**Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD**
Volume 8; Nomor 1 ; Januari 2025 ; Page 36-45
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
*https://ojs.trigunadharma.ac.id/index.php/jsk/index*

# Pengamanan Data Perusahaan Menggunakan Metode Advanced Encryption Standard

**Rahmad Rivaldi[1], Mukhlis Ramadhan[2], Yopi Hendro Syahputra[3]**
[1,2,3] Sistem Informasi, STMIK Triguna Dharma
Email: [1]rahmad.rvld@gmail.com, [2]mukhlisramadhan.tgd@gmail.com, [3]yopihendro@gmail.com
Email Penulis Korespondensi: [1]rahmad.rvld@gmail.com

**Article History:**
Received Dec 30th, 2024
Revised Jan 15th, 2025
Accepted Jan 31th, 2025

**Abstrak**

Penerimaan Negara bukan pajak adalah seluruh penerimaan pemerintah pusat yang tidak berasal dari penerimaan perpajakan. Hutan dipandang sebagai salah satu sumber penerimaan Negara bukan pajak.Hasil Hutan Bukan Kayu (HHBK) atau Non Timber Forest Product (NTFP) memiliki nilai yang sangat strategis, HHBK merupakan salah satu sumber daya hutan yang memiliki keunggulan komparatif dan bersinggungan langsung oleh masyarakat di sekitar hutan.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, PNBP, HHBK, Pengamanan Data

***Abstract***

*Non-tax state revenue is all central government revenue that does not come from tax revenue. Forests are seen as a source of non-tax state revenue. Non-Timber Forest Products (NTFP) have very strategic value, NTFPs are one of the forest resources that have comparative advantages and have direct contact with communities around the forest.In order to make it easier to secure the data resulting from analysis, a system was created that will make it easier for the palm oil research center to secure data resulting from analysis using a cryptographic system with the AES (Advanced Encryption Standard) method.The result of this research is the creation of a system that can carry out data security processes with a good level of security. Because AES provides a level of security based on complex secret keys so that it can keep the data to be secured confidential.*

*Keywords: Cryptography, AES, Advanced Encryption Standard, PPKS, Data Security*

## 1. PENDAHULUAN

Penerimaan terbesar sebuah Negara berasal dari pajak, namun selain penerimaan pajak ada pula penerimaan yang bukan berasal dari pajak yang memberikan kontribusi cukup besar, penerimaan tersebut disebut dengan Penerimaan Negara bukan pajak (PNBP) [1]. Penerimaan Negara bukan pajak adalah seluruh penerimaan pemerintah pusat yang tidak berasal dari penerimaan perpajakan. Hutan dipandang sebagai salah satu sumber penerimaan Negara bukan pajak [2].

Hasil Hutan Bukan Kayu (HHBK) atau *Non Timber Forest Product* (NTFP) memiliki nilai yang sangat strategis, HHBK merupakan salah satu sumber daya hutan yang memiliki keunggulan komparatif dan bersinggungan langsung oleh masyarakat di sekitar hutan [3].

Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan [4].

Keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan, karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan [5].

Salah satu cara dalam pengamanan data adalah dengan menggunakan teknik penyamaran data yang disebut dengan kriptografi. Kriptografi merupakan ilmu dan seni untuk menjaga pesan agar aman. "*Crypto*" berarti "*secret*" (rahasia) dan "*graphy*" berarti "*writing*" (tulisan). Para pelaku atau praktisi kriptografi disebut *cyrptographers*. Sebuah algoritma kriptografi, disebut *cipher*, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya persamaan kedua matematik tersebut memiliki hubungan matematis yang cukup erat[6].

Algoritma kriptografi terdiri dari dua bagian, yaitu fungsi enkripsi dan dekripsi. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode yang bisa dimengerti menjadi sebuah kode yang tidak bisa terbaca. Enkripsi dapat diartikan sebagai kode atau cipher. Proses yang dilakukan untuk mengamankan pesan (yang disebut *plainteks*) menjadi pesan yang tersembunyi (disebut *chiperteks*) adalah enkripsi (*encryption*). *Ciphertext* adalah pesan yang sudah tidak dapat

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8; Nomor 1 ; Januari 2025 ; Page 36-45
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

dibaca dengan mudah. Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext* disebut deskripsi (*decryption*) [7].

Hingga saat ini terdapat beberapa algoritma dalam kriptologi modern yang mulai dikenal sekitar tahun 1977. Di antara algoritma dalam kriptologi modern tersebut terdapat dua jenis algoritma, yaitu algoritma simestris dan algoritma asimetris. Di dalam algoritma simetris terdapat jenis algoritma *cipherblok* (block cipher), yaitu algoritma dengan proses enkripsi dimana data asli (*plaintext*) diubah ke dalam bentuk bit yang dibagi menjadi blok-blok dengan panjang bit yang sama, seperti AES (*Advanced Encryption Standard*) [8].

## 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

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[9].

### 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[10].

## 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

| S | I | H | A | B | A | K | S | A | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 53 | 49 | 48 | 41 | 42 | 41 | 4B | 53 | 41 | 20 | 20 | 20 | 20 | 20 | 20 | 20 |

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

| | | | |
|---|---|---|---|
| 53 | 42 | 41 | 20 |
| 49 | 41 | 20 | 20 |
| 48 | 4B | 20 | 20 |
| 41 | 53 | 20 | 20 |

3. Untuk mendapatkan kolom pertama pada sub kunci, langkah pertama yaitu dilakukan fungsi RotWord, yaitu dengan menggeser setiap bit pada kolom ke-4 ke atas 1 kali dari kunci ronde ke-0.

**Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD**
Volume 8; Nomor 1 ; Januari 2025 ; Page 36-45
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
*https://ojs.trigunadharma.ac.id/index.php/jsk/index*

| | | |
|---|---|---|
| 20 | *RotWord* | 20 |
| 20 | | 20 |
| 20 | → | 20 |
| 20 | | 49 |

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

| | | |
|---|---|---|
| 20 | → | B7 |
| 20 | → | B7 |
| 20 | → | B7 |
| 20 | → | B7 |

5. 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

| | | | | |
|---|---|---|---|---|
| B7 | | 59 | 01 | E5 |
| B7 | ⊕ | 49 | ⊕ 00 | = FE |
| B7 | | 48 | 00 | FF |
| B7 | | 41 | 00 | F6 |

6. 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

| | | | |
|---|---|---|---|
| C6 | | 42 | A7 |
| BF | ⊕ | 41 | = BF |
| B7 | | 48 | B7 |
| A5 | | 53 | A5 |

Kolom ke-3

| | | | |
|---|---|---|---|
| A7 | | 41 | E6 |
| BF | ⊕ | 20 | = 9F |
| B7 | | 20 | 97 |
| A5 | | 20 | 85 |

Kolom ke-4

| | | | |
|---|---|---|---|
| E6 | | 20 | C6 |
| 9F | ⊕ | 20 | = BF |
| 97 | | 20 | B7 |
| 85 | | 20 | A5 |

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

| | | | |
|---|---|---|---|
| E5 | A7 | E6 | C6 |
| FE | BF | 9F | BF |
| FF | B7 | 97 | B7 |
| F6 | A5 | 85 | A5 |

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

*RoundKey* Ke-8

| | | | |
|---|---|---|---|
| 71 | F0 | AD | D8 |
| 4A | D4 | 40 | 4E |
| 73 | 41 | 97 | ED |

*RoundKey* Ke-9

| | | | |
|---|---|---|---|
| 45 | B5 | 18 | C0 |
| 1F | CB | 8B | C5 |
| 92 | D3 | 44 | A9 |

*RoundKey* Ke-10

| | | | |
|---|---|---|---|
| D5 | 60 | 78 | B8 |
| CC | 07 | 8C | 49 |
| 4F | 9C | D8 | 71 |

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8; Nomor 1 ; Januari 2025 ; Page 36-45
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

| | | | |
|---|---|---|---|
| 41 | 98 | 91 | E0 |

| | | | |
|---|---|---|---|
| 20 | B8 | 29 | C9 |

| | | | |
|---|---|---|---|
| 9A | 22 | 0B | C2 |

**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.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 2 | 0 | , | 0 | 0 | 0 | | | | | | | | | |
| 34 | 32 | 30 | 2C | 30 | 30 | 30 | 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:

| | | | |
|---|---|---|---|
| 34 | 30 | 20 | 20 |
| 32 | 30 | 20 | 20 |
| 30 | 30 | 20 | 20 |
| 2C | 20 | 20 | 20 |

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

| | | | |
|---|---|---|---|
| 34 | 30 | 20 | 20 |
| 32 | 30 | 20 | 20 |
| 30 | 30 | 20 | 20 |
| 2C | 20 | 20 | 20 |

$\oplus$

| | | | |
|---|---|---|---|
| 53 | 42 | 41 | 20 |
| 49 | 41 | 20 | 20 |
| 48 | 4B | 20 | 20 |
| 41 | 53 | 20 | 20 |

$=$

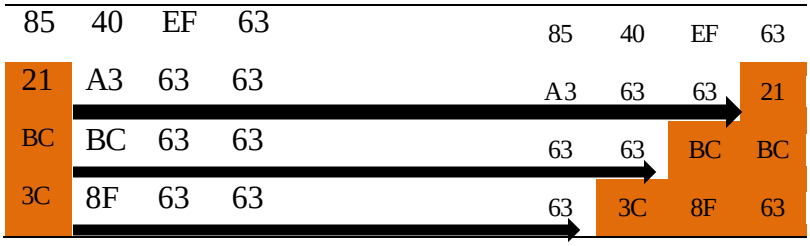
| | | | |
|---|---|---|---|
| 67 | 72 | 61 | 00 |
| 7B | 71 | 00 | 00 |
| 78 | 78 | 00 | 00 |
| 6D | 73 | 00 | 00 |

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

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 67 | 72 | 61 | 00 | → | 85 | 40 | EF | 63 |
| 7B | 71 | 00 | 00 | → | 21 | A3 | 63 | 63 |
| 78 | 78 | 00 | 00 | → | BC | BC | 63 | 63 |
| 6D | 73 | 00 | 00 | → | 3C | 8F | 63 | 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.



**Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD**
Volume 8; Nomor 1 ; Januari 2025 ; Page 36-45
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
*https://ojs.trigunadharma.ac.id/index.php/jsk/index*

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

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 85 | 40 | EF | 63 | | EF | 7A | 53 | 7A |
| A3 | 63 | 63 | 21 | → | 1E | 1F | 79 | 9D |
| 63 | 63 | BC | BC | | 45 | A1 | 65 | 84 |
| 63 | 3C | 8F | 63 | | 92 | B8 | F0 | FE |

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

*MixColumns*

| | | | |
|---|---|---|---|
| EF | 7A | 53 | 7A |
| 1E | 1F | 79 | 9D |
| 45 | A1 | 65 | 84 |
| 92 | B8 | F0 | FE |

⊕

*RoundKey* Ke-1

| | | | |
|---|---|---|---|
| E5 | A7 | E6 | C6 |
| FE | BF | 9F | BF |
| FF | B7 | 97 | B7 |
| F6 | A5 | 85 | A5 |

=

*AddRoundKey* Ke-1

| | | | |
|---|---|---|---|
| 0A | DD | B5 | BC |
| E0 | A0 | E6 | 22 |
| BA | 16 | F2 | 33 |
| 64 | 1D | 75 | 5B |

e. 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

| | | | |
|---|---|---|---|
| BD | BB | 33 | 31 |
| 27 | 13 | 22 | 69 |
| 20 | 72 | 67 | E0 |
| DF | 44 | E2 | 88 |

f. Hasil dari AddRoundKey pada ronde ke-10 merupakan hasil akhir dari proses enkripsi yaitu: BD2720DFBB137244332267E23169E088.

| | | | |
|---|---|---|---|
| BD | BB | 33 | 31 |
| 27 | 13 | 22 | 69 |
| 20 | 72 | 67 | E0 |
| DF | 44 | E2 | 88 |

**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.

| | | | |
|---|---|---|---|
| BD | BB | 33 | 31 |
| 27 | 13 | 22 | 69 |
| 20 | 72 | 67 | E0 |
| DF | 44 | E2 | 88 |

**Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD**
Volume 8; Nomor 1 ; Januari 2025 ; Page 36-45
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.

| | | | |
|---|---|---|---|
| BD | BB | 33 | 31 |
| 27 | 13 | 22 | 69 |
| 20 | 72 | 67 | E0 |
| DF | 44 | E2 | 88 |

⊕

| | | | |
|---|---|---|---|
| D5 | 60 | 78 | B8 |
| CC | 07 | 8C | 49 |
| 4F | 9C | D8 | 71 |
| 9A | 22 | 0B | C2 |

=

| | | | |
|---|---|---|---|
| 68 | DB | 4B | 89 |
| EB | 14 | AE | 20 |
| 6F | EE | BF | 91 |
| 45 | 66 | E9 | 4A |

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.

| | | | |
|---|---|---|---|
| 68 | DB | 4B | 89 |
| EB | 14 | AE | 20 |
| 6F | EE | BF | 91 |
| 45 | 66 | E9 | 4A |

| | | | |
|---|---|---|---|
| F7 | 9F | CC | F2 |
| 54 | 3C | 9B | BE |
| F4 | AC | 06 | 99 |
| D3 | EB | 5C | 68 |

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

| | | | |
|---|---|---|---|
| 68 | DB | 4B | 89 |
| 20 | EB | 14 | AE |
| BF | 91 | 6F | EE |
| 66 | E9 | 4A | 45 |

| | | | |
|---|---|---|---|
| F7 | 9F | CC | F2 |
| 54 | 3C | 9B | BE |
| F4 | AC | 06 | 99 |
| D3 | EB | 5C | 68 |

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

| | | | |
|---|---|---|---|
| F7 | 9F | CC | F2 |
| 54 | 3C | 9B | BE |
| F4 | AC | 06 | 99 |
| D3 | EB | 5C | 68 |

⊕

| | | | |
|---|---|---|---|
| 45 | B5 | 18 | C0 |
| 1F | CB | 8B | C5 |
| 92 | D3 | 44 | A9 |
| 20 | B8 | 29 | C9 |

=

| | | | |
|---|---|---|---|
| B2 | 2A | D4 | 32 |
| 4B | F7 | 10 | 7B |
| 66 | 7F | 42 | 30 |
| F3 | 53 | 75 | A1 |

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.

| | | | |
|---|---|---|---|
| B2 | 2A | D4 | 32 |
| 4B | F7 | 10 | 7B |

| | | | |
|---|---|---|---|
| 07 | FC | 03 | EA |
| E6 | 62 | 11 | EA |

**Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD**
Volume 8; Nomor 1 ; Januari 2025 ; Page 36-45
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
*https://ojs.trigunadharma.ac.id/index.php/jsk/index*

| | | | |
|---|---|---|---|
| 66 | 7F | 42 | 30 |
| F3 | 53 | 75 | A1 |

| | | | |
|---|---|---|---|
| 0B | 50 | 68 | 43 |
| 86 | 3F | 89 | 9B |

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

*Round* Ke-7

| | | | |
|---|---|---|---|
| AC | 61 | F8 | 09 |
| C3 | EB | B7 | 00 |
| 14 | 61 | EB | CB |
| DF | 8C | 92 | 23 |

*Round* Ke-8

| | | | |
|---|---|---|---|
| 67 | C1 | D5 | 65 |
| E0 | 8E | 93 | E1 |
| 89 | C3 | F4 | 47 |
| 39 | 43 | A4 | 9D |

*Round* Ke-9

| | | | |
|---|---|---|---|
| 85 | 40 | EF | 63 |
| A3 | 63 | 63 | 21 |
| 63 | 63 | BC | BC |
| 63 | 3C | 8F | 63 |

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

a. *InvShiftRows*

| | | | |
|---|---|---|---|
| 85 | 40 | EF | 63 |
| A3 | 63 | 63 | 21 |
| 63 | 63 | BC | BC |
| 63 | 3C | 8F | 63 |

| | | | |
|---|---|---|---|
| 85 | 40 | EF | 63 |
| 63 | 63 | 21 | A3 |
| BC | BC | 63 | 63 |
| 3C | 8F | 63 | 63 |

b. *InvSubBytes*

| | | | |
|---|---|---|---|
| 85 | 40 | EF | 63 |
| 63 | 63 | 21 | A3 |
| BC | BC | 63 | 63 |
| 3C | 8F | 63 | 63 |

| | | | |
|---|---|---|---|
| 67 | 72 | 61 | 00 |
| 7B | 71 | 00 | 00 |
| 78 | 78 | 00 | 00 |
| 6D | 73 | 00 | 00 |

c. *AddInvRoundKey*

| | | | |
|---|---|---|---|
| 67 | 72 | 61 | 00 |
| 7B | 71 | 00 | 00 |
| 78 | 78 | 00 | 00 |
| 6D | 73 | 00 | 00 |

| | | | |
|---|---|---|---|
| 53 | 42 | 41 | 20 |
| 49 | 41 | 20 | 20 |
| 48 | 48 | 20 | 20 |
| 41 | 53 | 20 | 20 |

| | | | |
|---|---|---|---|
| 34 | 30 | 20 | 20 |
| 32 | 30 | 20 | 20 |
| 30 | 30 | 20 | 20 |
| 2C | 20 | 20 | 20 |

Selanjutnya mengubah hasil kedalam bentuk teks berdasarkan kode ASCII

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 34 | 32 | 30 | 2C | 30 | 30 | 30 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 |

*PlainText*

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | 2 | 0 | , | 0 | 0 | 0 |

Hasil dari proses dekripsi yaitu: 8563BC3C4063BC8FEF21636363A36363 dan apabila diubah melalui kode ASCII maka akan mengembalikan teks yang diubah menjadi plaintext kembai yaitu “420,000”.

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8; Nomor 1 ; Januari 2025 ; Page 36-45
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

**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.

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8; Nomor 1 ; Januari 2025 ; Page 36-45
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

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.


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 dinas kehutanan sumatera utara, algoritma *advanced encryption standard* 128-bit berhasil diterapkan. Kebutuhan pada sistem telah sesuai dengan kebutuhan dalam pengamanan data hasil analisa di dinas kehutanan sumatera utara. Dalam penerapan sistem mengenai keamanan data hasil analisa di dinas kehutanan sumatera utara. Dinas kehutanan sumatera utara dapat digunakan dengan hasil keluaran *encode* dan *decode* yaitu *base* 64.

## UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada Bapak Mukhlis Ramadhan dan Bapak Yopi Hendro Syahputra 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.