**Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD**
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 55-64
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
*https://ojs.trigunadharma.ac.id/index.php/jsk/index*

# Pengamanan Data Hasil Analisa Menggunakan Metode Advanced Encryption Standard

**Azli Murti Lubis[1], Dicky Nofriansyah[2], Widiarti Ristamaya[3]**
[1,2,3] Sistem Informasi, STMIK Triguna Dharma
Email: [1]azli.murti06@gmail.com, [2]dickynofriansyah@ymail.com, [3]widiartirm87@gmail.com
Email Penulis Korespondensi: azli.murti06@gmail.com

**Article History:**
Received Dec 30th, 2024
Revised Jan 17th, 2025
Accepted Jan 31th, 2025

**Abstrak**

Pusat Penelitian Kelapa Sawit (PPKS) merupakan lembaga penelitian nirlaba milik pemerintah. Salah satu kendala yang dihadapi oleh Pusat Penelitian Kelapa Sawit (PPKS) dalam pengamanan data hasil analisa yang menyebabkan kerentanan data hasil analisa dapat di salah gunakan oleh pihak yang tidak bertanggung jawab. Agar mempermudah dalam proses pengamanan data hasil analisa maka dibuatlah sebuah sistem yang akan mempermudah pihak pusat penelitian kelapa sawit dalam pengamanan data hasil analisa dengan menggunakan sistem kriptografi dengan metode AES (*Advanced Encryption Standard*). Hasil dari penelitian ini adalah terciptanya sebuah sistem yang dapat melakukan proses pengamanan data dengan tingkat keamanan yang baik. Karena AES memberikan tingkat keamanan berdasarkan kunci rahasia yang kompleks sehingga dapat merahasiakan data yang akan diamankan.
**Kata Kunci** : Kriptografi, AES, *Advanced Encryption Standard*, PPKS, Pengamanan Data

***Abstract***

*Palm Oil Research Center (PPKS) is a non-profit research institution owned by the government. One of the obstacles faced by the Palm Oil Research Center (PPKS) is in securing the analysis data which causes the vulnerability of the analysis data to be misused by irresponsible parties. In order to facilitate the process of securing the data from the analysis, a system was created that would make it easier for the palm oil research center to secure the analysis data using a cryptographic system with the AES (Advanced Encryption Standard) method. The result of this research is the creation of a system that can perform the process of securing data with a good level of security. Because AES provides a level of security based on a complex secret key so that it can keep the data to be secured secret.*
***Keyword :*** *Cryptography, AES, Advanced Encryption Standard, PPKS, Data Security*

## 1. PENDAHULUAN

PPKS bernama APA (Algemeene Proefstation der AVROS/Algemeene Vereeniging van Rubberplanters ter Oostkust van Sumatra) yang didirikan pada tanggal 26 September 1916. APA merupakan sebuah lembaga penelitian perkebunan pertama di Sumatra. Pada saat itu, fokus utama penelitian APA adalah komoditi karet, setelah semakin berkembang APA juga menangani penelitian teh dan kelapa sawit [1].

Masalah keamanan data merupakan salah satu aspek penting dari sebuah sistem informasi. Keamanan data menjadi sangat penting untuk pengambilan keputusan. Keputusan yang diambil harus berdasarkan data yang diperoleh [2]. Hal ini membuat data menjadi sangat bahaya jika diketahui oleh pihak yang tidak berhak.

Penelitian ini mencoba untuk menerapkan keamanan menggunakan ilmu kriptografi pada data hasil analisa di Pusat Penelitian Kelapa Sawit Medan. Kriptografi adalah bagian dari ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan keamanan informasi, seperti itegritas data kerahasiaan dalam, keabsahan data, serta autentikasi data[3]. Kriptografi sendiri merupakan seni untuk mengamankan data yang didalamnya terdapat algoritma tertentu yang bertujuan sebagai confusion atau pembingungan, dengan cara mengubah teks asli (plaintext) menjadi teks yang tidak 1 2 bisa dibaca artinya secara langsung oleh manusia atau teks rahasia (ciphertext). Kriptografi mempunyai proses enkripsi dimana dapat mengubah teks atau data (plaintext) menjadi teks rahasia (ciphertext), kemudian sebaliknya proses deskripsi yang dapat mengembalikan teks rahasia (ciphertext) menjadi teks atau data (plaintext). Dalam proses ini digunakan kunci rahasia, semakin banyak kunci rahasia yang digunakan maka semakin bagus. Algoritma kriptografi diklasifikasikan menjadi dua yaitu algoritma simetris dan algoritma asimetris.

Algoritma simetris disebut juga algoritma kriptografi konvensional merupakan algoritma yang penggunaan kunci sama untuk melakukan proses enkripsi dan proses deskripsi. Bagian-bagian algoritma kunci simetris adalah Twofish, MARS, IDEA, DES (Data Encryption Standard), Blowfish, 3DES, AES (Advanced Encryption Standard) [4]. AES merupakan algoritma cryptographic yang penggunaannya untuk melakukan proses mengamankan data. Algoritma AES adalah blok ciphertext simetrik yang dapat melakukan enkripsi dan deskripsi informasi. Enkripsi mengubah data yang tidak dapat dibaca lagi disebut ciphertext, sebaliknya dekripsi adalah mengubah ciphertext menjadi bentuk semula yang

kita kenal sebagai plaintext. Algoritma AES menggunakan kunci kriptografi 128, 192, 256 bit untuk proses enkripsi dan dekripsi data pada blok 128 bit [5]. AES mampu memberikan kemanan yang luar biasa dan juga performansi yang baik [6], itulah mengapa pada penelitian pengamanan data hasil analisa di Laboratorium Pelayanan Pusat Penelitian Kelapa Sawit Medan yang dirancang menggunakan AES dalam implementasi keamanannya.

## 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:

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

### 2.2 Kriptografi

Kriptografi adalah seni dalam menjaga keamanan informasi dengan cara menjadikan pesan sebagai kode yang tidak dapat di pahami dan kemudian mengembalikan kode tersebut ke dalam bentuk aslinya saat dibutuhkan oleh orang yang berhak dengan cara otorisasi pengguna atau siapapun yang diizinkan untuk membacanya. Walau demikian, enkripsi dan deskripsi tidak menjamin seratus persen kemanan pesan dari modifikasi [7].

### 2.3 Advanced Encryption Standard (AES)

AES merupakan blok kode simetris untuk menggantikan DES (*Data Encryption Standard*). Algoritma AES merupakan 15 algoritma simetris yaitu menggunakan Kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES192, dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu round key untuk setiap putaran [14].

## 3. HASIL DAN PEMBAHASAN

### 3.1 Algoritma Sistem

Algoritma sistem merupakan penjelasan langkah-langkah dalam penyelesaian masalah dalam perancangan sistem keamanan data Hasil Analisa dengan menggunakan algoritma AES. Hal ini dilakukan untuk meningkatkan keamanan data Hasil Analisa tersebut.

#### 3.1.1 Proses Ekspansi Kunci

Kunci ronde (round key) dibutuhkan untuk proses enkripsi dan deskripsi pada algoritma Advanced Encryption Standard. Maksimal panjang kunci adalah 16 digit dan jumlah kunci ronde nya adalah 10 kunci ronde yang di peroleh dari proses ekspansi kunci. Pada kasus ini, kunci akan digunakan yaitu “CRUDE PALM OIL” Berikut adalah proses ekspansi kunci advanced encryption standard:

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

| C | R | U | D | E | | P | A | L | M | | O | I | L | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 45 | 52 | 55 | 44 | 45 | 20 | 50 | 41 | 4C | 4D | 20 | 4F | 49 | 4C | 20 | 20 |

2. Selanjutnya yaitu susun kunci yang telah diubah kedalam bentuk heksadesimal kedalam state berukuran 4 x 4 seperti dibawah ini :

| | | | |
|---|---|---|---|
| 43 | 45 | 4C | 49 |
| 52 | 20 | 4D | 4C |
| 55 | 50 | 20 | 20 |
| 44 | 41 | 4F | 20 |

| | | |
|---|---|---|
| 49 | *RotWord* | 4C |
| 4C | | 20 |
| 20 | → | 20 |
| 20 | | 49 |

**Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD**
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 55-64
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
*https://ojs.trigunadharma.ac.id/index.php/jsk/index*

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

| | | |
|---|---|---|
| 4C | → | 29 |
| 20 | → | B7 |
| 20 | → | B7 |
| 49 | → | 3B |

**2.** Tahap yang terakhir yaitu lakukan proses XOR antar kolom pertama dari kunci ronde ke-0, hasil dari SubBytes lalu di-XOR-kan lagi dengan Rcon. Kolom pertama (wi) pada kunci ronde selanjutnya (ronde ke-1) = K1

| | | | | | | |
|---|---|---|---|---|---|---|
| 29 | | 43 | | 01 | | 6B |
| B7 | ⊕ | 52 | ⊕ | 00 | = | E5 |
| B7 | | 55 | | 00 | | E2 |
| 3B | | 44 | | 00 | | 7F |

**3.** Untuk medapatkan kolom kedua, diperoleh dari proses XOR antara Wi dengan kolom kedua dari kunci ronde ke-2. Sedangkan untuk mendapatkan kolom ketiga dan keempat kunci ronde ke-1, dilakukan proses seperti memperoleh kolom kedua.

Kolom ke-2

| | | | | |
|---|---|---|---|---|
| 6B | | 45 | | 2E |
| E5 | ⊕ | 20 | = | C5 |
| E2 | | 50 | | B2 |
| 7F | | 41 | | 3E |

Kolom ke-3

| | | | | |
|---|---|---|---|---|
| 2E | | 4C | | 62 |
| C5 | ⊕ | 4D | = | 88 |
| B2 | | 20 | | 92 |
| 3E | | 4F | | 71 |

Kolom ke-4

| | | | | |
|---|---|---|---|---|
| 62 | | 49 | | 2B |
| 88 | ⊕ | 4C | = | C4 |
| 92 | | 20 | | B2 |
| 71 | | 20 | | 51 |

1. Dari seluruh proses diatas, maka telah didapatlah ekspansi kunci untuk ronde ke-1 yaitu :

| | | | |
|---|---|---|---|
| 6B | 2E | 62 | 2B |
| E5 | C5 | 88 | C4 |
| E2 | B2 | 92 | B2 |
| 7F | 3E | 71 | 51 |

Untuk mendapatkan kunci ronde ke-2 sampai ke-10, proses diatas diulang 10 kali.

*RoundKey* Ke-8

| | | | |
|---|---|---|---|
| F5 | AA | 27 | 9D |
| 55 | 0D | CB | A5 |
| 47 | 62 | B4 | EF |
| E4 | 9A | EF | D3 |

*RoundKey* Ke-9

| | | | |
|---|---|---|---|
| E8 | 42 | 65 | F8 |
| 8A | 87 | 4C | E9 |
| 21 | 43 | F7 | 18 |
| BA | 20 | CF | 1C |

*RoundKey* Ke-10

| | | | |
|---|---|---|---|
| C0 | 82 | E7 | 1F |
| 27 | A0 | EC | 05 |
| BD | FE | 09 | 11 |
| FB | DB | 14 | 08 |

**3.2 Proses Enkripsi**

Proses enkripsi akan dilakukan pada data hasil analisa. Plaintext yang dienkripsi adalah “2,09”, dengan proses enkripsi seperti berikut ini:

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

**Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD**
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 55-64
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
*https://ojs.trigunadharma.ac.id/index.php/jsk/index*

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | , | 0 | 9 | | | | | | | | | | | | |
| 32 | 2C | 30 | 39 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 |

2. Kemudian susun 16 byte pertama dari plaintext yang telah diubah ke bentuk heksadesimal kedalam state 4x4:

| | | | |
|---|---|---|---|
| 32 | 20 | 20 | 20 |
| 2C | 20 | 20 | 20 |
| 30 | 20 | 20 | 20 |
| 39 | 20 | 20 | 20 |

3. Lakukan XOR dengan kunci ronde ke-0. Proses ini dinamakan AddRoundKey.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 32 | 20 | 20 | 20 | | 43 | 45 | 4C | 49 | | 71 | 65 | 6C | 69 |
| ⊕ 2C | 20 | 20 | 20 | = | 52 | 20 | 4D | 4C | | 7E | 00 | 6D | 6C |
| 30 | 20 | 20 | 20 | | 55 | 50 | 20 | 20 | | 65 | 70 | 00 | 00 |
| 39 | 20 | 20 | 20 | | 44 | 41 | 4F | 20 | | 7D | 61 | 6F | 00 |

4. Hasil dari AddRoundKey diatas akan menjadi masukan untuk ronde ke-1 yang akan 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

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 71 | 65 | 6C | 69 | → | A3 | 4D | 50 | F9 |
| 7E | 00 | 6D | 6C | → | F3 | 63 | 3C | 50 |
| 65 | 70 | 00 | 00 | → | 4D | 51 | 63 | 63 |
| 7D | 61 | 6F | 00 | → | FF | EF | A8 | 63 |

   b. Lakukan ShiftRows pada hasil dari subtitusi SubBytes yang dieksekusi lewat pergeseran siklik secara memutar dengan geseran yang acak pada tiga baris terakhir state (baris pertama, r = 0, tidak digeser). Baris ke dua digeser secara siklik ke ke kiri sekali, baris ke tiga dua kali, dan baris ke empat tiga kali.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A3 | 4D | 50 | F9 | A3 | 4D | 50 | F9 |
| F3 | 63 | 3C | 50 | 63 | 3C | 50 | F3 |
| 4D | 51 | 63 | 63 | 63 | 63 | 4D | 51 |
| FF | EF | A8 | 63 | 63 | FF | EF | A8 |

   c. Transformasi MixColumns dengan mengoperasikan state kolom demi kolom pada state kolom, dengan mengkoversikan setiap kolom sebagai polinomial.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A3 | 4D | 50 | F9 | F8 | 42 | F2 | 1E |
| 63 | 3C | 50 | F3 | A3 | 6F | C8 | 5F |
| 63 | 63 | 4D | 51 → | A3 | AD | B0 | 4B |

**Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD**
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 55-64
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
*https://ojs.trigunadharma.ac.id/index.php/jsk/index*

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 63 | FF | EF | A8 | | | | 38 | 6D | 28 | F9 |

d. Langkah terakhir untuk mendapatkan enkripsi putaran pertama, lakukan XOR antara hasil MixColumns dengan RoundKey Ke-1, proses ini disebut AddRoundKey.

| *MixColumns* | | | | | *RoundKey* Ke-1 | | | | | *AddRoundKey* Ke-1 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| F8 | 42 | F2 | 1E | | 6B | 2E | 62 | 2B | = | 93 | 6C | 90 | 35 |
| A3 | 6F | C8 | 5F | ⊕ | E5 | C5 | 88 | C4 | | 46 | AA | 40 | 9B |
| A3 | AD | B0 | 4B | | E2 | B2 | 92 | B2 | | 41 | 1F | 22 | F9 |
| 38 | 6D | 28 | F9 | | 7F | 3E | 71 | 51 | | 47 | 53 | 59 | A8 |

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:

*AddRoundKey* Ke-10

| | | | |
|---|---|---|---|
| AF | B9 | E8 | F8 |
| 37 | 39 | F4 | FE |
| B3 | D4 | 40 | 53 |
| DF | 84 | 0F | BB |

Hasil dari AddRoundKey pada ronde ke-10 merupakan hasil akhir dari proses enkripsi yaitu: AF37B3DFB939D484E8F4400FF8FE53BB.

| | | | |
|---|---|---|---|
| AF | B9 | E8 | F8 |
| 37 | 39 | F4 | FE |
| B3 | D4 | 40 | 53 |
| DF | 84 | 0F | BB |

**3.3 Proses Dekripsi**

Kunci yang digunakan sama dengan yang digunakan pada proses enkripsi. Berikut adalah proses dekripsi dari hasil ciphertext yang telah diperoleh dari proses enkripsi sebelumnya.

| | | | |
|---|---|---|---|
| AF | B9 | E8 | F8 |
| 37 | 39 | F4 | FE |
| B3 | D4 | 40 | 53 |
| DF | 84 | 0F | BB |

**Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD**
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 55-64
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
*https://ojs.trigunadharma.ac.id/index.php/jsk/index*

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

| | | | |
|---|---|---|---|
| AF | B9 | E8 | F8 |
| 37 | 39 | F4 | FE |
| B3 | D4 | 40 | 53 |
| DF | 84 | 0F | BB |

⊕

| | | | |
|---|---|---|---|
| C0 | 82 | E7 | 1F |
| 27 | A0 | EC | 05 |
| BD | FE | 09 | 11 |
| FB | DB | 14 | 08 |

=

| | | | |
|---|---|---|---|
| 6F | 3B | 0F | E7 |
| 10 | 99 | 18 | FB |
| 0E | 2A | 49 | 42 |
| 24 | 5F | 1B | B3 |

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

1. Lakukan InvShiftRows 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, baris ke empat sekali.

| | | | |
|---|---|---|---|
| 6F | 3B | 0F | E7 |
| 10 | 99 | 18 | FB |
| 0E | 2A | 49 | 42 |
| 24 | 5F | 1B | B3 |

| | | | |
|---|---|---|---|
| 6F | 3B | 0F | E7 |
| FB | 10 | 99 | 18 |
| 49 | 42 | 0E | 2A |
| 5F | 1B | B3 | 24 |

2. Hasil dari InvShiftRows disubstitusikan dengan nilai pada tabel S-Box-1 (InvSubBytes).

| | | | |
|---|---|---|---|
| 6F | 3B | 0F | E7 |
| FB | 10 | 99 | 18 |
| 49 | 42 | 0E | 2A |
| 5F | 1B | B3 | 24 |

| | | | |
|---|---|---|---|
| 06 | 49 | FB | B0 |
| 63 | 7C | F9 | 34 |
| A4 | F6 | D7 | 95 |
| 84 | 44 | 4B | A6 |

3. XOR hasil dari InvSubBytes dengan RoundKey Ke-9. Proses ini disebut AddInvRoundKey.

| | | | |
|---|---|---|---|
| 06 | 49 | FB | B0 |
| 63 | 7C | F9 | 34 |
| A4 | F6 | D7 | 95 |
| 84 | 44 | 4B | A6 |

⊕

| | | | |
|---|---|---|---|
| E8 | 42 | 65 | F8 |
| 8A | 87 | 4C | E9 |
| 21 | 43 | F7 | 18 |
| BA | 20 | CF | 1C |

=

| | | | |
|---|---|---|---|
| EE | 0B | 9E | 48 |
| E9 | FB | B5 | DD |
| 85 | B5 | 20 | 8D |
| 3E | 64 | 84 | BA |

4. Hasil dari AddInvRoundKey ditransformasikan oleh InvMixColumns dengan mengoperasikan state kolom demi kolom. Operasi ini dilakukan pada state kolom, dengan mengkonversikan setiap kolom sebagai polinomial.
Lakukan perulangan sepertu yang diatas, hingga didapatkan hsail InvMixColumns seperti sebagai berikut.

| | | | |
|---|---|---|---|
| EE | 0B | 9E | 48 |

| | | | |
|---|---|---|---|
| 7C | 0C | 9D | 85 |

**Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD**
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 55-64
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
*https://ojs.trigunadharma.ac.id/index.php/jsk/index*

| | | | |
|---|---|---|---|
| E9 | FB | B5 | DD |
| 85 | B5 | 20 | 8D |
| 3E | 64 | 84 | BA |

| | | | |
|---|---|---|---|
| 6B | 1F | DB | 3F |
| 74 | F0 | 26 | 1F |
| DF | C2 | EF | 07 |

Proses diatas diulang sampai 10 kalo putaran (round). Berikut adalah hasil dari dekripsi hingga round ke 10:

*Round* Ke-7

| | | | |
|---|---|---|---|
| 45 | 35 | 62 | BA |
| 6E | 49 | 1E | FD |
| B1 | E7 | 26 | 67 |
| F7 | D1 | 3D | 9A |

*Round* Ke-8

| | | | |
|---|---|---|---|
| DC | 50 | 60 | 96 |
| AC | 09 | 14 | 5A |
| 93 | 99 | 83 | C0 |
| C2 | A0 | ED | CB |

*Round* Ke-9

| | | | |
|---|---|---|---|
| A3 | 4D | 50 | F9 |
| 63 | 3C | 50 | F3 |
| 63 | 63 | 4D | 51 |
| 63 | FF | EF | A8 |

Khusus round ke-10 transformasi InvMixColumns tidak dilakukan, cukup hanya InvShiftRows, InvSubBytes, dan AddInvRoundKey.

a. *InvShiftRows*

| | | | |
|---|---|---|---|
| A3 | 4D | 50 | F9 |
| 63 | 3C | 50 | F3 |
| 63 | 63 | 4D | 51 |
| 63 | FF | EF | A8 |

| | | | |
|---|---|---|---|
| A3 | 4D | 50 | F9 |
| F3 | 63 | 3C | 50 |
| 4D | 51 | 63 | 63 |
| FF | EF | A8 | 63 |

b. *InvSubBytes*

| | | | |
|---|---|---|---|
| A3 | 4D | 50 | F9 |
| F3 | 63 | 3C | 50 |
| 4D | 51 | 63 | 63 |
| FF | EF | A8 | 63 |

| | | | |
|---|---|---|---|
| 71 | 65 | 6C | 69 |
| 7E | 00 | 6D | 6C |
| 65 | 70 | 00 | 00 |
| 7D | 61 | 6F | 00 |

c. *AddInvRoundKey*

| | | | |
|---|---|---|---|
| 71 | 65 | 6C | 69 |
| 7E | 00 | 6D | 6C |
| 65 | 70 | 00 | 00 |
| 7D | 61 | 6F | 00 |

| | | | |
|---|---|---|---|
| 43 | 45 | 4C | 49 |
| 52 | 20 | 4D | 4C |
| 55 | 50 | 20 | 20 |
| 44 | 41 | 4F | 20 |

| | | | |
|---|---|---|---|
| 32 | 20 | 20 | 20 |
| 2C | 20 | 20 | 20 |
| 30 | 20 | 20 | 20 |
| 39 | 20 | 20 | 20 |

Selanjutnya mengubah hasil kedalam bentuk teks berdasarkan kode ASCII

32 2C 30 39 20 20 20 20 20 20 20 20 20 20 20 20

d. *PlainText*

2 , 0 9

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 55-64
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Hasil dari proses dekripsi yaitu: AF37B3DFB939D484E8F4400FF8FE53BB dan apabila diubah melalui kode ASCII maka akan mengembalikan teks yang diubah menjadi plaintext kembai yaitu "2,09".

**3.4 Implementasi Sistem**

a. *Form Login*

*Form Login* digunakan untuk mengamankan sistem dari *user-user* yang tidak bertanggung jawab sebelum masuk ke *Form* Utama. Berikut adalah tampilan *Form Login* :

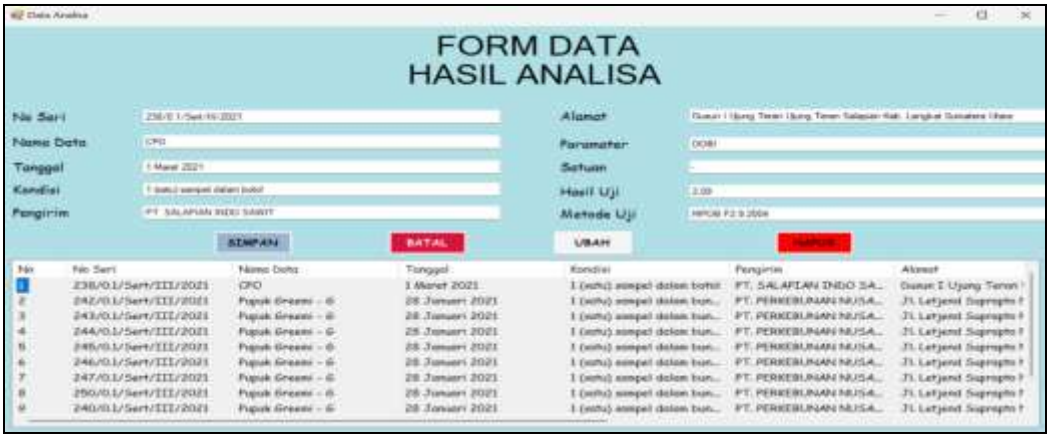

b. *Form* Menu Utama

Form Menu Utama digunakan sebagai penghubung untuk *Form* Data Hasil analisa, Menu AES dan ada beberapa *Form* lainnya.

c. *Form* Data Hasil analisa

*Form* Data Hasil analisa adalah *Form* pengolahan data hasil analisa dalam penginputan data, ubah data dan penghapusan data hasil analisa. Adapun *Form* hasil analisa adalah sebagai berikut.

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 55-64
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index



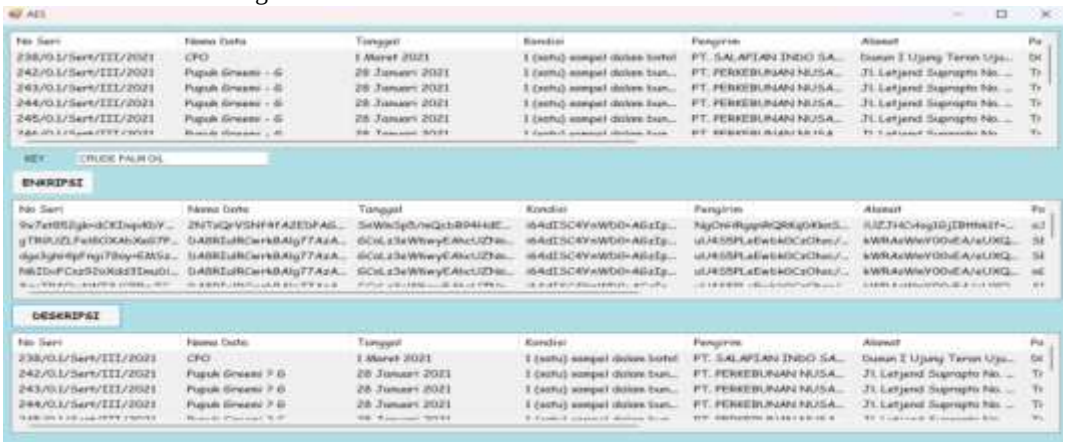

d. *Form* Proses AES

Dalam *Form* Proses AES dapat mengenkripsikan dan deskripsikan adalah sebagai berikut :

a. *Button* Proses Enskripsi berfungsi untuk memproses mengenkripsikan data hasil analisa.

b. *Button* Proses Deskripsi berfungsi untuk memproses mendekripsikan data hasil analisa.

c. *Button* Keluar berfungsi untuk kembali ke menu utama.




## 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 hasil analisa di laboratorium pelayanan pusat penelitian kelapa sawit medan, algoritma *advanced encryption standard* 128-bit berhasil diterapkan. Kebutuhan pada sistem telah sesuai dengan kebutuhan dalam pengamanan data hasil analisa di laboratorium pelayanan pusat penelitian kelapa sawit medan. Dalam penerapan sistem mengenai keamanan data hasil analisa di laboratorium pelayanan pusat penelitian kelapa sawit medan. pusat penelitian kelapa sawit medan dapat digunakan dengan hasil keluaran *encode* dan *decode* yaitu *base* 64.

## UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada Bapak Dicky Nofriyansyah dan Ibu Widiarti Ristamaya serta pihak-pihak yang telah mendukung terlaksananya penelitian ini.

## DAFTAR PUSTAKA

[1] Dr.Muhammad Abdul Ghani, *JEJAK PLANTERS DI TANAH DELI Dinamika Perkebunan di Sumatera Timur 1863-1996*. 2019.

[2] D. A. Wp, "Peningkatan Keamanan Data dengan Metode Cropping Selection Pseudorandom," vol. 4, no. 3, pp. 132–138, 2016.

[3] J. Pseudocode, "KOMUNIKASI BERBASIS TEKS," vol. III, no. September, pp. 129–136, 2016.

[4] R. Toyib, A. Wijaya, P. S. Informatika, F. Teknik, and U. M. Bengkulu, "ANALISIS PERBANDINGAN ALGORITMA SIMETRIS RIVEST CODE 5 DENGAN ALGORITMA SIMETRIS RIVEST CODE 6 ) ( Studi Kasus : SMK Negeri Seluma )," vol. 4, no. 2, pp. 203–209, 2018.

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

[6] A. F. Ramdhansya, E. Ariyanto, H. H. Nuha, F. Informatika, U. Telkom, and T. Buahbatu, "IMPLEMENTASI ADVANCED ENCRYPTION STANDARD ( AES ) PADA SISTEM KUNCI ELEKTRONIK KENDARAAN BERBASIS SISTEM," vol. 2014, no. semnasIF, pp. 92–98, 2014.

[7] S. Wardoyo, R. Fahrizal, and Z. Imanullah, "Aplikasi Teknik Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android," vol. 3, no. 1, pp. 43–53, 2014.

[8] W. H. Haji, S. Mulyono, J. S. Informasi, F. I. Komputer, U. Mercu, and B. Jakarta, "IMPLEMENTASI RC4 STREAM CIPHER UNTUK KEAMANAN BASIS DATA," vol. 2012, no. Snati, pp. 15–16, 2012.

[9] H. Pandiangan, S. Sijabat, P. Studi, and T. Informatika, "PERANCANGAN MEDIA PENGIRIMAN PESAN TEKS DENGAN PENYANDIAN PESAN MENGGUNAKAN ALGORITMA RC4 BERBASIS WEB," vol. 19, no. 1, pp. 63–71, 2016.

[10] K. K. Kriptografi and C. Transposition, "ANALISA DAN IMPLEMENTASI KRIPTOGRAFI PADA PESAN RAHASIA," vol. 3, no. 1, pp. 1–11, 2017.

[11] A. Fauzi and Y. Maulita, "PERANCANGAN APLIKASI KEAMANAN PESAN MENGGUNAKAN ALGORITMA ELGAMAL DENGAN MEMANFAATKAN ALGORITMA ONE TIME," vol. 1, no. 1, 2017.

[12] S. Utara and K. Publik, "KEAMANAN DATA DENGAN METODE KRIPTOGRAFI KUNCI PUBLIK," vol. V, no. 2, pp. 11–15, 2016.

[13] S. A. Jaju, "A Modified RSA Algorithm to Enhance Security for Digital Signature," 2015.