Jurnal CyberTech

Vol.2. No.2, Februari 2019, pp. 297~311
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Implementasi Kriptografi Dengan Metode AES(Advance Encryption Standard) Untuk Mengamankan Data Penjualan Di Toko Sweet Amirah

Astri Handayani*, Nurcahyo Budi Nugroho, Rico Imanta Ginting****

* Sistem Informasi (SI), STMIK Triguna Dharma
** Sistem Informasi (SI), STMIK Triguna Dharma

Article Info

Article history:
Received Feb 12th, 2019
Revised Feb 20th, 2019
Accepted Feb 30th, 2019

Keyword:
Kriptografi
Metode AES
Data Penjualan
Toko Sweet Amirah

ABSTRACT

Perusahaan Swasta besar ataupun perusahaan kecil, biasanya mereka juga memiliki beberapa aset data ataupun informasi yang bersifat privasi, contohnya : data keuangan, data client dan data penjualan. Adapun salah satu usaha di kota medan yang memiliki data yang sangat penting dan untuk melindungi dari kecurangan adalah usaha Toko Sweet Amirah yang salah satu cabang toko di Komplek JCity. Dimana setiap toko cabang memiliki data penjualan yang berisikan dari hasil penjualan toko dan stok toko. Data penjualan ini sangat penting bagi perusahaan, dikarenakan jika terdapat kecurangan maka akan mengalami kerugian yang sangat fatal. Maka dari itu, pemilik usaha ingin menerapkan suatu sistem yang dapat melindungi data penjualan mereka agar data menjadi privasi dan tidak dapat dilakukan perubahan secara sembarangan

Berdasarkan penjelasan permasalahan yang diterangkan diatas, ada pengetahuan dalam bidang keamanan yaitu kriptografi yang dapat digunakan dalam pengamanan data yang dimiliki oleh Toko Sweet Amirah untuk menjaga kerahasian data penjualan dari pihak-pihak yang tidak berhak mengetahui data tersebut. Kriptografi merupakan pengetahuan dan seni untuk melindungi kerahasiaan pesan (data atau informasi) dengan teknik merahasiakan ke dalam bentuk kode yang tidak memiliki arti. Dimana salah satu metode yang dapat digunakan dalam proses keamanan data dan memiliki keamanan yang cukup baik adalah metode AES.

Adapun hasil keamanan yang akan didapatkan dengan menggunakan metode AES ini adalah kemanan data yang dengan tingkat keamanan yang cukup baik, data akan diamankan dengan menggunakan kunci yang telah dibuat dan dirahasiakan. Hasil enkripsi dari metode AES dalam sistem ini yaitu berupa karakter.

Corresponding Author: First Author
Nama : Astri Handayani
Program Studi : Sistem Informasi
STMIK Triguna Dharma
Email: astrihanday@gmail.com

1. PENDAHULUAN

Pada zaman sekarang ini perkembangan teknologi informasi sangatlah cepat. Baik itu *hardware* maupun *software*, orang-orang yang berhubungan dengan teknologi atau seorang pengembang dalam dunia teknologi terus melakukan perubahan dengan menyesuaikan kebutuhan manusia. Tentunya, hal ini sangat baik untuk dapat membantu pekerjaan manusia, namun sisi negatifnya juga pasti ada. Semakin berkembangnya teknologi, maka sudah dapat dipastikan kita bisa mendapatkan sumber informasi secara

cepat dan bisa dari belahan dunia manapun. Adapun sisi negatif dari perkembangan teknologi ini tentunya bagi beberapa orang maupun instansi perusahaan sangatlah menjadi hal yang harus diwaspadai, dikarenakan mereka mempunyai data atau informasi khusus (privasi) dan tidak boleh diketahui oleh pihak lain yang tidak ikut berkepentingan didalamnya.

Perusahaan Swasta besar ataupun perusahaan kecil, biasanya mereka juga memiliki beberapa aset data ataupun informasi yang bersifat privasi, contohnya : data keuangan, data client dan data penjualan. Adapun salah satu usaha di kota medan yang memiliki data yang sangat penting dan untuk melindungi dari kecurangan adalah usaha Toko Sweet Amirah yang salah satu cabang toko di Komplek JCity. Dimana setiap toko cabang memiliki data penjualan yang berisikan dari hasil penjualan toko dan stok toko. Data penjualan ini sangat penting bagi perusahaan, dikarenakan jika terdapat kecurangan maka akan mengalami kerugian yang sangat fatal. Maka dari itu, pemilik usaha ingin menerapkan suatu sistem yang dapat melindungi data penjualan mereka agar data menjadi privasi dan tidak dapat dilakukan perubahan secara sembarangan.

Berdasarkan penjelasan permasalahan yang diterangkan diatas, ada pengetahuan dalam bidang keamanan yaitu kriptografi yang dapat digunakan dalam pengamanan data yang dimiliki oleh Toko Sweet Amirah untuk menjaga kerahasian data penjualan dari pihak-pihak yang tidak berhak mengetahui data tersebut.

Kriptografi merupakan pengetahuan dan seni untuk melindungi kerahasiaan pesan (data atau informasi) dengan teknik merahasiakan ke dalam bentuk kode yang tidak memiliki arti [1]. Untuk metode yang dapat digunakan mengamankan data transaksi member Toko Sweet Amirah agar mempunyai tingkat keamanan yang tinggi maka akan digunakan metode AES.

Metode AES adalah algoritma *chipher* blok menggunakan teknik substitusi, pemutasian dan sejumlah putaran pada setiap blok yang akan di enkripsi dan deskripsi [2]. AES mempunyai keunggulan dalam keamanan, kecepatan dan karakteristik algoritma beserta implementasinya [3].

Adapun sebagai penguat digunakan Metode AES dalam mengamankan data penjualan di Toko Sweet Amirah, sebagai referensinya adalah penelitian yang telah dilakukan berdasarkan jurnal "Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store" dimana penelitian dilakukan di Ramayana Department Store oleh Sunil Setti dkk [4].

2. KAJIAN PUSTAKA

2.1 Pengertian Penjualan

Penjualan adalah sejumlah total yang dikenakan kepada pelanggan untuk barang dagangan yang dijual, termasuk penjualan tunai dan kredit. Penjualan bisa diartikan dengan proses pemenuhan kebutuhan penjual dan pembeli baik secara tunai maupun kredit [5].

Penjualan merupakan salah satu fungsi pemasaran yang sangat penting dan menentukan bagi perusahaan dalam mencapai tujuan perusahaan yaitu memperoleh laba untuk menjaga kelangsungan hidup perusahaan [6].

2.2 Kriptografi (Security System)

Kriptografi (Cryptography) berasal dari bahasa yunani, Cyptos artinya secret atau rahasia sedangkan graphein berarti: writing atau tulisan. Sehingga kriptografi berarti secret writing atau tulisan rahasia. Menurut Bruce Scheiner (1996): Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan sedangkan menurut Menezes (1996) [7]: kriptografi adalah limu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi dan anti penyangkalan. Kriptografi dapat diartikan sebagai ilmu untuk menjaga kerahasiaan informasi dengan metode dan teknik matematika yang mencakup *confidentiality*, *integrity*, *authentication* dan *non*-repudiation.

Kriptografi adalah suatu bidang ilmu atau seni yang mempelajari tentang mekanisme dalam menjaga kerahasiaan pesan. Dalam menjaga kerahasiaan pesan, pesan tersebut akan diubah menjadi data acak atau data yang disandi sehingga hanya pengguna yang memiliki akses terhadap pesan tersebut yang dapat membaca isi pesan Kriptografi merupakan suatu teknik penyembunyian pesan dimana pesan tersebut hanya dapat diketahui oleh orang tertentu dimana pesan itu sering disebut dengan enkripsi [8].

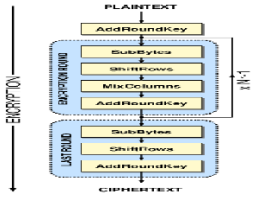
2.3 Metode AES(Advanced Cryption Standard)

Pada November 2001 *National Institute of Standard and Technology* (NIST) mensosialisasikan sebuah standar baru enkripsi yang dikembangkan dari algoritma DES (Data Encryption Standard) melalui seleksi ketat dengan algoritma lainya dan diberi nama Algoritma *Advanced Encryption Standard* (AES) atau

algoritma Rijindael. Algoritma ini dicetuskan oleh Vincent Rijmen dan Joan Daemen yang menjadi pemenang saat lomba seleksi algoritma baru pengganti DES. “Alasan utama terpilihnya algoritma ini adalah algoritma ini memiliki keseimbangan antara keamanan serta fleksibilitas dalam berbagai platform software dan hardware”[10].

AES sendiri memiliki tipe yang terbagi berdasarkan panjang blok data seperti AES128, AES-192, AES-256 dimana masingmasing AES memiliki panjang blok sebanyak 128 bit, 192 bit, dan 256 bit. Berikut ilustrasi enkripsi dan dekripsi AES [12]:

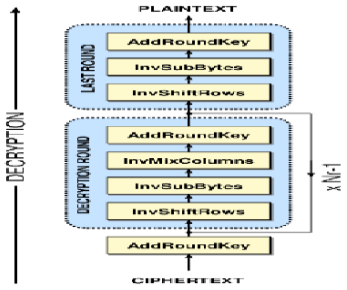
1. Enkripsi AES



Gambar 2.1 Enkripsi AES

Gambar 2.1 Menjelaskan tentang Proses enkripsi AES 128 bit dengan key dan plaintext 128 bit yaitu pertama Addroaundkey, Subbyte, Shiftrows, dan Mixcolumns sebanyak 10 kali putaran. Namun pada putaran terakhir tidak dilakukan lagi proses Mixcolumns langsung ke proses Addraoundkey.

2. Deskripsi AES



Gambar 2.8 Deskripsi AES

Gambar 2.8 menjelaskan tentang alur dari proses dekripsi AES proses ini merupakan proses kebalikan dari proses enkripsi yakni InvAddrows, invShiftrows, InvSubbyte, dan InvMixcolumns, dengan kunci round yang sama dengan proses enkripsi [12].

3. METODE PENELITIAN

3.1 Metode Penelitian

Metode penelitian adalah cara ilmiah yang dilakukan untuk mendapatkan suatu informasi atau data yang dibutuhkan untuk keperluan dalam penelitian. Metode penelitian ini digunakan agar mendapatkan informasi atau data yang valid agar dapat dikembangkan menjadi suatu informasi yang dapat membantu dalam pekerjaan. Adapun metode penelitian yang digunakan dalam penelitian ini yaitu:

1. *Data Collecting* atau Pengumpulan Data
   Dalam proses pengumpulan data yang dilakukan dalam penelitian ini ada 2 tahapan yang dilakukan, yaitu:
   a. Observasi
      Observasi yang dilakukan adalah dengan cara melakukan pengamatan langsung ke tempat riset yaitu Toko Sweet Amirah. Observasi ini dilakukan untuk mencari sumber informasi dan data yang diperlukan.
   b. Wawancara
      Wawancara yang dilakukan adalah dengan cara melakukan tanya jawab secara langsung kepada pemilik usaha Toko Sweet Amirah untuk memenuhi kebutuhan data riset dan untuk validasi data.
2. Studi Literatur atau Kajian Pustaka

Dalam studi literatur dilakukan dengan cara mengumpulkan data referensi sebagai bahan untuk mendukung memenuhi kebutuhan yaitu referensi dari kebutuhan penelitian ini. Adapun referensi yang digunakan adalah referensi dari 19 jurnal nasional dan 1 buku untuk sebagai pendukung penelitian ini.

3.2 Algoritma Sistem

Algoritma sistem ini merupakan langkah yang sistematis digunakan untuk memecahkan suatu permasalahan. Setiap susunan logis yang diurutkan berdasarkan sistematika tertentu yang dipakai untuk menyelesaikan permasalahan termasuk sebagai sebuah algoritma. Algoritma sistem pada penelitian ini akan digambarkan dengan *flowchart.*

3.3.1 Penyelesaian Metode AES

Adapun penyelesaian metode AES dalam penelitian ini yaitu dengan melakukan pengenkripsian Transaksi Data Member pada Toko Sweet Amirah. Adapun contoh yang akan di enkripsi yaitu dengan Plaintext: Mentari dan Key: TOKOSWEETAMIRAHH. Adapun proses penyelesaian enkripsi dan dekripsi dari contoh data yang akan di amankan adalah sebagai berikut:

1. Perhitungan Enkripsi
   Plaintext: Mentari (16 ASCII characters)
   Plaintext dalam Hexadecimal (128 bits): 4D 45 4E 54 41 52 49 14 14 14 14 14 14 14 14 14
   Key: TOKOSWEETAMIRAHH (16 ASCII characters)
   Key dalam Hexadecimal (128 bits): 54 4F 4B 4F 53 57 45 45 54 41 4D 49 52 41 48 48
   a. Key Schedule

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 3.4 Nilai S-Box

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Gambar 3.5 Nilai Rcon

Dengan menggunakan

				Wi-1 Wi				Wi-2 Wi					Wi-10 Wi			
54	53	54	52													
4F	57	41	41													
4B	45	4D	48									…				
4F	45	49	48													

Mencari nilai Wi-1 Wi:

41		83	
48	=	52	SubBytes
48		52	
52		00	

54		83		01		D6
4F	□	52	□	00	=	1D
4B		52		00		19

4F	00	00	4F

Adapun perhitungan secara manualnya seperti berikut:
54 (Hex) = 01010100
83 (Hex) = 10000011
01 (Hex) = 00000001 □
Hasil = 11010110 (Bin) = D6 (Hex)

				Wi-1 Wi				Wi-2 Wi					Wi-10 Wi			
54	53	54	52	D6												
4F	57	41	41	1D												
4B	45	4D	48	19								…				
4F	45	49	48	4F												

53		D6	=	85
57	□	1D		4A
45		19		5C
45		4F		A

Adapun perhitungan secara manualnya seperti berikut:
53 (Hex) = 01010011
D6 (Hex) = 11010110 □
Hasil = 10000101 (Bin) = 85 (Hex)
Dengan dilakukan perhitungan seperti jalan di atas, maka didapatkan hasil untuk Key Schedule sebagai berikut:

				Wi-1 Wi				Wi-2 Wi					Wi-10 Wi			
54	53	54	52	D6	85	D1	83	02	87	56	D5		52	31	4F	31
4F	57	41	41	1D	4A	0B	4A	D6	9C	97	DD		94	40	B1	5B
4B	45	4D	48	19	5C	11	59	32	6E	7F	26	…	8C	14	EE	A1
4F	45	49	48	4F	0A	43	0B	A3	A9	EA	E1		20	A4	2D	66

Cipher Key Round 1 Round 2 Round 10

b. SubBytes

4D	41	14	14		54	53	54	52		19	12	40	46
45	52	14	14	□	4F	57	41	41	=	0A	05	55	55
4E	49	14	14		4B	45	4D	48		05	0C	59	5C
54	14	14	14		4F	45	49	48		1B	51	5D	5C

19	12	40	46		D4	C9	09	5A
0A	05	55	55	Konversi dengan	67	6B	FC	FC
05	0C	59	5C	menggunakan S-Box =	6B	FE	CB	4A
1B	51	5D	5C		AF	D1	4C	4A

c. ShiftRows

D4	C9	09	5A	
67	6B	FC	FC	<----- Rotate over 1 byte
6B	FE	CB	4A	
AF	D1	4C	4A	

D4	C9	09	5A
6B	FC	FC	67
6B	FE	CB	4A
AF	D1	4C	4A

D4	C9	09	5A

6B	FC	FC	67
CB	4A	6B	FC
AF	D1	4C	4A

<----- Rotate over 2 byte

D4	C9	09	5A
6B	FC	FC	67
CB	4A	6B	FC
AF	D1	4C	4A

D4	C9	09	5A
6B	FC	FC	67
CB	4A	6B	FC
4A	AF	D1	4C

<----- Rotate over 3 byte

D4	C9	09	5A
6B	FC	FC	67
CB	4A	6B	FC
4A	AF	D1	4C

d. MixColumns

D4	C9	09	5A
6B	FC	FC	67
CB	4A	6B	FC
4A	AF	D1	4C

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} D4 \\ 6B \\ CB \\ 4A \end{bmatrix}$$

Karena hasil untuk kolom pertama sudah didapatkan, maka dilakukan perhitungan untuk kolom berikutnya sehingga didapatkan hasil akhir dari MixColumn sebagai berikut:

D4	C9	09	5A
6B	FC	FC	67
CB	4A	6B	FE
4A	AF	D1	4C

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} D4 \\ 6B \\ CB \\ 4A \end{bmatrix} = \begin{bmatrix} 8F \\ 0E \\ EC \\ 53 \end{bmatrix}$$

Hasil MixColumnnya adalah sebagai berikut:

8F	73	B7	AF
0E	5B	86	C1
EC	4B	4B	0E
53	B3	35	EF

e. AddRoundKey

Adapun Pencarian AddRoundKey 1 adalah sebagai berikut:

8F	73	B7	AF
0E	5B	86	C1
EC	4B	4B	0E
53	B3	35	EF

MixColumn

□

D6	85	D1	83
1D	4A	0B	4A
19	5C	11	59
4F	0A	43	0B

RoundKey 1

=

59	F6	66	2C
13	11	8D	8B
F5	17	5A	57
1C	B9	76	E4

AddRoundKey 1

Untuk cara perhitungannya dengan melakukan Xor terhadap kolom MixColumn dengan RoundKey, dengan contoh sebagai berikut:

8F		D6	=	59	------>
0E		1D			
EC		19			
53		4F			

8F (Hex) = 1000 1111 (Bin)
D6 (Hex) = 1101 0110 (Bin)
Hasil Xor = 0101 1001 (Bin) = 59 (Hex)

Dengan cara yang sama, sehingga dihasilkan untuk AddRoundKey 1 sebagai berikut:

59	F6	66	2C
13	11	8D	8B
F5	17	5A	57
1C	B9	76	E4

Untuk mendapatkan hasil akhir dari Enkripsi Metode AES, lakukan 4 tahapan proses transformasi tersebut dilakukan sembilan kali lagi (dengan total sepuluh kali transformasi). Namun, untuk transformasi MixColumns tidak dilakukan pada transformasi terkahir (ke-10).

	Round 2				Round 3			
After SubBytes	CB	42	33	71	A6	26	C6	BC
	7D	82	5D	3D	37	59	56	4D
	E6	F0	BE	5B	5C	BC	4A	EE
	9C	56	38	69	2B	D6	E8	73
After ShiftRows	CB	42	33	71	A6	26	C6	BC
	82	5D	3D	7D	59	56	4D	37
	BE	5B	E6	F0	4A	EE	5C	BC
	69	9C	56	38	73	2B	D6	E8
After MixColumns	C7	A4	91	AD	85	73	CA	6E
	64	89	2E	B8	B9	88	6E	E5
	95	16	23	BF	FE	CA	52	CB
	A8	E3	22	6E	04	84	F7	9F
Round Key	02	87	56	D5	C7	40	16	C3
	D6	9C	97	DD	21	BD	2A	F7
	32	6E	7F	26	CA	A4	DB	FD
	A3	A9	EA	E1	A0	09	E3	02
After AddRoundKey	C5	23	C7	78	42	33	DC	AD
	B2	15	B9	65	98	35	44	12
	A7	78	5C	99	34	6E	89	36
	0B	4A	C8	8F	A4	8D	14	9D

Sampai hasil AddRoundKey ke-10 sebagai berikut:

Round 10

E5	6C	99	B4
21	E1	33	6E
2E	72	BE	E5
DD	9D	2B	57

E5	6C	99	B4
E1	33	6E	21
BE	E5	2E	72
57	DD	9D	2B

52	31	4F	31
94	40	B1	5B
8C	14	EE	A1
20	A4	2D	66

=

B7	5D	D6	85
75	73	DF	7A
32	F1	C0	D3
77	79	B0	4D

Dari hasil perhitungan di atas, maka didapatkan hasil Enkripsi dengan bilangan Hexadecimal: B7 75 32 77 5D 73 F1 79 D6 DF C0 B0 85 7A D3 4D. Untuk penjabaran hasil dari Enkripsinya adalah sebagai berikut:

Tabel 3.1 Hasil Enkripsi

No.	Round	Kode ASCII	Karakter
1	B7	183	.
2	75	117	u
3	32	50	2
4	77	119	w
5	5D	93	]
6	73	115	s
7	F1	241	ñ
8	79	121	y
9	D6	214	Ö
10	DF	223	ß
11	C0	192	À
12	B0	176	o
13	85	133	...
14	7A	122	z
15	D3	211	Ó
16	4D	77	m

2. Perhitungan Dekripsi
   Untuk melakukan dekripsi data dari hasil Enkripsi sebelumnya yaitu dengan menggunakan kunci yang sama pada proses Enkripsi. Berikut adalah proses dekripsi dari hasil Ciphertext yang telah diperoleh dari proses Enkripsi.

B7	75	32	77	5D	73	F1	79	D6	DF	C0	B0	85	7A	D3	4D

Kemudian susun 16 *byte* pertama dari Ciphertext yang telah diubah ke bentuk Hexadecimal ke dalam state 4x4:

B7	5D	D6	85
75	73	DF	7A
32	F1	C0	D3
77	79	B0	4D

Lakukan XOR antara Ciphertext dengan RoundKey Ke-10. Proses ini dinamakan AddInvRoundKey.

B7	5D	D6	85
75	73	DF	7A

⊕

52	31	4F	31
94	40	B1	5B

=

E5	6C	99	B4
E1	33	6E	21

32	F1	C0	D3
77	79	B0	4D

8C	14	EE	A1
20	A4	2D	66

BE	E5	2E	72
57	DD	9D	2B

Proses AddInvRoundKey di atas masih dalam initial-round, dan akan menjadi masukan untuk ronde ke -1 yang akan diproses dengan 4 transformasi yaitu InvShiftRows, InvShiftRows, AddInvRoundKey dan InvMixColumns.

a. InvShiftRows, lakukan tahapan ini pada hasil initial-round dari AddInvRoundKey yang dieksekusi lewat pergeseran siklik secara memutar. Baris ke dua digeser secara siklik ke kiri tiga kali, baris ke tiga dua kali dan baris ke empat sekali.

E5	6C	99	B4
E1	33	6E	21
BE	E5	2E	72
57	DD	9D	2B

E5	6C	99	B4
21	E1	33	6E
2E	72	BE	E5
DD	9D	2B	57

b. Dari hasil InvShiftRows disubtitusikan dengan nilai pada tabel Inves S-Box, yang dapat dilihat pada gambar berikut:

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Gambar 3.6 Inves S-Box

E5	6C	99	B4
21	E1	33	6E
2E	72	BE	E5
DD	9D	2B	57

→

2A	B8	F9	C6
7B	E0	66	45
C3	1E	5A	2A
C9	75	0B	DA

c. XOR hasil dari InvSubBytes dengan RoundKey ke-9. Proses ini disebut AddInvRoundKey

2A	B8	F9	C6
7B	E0	66	45
C3	1E	5A	2A
C9	75	0B	DA

□

E3	63	7E	7E
10	D4	F1	EA
3F	98	FA	4F
D3	84	89	4B

=

C9	DB	87	B8
6B	34	97	AF
FC	86	A0	65
1A	F1	82	91

d. Hasil dari AddInvRoundKey ditransformasikan oleh InvMixColumns dengan mengoperasikan state kolom demi kolom. Operasi ini dilakukan pada state kolom, dengan mengkoversikan setiap kolom sebagai polinominal.

0E	0B	0D	09
09	0E	0B	0D
0D	09	0E	0B
0B	0D	09	0E

X

$S_{0.1}$
$S_{1.1}$
$S_{2.1}$
$S_{3.1}$

=

$S^{1}_{0.1}$
$S^{1}_{1.1}$
$S^{1}_{2.1}$
$S^{1}_{3.1}$

$$s^{0.1} = ([0E].S_{0.1}) \text{Xor } ([0B].S_{1.1}) \text{Xor} ([0D].S_{2.1}) \text{Xor} ([09].S_{3.1})$$
$$= ([0E].S_{0.1}) = (0E).(C9)$$
$$= ([0E].S_{0.1}) = (1110).(1100\ 1001)$$

$= ([0E].S_{0.1}) = (x^3 + x^2 + x)(x^7 + x^6 + x^3 + 1)$
$= ([0E].S_{0.1}) = x^{10} + x^9 + x^9 + x^8 + x^5 + x^8 + x^7 + x^4 + x + 1$
$= ([0E].S_{0.1}) = x(x^5 + x^4 + x + 1)x^7 + x^5 + x^4 + x + 1$
$= ([0E].S_{0.1}) = x^6 + x^5 + x^2 + x + x^7 + x^5 + x^4 + x + 1$
$= ([0E].S_{0.1}) = x^7 + x^6 + x^4 + x^2 + 1$
$= ([0E].S_{0.1}) = \mathbf{1101\ 0101}$
$= ([0B].S_{1.1}) = (0B).(6B)$
$= ([0B].S_{1.1}) = (1011).(0110\ 1011)$
$= ([0B].S_{1.1}) = (x^3 + x + 1)(x^6 + x^5 + x^3 + x + 1)$
$= ([0B].S_{1.1}) = x^9 + x^8 + x^6 + x^4 + x^3 + x^7 + x^5 + x^4 + x^2 + 1$
$= ([0B].S_{1.1}) = x^9 + x^6 + x^5 + x^2 + 1$
$= ([0B].S_{1.1}) = x(x^4 + x^3 + x + 1) + x^6 + x^5 + x^2 + 1$
$= ([0B].S_{1.1}) = x5+x4+x2 = ([0B].S_{1.1}) = x^5 + x^4 + x^2 + x + x^6 + x^5 + x^2 + 1$
$= ([0B].S_{1.1}) = x^6 + x^4 + x + 1$
$= ([0B].S_{1.1}) = \mathbf{0101\ 0011}$
$= ([0D].S_{2.1}) = (0D).(FC)$
$= ([0D].S_{2.1}) = (1101).(0110\ 1101)$
$= ([0D].S_{2.1}) = (x^3 + x^2 + 1)(x^6 + x^5 + x^3 + x^2 + 1)$
$= ([0D].S_{2.1}) = x^9 + x^8 + x^6 + x^5 + x^7 + x^5 + x^8 + x^7 + x^5 + x^4 + 1$
$= ([0D].S_{2.1}) = x^9 + x^6 + x^5 + x^4 + 1$
$= ([0D].S_{2.1}) = x(x^4 + x^3 + x + 1) + x^6 + x^5 + x^4 + 1$
$= ([0D].S_{2.1}) = x^5 + x^4 + x^2 + x) + x^6 + x^5 + x^4 + 1$
$= ([0D].S_{2.1}) = x^6 + x^5 + x^2 + x + 1$
$= ([0D].S_{2.1}) = \mathbf{0110\ 0111}$
$= ([09].S_{3.1}) = (09).(1A)$
$= ([09].S_{3.1}) = (1001).(1111\ 1001)$
$= ([09].S_{3.1}) = (x^3 + 1)(x^7 + x^6 + x^5 + x^4 + x^3 + 1)$
$= ([09].S_{3.1}) = x^{10} + x^9 + x^8 + x^7 + x^6 + 1$
$= ([09].S_{3.1}) = x(x^5 + x^4 + x + 1) + x(x^4 + x^3 + x + 1) + (x^4 + x^3 + x + 1) + x^7 + x^6 + 1$
$= ([09].S_{3.1}) = (x^6 + x^5 + x^2 + x) + (x^5 + x^4 + x^2 + x) + (x^4 + x^3 + x + 1) + x^7 + x^6 + 1$
$= ([09].S_{3.1}) = x^7 + x^3 + x$
$= ([09].S_{3.1}) = \mathbf{1000\ 1000}$

$s^{0.1} = 0001\ 0000 = 10$
$s^{1.1} = ([0E].S_{0.1})\text{Xor}([0B].S_{1.1})\text{Xor}([0D].S_{2.1})\text{Xor}([09].S_{3.1})$
$s^{1.1} = 1101\ 0011 = D3$
$s^{1.2} = ([0E].S_{0.2})\text{Xor}([0B].S_{1.2})\text{Xor}([0D].S_{2.2})\text{Xor}([09].S_{3.2})$
$s^{1.2} = 1010\ 1101 = AD$
$s^{1.3} = ([0E].S_{0.3})\text{Xor}([0B].S_{1.3})\text{Xor}([0D].S_{2.3})\text{Xor}([09].S_{3.3})$
$s^{1.3} = 0010\ 1010 = 2A$

Lakukan perulangan seperti yang di atas, hingga didapatkan hasil InvMixColumns seperti berikut:

C9	DB	87	B8
6B	34	97	AF
FC	86	A0	65
1A	F1	82	91

→

10	45	82	75
D3	46	14	62
AD	33	C1	75
2A	A8	65	81

Proses di atas diulang sampai 10 kali putaran (round). Berikut adalah hasil dari Dekripsi hingga round ke 10:

Round 1

2B	E8	0C	3F

Round 2

91	15	9B	38

Round 3

4F	77	92	28

6E	6D	BD	80
C7	98	7A	D3
DF	EB	9C	57

D0	B8	33	01
B0	94	2E	CD
9C	F3	8D	42

AC	48	67	38
12	5F	FE	7D
70	9E	DD	F2

Round 4

DA	FC	42	97
78	47	8D	95
C0	FA	F2	26
1E	DB	1E	51

Round 5

00	FC	12	9E
B7	B3	7A	59
0D	09	98	E3
F9	D2	FA	92

Round 6

85	73	CA	6E
B9	88	6E	E5
FE	CA	52	CB
04	84	F7	9F

Round 7

C7	A4	91	AD
64	89	2E	B8
95	16	23	BF
A8	E3	22	6E

Round 8

8F	73	B7	AF
0E	5B	86	C1
EC	4B	4B	0E
53	B3	35	EF

Round 9

4D	41	14	14
45	52	14	14
4E	49	14	14
54	14	14	14

Untuk round ke-10 transformasi InvMixColumns tidak dilakukan, hanya transformasi InvShiftRow, InvSubBytes dan AddInvRoundKey. Berdasarkan proses yang dilakukan maka akan didapatkan hasil dalam bentuk karakter pada tabel ASCII sebagai berikut:

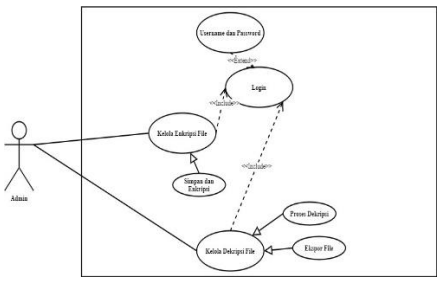
No.	Round	Kode ASCII	Karakter
1	4D	77	M
2	45	69	e
3	4E	78	n
4	54	84	t
5	41	65	a
6	52	82	r
7	49	73	i
8	14	20	
9	14	20	
10	14	20	
11	14	20	
12	14	20	
13	14	20	
14	14	20	
15	14	20	
16	14	20	

4. PEMODELAN DAN PERANCANGAN SISTEM

4.1 Pemodelan Sistem

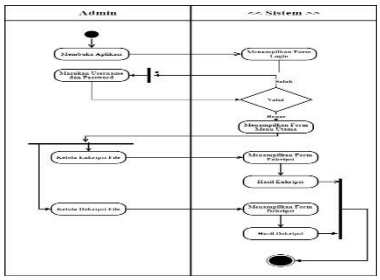
Pemodelan sistem merupakan gambaran nyata dengan aturan tertentu. Pada sistem informasi diperlukan pemodelan.

4.1.1 Use Case Diagram



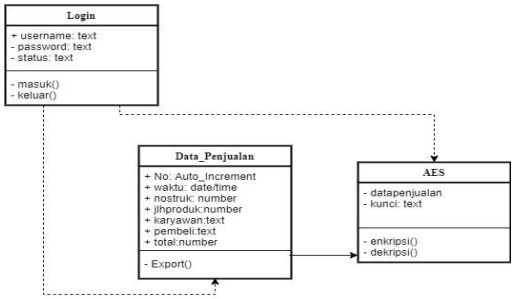
Gambar 4.1 Use Case Diagram

4.1.2 *Activity Diagram*



Gambar 4.2 Activity Diagram

4.1.3 *Class Diagram*



Gambar 4.3 Class Diagram

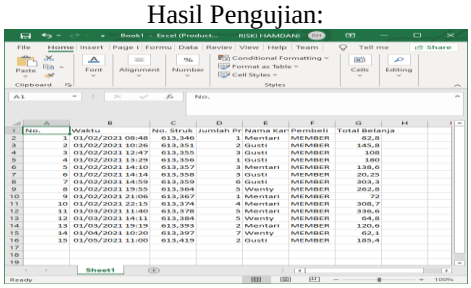
5. ANALISA DAN HASIL

5.1 Pengujian Program

Pengujian akan dilakukan dengan menggunakan *white box testing*. Adapun pengujian terhadap sistem yang telah dibangun dapat dilihat pada tabel berikut:

Tabel 5.1 Pengujian Sistem

No.	Skenario Pengujian	Hasil Yang Diharapkan	Kesimpulan
1	*Login* memasukan *username* dan *password* *Test Case*: 	Setelah *username* dan *password* dimasukan, ketika di klik tombol masuk maka akan tampil menu utama. Hasil Pengujian: 	Valid
2	Melakukan impor data penjualan, dan melakukan keamanan data. *Test Case*:	Hasil Akan di diamankan dengan metode AES dan disimpan ke *database*. Hasil Pengujian:	Valid

			
3	Melakukan Dekripsi File yang telah di enkripsi *Test Case*: 	Hasil data yang sudah di dekripsi Kembali, akan diexport kembali dalam bentuk file excel. Hasil Pengujian: 	Valid

5.2 Identifikasi Sistem

Identifikasi sistem merupakan penjelasan poin dari setiap kelebihan dan kekurangan sistem yang telah diketahui setelah dilakukan pengujian terhadap sistem yang telah dibangun.

5.2.1 Kelebihan Sistem

Adapun kelebihan aplikasi yang dibangun yaitu mengamankan data penjualan di Toko Sweet Amirah untuk melindungi kecurangan data penjualan adalah sebagai berikut:

1. Sistem dapat melakukan keamanan data dengan waktu yang efisien dan keamanan data cukup baik untuk pengamanannya.
2. Sistem dapat memberikan keamanan dan menjaga kerahasiaan data penjualan untuk menghindari kecurangan yang terjadi.
3. Sistem sangat mudah untuk digunakan.

5.2.2 Kekurangan Sistem

Adapun kekurangan sistem yang dibangun berdasarkan pengujian yang telah dilakukan terhadap sistem adalah sebagai berikut:

1. Sistem ini belum memiliki *form* perubahan dan penambahan *user* pengguna.
1. Sistem yang digunakan hanya dapat menampung upload data file excel

6. KESIMPULAN

Adapun kesimpulan dari penelitian ini berdasarkan dari rumusan masalah adalah sebagai berikut:

1. Dalam melakukan penerapan metode AES dalam kriptograpi untuk mengamankan data penjualan di Toko Sweet Amirah yaitu dengan membuat suatu kunci rahasia dan data yang akan diamankan berdasarkan penerapan langkah-langkah atau algoritma dari Metode AES untuk mendapatkan hasil keamanan data (*Chipertext*) .
2. Dalam proses perancangan sistem yang dibangun dengan penerapan kriptografi dengan metode AES yaitu berdasarkan perancangan UML yang telah dibuat dan disesuaikan berdasarkan kebutuhan dalam proses Algoritma metode AES untuk mendapatkan hasil enkripsi data penjualan dan melakukan dekripsi kembali terhadap data ketika dibutuhkan.
3. Dalam tahapan pengujian sistem kriptografi dengan metode AES dapat dilakukan dengan melakukan impor data penjualan kedalam sistem dan memasukan kata kunci sebagai sandi untuk mengamankan data kemudian proses keamanan akan disimpan secara otomatis ke dalam *database*, ketika data ingin dikembalikan maka harus memasukan kata kunci yang sama pada saat melakukan enkripsi data agar data dapat kembali seperti semula.

UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kehadirat Tuhan yang Maha Esa karena berkat rahmat Nya, yang masih memberikan kesehatan dan kesempatan sehingga dapat diselesaikan jurnal ilmiah ini dengan baik. Saya ucapkan terima kasih kepada ketua yayasan STMIK Triguna Dharma, kepada Bapak Nurcahyo Budi Nugroho, S.Kom., M.Kom selaku dosen pembimbing 1, kepada Bapak RicoImanta Ginting, S.Kom., M.Kom selaku dosen pembimbing 2 , kepada kedua orang tua saya yang selalu memberikan dukungan dan doa kepada saya dan tidak lupa kepada teman-teman saya seperjuangan.

REFERENSI

[1] O. Dakhi, M. Masril, R. Novalinda, J. Jufrinaldi, and A. Ambiyar, "Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher," *INVOTEK J. Inov. Vokasional dan Teknol.*, vol. 20, no. 1, pp. 27–36, 2020, doi: 10.24036/invotek.v20i1.647.

[2] R. Nuari, N. Ratama, J. T. Informatika, F. Teknik, and U. Pamulang, "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," vol. 1, no. 2, pp. 37–44, 2020.

[3] B. Anwar, Azanuddin, N. B. Nugroho, and R. Siregar, "Aplikasi Pengamanan Dokumen Penjualan Tiket Pesawat Di Pt . Benua Raya Jaya Tour And Travel Menggunakan Metode Advanced Encryption Standard (AES)," *J-Sisko Tech*, vol. 3, no. 1, pp. 96–102, 2020.

[4] S. Setti, I. Gunawan, B. E. Damanik, S. Sumarno, and I. O. Kirana, "Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 182, 2020, doi: 10.30865/jurikom.v7i1.1960.

[5] PT Mid Solusi Nusantara, "Pengertian Penjualan, Manfaat, dan Jenis-jenisnya." www.jurnal.id.

BIOGRAFI PENULIS

<table>
<tr>
<td>  </td>
<td>Nama : Astri Handayani
TTL : Pinangsori, 08 April 2000
Jenis Kelamin : Perempuan
Program Studi : Sistem Informasi STMIK Triguna Dharma
Deskripsi : Sedang Menempuh jenjang Strata Satu (S1) dengan program studi sistem informasi di STMIK Triguna Dharma.
Bidang Ilmu : Analisis Sistem Keamanan Komputer
E-mail : astrihanday@gmail.com</td>
</tr>
<tr>
<td>  </td>
<td>Nama : Nurcahyo Budi Nugroho, S.Kom., M.Kom.
NIDN : 0130038201
Jenis Kelamin : Laki-Laki
Program Studi : Sistem Informasi STMIK Triguna Dharma
Bidang Ilmu : Keamanan komputer dan Pengolahan Citra</td>
</tr>
<tr>
<td>  </td>
<td>Nama : Rico Imanta Ginting, S.Kom., M.Kom.
NIDN : 0102029002
Jenis Kelamin : Laki-Laki
Program Studi : Teknik Komputer STMIK Triguna Dharma
Bidang Ilmu : Kecerdasan Buatan</td>
</tr>
</table>