JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 4, Bulan 2024, Hal 440-449
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Implementasi Kriptografi Pengamanan Data Pemesanan Produk Menggunakan Meotode AES

Leonardi Sidabutar[1], Mukhlis Ramadhan[2], Zaimah Panjaitan[3]
[1,2,3] Sistem Informasi, STMIK Triguna Dharma
Email: [1]leonardisidabutar@gmail.com, [2]mukhlis_ramadhan@trigunadharma.ac.id, [3]zaimahp09@gmail.com
Email Penulis Korespondensi: leonardisidabutar@gmail.com

Abstrak
Data pemesanan produk adalah data yang berisikan tentang data calon konsumen yang hendak membeli produk melalui pemesanan online dari website. Data tersebut diinput oleh konsumen lalu disimpan oleh sistem ke dalam *database*. Data pemesanan produk yang diinput oleh konsumen adalah data yang penting bagi perusahaan. Pengamanan terhadap jaringan komputer yang terhubung dengan *database* sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh "orang dalam" atau pihak-pihak yang langsung berhubungan dengan *database* seperti administrator *database* atau pihak hosting sekalipun. Hal ini menyebabkan isi dari *database* seperti data pemesanan produk harus diamankan tanpa campur tangan administrator *database*. maka dari itu solusi yang tepat untuk mengamankan data pemesanan tersebut di dalam *database* adalah dengan menerapkan ilmu Kriptografi. Kriptografi dapat digunakan untuk mengamankan data. Oleh karena itu, pengguna *database* membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya. Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditunjukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Advanced Encryption Standard (AES) adalah algoritma kriptografi yang menjadi standard algoritma enkripsi kunci simetris pada saat ini. Dalam algoritma kriptografi AES-128, 1 blok plaintext berukuran 128 bit terlebih dahulu dikonversi menjadi matriks heksadesimal berukuran 4x4 yang disebut state. Setiap elemen state berukuran 1 byte.
Kata Kunci: Kriptografi, AES, Enkripsi, Pengamanan, Data Pemesanan, Plaintext

Abstract
Product order data is information containing details about prospective customers who intend to purchase products through online orders from the website. This data is input by the customer and then stored by the system in the database. The product order data input by the customer is important to the company. Securing the computer network connected to the database no longer guarantees data security because data breaches can be caused by "insiders" or parties directly connected to the database, such as database administrators or even hosting providers. This situation necessitates that the contents of the database, such as product order data, be secured without the involvement of the database administrator. Therefore, the appropriate solution to secure this order data in the database is by applying cryptography. Cryptography can be used to secure data. Hence, database users require assistance in fulfilling their security needs for the stored data. Cryptography is the art and science of protecting data transmission by transforming it into a specific code, intended only for those who have a key to revert the code back, ensuring the confidentiality of the data or message. The Advanced Encryption Standard (AES) is a cryptographic algorithm that is the standard for symmetric key encryption algorithms today. In the AES-128 cryptographic algorithm, a 128-bit plaintext block is first converted into a 4x4 hexadecimal matrix called a state. Each element of the state is 1 byte in size.
Keywords: *Cryptography, AES, Encryption, Security, Order Data, Plaintext*

1. PENDAHULUAN

PT. Sentral Sehat Sejahtera Indonesia merupakan sebuah perusahaan *direct selling* yang menjual produk kesehatan dan kecantikan melalui media aplikasi berbasis *website*. Bagi pihak konsumen, menggunakan *website* dapat membuat waktu berbelanja menjadi singkat. Tidak perlu lagi berlama-lama mengelilingi pusat pertokoan untuk mencari barang yang diinginkan. Calon pelanggan atau konsumen dapat menemukan *website*, membaca atau melihat detail produk, serta dapat melakukan pemesanan produk secara *online*. Di dalam aplikasi *website* pada perusahaan tersebut memiliki sebuah server. Data konsumen yang memesan produk tersebut disimpan di dalam *database*.

Database menjadi sangat penting dalam perusahaan saat ini dan *database* berisi informasi data penting perusahaan seperti data-data pemesanan produk konsumen. Keamanan *web database* adalah isu paling penting di dalam sebuah aplikasi *web* yang ditujukan untuk mendukung aktivitas *E-Commerce*[1] seperti melakukan pemesanan produk konsumen.

Data pemesanan produk adalah data yang berisikan tentang data calon konsumen yang hendak membeli produk melalui pemesanan online dari *website*. Data tersebut diinput oleh konsumen lalu disimpan oleh sistem ke dalam *database*. Data pemesanan produk yang diinput oleh konsumen adalah data yang penting bagi perusahaan. Pengamanan terhadap jaringan komputer yang terhubung dengan *database* sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh "orang dalam" atau pihak-pihak yang langsung berhubungan dengan database

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 4, Bulan 2024, Hal 440-449
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

seperti administrator *database* atau pihak *hosting* sekalipun. Hal ini menyebabkan isi dari *database* seperti data pemesanan produk harus diamankan tanpa campur tangan administrator *database*. maka dari itu solusi yang tepat untuk mengamankan data pemesanan tersebut di dalam *database* adalah dengan menerapkan ilmu Kriptografi.

Kriptografi dapat digunakan untuk mengamankan data. Oleh karena itu, pengguna database membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya. Penerapan kriptografi pada Penelitian ilmiah ini akan difokuskan bagaimana kriptografi dapat mengamankan data sampai pada level baris (*row*) dan kolom (*field*) dengan tetap memperhatikan integritas data dan kewenangan setiap pengguna *database*. Algoritma kriptografi yang akan digunakan ialah algoritma kriptografi simetris dan bersifat *stream cipher* sehingga data hasilenkripsi (*ciphertext*) mempunyai ukuran yang sama dengan data asli (*plaintext*). Teknik kriptografi simetris dipilih karena diharapkan dengan algoritma ini proses enkripsi-dekripsi data dapat dilakukan dengan waktu yang lebih cepat dibandingkan dengan algoritma kriptografi kunci publik (asimetris)[2].

Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditunjukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dalam kriptografi, data atau pesan yang dikirim melalui jaringan akan disamarkan sedemikian rupa. Sehingga data tersebut bisa diperoleh dan dibaca oleh orang lain, maka pihak yang tidak berhak atau berwenang tersebut tidak akan bisa mengerti arti dari data tersebut[3].

Advanced Encryption Standard (AES) adalah algoritma kriptografi yang menjadi standard algoritma enkripsi kunci simetris pada saat ini. Dalam algoritma kriptografi AES-128, 1 blok *plaintext* berukuran 128 bit terlebih dahulu dikonversi menjadi matriks heksadesimal berukuran 4x4 yang disebut *state*. Setiap elemen state berukuran 1 *byte*. Pada data teks, proses enkripsi diawali dengan mengkonversi teks menjadi kode ASCII dalam bilangan heksadesimal yang dibentuk menjadi matriks *byte* 4x4. Selanjutnya dilakukan beberapa transformasi dasar seperti *subbytes*, *shiftrows*, *mixcolumns*, dan *addrounkey*. Kriptografi AES 128 bit memiliki ruang kunci 128 bit yang merupakan nilai yang sangat besar dan dianggap aman untuk digunakan sehingga terhindar dari *brute force attack*[4].

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi adalah ilmu yang berdasarkan pada teknik matematika yang erat kaitanya dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentifikasi entitas. Jadi pengertian krriptografi modern adalah bukan hanya penyembunyian pesan, namun lebih pada sekumpulan teknik yang menyediakan keamaan informasi[5]. Kriptografi berasal dari bahasa Yunani, Menurut bahasa tersebut kata kriptografi dibagi menjadi dua kata yaitu "*kryptos*" dan "*graphein*". Kryptos berarti *secret* (rahasia) dan *graphein* writing (tulisan)[6]. Terdapat beberapa istilah penting dalam kriptografi yang harus diketahui antara lain yaitu[7]:

a. *Plaintext* (M) adalah pesan yang hendak dikirimkan (berisi data asli).
b. *Ciphertext* (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi
c. *Enkripsi* (fungsi E) adalah proses pengubahan *plaintext* menjadi *ciphertext*
d. *Dekripsi* (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*.
e. Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

2.2 Tujuan Kriptografi

Ilmu kriptografi terus berkembang, begitu juga dengan tujuannya tidak hanya untuk sekedar memberikan layanan keamanan tetapi juga untuk tujuan lain seperti berikut[8]:

a. *Authentication* : Agar penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi.
b. *Integrity*: Keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak.
c. *Non-repudiation* : Hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
d. *Authority* : Informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya
e. Confidentiality : Merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses
f. *Privacy* : Lebih kea rah data-data yang bersifat pribadi.
g. *Avialability* : Berhubungan dengan ketersediaan informasi ketika dibutuhkan
h. *Access Control* : Aspek ini berhubungan dengan cara pengaturan akses ke informasi. Hal ini biasanya berhubungan dengan masalah otentikasi dan privasi. Kontrol akses seringkali dilakukan dengan menggunakan kombinasi *user id* dan *password*.

2.3 *Advanced Encryption Standard*

Algoritma AES (*Advanced Encryption Standard*) merupakan algoritma cipher yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 4, Bulan 2024, Hal 440-449
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

terbaru yang dipublishkan oleh NIST (*National Institute Of Standard and Technology*) sebagai pengganti algoritma DES (Data Encryption Standard)yang sudah berakhir masa penggunanya. Algoritma DES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit[9].

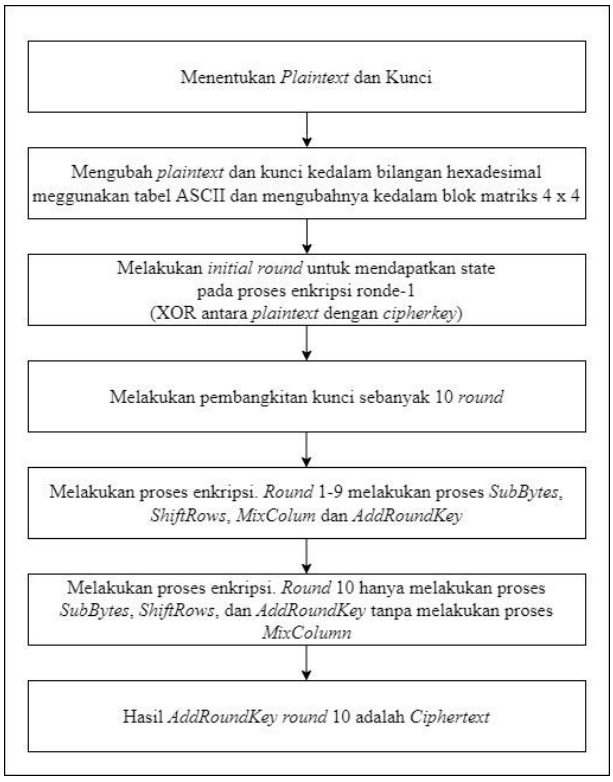
Tabel 1. Perbandingan Jumlah Panjang *Round* dan *Key* AES

AES	Jumlah Kunci	Ukuran Block	Jumlah Putaran
AES – 128	4	4	10
AES – 192	6	4	12
AES – 256	8	4	14

3. HASIL DAN PEMBAHASAN

3.1 Kerangka Kerja

Algoritma kriptografi yang digunakan untuk pembuatan sistem keamanan data pemesanan PT. Sentral Sehat Sejahtera adalah menggunakan algoritma Advanced Encryption Standard 128. Berikut kerangka kerja dari metode *Advanced Encryption Standard 128*.



Gambar 1. Kerangka Kerja Enkripsi AES 128

3.2 Penerapan Metode *Advanced Encryption Standard 128*

Garis besar algoritma AES Rijndael yang beroprasi pada blok 128-bit dengan kunci 128-bit (diluar proses pembangkitan *round key*) adalah sebagai berikut :

Add Round Key, melakukan XOR antara awal (*plaintext*) dengan *cipher key*.

a. Putaran sebanyak Nr-1 kali. Proses yang dilakukan pada setiap putaran adalah:
   1. *Sub Bytes* adalah subsitusi byte menggunakan table subsitusi (S-Box)
   2. *Shift Rows* adalah pergeseran baris-baris *array state* secara *wrapping*.
   3. *Mix Colums* adalah mengacak data di masing-masing kolom *array state*.
   4. *Add Round Key* adalah melakukan XOR antara *state* sekarang dengan *round key*.
b. Putaran terakhir, proses yang dilakukan untuk putaran terakhir adalah:
   1. *Sub Bytes* adalah subsitusi byte menggunakan table subsitusi (S-Box)
   2. *Shift Rows* adalah pergeseran baris-baris *array state* secara *wrapping*.
   3. *Add Round Key* adalah melakukan XOR antara *state* sekarang dengan *round key*.

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 4, Bulan 2024, Hal 440-449
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

3.3 Ekspansi Kunci

Ekspansi kunci dari metode AES 128 menjadi 1408-bit *subkey*[10], proses ini biasanya disebut dengan *keyschedule*. *Subkey* ini diperlukan untuk melakukan proses transformasi *addroundkey* pada setiap *round*. Pada kasus ini, kunci yang akan digunakan yaitu "PTSENTRALSEHATS3". Untuk lebih lengkapnya dapat dilihat di bawah ini adalah proses ekspansi kunci pada algoritma *Advanced Encryption Standard*.

1. Urutkan kunci kedalam blok berukuran 128 bit (16 kode ASCII). Lalu ubah kunci kedalam bentuk *hexadecimal*.

P	T	S	E	N	T	R	A	L	S	E	H	A	T	S	3
50	54	53	45	4E	54	52	41	4C	53	45	48	41	54	53	33

2. Susunan kunci yang telah diubah kedalam bentuk hexadecimal dalam state berukuran 4 x 4 seperti dibawah ini.

W_{i-4}			W_{i-1}
50	4E	4C	41
54	54	53	54
53	52	45	53
45	41	48	33

Cipherkey / kunci ronde ke - 0

3. Setelah itu untuk mendapatkan hasil kolom pertama pada sub kunci, langkah pertama yaitu lakukan fungsi *RotWord* yaitu dengan menggeser setiap bit pada kolom ke-4 ke atas 1 kali dari kunci ronde ke 0.

W_{i-1}

41	→	54	Hasil *RotWord*
54		53	
53		33	
33		41	

4. Kemudian hasil dari RotWord disubtitusikan dengan nilai pada tabel *S-Box* (*SubBytes*).

54	→	20	Hasil Substitusi *S-Box*
53	→	ED	
33	→	C3	
41	→	83	

RotWord

5. Tahap akhir untuk mendapatkan kolom pertama yaitu proses XOR antara kolom pertama dari kunci ronde ke 0, dan hasil dari *SubBytes* lalu di XOR-kan dengan kolom *RCon*.

Tabel 2. Tabel *RCon*

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

Key W_{i-4}		Hasil S-*Box*		Rcon Kol. 1		Kol. 1 *CipherKey*	
50	⊕	20	⊕	01	=	71	Kolom pertama (*wi*) pada kunci ronde selanjutnya (ronde ke-1)
54		ED		00		B9	
53		C3		00		90	
45		83		00		C6	

6. D Untuk mendapatkan kolom kedua, diperoleh dengan XOR antara wi dengan kolom kedua dari kunci ronde ke-0. Untuk mendapatkan kolom ketiga dan keempat kunci ronde ke-1, dilakukan proses seperti memperoleh kolom kedua.

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 4, Bulan 2024, Hal 440-449
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

4E		71	=	3F		4C		3F	=	73
54	⊕	B9		ED		53	⊕	ED		BE
52		90		C2		45		C2		87
41		C6		87		48		87		CF
Key Kol.2		*C.Key* Kol.1		*C.Key* Kol.2		*Key* Kol.3		*C.Key* Kol.2		*C.Key* Kol.3

41		73	=	32
54	⊕	BE		EA
53		87		D4
33		CF		FC
Key Kol.3		*C.Key* Kol.3		*C.Key* Kol.4

7. Dari seluruh proses diatas, maka diperoleh kunci untuk ronde ke-1

71	3F	73	32
B9	ED	BE	EA
90	C2	87	D4
C6	87	CF	FC

Algoritma *Advanced Encryption Standard* 128 bit ini memiliki 10 ronde sehingga diperlukan 10 kunci ronde (*round key*). Untuk mendapatkan kunci ronde ke-2 sampai ke-10,proses diatas diulang sampai 10 kali. Kunci masing-masing ronde akan digunakan saat proses enkripsi dan dekripsi. Dibawah ini akan menunjukkan bagaimana proses demi proses sebelum melakukan proses enkripsi dan dekripsi berikut in adalah hasil enkripsi *key* hingga ronde ke-10 yang nantinya akan digunakan dalam proses enkripsi dan dekripsi :

$$\begin{bmatrix} 71 & 3F & 73 & 32 \\ B9 & ED & BE & EA \\ 90 & C2 & 87 & D4 \\ C6 & 87 & CF & FC \end{bmatrix}$$
Kunci Ronde Ke-1

$$\begin{bmatrix} F4 & CB & B8 & 8A \\ F1 & 1C & A2 & 48 \\ 20 & E2 & 65 & B1 \\ E5 & 62 & AD & 51 \end{bmatrix}$$
Kunci Ronde Ke-2

$$\begin{bmatrix} A2 & 69 & D1 & 5B \\ 39 & 25 & 87 & CF \\ F1 & 13 & 76 & C7 \\ 9B & F9 & 54 & 05 \end{bmatrix}$$
Kunci Ronde Ke-3

$$\begin{bmatrix} 20 & 49 & 98 & C3 \\ FF & DA & 5D & 92 \\ 9A & 89 & FF & 38 \\ A2 & 5B & 0F & 0A \end{bmatrix}$$
Kunci Ronde Ke-4

$$\begin{bmatrix} 7F & 36 & AE & 6D \\ F8 & 22 & 7F & ED \\ FD & 74 & 8B & B3 \\ 8C & D7 & D8 & D2 \end{bmatrix}$$
Kunci Ronde Ke-5

$$\begin{bmatrix} 0A & 3C & 92 & FF \\ 95 & B7 & C8 & 25 \\ 48 & 3C & B7 & 04 \\ B0 & 67 & BF & 6D \end{bmatrix}$$
Kunci Ronde Ke-6

$$\begin{bmatrix} 75 & 49 & DB & 24 \\ 67 & D0 & 18 & 3D \\ 74 & 48 & FF & FB \\ A6 & C1 & 7E & 13 \end{bmatrix}$$
Kunci Ronde Ke-7

$$\begin{bmatrix} D2 & 9B & 40 & 64 \\ 68 & B8 & A0 & 9D \\ 09 & 41 & BE & 45 \\ 90 & 51 & 2F & 3C \end{bmatrix}$$
Kunci Ronde Ke-8

$$\begin{bmatrix} 97 & 0C & 4C & 28 \\ 06 & BE & 1E & 83 \\ E2 & A3 & 1D & 58 \\ D3 & 82 & AD & 91 \end{bmatrix}$$
Kunci Ronde Ke-9

$$\begin{bmatrix} 4D & 41 & 0D & 25 \\ 6C & D2 & CC & 4F \\ 63 & C0 & DD & 85 \\ E7 & 65 & C8 & 59 \end{bmatrix}$$
Kunci Ronde Ke-10

3.4 Enkripsi Kunci

Penjelasan mengenai proses enkripsi berupa data pemesanan produk pada PT. Sentral Sehat Sejahtera. Adapun contoh data pemesanan produk yaitu “HERRY INDRAYANTO”. Berikut ini adalah proses enkripsi dari *plaintext* tersebut.

1. Urutkan *plaintext* dalam blok dan ubah ke bilangan *hexadecimal*.

H	E	R	R	Y		I	N	D	R	A	Y	A	N	T	O
48	45	52	52	59	20	49	4E	44	52	41	59	41	4E	54	4F

2. Susun 16 *byte* pertama dari *plaintext* yang telah di ubah ke bentuk *hexadecimal* ke dalam *state* 4 x 4.

48	59	44	41
45	20	52	4E
52	49	41	54
52	4E	59	4F

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 4, Bulan 2024, Hal 440-449
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

3. *Plaintext* di atas diXOR-kan dengan *Cipherkey* atau kunci ronde ke-0. Proses ini dinamakan *AddRoundKey*.

48	59	44	41
45	20	52	4E
52	49	41	54
52	4E	59	4F

⊕

50	4E	4C	41
54	54	53	54
53	52	45	53
45	41	48	33

=

18	17	08	00
11	74	01	1A
01	1B	04	07
17	0F	11	7C

Plaintext *Cipherkey Round-0* *Ciphertext Round-0*

4. Hasil dari *AddRoundKey* diatas akan menjadi ronde ke-1 yang akan diproses dengan 4 transformasi, yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey*.
5. Pada transformasi *SubBytes*, setiap *byte* akan ditukar dengan table *S-Box*.

18	17	08	00
11	74	01	1A
01	1B	04	07
17	0F	11	7C

Ciphertext

SubBytes →

AD	F0	30	63
82	92	7C	A2
7C	AF	F2	C5
F0	76	82	10

Hasil substitusi *S-Box* (*SubBytes*)

6. Kemudian dilanjutkan dengan melakukan proses *ShitfRows*, yaitu menggeser setiap baris pada *state*.

Tetap →
Digeser 1 *byte* ke kiri →
Digeser 2 *byte* ke kiri →
Digeser 3 *byte* ke kiri →

AD	F0	30	63
82	92	7C	A2
7C	AF	F2	C5
F0	76	82	10

=

AD	F0	30	63
92	7C	A2	82
F2	C5	7C	AF
10	F0	76	82

Hasil substitusi *S-Box* Hasil *ShiftRows*

7. Proses selanjutnya yaitu *MixColumns*. Pada proses ini, dilakukan proses perkalian antara suatu polinominal tetap dengan *state* hasil *ShiftRows*.

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

×

AD	F0	30	63
92	7C	A2	82
F2	C5	7C	AF
10	F0	76	82

=

0E	4A	97	76
8F	AC	9D	14
F0	16	F0	39
AC	49	62	97

Nilai *MixColumn* Hasil *ShiftRows* Hasil *MixColumn*

8. Setelah hasil dari proses *MixColumns* diperoleh, langkah terakhir dari ronde ke-1 yaitu *AddRoundKey*. Proses *AddRoundKey* ini sama dengan sebelumnya, namun state hasil dari proses *MixColumns* diXOR-kan dengan kunci ronde ke-1. Dibawah ini adalah proses *AddRoundKey Round*-1.

0E	4A	97	76
8F	AC	9D	14
F0	16	F0	39
AC	49	62	97

⊕

71	3F	73	32
B9	ED	BE	EA
90	C2	87	D4
C6	87	CF	FC

=

7F	75	E4	44
36	41	23	FE
60	D4	77	ED
6A	CE	AD	6B

Hasil *MixColumn* *CipherKey Round-1* Hasil *AddRoundKey*

9. Begitu juga untuk ronde selanjutnya. Proses diatas akan diulangi sampai ronde ke-10. Hasil dari transformasi proses enkripsi untuk ronde ke-2 sampai ke-10 dapat dilihat di bawah ini.

<u>*Round 2*</u>

State

$$\begin{bmatrix} 7F & 75 & E4 & 44 \\ 36 & 41 & 23 & FE \\ 60 & D4 & 77 & ED \\ 6A & CE & AD & 6B \end{bmatrix}$$

SubBytes

$$\begin{bmatrix} D2 & 9D & 69 & 1B \\ 05 & 83 & 26 & BB \\ D0 & 48 & F5 & 55 \\ 02 & 8B & 95 & 7F \end{bmatrix}$$

ShiftRows

$$\begin{bmatrix} D2 & 9D & 69 & 1B \\ 83 & 26 & BB & 05 \\ F5 & 55 & D0 & 48 \\ 7F & 02 & 8B & 95 \end{bmatrix}$$

MixColumns

$$\begin{bmatrix} AB & 1C & 5F & 34 \\ B4 & 2C & E4 & 5C \\ 21 & 17 & EF & 2A \\ E5 & CB & DD & 51 \end{bmatrix}$$

RoundKey 2

$$\begin{bmatrix} F4 & CB & B8 & 8A \\ F1 & 1C & A2 & 48 \\ 20 & E2 & 65 & B1 \\ E5 & 62 & AD & 51 \end{bmatrix}$$

AddRoundKey

$$\begin{bmatrix} 5F & D7 & E7 & 6E \\ 45 & 30 & 46 & 14 \\ 01 & F5 & 8A & 9B \\ 00 & A9 & 70 & 00 \end{bmatrix}$$

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 4, Bulan 2024, Hal 440-449
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Round 3

State	*SubBytes*	*ShiftRows*
5F D7 E7 6E	CF 0E 94 9F	CF 0E 94 9F
45 30 46 14	6E 04 5A FA	04 5A FA 6E
01 F5 8A 9B	7C E6 7E 14	7E 14 7C E6
00 A9 70 00	63 D3 51 63	63 63 D3 51

MixColumns	*RoundKey 3*	*AddRoundKey*
94 85 89 20	A2 69 D1 5B	36 EC 58 7B
26 E5 2C 23	39 25 87 CF	1F C0 AB EC
92 D9 F8 D5	F1 13 76 C7	63 CA 8E 12
F6 9A 9C 90	9B F9 54 05	6D 63 C8 95

Round 4

State	*SubBytes*	*ShiftRows*
36 EC 58 7B	05 CE 6A 21	05 CE 6A 21
1F C0 AB EC	C0 BA 62 CE	BA 62 CE C0
63 CA 8E 12	FB 74 19 C9	19 C9 FB 74
6D 63 C8 95	3C FB E8 2A	2A 3C FB E8

MixColumns	*RoundKey 4*	*AddRoundKey*
EC D4 9D 85	20 49 98 C3	CC 9D 05 46
6B 76 00 CE	FF DA 5D 92	94 AC 5D 5C
F3 61 5F 2A	9A 89 FF 38	69 E8 A0 12
F8 9A 66 1C	A2 5B 0F 0A	5A C1 69 16

Round 5

State	*SubBytes*	*ShiftRows*
CC 9D 05 46	4B 5E 6B 5A	4B 5E 6B 5A
94 AC 5D 5C	22 91 4C 4A	91 4C 4A 22
69 E8 A0 12	F9 9B E0 C9	E0 C9 F9 9B
5A C1 69 16	BE 78 F9 47	47 BE 78 F9

MixColumns	*RoundKey 5*	*AddRoundKey*
99 1F 89 B0	7F 36 AE 6D	E6 29 27 DD
0E 38 97 51	F8 22 7F ED	F6 1A E8 BC
C8 42 40 45	FD 74 8B B3	35 36 CB F6
22 00 FE BE	8C D7 D8 D2	AE D7 26 6C

Round 6

State	*SubBytes*	*ShiftRows*
E6 29 27 DD	8E A5 CC C1	8E A5 CC C1
F6 1A E8 BC	42 A2 9B 65	A2 9B 65 42
35 36 CB F6	96 05 1F 42	1F 42 96 05
AE D7 26 6C	E4 0E F7 50	50 E4 0E F7

MixColumns	*RoundKey 6*	*AddRoundKey*
B5 41 B4 AD	0A 3C 92 FF	BF 7D 26 52
A0 AA A9 BD	95 B7 C8 25	35 1D 61 98
E2 8D 8C 8B	48 3C B7 04	AA B1 3B 8F
94 FE A0 EA	B0 67 BF 6D	24 99 1F 87

Round 7

State	*SubBytes*	*ShiftRows*
BF 7D 26 52	08 FF F7 00	08 FF F7 00
35 1D 61 98	96 A4 EF 46	A4 EF 46 96
AA B1 3B 8F	AC C8 E2 73	E2 73 AC C8
24 99 1F 87	36 EE C0 17	17 36 EE C0

MixColumns	*RoundKey 7*	*AddRoundKey*
12 8A 7D A9	75 49 DB 24	67 C3 A6 8D
71 99 7A B4	67 D0 18 3D	16 49 62 89
4A AC DB 46	74 48 FF FB	3E E4 24 BD
70 EA 2F C5	A6 C1 7E 13	D6 2B 51 D6

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 4, Bulan 2024, Hal 440-449
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Round 8

State				*SubBytes*				*ShiftRows*			
67	C3	A6	8D	85	2E	24	5D	85	2E	24	5D
16	49	62	89	47	3B	AA	A7	3B	AA	A7	47
3E	E4	24	BD	B2	69	36	7A	36	7A	B2	69
D6	2B	51	D6	F6	F1	D1	F6	F6	F6	F1	D1

MixColumns				*RoundKey 8*				*AddRoundKey*			
9C	35	F9	CB	D2	9B	40	64	4E	AE	B9	AF
5F	19	4D	B9	68	B8	A0	9D	37	A1	ED	24
D3	71	F4	A0	09	41	BE	45	DA	30	4A	E5
6E	55	80	70	90	51	2F	3C	FE	04	AF	4C

Round 9

State				*SubBytes*				*ShiftRows*			
4E	AE	B9	AF	2F	E4	56	79	2F	E4	56	79
37	A1	ED	24	9A	32	55	36	32	55	36	9A
DA	30	4A	E5	57	04	D6	D9	D6	D9	57	04
FE	04	AF	4C	BB	F2	79	29	29	BB	F2	79

MixColumns				*RoundKey 9*				*AddRoundKey*			
F7	4E	53	3A	97	0C	4C	28	60	42	1F	12
03	85	31	23	06	BE	1E	83	05	3B	2F	A0
D1	CE	C3	60	E2	A3	1D	58	33	6D	DE	38
C7	D6	64	E7	D3	82	AD	91	14	54	C9	76

Round 10

State				*SubBytes*				*ShiftRows*			
60	42	1F	12	D0	2C	C0	C9	D0	2C	C0	C9
05	3B	2F	A0	6B	E2	15	E0	E2	15	E0	6B
33	6D	DE	38	C3	3C	1D	07	1D	07	C3	3C
14	54	C9	76	FA	20	DD	38	38	FA	20	DD

RoundKey 10				*AddRoundKey 10*				*AddRoundKey*			
4D	41	0D	25	9D	6D	CD	EC	9D	6D	CD	EC
6C	D2	CC	4F	8E	C7	2C	24	8E	C7	2C	24
63	C0	DD	85	7E	C7	1E	B9	7E	C7	1E	B9
E7	65	C8	59	DF	9F	E8	84	DF	9F	E8	84

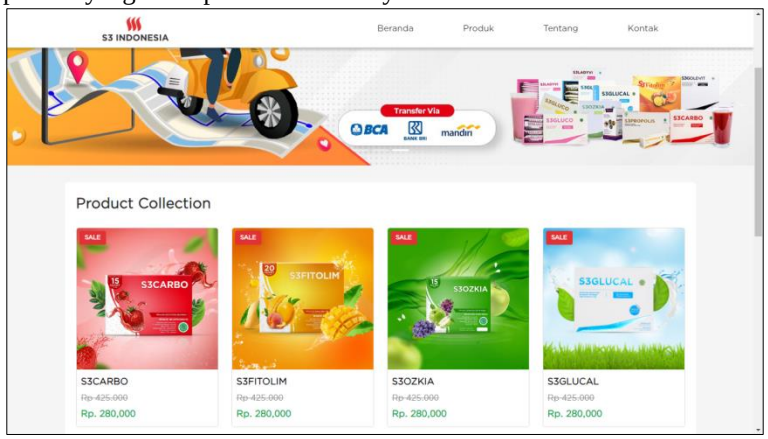
10. Hasil dari proses AddRoundKey pada ronde ke-10 merupakan hasil akhir proses enkripsi yaitu 9D8E7EDF6DC7C79FCD2C1EE8EC24B984

3.5 Hasil Tampilan Antarmuka

Berikut merupakan hasil dari tampilan antarmuka sistem yang telah dibangun.

a. Tampilan Halaman Utama

Halaman utama merupakan halaman awal *customer* mengakses sistem. Pada alaman utama *customer* dapat melihat seluruh data produk yang ditampilkan di dalamnya.

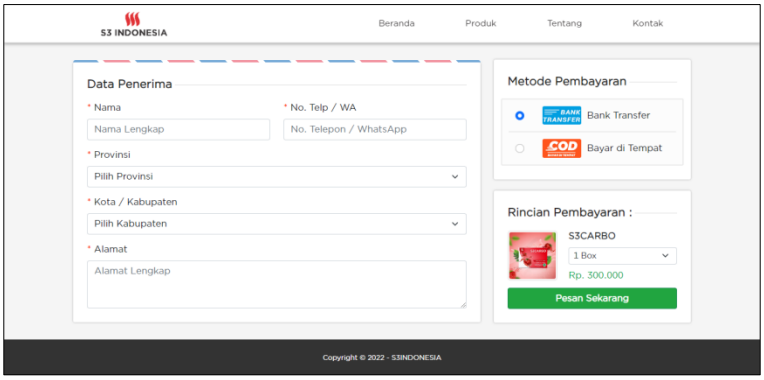


Gambar 2. Tampilan Halaman Utama

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 4, Bulan 2024, Hal 440-449
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

b. Tampilan Halaman Pemesanan Produk

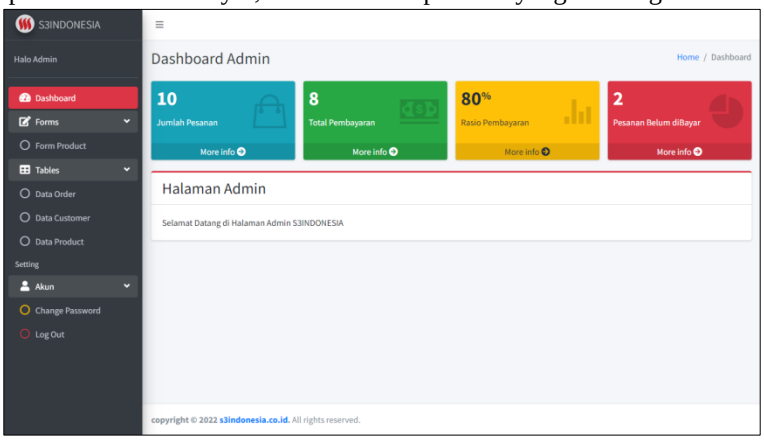
Halaman pemesanan produk menampilkan formulir untuk menginput data pemesanan produk *customer*. Data yang diinput akan dilakukan proses enkripsi terlebih dahulu oleh sistem sebelum disimpan ke dalam *database*.



Gambar 3. Tampilan Halaman Pemesanan Produk

c. Tampilan Halaman Dashboard Admin

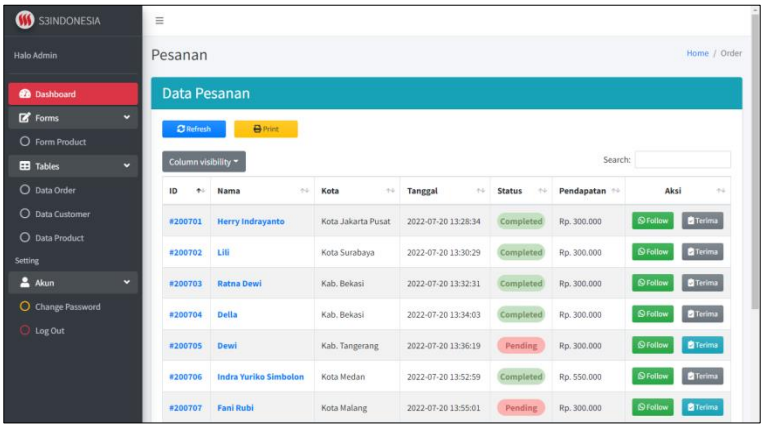
Pada halaman *dashboard* admin akan ditampilkan jumlah data pemesanan yang masuk, jumlah pemesanan yang telah dibayar, jumlah pesanan belum dibayar, dan rasio data pesanan yang dihitung oleh sistem.



Gambar 4. Tampilan Halaman Dashboard Admin

d. Tampilan Halaman Data Pemesanan Produk

Pada halaman data pemesanan produk admin akan ditampilkan seluruh data pemesanan produk yang telah didekripsi oleh sistem.



Gambar 5. Tampilan Halaman Data Pemesanan Produk

4. KESIMPULAN

Algoritma *Advanced Encryption Standard* 128 dapat digunakan dalam melakukan pengamanan data pemesanan produk pada PT. Sentral Sehat Sejahtera dengan melakukan enkripsi setiap data pemesanan produk yang diinput oleh *customer* menjadi bentukk kode-kode yang tidak dapat diketahui lagi artinya dengan menggunakan algoritma perhitungan metode AES 128. sistem keamanan data pemesanan produk PT. Sentral Sehat Sejahtera dirancang dengan

menentukan *use case*, *activity diagram* dan *class diagram* terlebih dahulu. Dengan demikian akan didapatkan alur cara kerja sistem yang akan dibuat sehingga dapat dirancang struktur *database* dan antarmuka sistem.

UCAPAN TERIMAKASIH

Terima kasih diucapkan kepada Bapak Mukhlis Ramadhan dan Ibu Zaimah Panjaitan, serta pihak-pihak yang telah mendukung dalam proses penyelesaian penelitian ini yang tidak dapat disebutkan satu persatu.

DAFTAR PUSTAKA

[1] J. Raden and S. No, "PENGAMANAN DATA MySQL PADA E-COMMERCE DENGAN ALGORITMA AES 256," *Semin. Nas. Sist. Inf. Indones.*, pp. 1–8, 2016.
[2] H. Purwanto, "PENERAPAN KEAMANAN BASIS DATA DENGAN TEKNIK ENKRIPSI," *J. Univ. Suryadarma*, pp. 12–25, 2016.
[3] J. I. Mulawarman *et al.*, "IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD," *J. Inform. Mulawarman*, vol. 10, no. 1, 2015.
[4] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *J. Mat. UNISBA*, vol. 15, no. 1, pp. 7–14, 2016.
[5] A. D. Hidayat and I. Afrianto, "Sistem Kriptografi Citra Digital Pada Jaringan Intranet Menggunakan Metode Kombinasi Chaos Map Dan Teknik Selektif," *J. UNIKOM*, vol. IX, no. 1, pp. 59–66, 2017.
[6] A. C. Purwadi,Hendra Jaya, "APLIKASI KRIPTOGRAFI ASIMETRIS DENGAN METODE DIFFIE-HELLMAN DAN ALGORITMA ELGAMAL UNTUK KEAMANAN TEKS," *J. Ilm. Saintikom*, vol. 13, pp. 183–196, 2014.
[7] L. L. H. Rizky Tahara Shita, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES 128BIT DAN ELGAMAL UNTUK PENGAMANAN E-MAIL PADA BANDARA INTERNASIONAL SULTAN MAHMUD BAHARUDDIN II PALEMBANG," *J. Univ. Budi Luhur*, 2016.
[8] M. Qamal, "KRIPTOGRAFI FILE CITRA MENGGUNAKAN ALGORITMA TEA (TINY ENCRYPTION ALGORITHM)," *J. Univ. Mallikusaleh*, vol. 5, 2014.
[9] A. R. Voni Yuniati, Gani Indriyanta, "ENKRIPSI DAN DEKRIPSI DENGAN ALGORITMA AES 256 UNTUK SEMUA JENIS FILE," *J. Inform.*, vol. 5, no. 1, 2016.
[10] A. H. Aji Fitrah Marisman, "PEMBANGUNAN APLIKASI PEMBANDING KRIPTOGRAFI DEN_GAN CAESAR CIPHER DAN ADVANCE ENCRYPTION STANDARD (AES) UNTUK FILE TEKS," *J. Penelit. Komun. dan Opini Publik*, vol. 19, pp. 213–222, 2015.