JDSP
Jurnal Data Science Penusa

Implementasi Algoritma *Advanced Encryption Standard* (Aes) Dalam Pengamanan Data Penjualan

Alpon Josua [1)], Anita Sindar Ros Maryana Sinaga[2)]
[1,2)] STMIK Pelita Nusantara, Teknik Informatika,
[1)] alponjosua@gmail.com
[2)] nitamaryana76@gmail.com

Received: 30 Januari 2025 Accepted: 16 Februari 2025 Published: 22 Februari 2025
Pg. 127-143

OPEN ACCESS

***Alpon Josua**

Kata Kunci:
Keamanan Komputer, Keamanan Data dan Informasi, Kriptografi, Algoritma AES, Data Penjualan

JDSP: Jurnal Data Science Penusa is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Abstrak : Keamanan data atau informasi adalah hal yang dibutuhkan saat ini, dimana perkembangan teknologi internet memungkinkan semua orang dapat mengakses informasi yang bersifat rahasia, sehingga dibutuhkan penanganan dalam keamanan data, salah satunya adalah Kiptografi yang digunakan untuk menyandikan informasi sehingga tidak dapat dibaca oleh orang lain. Penelitian ini menerapkan metode *Adnavced Encryption Standart* (AES) 128 salah satu algoritma kriptografi untuk pengamanan data penjualan pada CV. Sinar Tanjung Mandiri. Algoritma AES dipilih karena memliki tingkat pengamanan informasi yang bagus. AES 128 memiliki proses enkripsi yang cukup panjang dalam menghasilkan *chipertext* dari *plainteks*, proses tersebut meliputi *initial state*, ekspansi kunci sebanyak 10 *round*, dan proses enkripsi 10 *round* dengan operasi aritmatika seperti pertukaran nilai *byte,* pergeseran nilai *byte,* operasi matriks bidang galois, dan operasi *X-Or*. Dengan demikian implementasi algoritma AES 128 diharapkan dapat memberikan keamanan terhadap data penjualan Cv. Sinar Tanjung Mandiri.

PENDAHULUAN

Komputer telah berkembang semakin pesat, yang awal mula digunakan untuk operasi aritmatika sederhana hingga menjadi teknologi komunikasi yang canggih, perkembangan teknologi komunikasi komputer dimulai dari terkoneksinya komputer pada jaringan telepon, jaringan memberikan kemampuan pengguna untuk mengakses komputer dari lokasi yang jauh dan berbeda dengan kemampuan ini penggunaan komputer mulai mengarah sebagai penyimpanan informasi secara *online* dan terkoneksi dengan jaringan secara bersama-sama, dengan kemampuan komputer dan penggunaan komputer sebagai penyimpanan informasi sehingga membutuhkan tindakan pengamanan data dan informasi.

Keamanan data dan informasi dibutuhkan untuk menjaga dan melindungi kerahasiaan sebuah informasi, data dan informasi memiliki banyak bentuk seperti foto, video, teks, kode, dan lainnya informasi juga memiliki sumber yang berbeda seperti informasi yang bersumber dari data pribadi, informasi dari suatu organisasi ataupun suatu perusahaan, umumnya data dan informasi yang bersifat sensitif disimpan tersendiri dan hanya dapat diakses oleh pengguna tertentu, upaya tersebut dilakukan untuk mencegah penyalahgunaan data dan informasi sehingga tidak merugikan pihak terkait, salah satu data yang bersifat sensitif adalah data penjualan.

CV. Sinar Tanjung Mandiri merupakan perusahaan dagang barang elektronik, perusahaan memiliki data penjualan yang mencatat setiap transaksi produk yang dipasarkan, perusahaan menggunakan data penjualan sebagai acuan untuk menyediakan stok barang, audit keuangan perusahaan, juga audit pajak setiap transakasi penjualan atau PPN. Dari hasil observasi informasi penjualan disimpan dalam bentuk *file excel* tanpa ada pengamanan data, hal ini rawan terhadap pencurian data dan manipulasi data oleh pihak yang tidak bertanggung jawab yang dapat merugikan perusahaan. Untuk menghindari kerugian akibat pencurian data dan manipulasi data diperlukan sistem pengamanan data dan informasi pada data penjualan.

Salah satu teknologi dalam keamanan data dan informasi adalah kriptografi, dalam hal ini kriptografi mengubah informasi asli menjadi teks sandi dengan maksud menyembunyikan (Jayana et al., 2022). Kriptografi memiliki beberapa jenis seperti simetris, asimetris, dan hibrida, dalam kriptografi simetris terdapat algoritma *Advanced Encryption Standard* (AES), algoritma AES menggunakan kunci yang sama untuk proses enkripsi dan dekripsi (Sitepu, 2022), AES memiliki 3 (tiga) jenis kunci yaitu 128, 192 dan 256 bit, masing-masing terdapat perbedaan dalam panjang blok dalam proses enkripsi dan dekripsi. Algoritma AES telah digunakan untuk menyelesaikan masalah pengamanan dokumen (Azhari et al., 2022), sistem pengamanan pintu otomatis berbasis RFID (Pratiwi, A., Fauzi, A., & Kusumaningrum, 2022).

Penelitian ini bertujuan menerapkan Algoritma *Advanced Encryption Standard* (AES) pada data sistem penjualan, Dari pembahasan latar belakang penelitian ini berjudul, "Implementasi Algoritma *Advanced Encryption Standard* (AES) Pada Pengamanan Data Penjualan."

TINJAUAN LITERATUR

Keamanan Data

Keamanan merupakan aspek penting dari sebuah sistem informasi, keamanan dapat diartikan suatu keadaan bebas dari bahaya istilah ini merujuk pada tindak kejahatan, dan segala bentuk kecelakaan (Sindar, 2020).

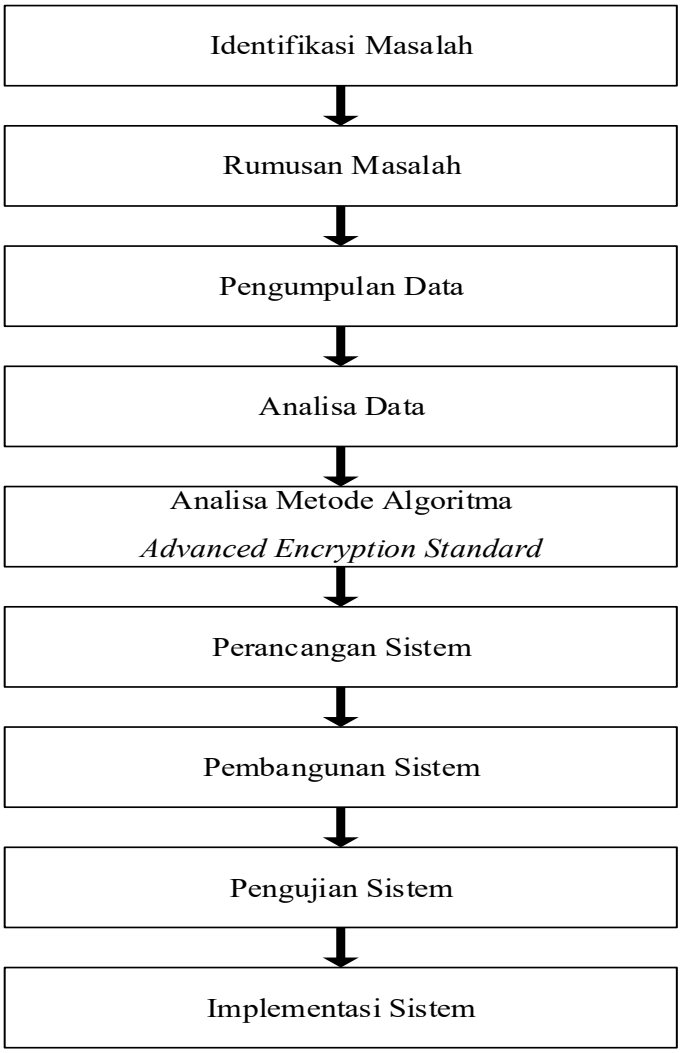
Kriptografi

Kriptografi berasal dari bahasa yunani yaitu *Crypto* berarti rahasia dan *graphia* berarti tulisan, dengan pengertian lainnya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan atau data dengan cara mengubah informasi asli menjadi kode sandi yang sulit diketahui (Sindar, 2020).

Algoritma *Advanced Encryption Standard* (AES)

Algoritma *Advanced Encryption Standart* (AES) adalah Algoritma yang dijadikan standart enkripsi oleh *National Institute of Standards and Technology* (NIST). Algoritma AES merupakan suatu Algoritma simetri yang menggunakan kunci yang sama pada proses enkripsi dan dekripsi, Algorima AES mempunyai pilihan kunci 128, 192, 256 bit yang dikombinasikan dengan panjang blok 128 bit sebagai standart Algoritma AES, untuk melakukan proses enkripsi dan dekripsi (Cristy & Riandari, 2021).

METODE PENELITIAN



Gambar 1 Kerangka Kerja Penelitian

Berikut penjelasan dari Gambar 1 :

Identifikasi Masalah

Pada tahap ini dilakukan identifikasi mengenai permasalahan-permasalahan pokok pada penelitian yang dilakukan. Masalah utama adalah data penjualan yang disimpan hanya dalam bentuk file *Microsoft Excel*, pengamanaan dilakukan guna menghindari penyalahgunaan, pencurian, hingga rekayasa data oleh pihak-pihak yang tidak bertanggung jawab.

Rumusan masalah

Pada tahap ini ditentukan perumusan masalah yang akan diselesaikan yaitu, bagaimana menerapkan metode *Advanced Encryption Standart* (AES) dan bagaimana membangun sistem yang dapat menggamankan data penjualan.

Pengumpulan Data

a. Observasi
   Observasi dilakukan pada CV. Sinar Tanjung Mandiri dengan cara melakukan pengamatan pada mekanisme penjualan perusahaan.
b. Wawancara
   Wawancara dilakukan langsung kepada penanggung jawab penjualan pada CV. Sinar Tanjung Mandiri.
c. Studi Dokumentasi
   Pengumpulan data melalui proses dokumentasi dari data penjualan yang sudah ada tersimpan.
d. Studi Literatur
   Pengumpulan jurnal atau buku yang terkait dengan judul penelitian.

Analisa Data

Pada tahap ini dilakukan analisa terhadap data penjualan CV. Sinar Tanjung Mandiri.

Analisa Metode Algoritma *Advanced Encryption Standart*

Pada tahap ini dilakukan penerapan metode *Advanced Encryption Standart* dalam pengamanan data penjualan CV. Sinar Tanjung Mandiri.

Perancangan Sistem

Pada tahap ini sistem dirancang menggunakan UML yang terdiri dari *Use case* Diagram, *Activity* Diagram, dan *Class* Diagram.

Pembangunan Sistem

Dalam tahap ini sistem dibangun berbasis *website* dengan menggunakan bahasa pemrograman PHP dan MySQL sebagai basis datanya.

Pengujian Sistem

Pada tahap ini menggunakan metode *black box testing* dalam pengujian sistem. Pengujian dilakukan dengan memberikan input tertentu dan memeriksa output yang dihasilkan untuk memastikan dahwa sistem berperilaku sesuai dengan spesifikasi yang diharapkan dan data terenkripsi.

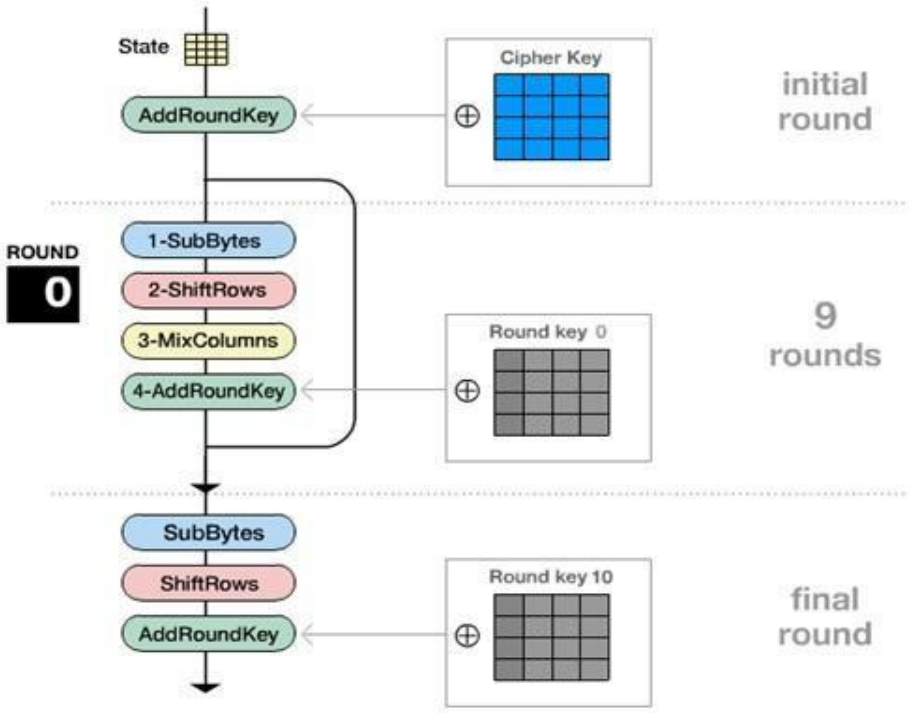
Implementasi Sistem

Setelah tahap pengujian selesai maka tahap selanjutnya adalah melakukan implementasi sistem.

PEMBAHASAN

Algoritma AES sendiri memiliki beberapa mode operasi dalam proses enkripsi dan dekripsi, pada penelitian ini penulis menggunakan mode operasiECB (*Electronic CodeBook*) mode operasi paling sederhana pada AES.

Tahapan dan proses enkripsi pada Algoritma AES :



Gambar 2 Tahapan Proses Enkripsi pada Algoritma AES

Berikut tahapan peoses enkripsi pada algoritma AES dengan hasil data riset yang telah dilakukan peneliti :

Initial Round

Langkah pertama dalam algoritma AES adalah *Initial Round* pada tahap ini *plainteks* di X-OR dengan *chiperkey*.

Plainteks : "AC PANASONIC 1PK"

ChiperKey : "KRIPTOGRAFIAESKU"

Karakter terlebih dahulu di urutkan dan di konversi ke *hexadecimal* :

A	C		P	A	N	A	S	O	N	I	C		1	P	K
41	43	20	50	41	4E	41	53	4F	4E	49	43	20	31	50	4B

K	R	I	P	T	O	G	R	A	F	I	A	E	S	K	U
4B	52	49	50	54	4F	47	52	41	46	49	41	45	53	4B	55

Langkah *initial round* dapat dilakukan dengan cara melakukan X-OR setiap nilai bit setiap karakter dari *plainteks* dan *chiperteks* :

41 = 0100 0001
4B = 0100 1010 X-OR
0000 1010 = 0A

43 = 0100 0011
52 = 0101 0010 X-OR
0001 0001 = 11

20 = 0010 0000
49 = 0100 1001 X-OR
0110 1001 = 69

50 = 0101 0000
50 = 0101 0000 X-OR
0000 0000 = 00

41 = 0100 0001
54 = 0101 0100 X-OR
0001 0101 = 15

4E = 0100 1110
4F = 0100 1111 X-OR
0000 0001 = 01

41 = 0100 0001
47 = 0100 0111 X-OR
0000 0110 = 06

53 = 0101 0011
52 = 0101 0010 X-OR
0000 0001 = 01

4F = 0100 1111
41 = 0100 0001 X-OR
0000 1110 = 0E

4E = 0100 1110
46 = 0100 0110 X-OR
0000 1000 = 08

49 = 0100 1001
49 = 0100 1001 X-OR
0000 0000 = 00

43 = 0100 0011
41 = 0100 0001 X-OR
0000 0010 = 02

20 = 0010 0000
41 = 0100 0101 X-OR
0110 0101 = 65

31 = 0011 0001
53 = 0101 0011 X-OR
0110 0010 = 62

50 = 0101 0000
4B = 0100 1011 X-OR
0001 1011 = 1B

4B = 0100 1011
55 = 0101 0101 X-OR
0001 1110 = 1E

Blok state hasil *plainteks X-Or chiperkey*

0A	15	0E	65
11	01	08	62
69	06	00	1B
00	01	02	1E

Pembangkitan Kunci / *ekspansi key*

Pada tahap *ekspansi key* terjadi 3 operasi *RotWord***,** *SubWord,* dan *Rcon.* Sebelum melakukan 3 operasi jadikan blok state urutan *chiperkey* yang didapat pada proses sebelumnya

wi-4			wi-1	wi			
4B	54	41	45				
52	4F	46	53				
49	47	49	4B				
50	52	41	55				
Blok *chiperkey* "KRIPTOGRAFIAESKU"				*Round* 1			

Jika wi dikolom 1, maka wi-1 adalah

45
53
4B
55

Rotword wi-1, dilakukan pergeseran satu kali ke kiri atau dalam model blok ke atas satu kali yang paling atas menjadi paling bawah.

45		53
53	*Rotword* wi-1 Menjadi →	4B
4B		55
55		45

Subword yaitu pertukaran setiap byte dengan tabel S-Box, Untuk pertukuran byte dengan tabel S-Box, karakter ke-1 untuk baris karakter ke-2 untuk kolom.

53		ED
4B	*SubWord* wi-1 hasil *RotWord* menjadi →	B3
55		FC
45		6E

Operasi selanjutnya adalah *Rcon*, dengan melakukan *X-Or wi-1, wi-4*, dan tabel *Rcon* untuk setiap *round*.

wi-1 ⊕ *wi-4* ⊕ *Rcon [1]*

ED		4B		01		A7
B3	⊕	52	⊕	00	=	E1
FC		49		00		B5
6E		50		00		3E

Hasil untuk kolom 1 *Round* 1 :

4B	54	41	45	A7			
52	4F	46	53	E1			
49	47	49	4B	B5			
50	52	41	55	3E			
Blok *chiperkey* "KRIPTOGRAFIAESKU"				*Round* 1			

Ekspansi kunci kolom 2 – 4 dinyatakan dengan rumus *wi-1* ⊕ *wi-4*.
Ekspansi kolom 2 :

wi-1		wi-4		
A7		54		F3
E1	⊕	4F	=	AE
B5		47		F2
3E		52		6C

Ekspansi kolom 3 :

wi-1		wi-4		
F3		41		B2
AE	⊕	46	=	E8
F2		49		BB
6C		41		2D

Ekspansi kolom 4 :

wi-1		wi-4		
B2		45		F7
E8	⊕	53	=	BB
BB		4B		F0
2D		55		78

Hasil untuk kolom 4 *round* 1 :

4B	54	41	45	A7	F3	B2	F7
52	4F	46	53	E1	AE	E8	BB
49	47	49	4B	B5	F2	BB	F0
50	52	41	55	3E	6C	2D	78
Blok *chiperkey* "KRIPTOGRAFIAESKU"				*Round* 1			

Untuk mendapatkan RoundKey ke-2 sampai dengan RoundKey ke-10, proses di atas diulang sebanyak 10 kali.

Proses enkripsi

Proses enkripsi terjadi sebannyak 10 *round,* proses enkripsi terdapat 4 operasi *Subbytes, Shiftrows, Mixcolumn, AddRoundKey.*

Subbytes

dengan melakukan pertukaran *Bytes* dari hasil *plainteks* ⊕ *chiperkey* pada tahap *Initial Round,* dengan tabel S-Box.

0A	15	0E	65
11	01	08	62
69	06	00	1B
00	01	02	1E
Blok hasil *plainteks* ⊕ *chiperkey*			

Di *Subbyte* dengan S-Box menjadi →

67	59	AB	4D
82	7C	30	AA
F9	6F	63	AF
63	7C	77	72

Shiftrows

Pada operasi *Shiftrows* dilakukan pergeseran *byte* pada blok hasil *Subbyte* dengan aturan :

- Baris ke-1 digeser 0 kali kekiri
- Baris ke-2 digeser 1 kali kekiri
- Baris ke-3 digeser 2 kali kekiri
- Baris ke-4 digeser 3 kali kekiri

0 ←	67	59	AB	4D	Menjadi →	67	59	AB	4D
1 ←	82	7C	30	AA		7C	30	AA	82
2 ←	F9	6F	63	AF		63	AF	F9	6F
3 ←	63	7C	77	72		72	63	7C	77

Mixcolumn

Pada operasi *Mixcolumn* dilakukan perkalian antara blok dari hasil *Shiftrows* dengan matriks tetap (*constant matrix*) pada algoritma AES. Algoritma AES menggunakan operasi aritmatika *Galois Field* (GF(2^8)), dimana operasi penjumlahan pada *Galois* adalah X-OR, dan setiap elemen dalam GF(2^8)) dapat direpresentasikan sebagai polinomial biner maksimal 8 bit, jika perkalian melebihi 8 bit maka dilakukan reduksi *modulo polinomial irreducible* yang direpresentasikan dalam bentuk biner sebagai "100011011" atau dalam hexadecimal sebagai 11B.

Constant matrix $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$ X

67	59	AB	4D
7C	30	AA	82
63	AF	F9	6F
72	63	7C	77

Blok hasil Shiftrows

Operasi perkalian matriks :

$$[02 \quad 03 \quad 01 \quad 01] \text{ X } \begin{matrix} 67 \\ 7C \\ 63 \\ 72 \end{matrix}$$

$$=(\{02\}.\{67\}) \oplus (\{03\}.\{7C\}) \oplus (\{01\}.\{63\}) \oplus (\{01\}.\{72\})$$
$$=\{CE\} \oplus \{84\} \oplus \{63\} \oplus \{72\}$$
=5B

$$[01 \quad 02 \quad 03 \quad 01] \text{ X } \begin{matrix} 67 \\ 7C \\ 63 \\ 72 \end{matrix}$$

$$=(\{01\}.\{67\}) \oplus (\{02\}.\{7C\}) \oplus (\{03\}.\{63\}) \oplus (\{01\}.\{72\})$$
$$=\{67\} \oplus \{F8\} \oplus \{A5\} \oplus \{72\}$$
=48

$$[01 \quad 01 \quad 02 \quad 03] \text{ X } \begin{matrix} 67 \\ 7C \\ 63 \\ 72 \end{matrix}$$

$$=(\{01\}.\{67\}) \oplus (\{01\}.\{7C\}) \oplus (\{02\}.\{63\}) \oplus (\{03\}.\{72\})$$
$$=\{67\} \oplus \{7C\} \oplus \{C6\} \oplus \{96\}$$
=4B

$$[03 \quad 01 \quad 01 \quad 02] \text{ X } \begin{matrix} 67 \\ 7C \\ 63 \\ 72 \end{matrix}$$

$$=(\{03\}.\{67\}) \oplus (\{01\}.\{7C\}) \oplus (\{01\}.\{63\}) \oplus (\{02\}.\{72\})$$
$$=\{A9\} \oplus \{7C\} \oplus \{63\} \oplus \{E4\}$$

$$=\{52\}$$

$$[02 \quad 03 \quad 01 \quad 01] \ X \begin{matrix} 59 \\ 30 \\ AF \\ 63 \end{matrix}$$

$$=(\{02\}.\{59\}) \oplus (\{03\}.\{30\}) \oplus (\{01\}.\{AF\}) \oplus (\{01\}.\{63\})$$
$$=\{B2\} \oplus \{50\} \oplus \{AF\} \oplus \{63\}$$
$$=\{2E\}$$

$$[01 \quad 02 \quad 03 \quad 01] \ X \begin{matrix} 59 \\ 30 \\ AF \\ 63 \end{matrix}$$

$$=(\{01\}.\{59\}) \oplus (\{02\}.\{30\}) \oplus (\{03\}.\{AF\}) \oplus (\{01\}.\{63\})$$
$$=\{59\} \oplus \{60\} \oplus \{EA\} \oplus \{63\}$$
$$=\{B0\}$$

$$[01 \quad 01 \quad 02 \quad 03] \ X \begin{matrix} 59 \\ 30 \\ AF \\ 63 \end{matrix}$$

$$=(\{01\}.\{59\}) \oplus (\{01\}.\{30\}) \oplus (\{02\}.\{AF\}) \oplus (\{03\}.\{63\})$$
$$=\{59\} \oplus \{30\} \oplus \{45\} \oplus \{A5\}$$
$$=\{89\}$$

$$[03 \quad 01 \quad 01 \quad 02] \ X \begin{matrix} 59 \\ 30 \\ AF \\ 63 \end{matrix}$$

$$=(\{03\}.\{59\}) \oplus (\{01\}.\{30\}) \oplus (\{01\}.\{AF\}) \oplus (\{02\}.\{63\})$$
$$=\{EB\} \oplus \{30\} \oplus \{AF\} \oplus \{C6\}$$
$$=\{B2\}$$

$$[02 \quad 03 \quad 01 \quad 01] \ X \begin{matrix} AB \\ AA \\ F9 \\ 7C \end{matrix}$$

$$=(\{02\}.\{AB\}) \oplus (\{03\}.\{AA\}) \oplus (\{01\}.\{F9\}) \oplus (\{01\}.\{7C\})$$
$$=\{4D\} \oplus \{E5\} \oplus \{F9\} \oplus \{7C\}$$
$$=\{2D\}$$

$$[01 \quad 02 \quad 03 \quad 01] \ X \begin{matrix} AB \\ AA \\ F9 \\ 7C \end{matrix}$$

$$=(\{01\}.\{AB\}) \oplus (\{02\}.\{AA\}) \oplus (\{03\}.\{F9\}) \oplus (\{01\}.\{7C\})$$
$$=\{AB\} \oplus \{4F\} \oplus \{10\} \oplus \{7C\}$$
$$=\{88\}$$

$$[01 \quad 01 \quad 02 \quad 03] \ X \begin{matrix} AB \\ AA \\ F9 \\ 7C \end{matrix}$$

$$=(\{01\}.\{AB\}) \oplus (\{01\}.\{AA\}) \oplus (\{02\}.\{F9\}) \oplus (\{03\}.\{7C\})$$
$$=\{AB\} \oplus \{AA\} \oplus \{E9\} \oplus \{84\}$$
$$=\{6C\}$$

$$[03 \quad 01 \quad 01 \quad 02] \ X \begin{matrix} AB \\ AA \\ F9 \\ 7C \end{matrix}$$

$$=(\{03\}.\{AB\}) \oplus (\{01\}.\{AA\}) \oplus (\{01\}.\{F9\}) \oplus (\{02\}.\{7C\})$$
$$=\{E6\} \oplus \{AA\} \oplus \{F9\} \oplus \{F8\}$$
$$=\{4D\}$$

$$[02 \quad 03 \quad 01 \quad 01] \text{ X } \begin{matrix} 4D \\ 82 \\ 6F \\ 77 \end{matrix}$$
$$=(\{02\}.\{4D\}) \oplus (\{03\}.\{82\}) \oplus (\{01\}.\{6F\}) \oplus (\{01\}.\{77\})$$
$$=\{9A\} \oplus \{9D\} \oplus \{6F\} \oplus \{77\}$$
$$=\{1F\}$$

$$[01 \quad 02 \quad 03 \quad 01] \text{ X } \begin{matrix} 4D \\ 82 \\ 6F \\ 77 \end{matrix}$$
$$=(\{01\}.\{4D\}) \oplus (\{02\}.\{82\}) \oplus (\{03\}.\{6F\}) \oplus (\{01\}.\{77\})$$
$$=\{4D\} \oplus \{1F\} \oplus \{B1\} \oplus \{77\}$$
$$=\{94\}$$

$$[01 \quad 01 \quad 02 \quad 03] \text{ X } \begin{matrix} 4D \\ 82 \\ 6F \\ 77 \end{matrix}$$
$$=(\{01\}.\{4D\}) \oplus (\{01\}.\{82\}) \oplus (\{02\}.\{6F\}) \oplus (\{03\}.\{77\})$$
$$=\{4D\} \oplus \{82\} \oplus \{DE\} \oplus \{99\}$$
$$=\{88\}$$

$$[03 \quad 01 \quad 01 \quad 02] \text{ X } \begin{matrix} 4D \\ 82 \\ 6F \\ 77 \end{matrix}$$
$$=(\{03\}.\{4D\}) \oplus (\{01\}.\{82\}) \oplus (\{01\}.\{6F\}) \oplus (\{02\}.\{77\})$$
$$=\{D7\} \oplus \{82\} \oplus \{6F\} \oplus \{EE\}$$
$$=\{D4\}$$

Hasil operasi *Mixcolumn round* 1 :

5B	2E	2D	1F
48	B0	88	94
4B	89	6C	88
52	B2	4D	D4

AddRoundKey

Operasi *AddRoundKey* dilakukan X-OR hasil *Mixcolumn* dengan kunci dari proses pembangkitan kunci (*ekspansi key*) untuk setiap *round*.

5B	2E	2D	1F		A7	F3	B2	F7
48	B0	88	94		E1	AE	E8	BB
4B	89	6C	88	$\oplus$	B5	F2	BB	F0
52	B2	4D	D4		3E	6C	2D	78
Blok hasil operasi *Mixcolumn*					Blok hasil ekspansi *chiperkey* untuk *round* 1			

FC	DD	9F	E8
A9	1E	60	2F
FE	7B	D7	78
6C	DE	60	AC
Blok hasil operasi *AddRoundKey round* 1			

Proses diatas akan diulangi untuk round ke-2 sampai dengan round ke-10. Namun, pada round ke 10 operasi MixColumns tidak lagi dilakukan. Berikut hasil proses enkripsi round ke-2 sampai dengan round ke-10.

B0	7A	1F	8A		E3	07	C8	55
8C	11	24	0A		02	5E	FF	5C
26	36	4D	1F	⊕	B1	34	14	B0
F2	D8	FB	63		B3	A3	F4	90
Blok hasil operasi *Mixcolumn*					Blok hasil ekspansi *chiperkey* untuk *round* 10			

53	7D	D7	DF
8E	4F	DB	56
97	02	59	AF
41	7B	0F	F3

Blok hasil *AddRoundKey Round* 10

Hasil *chipertext* yang didapat dari plainteks "AC PANASONIC 1PK" dengan key "KRIPTOGRAFIAESKU" sebagai berikut :

HEX	53	8E	97	41	7D	4F	02	7B	D7	DB	59	0F	DF	56	AF	F3
DEC	83	142	151	65	125	79	2	123	215	219	89	15	223	86	175	243
chipertext	S	Ž	—	A	}	O		{	×	Û	Y		ß	V	¯	ó

Proses dekripsi

Proses dekripsi merupakan proses pengembalian *chipertext* menjadi *plainteks* atau teks awal sebelum dilakukan enkripsi, proses ini adalah kebalikan dari proses enkripsi atau *invers*.

Invers addroundkey round 0

Proses dekripsi dimulai dari *Invers addroundkey round* 0, dimana *chipertext* di *addroundkey* dengan *roundkey* hasil *ekspansi key* round 10

53	7D	D7	DF		E3	07	C8	55		B0	7A	1F	8A
8E	4F	DB	56		02	5E	FF	5C		8C	11	24	0A
97	02	59	AF	⊕	B1	34	14	B0	=	26	36	4D	1F
41	7B	0F	F3		B3	A3	F4	90		F2	D8	FB	63
Chipertext					*Roundkey* 10								

Dekripsi *round* 1

Invers Shiftrows

Operasi *Invers Shiftrows* kebalikan dari operasi *Shiftrows*, operasi *invers* dilakukan dengan pergeseran *byte* ke kanan bukan ke kiri.

→0	B0	7A	1F	8A		B0	7A	1F	8A
→1	8C	11	24	0A	Menjadi	0A	8C	11	24
→2	26	36	4D	1F	→	4D	1F	26	36
→3	F2	D8	FB	63		D8	FB	63	F2

Invers Subbytes

Operasi *Invers Subbytes,* menggunakan tabel *invers* S-Box

B0	7A	1F	8A
0A	8C	11	24
4D	1F	26	36
D8	FB	63	F2
Blok hasil *shiftrows*			

Di *Subbyte* dengan inverse S-Box menjadi →

FC	BD	CB	CF
A3	F0	E3	A6
65	CB	23	24
2D	63	00	04

Addroundkey

Pada proses dekripsi, Operasi setelah *Subbytes* adalah *Addroundkey*

FC	BD	CB	CF		DF	E4	CF	9D		23	59	04	52
A3	F0	E3	A6		4B	5C	A1	A3		E8	AC	42	05
65	CB	23	24	⊕	F2	85	20	A4	=	97	4E	03	80
2D	63	00	04		ED	10	57	64		C0	73	57	60
Hasil *Subbytes*					*Roundkey* 9								

Invers Mixcolumn

Pada operasi *Mixcolumn* menggunakan *constant matrix invers* yang merupakan kebalikan *constant matriks* pada proses enkripsi

Constant matrix $\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$ X

23	59	04	52
E8	AC	42	05
97	4E	03	80
C0	73	57	60

Blok hasil *Addroundkey*

58	26	16	E1
A6	F0	16	E3
CF	BA	35	46
AD	A4	27	F3

Blok hasil *Invers Mixcolumn Round* 1

Proses diatas akan diulangi untuk round ke-2 sampai dengan round ke-10. Namun, pada round ke 10 operasi MixColumns tidak lagi dilakukan. hasil proses dekripsi round ke-2 sampai dengan round ke-10.

Addroundkey

0A	15	0E	65		4B	54	41	45		41	41	4F	20
11	01	08	62		52	4F	46	53		43	4E	4E	31
69	06	00	1B	⊕	49	47	49	4B	=	20	41	49	50
00	01	02	1E		50	52	41	55		50	53	43	4B
Hasil *Subbytes*					*Roundkey* 0 / chiperkey								

HEX	41	43	20	50	41	4E	41	53	4F	4E	49	43	20	31	50	4B
charakter	A	C		P	A	N	A	S	O	N	I	C		1	P	K

KESIMPULAN

Berdasarkan uraian permasalahan dan pembahasan pada bab sebelumnya penulis ingin menyampaikan Berdasarkan uraian permasalahan dan pembahasan penulis menyampaikan Kesimpulan

Sistem ini mampu untuk melakukan enkripsi pada data yang diinput sehingga dapat untuk meningkatkan keamanan data.

Sistem yang dibuat tidak akan dapat melakukan dekripsi pada data enkripsi jika kunci yang dimasukan berbeda dengan kunci yang digunakan untuk proses enkripsi.

Algoritma AES 128 dapat diimplementasikan untuk membuat Sistem Pengamanan Data Penjualan pada Cv. Sinar Tanjung Mandiri.

REFERENCES

Prameshwari, A., & Sastra, N. P. (2018). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. *Eksplora Informatika*, *8*(1), 52. https://doi.org/10.30864/eksplora.v8i1.139

Sindar, A. (2020). *Buku Keamanan Komputer*. CV INSAN CENDEKIA MANDIRI. https://books.google.co.id/books?hl=id&lr=&id=pwcIEAAAQBAJ&oi=fnd&pg=PA2&dq=keamanan+Komputer+anita+sindar&ots=kBuKiGw6KY&sig=hSEQh8TyeZeRLCGm0VTjvB5jxC8&redir_esc=y#v=onepage&q=keamanan Komputer anita sindar&f=false

Pratiwi, A., Fauzi, A., & Kusumaningrum, D. (2022). Sistem Pengamanan Pintu Otomatis Berbasis RFID Menggunakan Metode AES. *Journal.Ubpkarawang.Ac.Id*, *III*(2), 202. http://journal.ubpkarawang.ac.id/mahasiswa/index.php/ssj/article/view/441

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*, *2*(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390

Harianto, K., Pratiwi, H., & Suhariyadi, Y. (2019). Sistem Monitoring Lulusan Perguruan Tinggi Dalam Memasuki Dunia Kerja Menggunakan Tracer Study. *J-SAKTI (Jurnal Sains Komputer Dan Informatika)*, *3*(2), 295. https://doi.org/10.30645/j-sakti.v3i2.148

Mesran, M., Diansyah, T. M., & Fadlina, F. (2019). Implemententasi Metode Rank Order Cendroid (ROC) dan Operational Competitiveness Rating Analysis (OCRA) dalam Penilaian Kinerja Dosen Komputer Menerapkan (Studi Kasus: STMIK Budi Darma). *Prosiding Seminar Nasional Riset Information Science (SENARIS)*, *1*(September), 822. https://doi.org/10.30645/senaris.v1i0.89

Mesran, Nasution, S. D., & Waruwu, F. T. (2019). *Merancang Aplikasi Penjualan dengan Visual Basic* (Mesran (ed.)). Penerbit Green Press (STMIK Budi Darma).

Harianto, K., Pratiwi, H., & Suhariyadi, Y. (2019). *Sistem Monitoring Lulusan Perguruan Tinggi Dalam Memasuki Dunia Kerja Menggunaan Tracer Study* (Lutfiah (ed.)).

Yendrianof, D., Romindo, Sari, A. N., Tantriawan, H., Putri, E. E., Manuhutu, M. A., Defiariany, R. T., Putri, N. E. P., Jamaludin, T. P., Simarmata, J., Rismayani, & Aisa, S. (2022). *Analisis dan Perancangan Sistem Informasi* (A. Karim (ed.); Cetakan 1). Yayasan Kita Menulis.

Utami, F. H. (2022). *Aplikasi Pelayanan Antrian Pasien Menggunakan Metode FCFS Menggunakan PHP dan MySQL*. *18*(1), 153–160.

Giovani, A. P., Ardiansyah, A., Haryanti, T., Kurniawati, L., & Gata, W. (2020). Analisis Sentimen Aplikasi Ruang Guru Di Twitter Menggunakan Algoritma Klasifikasi. *Jurnal Teknoinfo*, *14*(2), 115. https://doi.org/10.33365/jti.v14i2.679

Hermiati, R., Asnawati, A., & Kanedi, I. (2021). Pembuatan E-Commerce Pada Raja Komputer Menggunakan Bahasa Pemrograman Php Dan Database Mysql. *Jurnal Media Infotama*, *17*(1), 54–66. https://doi.org/10.37676/jmi.v17i1.1317

Cristy, N., & Riandari, F. (2021). Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan. *Jurnal Ilmu Komputer Dan Sistem Informasi*, *4*(2), 75–85.

Putri, R. E., & Putra, R. R. (2019). Perancangan Aplikasi Rekam Medis Menggunakan Bahasa Pemograman VB.Net 2010. *Jurnal Teknik Dan Informatika*, *5*(2), 49–55.

Nuari, R., & Ratama, N. (2020). Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping. *Journal Of Artificial Intelligence And Innovative Applications*, *1*(2), 2716–1501. http://openjournal.unpam.ac.id/index.php/JOAIIA

Munir, R. (2019). KRIPTOGRAFI Kuliah Pengantar. In *Informatika, Bandung* (pp. 1–61). https://scholar.google.co.id/citations?user=ugYa9lEAAAAJ&hl=id

Sari, I. Y., Muttaqin, Jamaludin, Simarmata, J., Rahman, M. A., Iskandar, A., Pakpahan, A. F., Karim, A., Sugianto, Giap, Y. C., Hazriani, Yendrianof, D., & Manullang, S. O. (2021). *Keamanan Data dan Informasi*.

Ariyus, D., & Amikom, U. (2023). *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. https://books.google.co.id/books?id=3SSTJONEmX0C

Nanda, D., Herlambang, R., Pravitasari, N., Korespondensi, P., & Pendahuluan, I. (2024). *Penerapan Kriptografi AES untuk Keamanan Data Aplikasi Pemesanan Bibit Ternak pada BPSI UAT*. *8*, 29–44.

Sitepu, D. A. (2022). Implementasi pengamanan data menggunakan algoritma Advanced Encryption Standart (AES). *Jurnal Ilmiah Kaputama (JIKA)*, *6*(1), 49–58.

Prehanto, D. R. (2020). *Buku Ajar Konsep Sistem dan Informasi*. SCOPINDO Media Pustaka.

Jayana, M. A., Rafael, D., & Rahman, A. A. (2022). Implementasi Pengamanan Data Pengarsipan Dengan Metode Algoritma Kriptografi Aes Studi Kasus Pada Bank Bjb Kcp Pasteur Bandung. *Prosiding Seminar Sosial Politik, Bisnis, Akuntansi Dan Teknik*, *4*, 184. https://doi.org/10.32897/sobat.2022.4.0.1922

Nurnaningsih, D., & Permana, A. A. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes). *Jurnal Teknik Informatika*, *11*(2), 177–186. https://doi.org/10.15408/jti.v11i2.7811

Muharram, F., Azis, H., & Manga, A. R. (2018). Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES). *Proc. of the Seminar Nasional Ilmu Komputer Dan Teknologi Informasi*, *3*(2), 112–115.