JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 2, Maret 2024, Hal 252-263
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Pengamanan Data Penjualan Biji Kopi Sembekandua Menggunakan Metode Advanced Encryption Standard

Muhammad Wisnu Ramadhana[1], Abdullah Muhazir[2], Jaka Prayudha[3]
[1,2] Sistem Informasi, STMIK Triguna Dharma
[3] Sistem Komputer, STMIK Triguna Dharma
Email: [1]wisnudana12@gmail.com, [2]muhazir@gmail.com, [3]jaka.prayudha3@gmail.com
Email Penulis Korespondensi: wisnudana12@gmail.com

Abstrak
CV.Muda Kopi adalah sebuah perusahaan yang bergerak dalam pengelolahan tanaman kopi, biji kopi, dan ekspor impor kopi. Sehingga data dari setiap penjualan harus tercatat dengan baik dan data tidak boleh tersebar diluar dari perusahaan, maka data penjualan hanya bisa dibuka oleh Admin atau Pemimpin perusahaan. Permasalahan yang ada di CV.Muda Kopi yaitu arsip data belum memiliki sistem keamanan, sehingga memungkinkan adanya pihak yang tidak bertanggung jawab untuk memodifikasi dan melakukan pencurian terhadap data-data tersebut. Solusi untuk membantu CV.Muda Kopi dalam mengamankan data penjualan dapat dilakukan dengan membuat sistem keamanan kriptografi yang mempelajari teknik matematika mengenai keamanan data seperti kerahasiaan, integritas, dan otentikasi. Dalam penyelesaian masalah terkait pengamanan data penjualan metode yang digunakan adalah algoritma *advanced encryption standard* yang merupakan standard kriptografi simetri dengan panjang kunci yang digunakan yaitu 128 bit dengan kemungkinan tahan terhadap serangan *exhaustive key search*.
Kata Kunci: E-Security, Keamanan data, Database, Kopi, AES

Abstract
CV.Muda Coffee is a company engaged in the management of coffee plants, coffee beans, and export and import of coffee. So that data from each sale must be recorded properly and data must not be spread outside the company, then sales data can only be opened by the Admin or Company Leader. The problem in CV.Muda Kopi is that data archives do not have a security system, so that it is possible for irresponsible parties to modify and steal these data. Solutions to assist CV.Muda Kopi in securing sales data can be done by creating a cryptographic security system that studies mathematical techniques regarding data security such as confidentiality, integrity and authentication. In solving problems related to securing sales data, the method used is the advanced encryption standard algorithm, which is a standard symmetric cryptography with a key length of 128 bits and the possibility of being resistant to exhaustive key search attacks.
Keywords*: E-Security, Data security, Database, Copy, AES*

1. PENDAHULUAN

Kopi merupakan salah satu hasil komoditi perkebunan yang memiliki nilai ekonomis yang cukup tinggi di antara tanaman perkebunan lainnya dan berperan penting sebagai sumber devisa negara. Kopi tidak hanya berperan penting sebagai sumber devisa melainkan juga merupakan sumber penghasilan bagi tidak kurang dari satu setengah juta jiwa petani kopi di Indonesia[1]. CV.Muda Kopi adalah perusahaan yang telah bergerak dalam mengelola biji kopi. Menjual biji kopi Sembekandua Arabika, bubuk kopi Arabika dan Robusta. CV.Muda Kopi sudah melakukan penjualan ke seluruh wilayah Indonesia dan luar negeri.

CV.Muda Kopi pernah mengalami sebuah kejadian manipulasi data penjualan yang dilakukan oleh salah satu karyawan sehingga membuat perusahaan mengalami kerugian. Data Penjualan CV.Muda Kopi adalah salah satu data yang bersifat rahasia disimpan dalam arsip elektronik, yang mana hanya pihak-pihak tertentu saja yang dapat menerima dan mengubah data tersebut (Pemimpin perusahaan dan beberapa Pegawai tertentu). Namun hal ini, tidak terlepas dari adanya ancaman manipulasi dan pencurian data oleh pihak-pihak yang tidak berwenang seiring persaingan bisnis di bidang kopi yang semakin sengit, sehingga pentingnya pengamanan pada data penjualan untuk menjaga keakuratan dan kerahasiaan data.

Dalam penerapan keamanan data digital dapat dilakukan dengan beberapa cara, seperti dengan menerapkan teknik penyamaran data (*cryptography*). Kriptografi adalah bidang yang mempelajari teknik atau ilmu matematika, kriptografi berkaitan dengan keamanan informasi, kerahasiaan data, integritas data, dan otentikasi data[2]. Dalam cabang ilmu kriptografi, terdapat dua proses yang sangat penting harus dilakukan, yaitu: proses enkripsi dan dekripsi. Proses enkripsi adalah proses mengubah informasi menjadi bentuk lain yang tidak dapat dipahami menggunakan algoritma tertentu, sedangkan proses dekripsi adalah proses memulihkan informasi yang dienkripsi sehingga dapat dipahami kembali[3].

Salah satu algoritma pada kriptografi adalah AES (*Advanced Encryption Standard)* yang termasuk dalam kelompok *block cipher* yang dapat mengenkripsi atau menyandikan dan dekripsi sebuah informasi. AES adalah sebuah algoritma *block cipher* dengan karakteristik sebagai berikut: Biasanya menggunakan sistem permutasi dan penggantian (*P-Box* dan *S-Box)*. Ada tiga jenis AES berdasarkan panjang kunci pada umumnya, yaitu AES-128, AES-192, dan AES-256.[4]

Penggunaan *E-Security* dengan menggunakan metode AES-128 sangatlah tepat dalam penelitian ini, didukung oleh beberapa penelitian sebelumnya tentang Keamanan Data dengan metode yang sama, seperti penelitian yang membahas tentang : Keamanan Data Gaji Karyawan pada PT. Capella Medan yang bergerak pada bidang otomotif[5]

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 2, Maret 2024, Hal 252-263
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

dan Keamanan Database Data Pelanggaran Hukum Disiplin Prajurit pada Pengadilan Militer I-02 Medan[6].

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Dalam melakukan penelitian, langkah atau cara tertentu digunakan sebagai pedoman dalam proses penelitian agar hasil penelitian dapat memenuhi tujuan yang telah ditetapkan. Jika metode tersebut dipelajari dengan baik maka akan diperoleh hasil penelitian yang lebih baik. Metodologi penelitian ini adalah sebagai berikut:

a. Teknik Pengumpulan Data (*Data Collecting*)
   Data Collecting adalah suatu teknik pengumpulan data yang digunakan untuk mencari informasi yang dibutuhkan dalam penelitian.
   1. Pengamatan Langsung (*Observasi*)
   2. Wawancara (*Interview*)

2.2 Kriptografi

Kata kriptografi berasal dari bahasa Yunani, yang terdiri dari dua kata, yaitu *cryptós* yang berarti tersembunyi dan *gráphein* yang berarti tulisan[7]. Jadi, kriptografi dapat dikatakan seni tulisan dalam hal pengamanan data rahasia. Data yang penting perlu dilakukan pengamanan, dan hal yang paling sering dilakukan adalah kriptografi. Menurut Rinaldi Munir, kriptografi adalah bidang yang mempelajari teknik matematika yang berkaitan dengan keamanan data atau informasi, seperti kerahasiaan, integritas, dan otentikasi.[8]

2.3 Advanced Encrytion Standard

Advanced Encryption Standard merupakan standar kriptografi simetri pengganti DES (*Data Encryption Standard)* yang dianggap lemah dalam faktor keamanan, karena dalam waktu yang singkat kunci enkripsi DES sudah dapat ditemukan. Algoritma AES memiliki ukuran blok 128-bit dengan panjang kunci 128-bit, 192-bit, dan 256-bit untuk memproses blok data dengan mode penyandian blok (*block chiper*).

2.3.1 Proses Ekspansi Advanced Encryption Standard 128-bit

Kunci ronde dibutuhkan untuk setiap ronde transformasi penyandian AES. *Key schedule* adalah proses untuk mendapatkan ekspansi kunci, dimana Nb (Nr + 1) *word*, sehingga AES 128 bit menghasilkan 4(10+1) = 40 *word* = 44 x 32 bit = 1408 bit *subkey*. *Subkey* ini diperlukan karena setiap *round* merupakan suatu inisial dari Nb *word* untuk Nr=0, Nb untuk Nr=1, dan 3 untuk Nr=2,.... dari operasi ini akan didapatkan *key schedule* yang berisi *array linier* 4 *byte word* (wi),0=i(Nr+1)[9].

Langkah-langkah yang terdapat pada proses ekspansi kunci AES 128bit adalah seperti berikut ini:

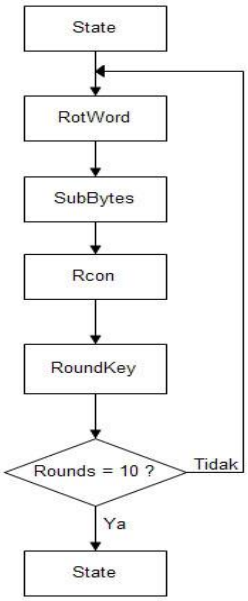
1. *RotWord*, yaitu mengambil masukan empat *byte* kata [a0, a1, a2, a3] dan melakukan perputaran permutasi menjadi [a1, a2, a,3, a0].
2. *SubWord*, mensubsitusi hasil *RotWord* dengan *S-Box Rijndael.*
3. *Rcon*, yaitu melakukan operasi XOR antara kolom pertama dari *RoundKey* ke-0 dengan hasil *SubWord* dan *Round Constanta* (*Rcon*).

Tabel 1. *Rcon*

01	02	04	08	10	20	40	80	1B	3C
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

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 2, Maret 2024, Hal 252-263
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

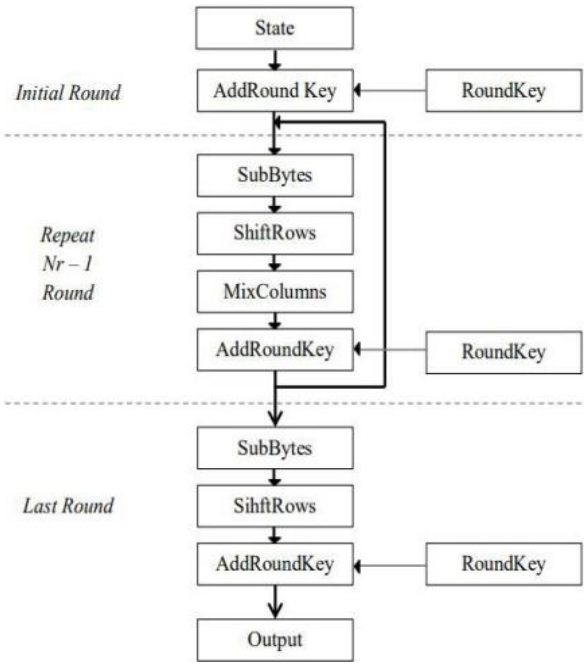
Proses ekspansi kunci *Advanced Encryption Standard* 128 bit dapat digambarkan seperti dibawahini:



Gambar 1. Proses ekspansi kunci AES 128-bit

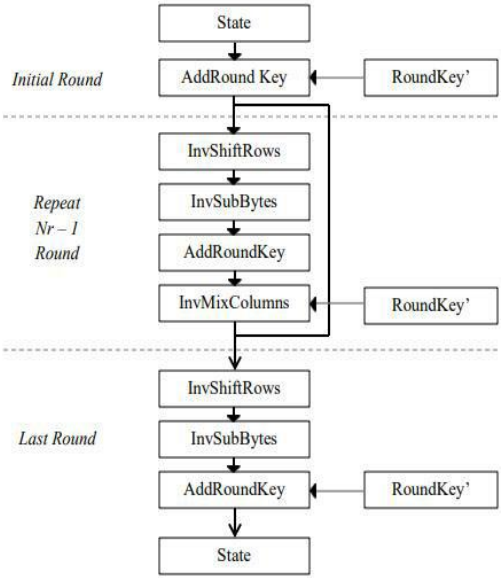
2.3.1 Proses Enkripsi dan Dekripsi Advanced Encryption Standard 128 bit

Proses Enkripsi adalah proses mengubah pesan (*plaintext*) menjadi pesan yang disandikan sehingga pihak lain tidak dapat membaca isi pesan[9]. Sedangkan proses Dekripsi adalah proses pengembalian *chiperteks* menjadi pesan awal yang dapat dibaca. Secara keseluruhan algoritma dekripsi merupakan kebalikan dari algoritma enkripsi, yang berupa transformasi invers. Proses enkripsi dan dekripsi dapat digambarkan seperti berikut[9]:



Gambar 2. Proses enkripsi AES 128-bit

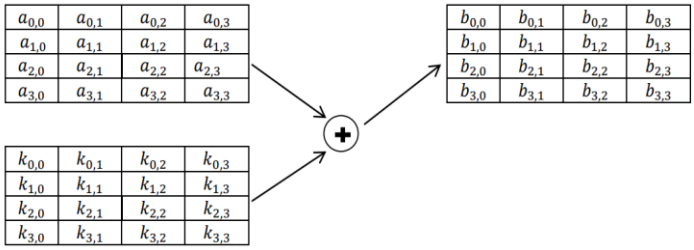
JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 2, Maret 2024, Hal 252-263
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi



Gambar 3. Proses dekripsi AES 128-bit

Awalnya pesan yang akan diamankan dibentuk menjadi sebuah *state* yang kemudian dilakukan tranformasi yang berulang (*round*). Pada proses enkripsi, algoritma AES menggunakan 4 jenis transformasi, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns* dan *AddRoundKey* [10]:

1. *AddRoundKey*, sebagai transformasi penambahan kunci dengan melakukan operasi XOR *state* antara *round key* dengan *plainteks* seperti di bawah ini*:*



Gambar 4. Proses *AddRoundKey*

2. *SubBytes*, sebagai transformasi subsitusi, tahap ini akan dilakukan penukaran isi matriks yang ada dengan maktris lain yang disebut S-Box.

Tabel 2. Tabel subsitusi untuk *Subbytes*

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

3. *InvSubBytes*, proses yang terjadi sama dengan proses *SubBytes* pada enkripsi, hanya saja pada *InvSubBytes* menggunakan inversi S-Box terdahulu.

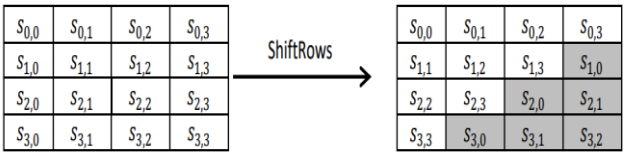
JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 2, Maret 2024, Hal 252-263
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Tabel 3. Tabel subsitusi untuk *InvSubBytes*

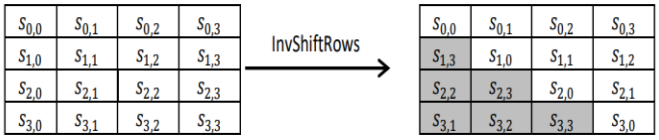
Hex	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	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

x

4. *ShiftRows*, sebagai transformasi permutasi atau dilakukannya pergeseran secara wrapping pada 3 baris *array state*, dimana jumlah pergeseran bergantung pada nilai baris (r). Baris r=1 digeser sejauh 1 *byte*, baris r=2 digeser sejauh 2 *byte*, dan baris r=3 digeser sejauh 3 *byte*. Baris r=0 tidak digeser. Arah pergeseran proses *InvShiftRows* adalah kekanan untuk tiap – tiap baris pada tiga baris terakhir di dalam *state.* Prosesnya dapat dilihat di bawah ini[9].



Gambar 2.5 *ShiftRows*



Gambar 5. *InvShiftRows*

5. *MixColumns*, sebagai transformasi pengacakan atau mengalikan tiap elemen dari *block chipper* dengan matriks menggunakan *dot product*, yang nantinya perkalian keduanya dimasukkan ke dalam *block chipper* baru[10]. Aturan dalam operator *polynomial* adalah jika dikali 01 maka hasilnya tetap, jika dikali 02 maka *bitshift* 1x ke kiri jika MSB = 0 dan *bitshift* 1x ke kiri diikuti operasi XOR dengan 11B (0001 0001 1011) jika MSB = 1, dan jika dikali 03 maka dilakukan operasi dikali 02 dan XOR dengan bilangan *hexadecimal* pada hasil bilangan *ShiftRows* itu sendiri. Berikut adalah uraian perkalian antara *polynomial* dengan hasil *ShiftRows* [11].

$$S'(x) = a(x) \oplus s(x)$$

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

$$S'_{0,c} = (\{02\} \text{ x } S_{0,c}) \oplus (\{03\} \text{ x } S_{1,c}) \oplus (\{01\} \text{ x } S_{2,c}) \oplus (\{01\} \text{ x } S_{3,c})$$
$$S'_{1,c} = (\{01\} \text{ x } S_{0,c}) \oplus (\{02\} \text{ x } S_{1,c}) \oplus (\{03\} \text{ x } S_{2,c}) \oplus (\{01\} \text{ x } S_{3,c})$$
$$S'_{2,c} = (\{01\} \text{ x } S_{0,c}) \oplus (\{01\} \text{ x } S_{1,c}) \oplus (\{02\} \text{ x } S_{2,c}) \oplus (\{03\} \text{ x } S_{3,c})$$
$$S'_{3,c} = (\{03\} \text{ x } S_{0,c}) \oplus (\{01\} \text{ x } S_{1,c}) \oplus (\{01\} \text{ x } S_{2,c}) \oplus (\{02\} \text{ x } S_{3,c})$$

Tranformasi *InvMixColumn* digambarkan sebagai perkalian matriks seperti yang terlihat di bawah ini.

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 2, Maret 2024, Hal 252-263
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

3. HASIL DAN PEMBAHASAN

3.1 Algoritma Sistem

Adapun algoritma dalam metode Advanced Encryption Standard yang akan digunakan untuk menyelesaikan permasalahan adalah melakukan proses ekspansi kunci, enkripsi, dan dekripsi.

3.1.1 Ekspansi Kunci

Ekspansi kunci dibutuhkan untuk proses enkripsi dan deskripsi pada algoritma *Advanced Encryption Standard*. Maksimal panjang kunci pada algoritma *Advanced Encryption Standard* 128 bit adalah 16 digit yang membutuhkan adalah 10 kunci ronde dalam ekspansi kunci. Kunci yang digunakan pada kasus ini adalah "SEMBEKANDUA KOPI". Berikut adalah proses ekspansi kunci *advanced encryption standard* [12]:

1. Urutkan *plaintext* kunci kedalam blok berukuran 128 bit (16 Kode ASCII), kemudian kunci diubah kedalam bentuk *Hexadecimal.*

S	E	M	B	E	K	A	N	D	U	A		K	O	P	I
53	45	4D	42	45	4B	41	4E	44	55	41	20	4B	30	50	49

2. Selanjutnya adalah mengubah kunci yang telah diubah ke dalam *state* 4 x 4 seperti berikut:

53	45	44	4B
45	4B	55	30
4D	41	41	50
42	4E	20	49

→ *RoundKey* ke-0

3. Setelah itu, melakukan fungsi *RotWord*, yaitu dengan menggeser setiap bit pada kolom 4 ke atas 1 kali menggunakan *RoundKey* ke-0 untuk menghasilkan *RoundKey* ke-1.

4B	→	30
30		50
50		49
49		4B

4. Setelah itu, melakukan substitusi hasil dari *RotWord* dengan nilai yang ada pada tabel S-Box (*SubBytes*)

30	→	04
50	→	53
49	→	3B
4B	→	B3

5. Selanjutnya, untuk mendapatkan kolom pertama dari *RoundKey* ke-1 adalah proses XOR antara kolom pertama dari *RoundKey* ke-0 dan hasil dari *SubBytes* di XOR-kan dengan *Rcon*.

Tabel 3.1 *Rcon*

01	02	04	08	10	20	40	80	1B	3C
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

53	⊕	04	⊕	01	⊕	56	Kolom ke-1
45		53		00		16	
4D		3B		00		76	
42		B3		00		F1	

6. Untuk mendapatkan nilai kolom selanjutnya dilakukan XOR antara kolom pertama (Wi) dengan kolom kedua dari *RoundKey* ke-0, kemudian untuk mendapatkan kolom berikutnya lakukan proses seperti kolom kedua.

45	⊕	56	⊕	13	Kolom ke-2
4B		16		5D	
41		76		37	
4E		F1		BF	

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 2, Maret 2024, Hal 252-263
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

44		13		57	Kolom ke-3
55	⊕	5D	⊕	08	
41		37		76	
20		BF		9F	

4B		57		1C	Kolom ke-4
30	⊕	08	⊕	38	
50		76		26	
49		9F		D6	

7. Dari seluruh proses yang telah dilakukan seperti di atas, maka didapatlah *RoundKey* ke-1, yaitu :

56	13	57	1C
16	5D	08	38
76	37	76	26
F1	BF	9F	D6

Untuk mendapatkan *RoundKey* ke-2 sampai dengan *RoundKey* ke-10, proses di atas diulang sebanyak 10 kali. Di bawah ini merupakan hasil ekspansi kunci dari setiap *round* yang akan digunakan untuk proses enkripsi dan dekripsi

RoundKey ke-1 *RoundKey* ke-2 *RoundKey* ke-10

56	13	57	1C
16	5D	08	38
76	37	76	26
F1	BF	9F	D6

53	40	17	0B
E1	BC	B4	8C
80	B7	C1	E7
6D	D2	4D	9B

FA	52	E2	…
33	AA	C4	44
A3	C4	1E	AB
E5	67	62	62

3.2 Proses Enkripsi

Proses enkripsi akan dilakukan pada data penjualan CV.Muda kopi. *Plaintext* yang dienkripsi adalah "PENJUALAN BULAN1", dengan proses enkripsi seperti berikut ini:

1. *Plaintext* diurutkan kedalam blok dan diubah kedalam bentuk bilangan *hexadecimal*.

P	E	N	J	U	A	L	A	N		B	U	L	A	N	1
50	45	4E	4A	55	41	4C	41	4E	20	42	55	4C	41	4E	31

2. *Plaintext* yang diubah ke *hexadecimal* yang telah disusun 16 *byte* pertama dibentuk kedalam *state* 4 x 4.

50	55	4E	4C
45	41	20	41
4E	4C	42	4E
4A	41	55	31

3. Selanjutnya proses *AddRoundKey*, pada proses ini XOR-kan *plaintext* dengan *RoundKey* ke-0.

50	55	4E	4C		53	45	44	4B		03	10	0A	07
45	41	20	41	⊕	45	4B	55	30	=	00	0A	75	71
4E	4C	42	4E		4D	41	41	50		03	0D	03	1E
4A	41	55	31		42	4E	20	49		08	0F	75	78

4. Hasil dari *AddRoundKey* diatas akan menjadi *round* ke-1 untuk diproses dengan 4 transformasi, yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey*.
   a. Transformasi pertama yaitu *SubBytes*, pada tahap ini setiap *byte* akan ditukar dengan nilai pada tabel *S-Box*.

03	10	0A	07
00	0A	75	71
03	0D	03	1E
08	0F	75	78

→

7B	CA	67	C5
63	67	9D	A3
7B	D7	7B	72
30	76	9D	BC

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 2, Maret 2024, Hal 252-263
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

b. Transformasi berikutnya adalah *ShiftRows*, baris pertama tidak ada pergeseran, baris kedua dilakukan pergeseran 1 *byte* ke kiri, pada baris ketiga digeser 2 *byte* ke kiri dan baris keempat digeser 3 *byte* ke kiri.

7B	CA	67	C5
63	67	9D	A3
7B	D7	7B	72
30	76	9D	BC

→

7B	CA	67	C5
67	9D	A3	63
7B	72	7B	D7
BC	30	76	9D

c. Selanjutnya adalah proses *MixColumns*, dimana proses ini akan melakukan perkalian antara dot product dengan *state* hasil dari *ShiftRows*.

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

X

7B	CA	67	C5
67	9D	A3	63
7B	72	7B	D7
BC	30	76	9D

d. Tranformasi akhir dari *round* ke-1 adalah *AddRoundKey*, hasil dari *MixColumns* akan di XOR-kan dengan *RoundKey* ke-1, seperti dibawah ini.

98	71	3D	7E
84	4D	C1	FC
35	E3	A8	AF
F2	CA	9D	C1

⊕

56	13	57	1C
16	5D	08	38
76	37	76	26
F1	BF	9F	D6

=

CE	62	6A	62
92	10	C9	C4
43	D4	DE	89
03	75	02	17

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

Round ke-10

SubBytes

1E	5E	89	E9
26	20	1E	D4
09	BF	31	5A
1A	61	8D	1C

ShiftRows

1E	5E	89	E9
20	1E	D4	26
31	5A	09	BF
1C	1A	61	8D

RoundKey ke-10

FA	52	E2	E4
33	AA	C4	44
A3	C4	1E	AB
E5	67	62	62

AddRoundKey

E4	0C	6B	0D
13	B4	10	62
92	9E	17	14
F9	7D	03	EF

Hasil dari proses enkripsi yaitu: E41392F90CB49E7D6B1017030D6214EF

3.3 Proses Dekripsi

Proses-proses transformasi pada dekripsi dalam metode *Advanced Encryption Standard* yaitu *InvSubBytes*, *InvShiftRows*, *InvMixColumns* dan *AddRoundKey*. *AddRoundKey* merupakan transformasi yang bersifat *self-invers*. Kunci yang digunakan sama dengan yang digunakan pada proses enkripsi. Berikut adalah proses dekripsi dari hasil ciphertext yang telah diperoleh dari proses enkripsi sebelumnya. Berikut adalah proses dekripsi dari *chipertext* "E41392F90CB49E7D6B1017030D6214EF" :

Round ke-2

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 2, Maret 2024, Hal 252-263
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

InvShiftRows

60	D2	D1	10
4F	16	B9	55
7C	88	C0	16
4C	78	94	D2

InvSubBytes

90	7F	51	7C
92	FF	DB	ED
01	97	1F	FF
5D	C1	E7	7F

RoundKey ke-8

32	A9	18	B6
4E	7F	F7	EE
AB	A7	BD	6F
C4	08	87	05

AddRoundKey

A2	D6	49	CA
DC	80	2C	03
AA	30	A2	90
99	C9	60	7A

InvMixColumn

6D	6F	EA	10
2C	64	E8	E1
FF	CC	54	0C
F3	68	F1	DE

Round ke-10

InvShiftRows

7B	CA	67	C5
63	67	9D	A3
7B	D7	7B	72
30	76	9D	BC

InvSubBytes

03	10	0A	07
00	0A	75	71
03	0D	03	1E
08	0F	75	78

RoundKey ke-0

53	45	44	4B
45	4B	55	30
4D	41	41	50
42	4E	20	49

AddRoundKey

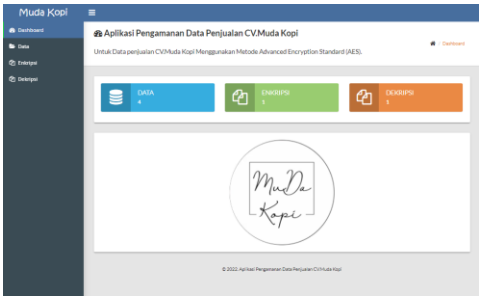
50	55	4E	4C
45	41	20	41
4E	4C	42	4E
4A	41	55	31

Hasil dari proses dekripsi yaitu: 50454E4A55414C414E2042554C414E31 dan apabila diubah melalui kode ASCII maka akan mengembalikan teks yang diubah menjadi plaintext kembai yaitu “PENJUALAN BULAN1”.

3.4 Implementasi Sistem

a. Tampilan Menu Utama (Dashboard)

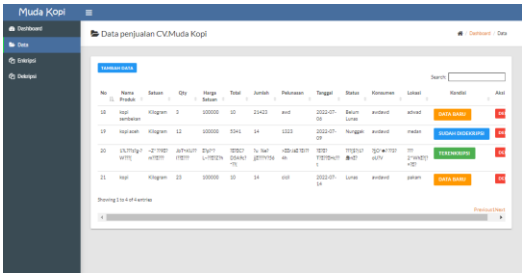
Berikut adalah menu utama (*Darshboard*) dari *website* yang dirancang sebagai halaman paling awal dari sistem yaitu:



Gambar 6. Tampilan Menu Utama (*Dashboard*)

b. Tampilan Halaman Menu Data

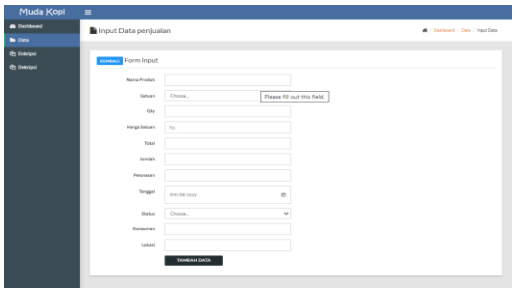
Berikut adalah halaman menu data untuk melihat isi dari data penjualan biji kopi sembekandua :



Gambar 7. Tampilan Menu Data

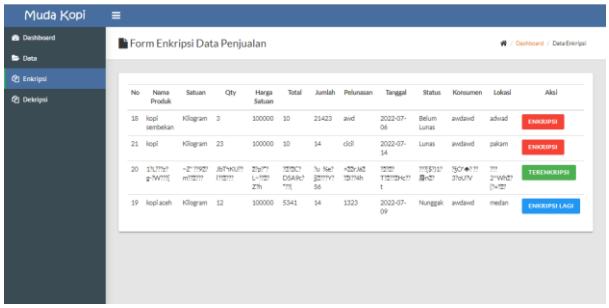
JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 2, Maret 2024, Hal 252-263
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

c. Tampilan Halaman Tambah Data
Berikut adalah halaman tambah data untuk menambahkan data pada penjualan biji kopi sembekandua :



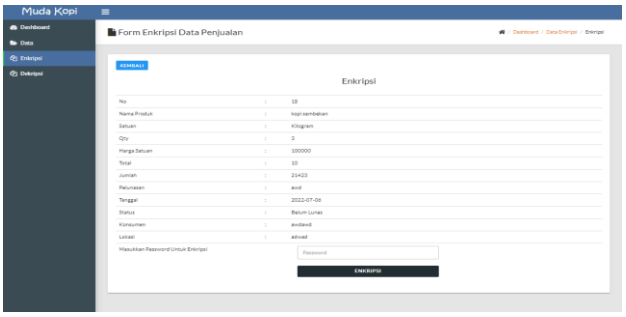
Gambar 8. Tampilan Tambah Data

d. Tampilan Halaman Menu Enkripsi
Berikut adalah halaman enkripsi untuk melakukan enkripsi terhadap data penjualan yang akan di amankan yaitu:



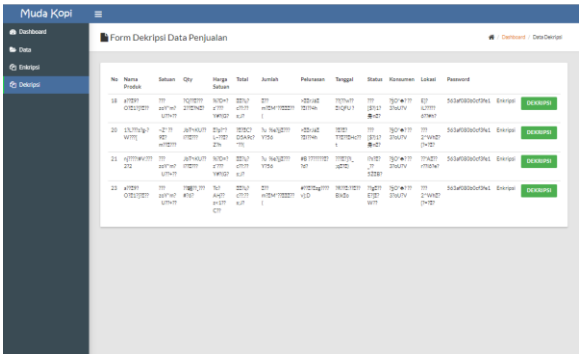
Gambar 9. Tampilan Menu Enkripsi

e. Tampilan Halaman Menu Enkripsi Data
Berikut adalah halaman enkripsi data untuk melakukan enkripsi terhadap data penjualan yang akan di amankan yaitu:



Gambar 10. Tampilan Menu Enkripsi Data

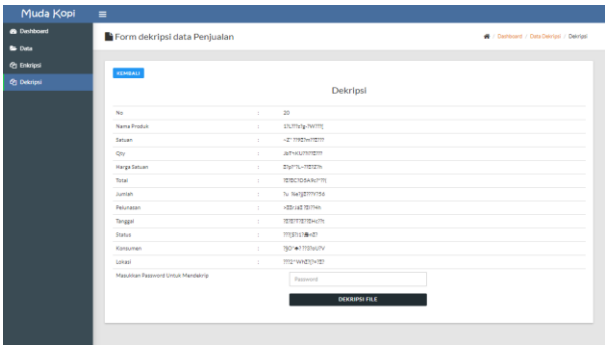
f. Tampilan Halaman Menu Dekripsi
Berikut adalah halaman dekripsi untuk melakukan dekripsi terhadap data penjualan yang telah di amankan yaitu:



Gambar 11. Tampilan Menu Dekripsi

JURNAL SISTEM INFORMASI TGD
Volume 3, Nomor 2, Maret 2024, Hal 252-263
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

g. Tampilan Halaman Menu Dekripsi Data
Berikut adalah halaman dekripsi data untuk melakukan dekripsi terhadap data penjualan yang telah di amankan yaitu:



Gambar 12. Tampilan Menu Dekripsi Data

4. KESIMPULAN

Setelah dilakukan penelitian, dan berdasarkan uraian pada bab-bab sebelumnya, maka kesimpulan dari penelitian ini yaitu Berdasarkan hasil analisa, dalam penyelesaian masalah pengamanan data penjualan biji kopi sembekandua pada CV.Muda Kopi, algoritma *advanced encryption standard* 128-bit berhasil diterapkan. Kebutuhan pada sistem telah sesuai dengan kebutuhan dalam pengamanan data penjualan biji kopi sembekandua pada CV.Muda Kopi. Dalam penerapan sistem *E-Security* berbasis *web* mengenai keamanan data penjualan biji kopi sembekandua pada CV.Muda Kopi dapat digunakan dengan hasil keluaran *encode* dan *decode* yaitu *base* 64.

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada Bapak Abdullah Muhazir dan Bapak Jaka Prayudha serta pihak-pihak yang telah mendukung terlaksananya penelitian ini.

DAFTAR PUSTAKA

[1] B. Marhaenanto, D. W. Soedibyo, and M. Farid, "Penentuan lama Sangrai Kopi Terhadap Variasi Derajat Sangrai Menggunakan Model Warna Rgb Pada Pengolahan Citra Digital (Digital Image Processing)," *J. Agroteknologi*, vol. 09, no. 02, pp. 1–10, 2015, [Online]. Available: https://jurnal.unej.ac.id/index.php/JAGT/article/view/3536.

[2] R. Firmansyah and A. A. Permana, "Implementasi Keamanan Pesan Teks Menggunakan Kriptografi Algoritma RSA dengan Metode Waterfall Berbasis Java," vol. 4, no. 1, pp. 217–221, 2019.

[3] A. Y. Mulyadi, E. P. Nugroho, and R. R. J. P, "Implementasi Algoritma AES 128 dan SHA – 256 Dalam Pengkodean pada Sebagian Frame Video CCTV MPEG-2," *JATIKOM J. Teor. dan Apl. Ilmu Komput.*, vol. 1, no. 1, pp. 33–39, 2018.

[4] D. Novianto and Y. Setiawan, "Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Ilm. Inform. Glob.*, vol. 9, no. 2, pp. 83–89, 2019, doi: 10.36982/jig.v9i2.561.

[5] J. Prayudha, "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," vol. 18, no. SAINTIKOM, pp. 119–129, 2019.

[6] K. Zalukhu, Y. Syahra, and T. Syahputra, "Implementasi Sistem Keamanan Database Data Menggunakan Algoritma Advanced Encryption Standard 128 Bit pada Pengadilan Militer I-02 Medan," vol. 3, no. 2, pp. 138–150, 2020.

[7] A. Randi, K. Lazuardy, S. Chandra, and A. Dharma, "Implementasi Algoritma Advanced Encryption Standard pada Aplikasi Chatting berbasis Android," vol. 3, no. 2, pp. 1–10, 2020.

[8] R. Munir, "Kriptografi," in *2*, 2019.

[9] Y. Putra, Y. Yunus, and S. Sumijan, "Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) Terhadap Seragan Cross Site Scripting," *J. Sistim Inf. dan Teknol.*, vol. 3, 2020, doi: 10.37034/jsisfotek.v3i2.110.

[10] G. Grehasen and S. Mulyati, "Pengamanan Database Pada Aplikasi Test Masuk Karyawan Baru Berbasis Web Menggunakan Algoritma Kriptografi AES-128 Dan RC4 Geri," vol. 14, no. 1, pp. 52–60, 2017.

[11] I. Rosmayati, W. Wahyuningsih, E. F. Harahap, and H. S. Hanifah, "Implementasi Data Mining pada Penjualan Kopi Menggunakan Algoritma Apriori," *J. Algoritm.*, vol. 20, no. 1, pp. 99–107, 2023, doi: 10.33364/algoritma/v.20-1.1259.

[12] T. Handayani, N. Hidayat, and R. Taufiq, "Rancang Bangun Sistem Informasi Data Penjualan Berbasis Web Pada Kedai Payon Kopi," *Semin. Nas. Multi Disiplin Ilmu*, pp. 188–193, 2020.