000 000101 001001 010010 001011 100100 001110 001011
C4 : 0000111 1111100 0000000 0000000 D4 : 1110110 01100001 0101000 0001111 K4 : 001001 000101 001001 010000 001101 100010 100111 101010
C5 : 0001111 1111000 0000000 0000000 D5 : 1101100 1100000 0101000 0001111 K5 : 001001 000101 000101 010000 010101 100110 000101 001111
C6 : 00111111 1110000 0000000 0000000 D6 : 1011001 1000001 0100000 0111111 K6 : 001001 100101 000101 010000 011001 001000 100101 011111
C7 : 0111111 1100000 0000000 0000000 D7 : 0110011 0000010 1000000 1111111 K7 : 000001 100100 000101 010000 111001 111000 000111 001000
C8 : 1111111 1000000 0000000 0000000 D8 : 1100110 0000101 0000001 1111110 K8 : 000011 100100 000101 010001 010001 111010 010011 011010
C9 : 1111111 0000000 0000000 0000001 D9 : 1001100 0001010 0000011 1111101 K9 : 000011 110100 0000100 010001 110000 001011 011101 000011
C10 : 1111110 0000000 0000000 0000011 D10 : 0011000 0010100 0000111 1111011 K10 : 000011 110100 000100 001001 011011 011001 010101 001001
C11 : 1111100 0000000 0000000 0000111 D11 : 0110000 0101000 0001111 1110110 K11 : 000011 110010 0000110 001001 011111 101001 011000 101000
C12 : 1111000 0000000 0000000 0011111 D12 : 1100000 1010000 0001111 1110110 K12 : 000010 110000 000110 001001 010011 101001 010000 101110
C13 : 1110000 0000000 0000000 0011111 D13 : 1000001 0100000 0111111 0011111 K13 : 000110 110000 000010 001001 001110 000101 110101 100010
C14 : 1100000 0000000 0000000 0111111 D14 : 0000010 1000000 1111111 0110011 K14 : 000110 010000 100010 001001 010011 001101 110110 101100
C15 : 1000000 0000000 0000000 1111111 D15 : 0000101 0000001 1111110 1100110 K15 : 000010 010000 100010 001000 000011 001111 100000 111000
C16 : 0000000 0000000 0000001 1111111 D16 : 0001010 0000011 1111101 1001100 K16 : 000100 010010 100010 001000 100010 000100 110011 110001

1. Melakukan Ekspansi Data
   2. Pada tahap ini ekspansi data Ri-1 32 bit menjadi Ri 48 bit dengan 16 kali putaran dengan nilai perputaran 1<= i <= 16 menggunakan tabel ekspansi

. Berikut hasil *output*nya:

Interaksi	Hasil
1	E(R0) = 000000 000000 000000 000000 000011 110000 000011 110101 K1 = 101000 001001 001001 000010 101100 110010 010110 000111---------- XOR A1 = 111000 001011 111011 101110 100111 100001 001100 110101 B2 = 0011 0010 0001 0011 0111 0100 1000 1001 P(B1) = 11101100 01000100 00001010 10001011 L0 = 00000000 00000000 01011000 00011010 ----------XOR R1 = 11101100 01000100 01010010 10010001
2	E(R1) = 111101 011000 001000 001000 001010 100101 010010 100011 K2 = 101000 000001 001001 010010 001001 110011 001100 101111 ---------- XOR A2 = 010101 011001 000001 011010 000011 010110 011110 001100 B2 = 0000 0000 1000 0100 0011 0111 0101 1001 P(B2) = 00101010 00110000 00111001 10001000 L1 = 11101100 01000100 01010010 10010001 ----------XOR R2 = 11000110 01110100 01101011 00011001
3	(R2) = 111000 001100 001110 101000 001101 010110 100011 110011 K3 = 001000 000101 001001 010010 001011 100100 001110 001011 ---------- XOR A3 = 11000 001001 000111 101010 000110 110010 101101 111000 B3 = 0111 0011 0011 0101 0010 0010 0001 0001 P(B3) = 11000110 00100000 11011010 10000110 L2 = 11000110 01110100 01101011 00011001 ----------XOR R3 = 00000000 01010100 10110001 10011111
4	E(R3) = 100000 000000 001010 101001 010110 100011 110011 111110 K4 = 001001 000101 001001 010000 001101 100010 100111 101010 ---------- XOR A4 = 101001 000101 000011 111001 011011 000001 010100 010100 B4 = 1001 0010 1001 1001 1011 1000 0001 0011 P(B4) = 11110111 10000010 00001001 11000010 L3 = 00000000 01010100 10110001 10011111 ----------XOR R4 = 11110111 11010110 10111000 01011101
5	E(R4) = 111110 101111 111010 101101 010111 110000 001011 111011 K5 = 001001 000101 000101 010000 010101 100110 000101 001111 ---------- XOR A5 = 110111 101010 111111 111101 000010 010110 001110 110100 B5 = 0010 0001 0000 0010 0010 0111 0010 0111 P(B5) = 00000000 01100010 01101110 10101000 L4.R3 = 11110111 11010110 10111000 01011101 ----------XOR R5 = 11110111 10110100 11110110 11110101
6	E(R5) = 111110 101111 110110 101001 011110 101101 011110 101011 K6 = 001001 100101 000101 010000 011001 001000 100101 011111 ---------- XOR A6 = 110111 001010 110011 111001 000111 100101 111011 B6 = 0111 0000 0010 0010 0011 1001 0110 0010 P(B6) = 00110000 01010010 10100110 10000110 L5. R4 = 11110111 10110100 11110110 11110101 ----------XOR R6 = 11000111 11100110 01010000 01110011
7	E(R6) = 111000 001111 111100 001100 001010 100000 001110 100111 K7 = 000001 100100 000101 010000 111001 111000 000111 001000 ---------- XOR A7 = 111001 101011 111001 011100 110011 011000 001001 B7 = 0110 1000 0101 0101 0001 0110 0000 0000 P(B7) = 10100100 00101001 10010010 00001000 L6.r5 = 11000111 11100110 01010000 01110011 ----------XOR R7 = 01100011 11001111 11000010 01111011
8	E(R7) = 101100 000111 111001 011111 111000 000100 001111 110110 K8 = 000011 100100 000101 010001 010001 111010 010011 011010 ---------- XOR A8 = 101111 100011 111100 001110 101001 111010 011100 101100 B8 = 0010 1000 0100 0100 0100 0110 0101 0011 P(B8) = 00000110 00111111 00111010 00001100 L7.R6 = 01100011 11001111 11000010 01111011 ----------XOR R8 = 01100101 11110000 11111000 01110111
9	(R8) = 101100 001011 111110 011111 110000 001110 101111 111101 K9 = 000011 110100 000100 010001 110000 001011 011101 000011 ---------- XOR A9 = 101111 111111 111010 001110 000000 000101 110010 111110 B9 = 0101 0001 0011 0011 0110 0000 0010 1001 P(B9) = 10001100 01000100 11001100 10000110 L8.R7 = 01101011 10010000 10101111 01111010 ----------XOR R9 = 11100111 11010100 01100011 11111100
10	E(R9) = 101110 101011 110111 111101 010011 110101 011010 100110 K10 = 000011 110100 000100 001001 011011 011001 010101 001001---------- XOR A10 = 101101 011111 110011 110100 001000 101100 001111 101111 B10 = 0010 0101 0010 0000 0001 0000 0101 0001 P(B10) = 00100010 00010000 11001000 00010110 L9.R8 = 01110101 10111110 10011010 11010011 ----------XOR R10 = 101010111 10101110 01010010 11000101
	E(R10) = 101110 101011 110101 011100 001010 100101 011000 001010 K11 = 000011 110010 000110 001001 011111 101001 011000 101000 ---------- XOR

11	A11 = 101101 011001 110011 010101 010101 001100 000000 100010 B11 = 0100 0110 0000 0011 0111 0011 0001 0100 P(B11) = 11100010 01100100 10100000 10110000 L10R9 = 01110101 10101110 01010010 11000101 ----------XOR R11 = 10010111 11001010 11110010 01110101
12	E(R11) = 110010 101111 111001 011101 011110 100110 001110 101011 K12 = 000010 110000 000110 001001 010011 101001 010000 101110 ---------- XOR A12 = 110000 011111 111111 010100 001101 001111 011110 000101 B12 = 1000 0110 0100 0010 0100 1001 00101 0001 P(B12) = 01010010 11010101 00101000 00010000 L11.R10= 10010111 11001010 11110010 01110101 ----------XOR R12 = 11000101 00011111 11111010 01110101
13	E(R12) = 111000 001010 100011 111111 111111 110100 001100 001011 K13 = 000110 110000 000010 001001 001110 000101 110101 100010---------- XOR A13 = 111110 111010 100001 110110 110001 110001 111001 B13 = 0001 0101 0101 0111 0011 0000 0100 0110 P(B13) = 10100100 01010011 01010000 10110010 L12.R11= 11000101 00011111 11111010 01100101 ----------XOR R13 = 01100001 01001100 10101010 11010111
14	(R13) = 101100 000010 101001 011001 010101 010101 011010 101110 K14 = 000110 010000 100010 001001 010011 001101 110110 101100 ---------- XOR A14 = 101010 010010 001011 010000 000110 011000 101101 B14 = 1001 0000 1000 0100 0111 0001 0000 1000 P(B14) = 00101000 10000100 00110001 10000010 L13.R12= 01100001 01001100 10101010 11010111 ----------XOR R14 = 01001001 11001000 10011011 01010101
15	E(R14) = 101001 010011 111001 010001 010011 110110 101010 101010 K15 = 000010 010000 100010 001000 000011 001111 100000 111000 ---------- XOR A15 = 101011 000011 011011 011001 010000 111001 001010 B15 = 0001 0110 0000 0100 1001 0011 0000 P(B15) = 00100011 00100000 00110100 00010010 L14.R13= 01001001 11001000 100110110101010 1 ----------XOR R15 = 01101010 11101000 10101111 01000111
16	E(R15) = 101101 010101 011101 010001 010101 011110 101000 001110 K16 = 000100 010010 100010 001000 100010 000100 110011 110001 ---------- XOR A16 = 10101 000111 111111 011001 110111 011010 011011 111111 P(B16) = 00111010 00010100 00011000 00010000 L15.R14= 01101010 11101000 10101111 01000111 ----------XOR R16 = 01010000 11111100 10110111 01010111

3.3.2 Proses Dekripsi

Dekripsi yaitu kebalikan dari proses enkripsi yaitu proses konversi data yang sudah dienkripsi (ciphertext) kembali menjadi data aslinya (Original Plaintext) sehingga dapat dibaca atau dimengerti kembali.Pesan yang akan dienkripsi disebut plaintext yang dimisalkan plaintext (P), proses enkripsi dimisalkan enkripsi (E), proses dekripsi dimisalkan dekripsi (D), dan pesan yang sudah dienkripsi disebut ciphertext yang dimisalkan ciphertext (C)dalam proses enkripsi terdapat beberapa langkah-langkah sebagai berikut :

1. Melakukan Permutasi Terhadap Cipher Bit

Cipher dalam biner = atau dalam bentuk hexa = **01101011 10111000 11111001 11000000 1000010 11000111 11110101 11100100 = 54 52 55 48 48 41 59 55**

Kemudian bit pada cipher dipecah menjadi 2 bagian yaitu L0 dan R0, sehingga hasilnya sebagai berikut:

L0 = 11101101 01000110 01100000 01100101

R0 = 11111110 11000101 00000111 00110001

Lakukan perhitungan kembali:

16	P(B16) = 11101110 01000100 10111000 10101001 L15 = 01101101 01000110 11100000 01100101 ---------- XOR R16 = 10000011 00000010 01011000 11001100
15	P(B15) = 00011100 00000001 00100110 10010010 L14 = 11111110 11000111 00000111 00110001 ---------- XOR R15 = 11100010 11000110 00100001 10100011
14	P(B14) = 10000010 00110001 01000000 00001110 L13 = 01100001 01001100 10101010 11010111 ---------- XOR R14 = 11100011 01111101 11101010 11011001
13	P(B13) = 10100100 01010011 01010000 10110010 L12 = 11100010 11000110 00100001 10100011 ---------- XOR R13 = 01000110 10010101 01110001 00010001
12	P(B12) = 01010010 11010101 00101000 00010000 L11 = 11000101 00011111 11111010 01110101 ---------- XOR

	R12 = 10010111 11001010 11010010 01100101
11	P(B11) = 11100010 01100100 10100000 10110000 L10 = 10010111 11001010 11110010 01110101 --- XOR R11 = 01110101 10101110 01010010 11000101
10	P(B10) = 00100010 00010000 11001000 00010110 L9 = 101010111 10101110 01010010 11000101---------- ----------XOR R10 = 100010101 101101110 10011010 11010011
9	P(B9) = 10001100 01000100 11001100 10000110 L8 = 11100111 11010100 01100011 11111100 --- XOR R9 = 01101011 10010000 10101111 01111010
8	P(B8) = 00000110 00111111 00111010 00001100 L7 = 01100101 11110000 11111000 01110111 --- XOR R8 = 01100011 11001111 11000010 01111011
7	P(B7) = 10100100 00101001 10010010 00001000 L6 = 01100011 11001111 11000010 01111011 --- XOR R7 = 11000111 11100110 01010000 01110011
6	P(B6) = 00110000 01010010 10100110 10000110 L5 = 11000111 11100110 01010000 01110011 --- XOR R6 = 11110111 10110100 11110110 11110101
5	P(B5) = 00000000 01100010 01101110 10101000 L4 = 11110111 10110100 11110110 11110101 --- ---XOR R5 = 11110111 11010110 10011000 01011101
4	P(B4) = 11110111 10000010 00001001 11000010 L3 = 11110111 11010110 10111000 01011101---------- ----------XOR R4 = 00000000 01010100 10110001 10000011
3	P(B3) = 11000110 00100000 11011010 10000110 L2 = 00000000 01010100 10110001 10011111 --- ---XOR R3 = 11000110 01110100 01101011 00011001
2	P(B2) = 00101010 00110000 00111001 10001000 L1 = 11000110 01110100 01101011 00011001 --- ---XOR R2 = 11101100 01000100 01010010 10010001
1	P(B1) = 11101100 01000100 00001010 10001011 L0 = 11101100 01000100 01010010 10010001 --- ---XOR R1 = 00000000 00000000 01011000 00011010

Menghasilkan *output*:

Cipher dalam biner = **01010100 01010010 01010101 01001011 01001011 01000001 01011101 11110101** Cipher dalam bentuk hexa = **54 52 55 4B 4B 41 5D F5**

Dan dalam bentuk karakter (*plaintext*) = **"TRUKKAYU"**

4 PENGUJIAN DAN IMPLEMENTASI

Dalam implementasi dan pengujian program keamanan data transaksi biaya sewa angkutan truk dengan metode DES membutuhkan 2 buah perangkat yaitu, perangkat lunak (Software) dan perangkat keras (Hardware).

4.1 Implementasi

Berikut hasil sistem implementasi metode DES (Data Encryption Standard) untuk keamanan data transaksi biaya sewa angkutan truk di PTPN II.

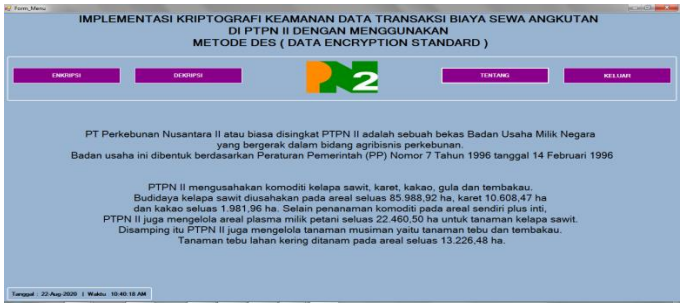
4.1.1 Tampilan Halaman Menu Utama Sebelum Akses Login

Menu form login merupakan sebuah tampilan menu awal dari program yang dimana user akan mengisi user name dan password untuk bisa masuk atau login ke menu utama. Gambar tampilan form login dapat dilihat pada gambar dibawah ini :

Gambar 4.1 Halaman Menu Utama Sebelum Akses Login

4..1.2 Tampilan Halaman Menu Utama Setelah Akses Login

Berikut ini merupakan menu utama dari Data Transaksi Biaya Sewa Angkutan Truk berfungsi untuk memunculkan form sesuai nama sub menunya. Gambar halaman utama aplikasi keamanan data ini dapat dilihat dibawah ini:



Gambar 4.2 Halaman Menu Utama Setelah Akses Login

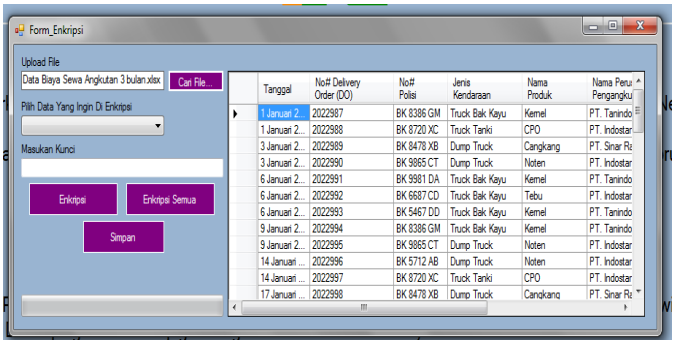
4.2 Pengujian Sistem

Setelah melalui tahap implementasi maka langkah selanjutnya adalah melakukan pengujian sistem. Berikut dibawah ini tahap pengujian sistem.

4.2.1 Proses Enkripsi

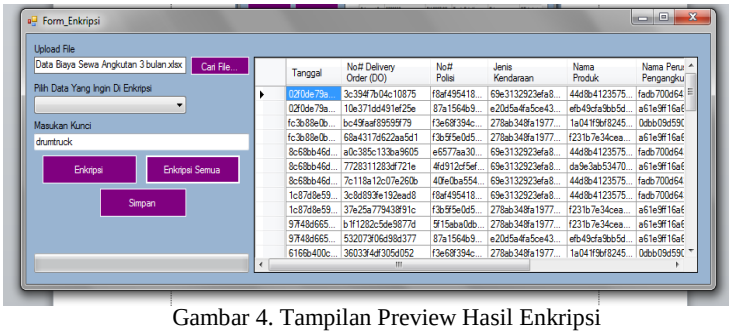
Proses enkripsi ini berfungsi untuk melakukan proses perubahan data atau penyamaran data tetapi sebelum melakukan enkripsi data tersebut bisa memanipulasi seperti tambah, ubah, dan hapus. Prosesnya ialah :

1. Mengunggah file excel lalu file excel akan ditampilkan kedalam list view



Gambar 3. Tampilan Preview Tampil Data

1. Setelah itu masukkan kunci enkripsi di kolom kunci kemudian melakukan proses enkripsi dengan cara menekan tombol enkripsi atau enkripsi semua, lalu hasilnya akan di tampilkan kedalam list view. Tampilkan form sebagai berikut:

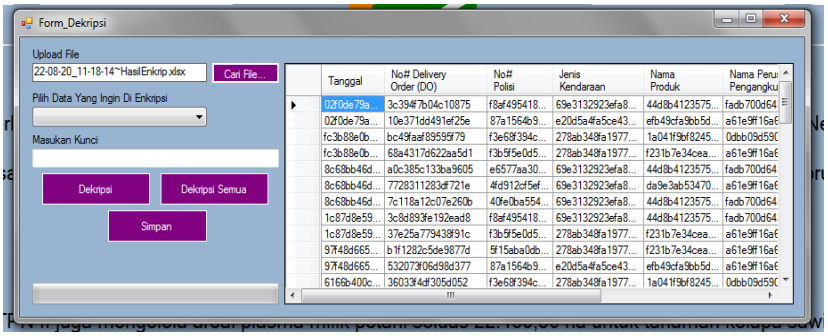


Gambar 4. Tampilan Preview Hasil Enkripsi

4.2.2 Proses Dekripsi

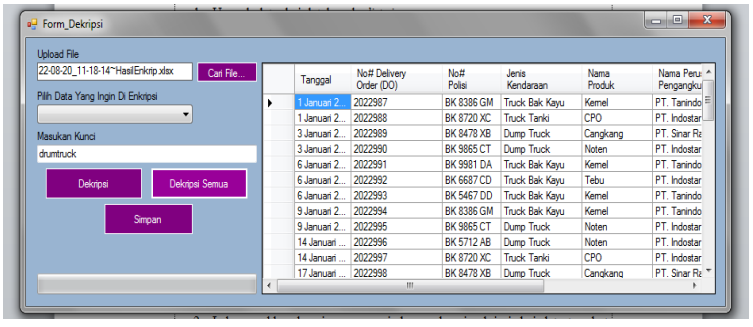
Proses Dekripsi ini berfungsi untuk melihat data yang sebenarnya setelah di enkripsi. Proses nya ialah :

1. Unggah data dari database ke list view.



Gambar 5.Tampilan Preview Data Dekripsi

2. Lalu masukkan kunci yang sesuai dengan kunci enkripsi dari data tersebut, lalu tekan tombol dekripsi atau tombol dekripsi semua. Hasil dekripsi nya dapat dilihat dibawah ini :



Gambar 6. Tampilan Preview Hasil Dekripsi

5 Kesimpulan

Berdasarkan analisa pada permasalahan yang terjadi dalam kasus yang diangkat tentang Implementasi Kriptografi Keamanan Data Transaksi Biaya Sewa Angkutan Truk Di PTPN II Mengunakan Metode DES (Data Encryption Standard) maka dapat ditarik kesimpulan sebagai berikut :

1. Dengan menggunakan metode DES (Data Encryption Standard) dapat membantu mengamankan Data Transaksi Biaya Sewa Angkutan Truk di PTPN II.
2. Aplikasi yang dirancang dapat menjadi solusi pemecah masalah dalam hal pengamanan data transaksi biaya sewa angkutan truk di PTPN II.
3. Mengimplementasikan aplikasi pengamanan data e – rapor menggunakan metode DES dapat mengingkatkan keamanan data.

UCAPAN TERIMA KASIH

Puji syukur kehadirat Allah SWT atas izin-Nya yang telah melimpahkan rahmat dan karunia-Nya sehingga dapat menyelesaikan jurnal ilmiah ini. Pada kesempatan ini diucapkan terima kasih yang sebesar-besarnya kepada Ibunda terkasih Ny. Supiyati atas doa dan dukungan, serta arahan dan bantuan dari berbagai pihak. Oleh karena itu dengan segala kerendahan hati, diucapkan terima kasih yang sebesar-besarnya kepada Bapak Rudi Gunawan, SE., M.Si., selaku Ketua Sekolah Tinggi Manajemen Informatika Dan Komputer (STMIK) Triguna Dharma Medan. Bapak Dr. Zulfian Azmi, ST., M.Kom., selaku Wakil Ketua I Bidang Akademik STMIK Triguna Dharma Medan. Bapak Marsono, S.Kom., M.Kom., selaku Ketua Program Studi Sistem Informasi STMIK Triguna Dharma Medan. Bapak Nurcahyo Budi Nugroho, S.Kom., M.Kom., selaku Dosen Pembimbing I yang telah memberikan saran, arahan, dukungan serta motivasi, sehingga penelitian ini dapat terselesaikan dengan baik dan tepat waktu. Bapak Sri Murniyanti, S.S., M.M., selaku Dosen Pembimbing II yang telah memberikan bimbingan tata cara penulisan, saran dan motivasi sehingga penelitian ini dapat terselesaikan dengan baik dan tepat waktu. Seluruh Dosen, Staff dan Pegawai di STMIK Triguna Dharma Medan.

REFERENSI

[1] M. K. Harahap, "Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad," InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan), vol. 1, no. 1, pp. 61–64, 2016, doi: 10.30743/infotekjar.v1i1.43.

[2] A. Tantoni and M. T. A. Zaen, "Implementasi Double Caesar Cipher Menggunakan Ascii," J. Inform. dan Rekayasa Elektron., vol. 1, no. 2, p. 24, 2018, doi: 10.36595/jire.v1i2.56.

[3] P. Sulistyorini, "Pemodelan Visual dengan Menggunakan UML dan Rational Rose," J. Teknol. Inf. Din. Vol., vol. XIV, no. 1, pp. 23–29, 2009.

[4] D. A. Meko, "Jurnal Teknologi Terpadu Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , STIMIK Kupang Jurnal Teknologi Terpadu," J. Teknol. Terpadu, vol. 4, no. 1, pp. 8–15, 2018.

[5] M. Hudori, "Perencanaan Kebutuhan Kendaraan Angkutan Tandan Buah Segar di Perkebunan Kelapa Sawit," Ind. Eng. J., vol. 5, no. 1, pp. 22–27, 2016,[Online].Available: https://www.journal.unimal.ac.id/miej/article/download/147/117.

[6] S. Santoso and R. Nurmalina, "Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas (Studi Kasus Politeknik Negeri Tanah Laut)," J. Integr., vol. 9, no. 1, pp. 84–91, 2017.

[7] M Teguh Prihandoyo, "Unified Modeling Language (UML) Model Untuk Pengembangan Sistem Informasi Akademik Berbasis Web," J. Inform. J. Pengemb. IT, vol. 3, no. 1, pp. 126–129, 2018.

[8] D. Wira, T. Putra, and R. Andriani, "Unified Modelling Language (UML) dalam Perancangan Sistem Informasi Permohonan Pembayaran Restitusi SPPD," vol. 7, no. 1, 2019.

[9] A. A. Permana, D. Nurnaningsih, P. Studi, T. Informatika, F. Teknik, and U. M. Tangerang, "Application of cryptography with data encryption standard (des) algorithm in picture 1,2," pp. 9–14, 2020.

[10] A. Priatmoko and E. Harahap, "Implementasi Algoritma DES Menggunakan MATLAB," Matematika, vol. 16, no. 1, pp. 11–19, 2017, doi: 10.29313/jmtm.v16i1.3360.

[11] M. M. Amin, "Komunikasi Berbasis Teks," J. Pseudocode, vol. III, no. September, pp. 129–136, 2016.

[12] M. Natsir, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java," J. Format, vol. 6, no. 1, p. 93, 2017.

[13] Verawati and P. D. Liksha, "Aplikasi Akuntansi Pengolahan Data Jasa Service Pada Pt. Budi Berlian Motor Lampung," J. Sist. Inf. Akunt., vol. 1, no. 1, pp. 1–14, 2018.

[14] P. A. Udayana and N P. Sastra , "Perbandingan Performansi Pengamanan File Backup LPSE Menggunakan Algoritma DES Dan AES," *Teknologi Elektro, Vol. 15, No. 01, Januari - Juni 2016.*

[15] F. S. Mawu and T. K. Sendow, J .E Waani, "TINJAUAN TARIF ANGKUTAN UMUM DALAM KOTA AKIBAT PERUBAHAN HARGA BBM (STUDI KASUS : TRAYEK PUSAT KOTA - MALALAYANG)," Jurnal Sipil Statik Vol.4 No.3 Maret 2016 (165-173) ISSN: 2337-6732.

[16] B. S. Hasugian, " PERANAN KRIPTOGRAFI SEBAGAI KEAMANAN SISTEM INFORMASI PADA USAHA KECIL DAN MENENGAH," Jurnal Warta Edisi : 53 Juli 2017 | ISSN : 1829 – 7463.

[17] A.A. Permana and D. Nurnaningsih, " RANCANGAN APLIKASI PENGAMANAN DATA DENGAN ALGORITMA *ADVANCED ENCYPTION STANDARD (AES)," JURNAL TEKNIK INFORMATIKA VOL 11 NO. 2, OKTOBER 2018.*

[18] D. Ritonga and J. A. Timboeleng, Oscar H. Kaseke, "ANALISA BIAYA TRANSPORTASI ANGKUTAN UMUM DALAM KOTA MANADO AKIBAT KEMACETAN LALU LINTAS (Studi Kasus: Angkutan Umum Trayek Pusat Kota 45-Malalayang)," Jurnal Sipil Statik Vol.3 No.1, Januari 2015 , pp. 58-67.

[19] D. Adhar, "IMPLEMENTASI ALGORITMA DES (DATA ENCRYPTION STANDARD) PADA ENKRIPSI DAN DESKRIPSI SMS BERBASIS ANDROID," Jurnal Teknik Informatika Kaputama (JTIK) Vol. 3 , No. 2, Juli 2019, pp. 53-60.

[20] D. A. Ramadhan, J. Soesatrijo, and T. Suryanto, "Perbandingan Alat Transportasi Tandan Buah Segar (TBS) antara Dump truck dan Truk Bak Kayu pada Masa Tanaman Menghasilkan", Jurnal Citra Widya Edukasi Vol XI No. 2 Agustus 2019, pp.151-164.

BIOGRAFI PENULIS

	**Dela Oktami.** Kelahiran TG. Morawa, 03 Oktober 1997, anak pertama dari dua bersaudara ini merupakan seorang mahasiswa STMIK Triguna Dharma yang sedang dalam proses menyelesaikan skripsi.
	**Nurcahyo Budi Nugroho, S.Kom., M.Kom.** Beliau merupakan dosen tetap di STMIK Triguna Dharma Medan dan aktif sebagai pengajar pada bidang ilmu Sistem Informasi.
	**Sri Murniyanti, S.S., M.M.** Beliau merupakan dosen tetap di STMIK Triguna Dharma Medan dan aktif sebagai pengajar pada bidang ilmu Sistem Informasi.