Jurnal Salome: Multidisipliner Keilmuan
Vol. 1 No. 1 2023, hal. 42-56
e-ISSN: 2986-4968

APLIKASI KEAMANAN DATA PROGRAM ACARA TV PADA TVRI MENGGUNAKAN METODE AES

Ismail Lubis*
Universitas Potensi Utama Medan, Indonesia
ismaillubis90@gmail.com

Fujiati
Universitas Potensi Utama Medan, Indonesia
info@potensi-utama.ac.id

ABSTRACT

Confidentiality of data or information is very important information in an organization or a company which is a complete service. And in this technological age, it is an era where using a computer network where an irresponsible party can access a network access, this can result in the data transmission process being insecure because it is used by other parties who are not responsible for collect data or information that can be detrimental to certain parties. One way to maintain the security and confidentiality of data is to use cryptographic methods. In the field of cryptography, there are two very important concepts, namely encryption and description. The process of sending messages will go through an encryption process to convert the original text (plaintext) into ciphertext. So that it cannot be read or understood by other people and the confidentiality of the data and the integrity of the data to keep it safe.
Keywords: Data Security, PHP, Mysql, AES.

ABSTRAK

Kerahasiaan dari data atau informasi merupakan informasi yang sangat penting dalam suatu organisasi ataupun suatu perusahaan yang merupakan suatu kelengkapan pelayanan. Dan pada zaman teknologi ini merupakan suatu zaman yang dimana yang menggunakan suatu jaringan komputer yang dimana sutu pihak yang tidak bertanggung jawab dapat mengakses suatu akses jaringan tersebut, Hal tersebut dapat mengakibatkan proses pengiriman data menjadi tidak aman karena dimanfaatkan oleh pihak lain yang tidak bertanggung jawab untuk mengambil data maupun informasi yang bisa merugikan pihak tertentu. Salah satu cara untuk menjaga keamanan dan kerahasiaaan suatu data tersebut ialah dengan menggunakan metode kriptografi Dalam Bidang Kriptografi terdapat dua konsep yang sangat penting yaitu enkripsi dan deskripsi, Proses pengiriman pesan akan melalui proses enkripsi untuk mengubah teks asli (plaintext) menjadi teks sandi (ciphertext) sehingga tidak dapat dibaca atau dimengerti oleh orang lain dan kerahasiaan data dan Integritas Data tersebut agar tetap aman.
Kata Kunci*:* Keamanan Data, PHP, Mysql, AES

PENDAHULUAN

Teknologi komputer sangat dibutuhkan oleh kehidupan manusia terutama personal maupun kelompok (organisasi). Kelompok (organisasi) tersebut sangat membutuhkan adanya komputerisasi dalam setiap kegiatannya. Dari hal penggunaan komputerisasi tersebut, maka dibuatlah sebuah keamanan bagi seluruh aset-asetnya, terutama informasi-informasi dan data-data penting demi menjaga kerahasiaan informasi data tersebut. Dari keamanan data tersebut menimbulkan tuntutan akan tersedianya suatu sistem pengamanan data yang lebih baik agar dapat mengamankan data dari

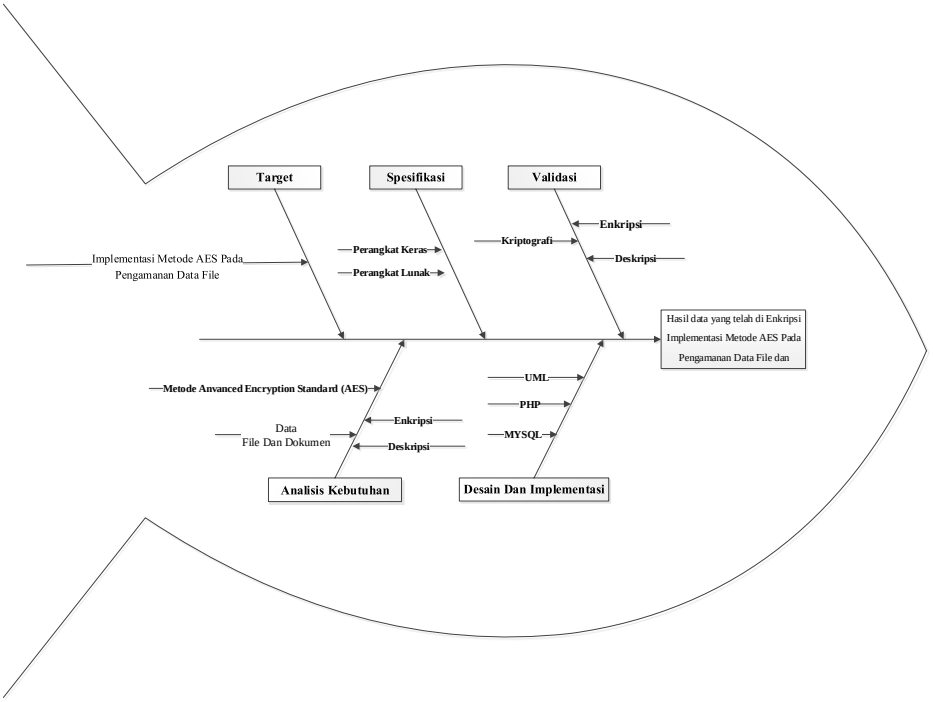
berbagai ancaman yang mungkin timbul. Ini merupakan latar belakang berkembangnya sistem keamanan data yang berfungsi untuk melindungi data yang ditransmisikan atau dikirimkan melalui suatu jaringan komunikasi.

Kerahasiaan dari data atau informasi merupakan informasi yang sangat penting dalam suatu organisasi ataupun suatu perusahaan yang merupakan suatu kelengkapan pelayanan. Dan pada zaman teknologi ini merupakan suatu zaman yang dimana yang menggunakan suatu jaringan komputer yang dimana sutu pihak yang tidak bertanggung jawab dapat mengakses suatu akses jaringan tersebut, Hal tersebut dapat mengakibatkan proses pengiriman data menjadi tidak aman karena dimanfaatkan oleh pihak lain yang tidak bertanggung jawab untuk mengambil data maupun informasi yang bisa merugikan pihak tertentu. Salah satu cara untuk menjaga keamanan dan kerahasiaaan suatu data tersebut ialah dengan menggunakan metode kriptografi Dalam Bidang Kriptografi terdapat dua konsep yang sangat penting yaitu enkripsi dan deskripsi, Proses pengiriman pesan akan melalui proses enkripsi untuk mengubah teks asli (plaintext) menjadi teks sandi (ciphertext) sehingga tidak dapat dibaca atau dimengerti oleh orang lain dan kerahasiaan data dan Integritas Data tersebut agar tetap aman maka dibutuhkan sebuah algortima yang dapat memproteksi file dan folder dokumen adalah Dengan Metode keamanan yang tepat dalam permasalahan ini ialah dengan metode Algoritma kriptografi AES (*Advanced Encryption Standard*). untuk enkripsi dan dekripsi data Algoritma *Advanced Encryption Standard* (AES) dipilih karena memiliki suatu tingkat keamanan pertukaran informasi yang cukup bagus, dan pada penelitian ini diuji coba file dan folder dokumen untuk melihat kecepatan waktu yang dibutuhkan selama proses enkripsi dan dekripsi.

Dalam hal ini juga ditambahkan sebuah sistem pendukung pada pengamanan data setelah melakukan teknik kriptografi dalam menjaga keamanan data informasi tersebut yaitu dengan teknik penyembunyian data atau disebut steganografi. Steganografi merupakan seni dan ilmu untuk menyembunyikan pesan dalam sebuah media pesan. Kerahasiaan pesan yang ingin disampaikan merupakan faktor utama dalam steganografi. Dengan demikian, metode *AES* diharapkan akan membuat pengamanan isi data file dan folder memiliki tingkat keamanan yang lebih tinggi khususnya untuk data yang bersifat rahasia pada TVRI Sumatera Utara sehingga data asli tersebut tidak dapat dibaca dan diterjemahkan oleh orang yang tidak bertanggung jawab.

METODE PENELITIAN

Tahapan metode *fishbone* dapat dilihat pada gambar 1 di bawah ini.



Gambar 1 : Model Fishbone

Penjelasan gambar I.1 Perancangan pengamanan data *file* dan folder pada model *fishbone:*

a. Target

Adapun target dari penelitian ini adalah dapat membangun suatu Sistem Keamanan pada file dan folder untuk meningkatkan keamanan pada TVRI Sumatera Utara

b. Analisis Kebutuhan

Dalam tahap ini dilakukan proses enkripsi dan enkripsi pada file dan dokumen pada TVRI Sumatera Utara. Dalam enkripsi dan deskripsi file dan dokumen perlu beberapa pemahaman terkait variable-variabel yang saling berhubungan satu sama lain. Pengimplementasi ini yang tepat dalam pengaman file dan folder pada TVRI Sumatera Utara menggunakan metode *Anvanced Encryption Standard* (AES).

c. Spesifikasi

Spesifikasi kebutuhan perangkat lunak adalah sebuah dokumen yang berisi pernyataan lengkap dari apa yang dapat dilakukan oleh perangkat lunak. Adapun spesifikasi kebutuhan dalam membangun sistem yang akan dirancang adalah sebagai berikut :

1. Spesifikasi Perangkat Keras

   Spesifikasi perangkat keras yang dibutuhkan adalah :

   - Laptop *Intel 2core*
   - RAM 2 *Gigabyte*
   - *Hard disk 500 Gigabyte*

2. Spesifikasi Perangkat Lunak
   - Sistem operasi Windows 10
   - *PHP* dan *Database MySQL Server*

d. Desain dan Implementasi

Perancangan dapat didefinisikan sebagai proses untuk mengaplikasikan berbagai macam teknik dan prinsip untuk tujuan pendefinisian secara rinci suatu perangkat, proses atau sistem agar dapat direalisasikan dalam suatu bentuk fisik. Perancangan menggunakan model UML untuk menggambarkan sistem. Sedangkan implementasi merupakan tahap pengkodean yang merupakan suatu proses translasi. Rancangan detil ditranslasikan ke dalam suatu bahasa pemrograman. Dalam hal ini implementasi menggunakan bahasa pemrograman *PHP* dan *database MySQL Server.*

e. Validasi

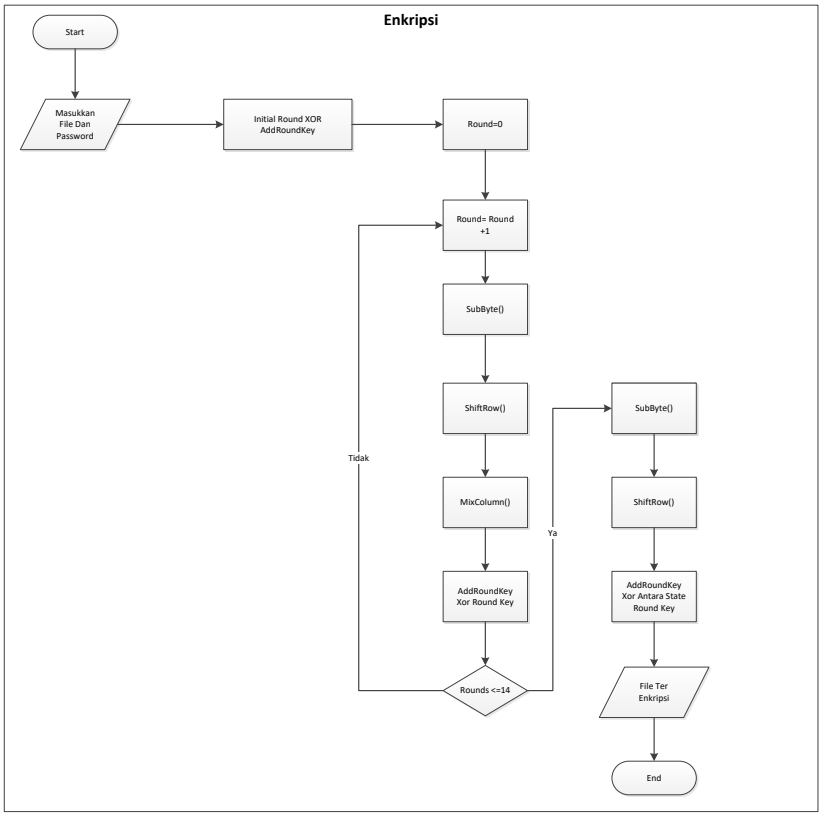
Validasi merupakan proses untuk menunjukkan seberapa besar nilai keakuratan program terhadap kondisi-kondisi saat pemakaian sebenarnya. Proses ini menjalankan skenario berdasarkan data dan lingkungan yang merepresentasikan dunia nyata dengan menggunakan mesin percobaan. Verifikasi program merupakan suatu metode yang digunakan untuk menjamin kebenaran suatu program. Verifikasi program melakukan simbolisasi masukan sehingga jaminan diberikan untuk semua data yang berlaku sebagai masukan.

f. Finalisasi

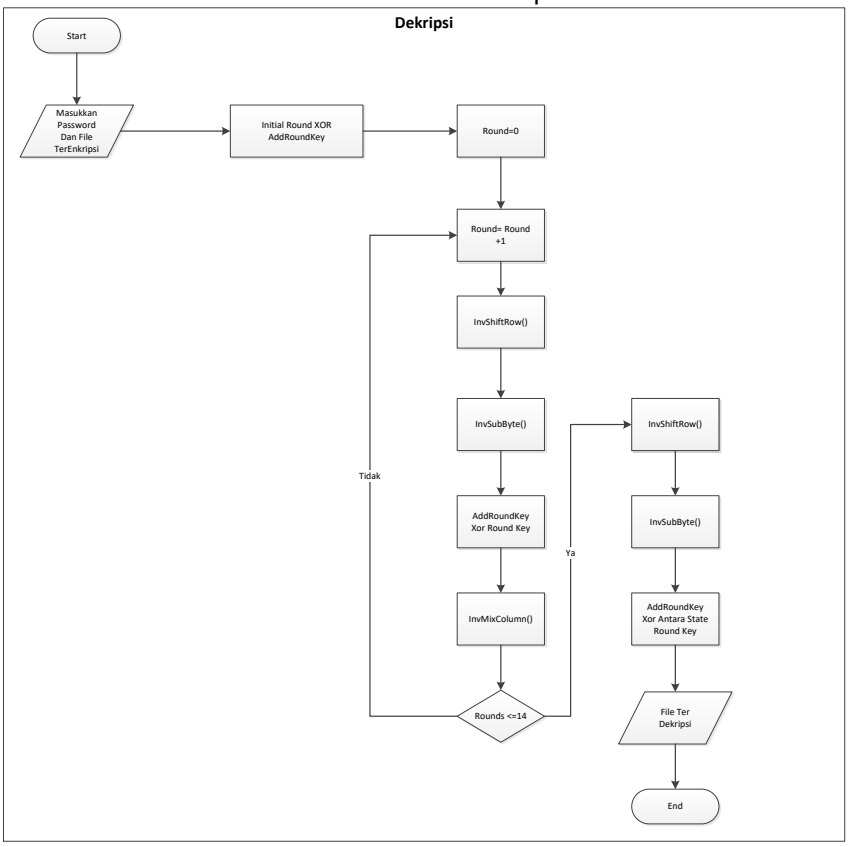
Pada tahapan ini adalah tahapan hasil dari sistem yang sudah dirancang dan berjalan sesuai rencana.

HASIL DAN PEMBAHASAN

Pada tahap ini proses dalam aplikasi dibuat sesuai dengan fungsi dari algoritma enkripsi dan dekripsi yang digunakan. Jika langkah-langkah dalam proses enkrip dan dekrip berlawanan dengan fungsi algoritma yang digunakan, maka proses yang di inginkan tidak akan berjalan. Langkah yang harus dilakukan dalam proses enkripsi dan dekripsi digambarkan dalam flowchart berikut :



Gambar 2. Flowchart Enkripsi AES



Gambar 3. Flowchart Dekripsi AES

Contoh Kasus Algoritma AES

Berikut ini adalah contoh kasus penggunaan Algoritma AES, untuk lebih jelasnya dapat dilihat sebagai berikut :

Misal, sebuah CipherText sebagai berikut :

CipherText : TwoOneNineTwo
Key : ThatsMyKungFu

Langkah selanjutnya adalah mengubah nama file dan juga kunci kedalam bentuk hexadesimal.

File :

T	w	O	O	n	E	N	I	N	e	T	w	O
54	77	6F	4F	6E	65	4E	69	6E	65	54	77	6F

Key :

T	h	A	T	s	M	Y	K	U	n	g	F	U
54	68	61	74	73	4D	79	4B	75	6E	67	46	75

Langkah selanjutnya yang dilakukan adalah mencari nilai Roundkey pertama, untuk mencari Roundkey pertama dapat dilakukan sebagai berikut :

w[0] = (54, 68, 61, 74)
w[1] = (73, 20, 6D, 79)
w[2] = (20, 4B, 75, 6E)
w[3] = (67, 20, 46, 75)
g(w[3]) :

- byte kiri bergeser dari w[3] : (20, 46, 75, 67)
- Substitusi Byte (S-Box): (B7, 5A, 9D, 85)
- Menambahkan putaran konstan (01, 00, 00, 00)
- Memberi : g(w[3]) = (B6, 5A, 9D, 85)

w[4] = w[0] g(w[3]) = (E2, 32, FC, F1) :

0101 0100 1011 0110	0110 1000 0101 1010	0110 0001 1001 1101	0111 0100 1000 0101
1110 0010 E2	0011 0010 32	1111 1100 FC	1111 0001 F1

w[5] = w[4] XOR w[1] = (91, 12, 91, 88)
w[6] = w[5] w[2] = (B1, 59, E4, E6)
w[7] = w[6] w[3] = (D6, 79, A2, 93)
Roundkey pertama : E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93
Round0 : 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
Round1 : E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79
Round2 : 56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7 FA
Round3 : D2 60 0D E7 15 7A BC 68 63 39 E9 01 C3 03
Round4 : A1 12 02 C9 B4 68 BE A1 D7 51 57 A0 14 52 49 5B
Round5 : B1 29 3B 33 05 41 85 92 D2 10 D2 32 C6 42 9B 69
Round6 : BD 3D C2 B7 B8 7C 47 15 6A 6C 95 27 AC 2E 0E 4E

Round7 : CC 96 ED 16 74 EA AA 03 1E 86 3F 24 B2 A8 31 6A
Round8 : 8E 51 EF 21 FA BB 45 22 E4 3D 7A 06 56 95 4B 6C
Round9 : BF E2 BF 90 45 59 FA B2 A1 64 80 B4 F7 F1 CB D8
Round10 :28 FD DE F8 6D A4 24 4A CC C0 A4 FE 3B 31 6F 26
Pertama dilakukan proses inisialisasi dengan operasi XOR antara State dan Key.

State Matrix dan Round key No.0 Matrix :

$$\begin{pmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{pmatrix} \qquad \begin{pmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{pmatrix}$$

XOR entri yang sesuai, misalnya, 69 XOR 4B = 22

0110 1001
0100 1011
0010 0010

State Matrix baru adalah :

$$\begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix}$$

Gantikan setiap entri (byte) dari matriks keadaan saat ini dengan entri yang sesuai di AES S-Box. Misalnya: byte 6E diganti dengan masuknya S-Box di baris 6 dan kolom E, yaitu, oleh 9F. Ini mengarah ke Matriks Status baru:

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

Lapisan non-linear ini untuk ketahanan terhadap serangan kriptanalisis yang berbeda dan linier. empat baris digeser secara siklis ke kiri dengan offset 0,1, 2, dan 3. State Matrix baru adalah :

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix}$$

Langkah pencampuran linier ini menyebabkan difusi bit pada beberapa putaran. Campur Kolom mengalikan matriks tetap terhadap Matriks Status saat ini :

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix} = \begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix}$$

Entri BA adalah hasil dari (02x63) XOR (03x2F) XOR (01xAF) XOR (01xA2):
02 x 63 = 00000010 x 01100011 = 11000110
03 x 2F = (02 x 2F) XOR 2F = (00000010 x 00101111) XOR 00101111 = 01110001
01 x AF = AF = 10101111 dan 01 x A2 = A2 = 10100010
Dikarenakan :

11000110
01110001
10101111
10100010
10111010

State Matrix dan Round key No.1 Matrix:

$$\begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix} \qquad \begin{pmatrix} E2 & 91 & B1 & D6 \\ 32 & 12 & 59 & 79 \\ FC & 91 & E4 & A2 \\ F1 & 88 & E6 & 93 \end{pmatrix}$$

XOR menghasilkan Matriks Status baru:

$$\begin{pmatrix} 58 & 15 & 59 & CD \\ 47 & B6 & D4 & 39 \\ 08 & 1C & E2 & DF \\ 8B & BA & E8 & CE \end{pmatrix}$$

Output AES setelah Putaran 1: 58 47 08 8B 15 B6 1C BA 59 D4 E2 E8 CD 39 DF CE
Putaran 2 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 6A & 59 & CB & BD \\ A0 & 4E & 48 & 12 \\ 30 & 9C & 98 & 9E \\ 3D & F4 & 9B & 8B \end{pmatrix} \qquad \begin{pmatrix} 6A & 59 & CB & BD \\ 4E & 48 & 12 & A0 \\ 98 & 9E & 30 & 9B \\ 8B & 3D & F4 & 9B \end{pmatrix}$$

Putaran 2 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} 15 & C9 & 7F & 9D \\ CE & 4D & 4B & C2 \\ 89 & 71 & BE & 88 \\ 65 & 47 & 97 & CD \end{pmatrix} \qquad \begin{pmatrix} 43 & 0E & 09 & 3D \\ C6 & 57 & 08 & F8 \\ A9 & C0 & EB & 7F \\ 62 & C8 & FE & 37 \end{pmatrix}$$

Putaran 3 setelah Pengganti Byte dan setlah Shift Rows:

$$\begin{pmatrix} 1A & AB & 01 & 27 \\ B4 & 5B & 30 & 41 \\ D3 & BA & E9 & D2 \\ AA & E8 & BB & 9A \end{pmatrix} \qquad \begin{pmatrix} 1A & AB & 01 & 27 \\ 5B & 30 & 41 & B4 \\ E9 & D2 & D3 & BA \\ A9 & AA & E8 & BB \end{pmatrix}$$

Putaran 3 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} AA & 65 & FA & 88 \\ 16 & 0C & 05 & 3A \\ 3D & C1 & DE & 2A \\ B3 & 4B & 5A & 0A \end{pmatrix} \qquad \begin{pmatrix} 78 & 70 & 99 & 4B \\ 76 & 76 & 3C & 39 \\ 30 & 7D & 37 & 34 \\ 54 & 23 & 5B & F1 \end{pmatrix}$$

Putaran 4 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} BC & 51 & EE & B3 \\ 38 & 38 & EB & 12 \\ 04 & FF & 9A & 18 \\ 20 & 26 & 39 & A1 \end{pmatrix} \qquad \begin{pmatrix} BC & 51 & EE & B3 \\ 38 & EB & 12 & 38 \\ 9A & 18 & 04 & FF \\ A1 & 20 & 26 & 39 \end{pmatrix}$$

Putaran 4 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} 10 & BC & D3 & F3 \\ D8 & 94 & E0 & E0 \\ 53 & EA & 9E & 25 \\ 24 & 40 & 73 & 7B \end{pmatrix} \qquad \begin{pmatrix} B1 & 08 & 04 & E7 \\ CA & FC & B1 & B2 \\ 51 & 54 & C9 & 6C \\ ED & E1 & D3 & 20 \end{pmatrix}$$

Putaran 5 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} C8 & 30 & F2 & 94 \\ 74 & B0 & C8 & 37 \\ D1 & 20 & DD & 50 \\ 55 & F8 & 66 & B7 \end{pmatrix} \qquad \begin{pmatrix} C8 & 30 & F2 & 94 \\ B0 & C8 & 37 & 74 \\ DD & 50 & D1 & 20 \\ B7 & 55 & F8 & 66 \end{pmatrix}$$

Putaran 5 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} 2A & 26 & 8F & E9 \\ 78 & 1E & 0C & 7A \\ 1B & A7 & 6F & 0A \\ 5B & 62 & 00 & 3F \end{pmatrix} \qquad \begin{pmatrix} 9B & 23 & 5D & 2F \\ 51 & 5F & 1C & 38 \\ 20 & 22 & BD & 91 \\ 68 & F0 & 32 & 56 \end{pmatrix}$$

Putaran 6 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 14 & 26 & 4C & 15 \\ D1 & CF & 9C & 07 \\ B7 & 93 & 7A & 81 \\ 45 & 8C & 23 & B1 \end{pmatrix} \qquad \begin{pmatrix} 14 & 26 & 4C & 15 \\ CF & 9C & 07 & D1 \\ 7A & 81 & B7 & 93 \\ B1 & 45 & 8C & 23 \end{pmatrix}$$

Putaran 6 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} A9 & 37 & AA & F2 \\ AE & D8 & 0C & 21 \\ E7 & 6C & B1 & 9C \\ F0 & FD & 67 & 3B \end{pmatrix} \qquad \begin{pmatrix} 14 & 8F & C0 & 5E \\ 93 & A4 & 60 & 0F \\ 25 & 2B & 24 & 92 \\ 77 & E8 & 40 & 75 \end{pmatrix}$$

Putaran 7 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} FA & 73 & BA & 58 \\ DC & 49 & D0 & 76 \\ 3F & F1 & 36 & 4F \\ F5 & 9B & 09 & 9D \end{pmatrix} \qquad \begin{pmatrix} FA & 73 & BA & 58 \\ 49 & D0 & 76 & DC \\ 36 & 4F & 3F & F1 \\ 9D & F5 & 9B & 09 \end{pmatrix}$$

Putaran 7 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} 9F & 37 & 51 & 37 \\ AF & EC & 8C & FA \\ 63 & 39 & 04 & 66 \\ 4B & FB & B1 & D7 \end{pmatrix} \qquad \begin{pmatrix} 53 & 43 & 4F & 85 \\ 39 & 06 & 0A & 52 \\ 8E & 93 & 3B & 57 \\ 5D & F8 & 95 & BD \end{pmatrix}$$

Putaran 8 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} ED & 1A & 84 & 97 \\ 12 & 6F & 67 & 00 \\ 19 & DC & E2 & 5B \\ 4C & 41 & 2A & 7A \end{pmatrix} \qquad \begin{pmatrix} ED & 1A & 84 & 97 \\ 6F & 67 & 00 & 12 \\ E2 & 5B & 19 & DC \\ 7A & 4C & 41 & 2A \end{pmatrix}$$

Putaran 8 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} E8 & 8A & 4B & F5 \\ 74 & 75 & EE & E6 \\ D3 & 1F & 75 & 58 \\ 55 & 8A & 0C & 38 \end{pmatrix} \qquad \begin{pmatrix} 66 & 70 & AF & A3 \\ 25 & CE & D3 & 73 \\ 3C & 5A & 0F & 13 \\ 74 & A8 & 0A & 54 \end{pmatrix}$$

Putaran 9 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 33 & 51 & 79 & 0A \\ 3F & 8B & 66 & 8F \\ EB & BE & 76 & 7D \\ 92 & C2 & 67 & 20 \end{pmatrix} \qquad \begin{pmatrix} 33 & 51 & 79 & 0A \\ 8B & 66 & 8F & 3F \\ 76 & 7D & EB & BE \\ 20 & 92 & C2 & 67 \end{pmatrix}$$

Putaran 9 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} B6 & E7 & 51 & 8C \\ 84 & 88 & 98 & CA \\ 34 & 60 & 66 & FB \\ E8 & D7 & 70 & 51 \end{pmatrix} \qquad \begin{pmatrix} 09 & A2 & F0 & 7B \\ 66 & D1 & FC & 3B \\ 8B & 9A & E6 & BE \\ 78 & 65 & C4 & 89 \end{pmatrix}$$

Putaran 10 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 01 & 3A & 8C & 21 \\ 33 & 3E & B0 & E2 \\ 3D & B8 & 8E & 04 \\ BC & 4D & 1C & A7 \end{pmatrix} \qquad \begin{pmatrix} 01 & 3A & 8C & 21 \\ E3 & B0 & E2 & 33 \\ 8E & 04 & 3D & 8C \\ A7 & BC & 4D & 1C \end{pmatrix}$$

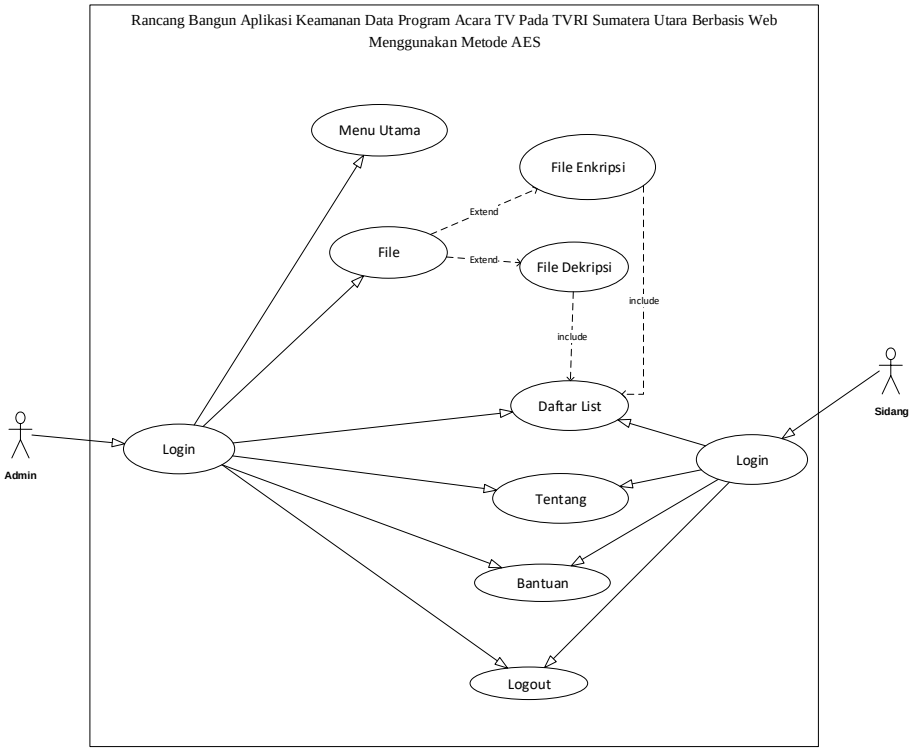
Putaran 10 setelah Roundkey (Perhatian: tidak ada kolom Mix di round terakhir):

$$\begin{pmatrix} 29 & 57 & 40 & 1A \\ C3 & 14 & 22 & 02 \\ 50 & 20 & 99 & D7 \\ 5F & F6 & B3 & 3A \end{pmatrix}$$

Cipher File yang dihasilkan adalah sebagai berikut :

29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A

Perilaku beserta tugas-tugas dari tiap–tiap elemen maupun aktor yang terlibat dalam sistem yang akan dirancang, akan digambarkan dalam diagram *use case* yang bertujuan untuk memberikan gambaran secara umum tentang sistem yang akan dirancang gambar 4 sebagai berikut:

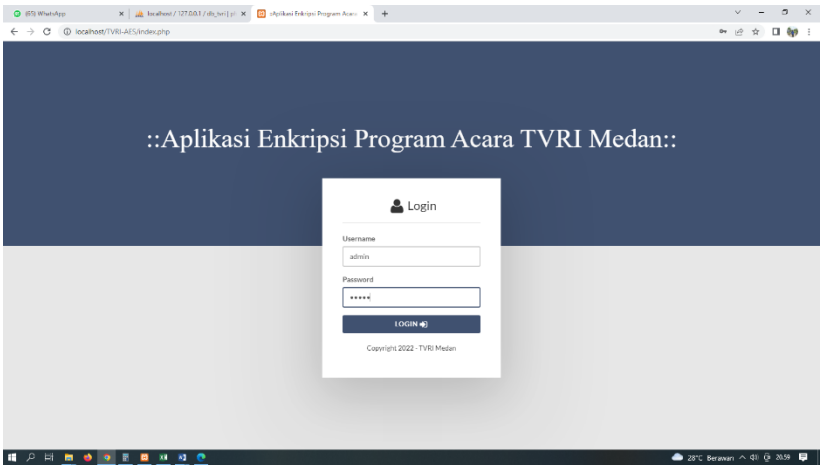


Gambar 4. *Use Case Diagram*

Adapun tampilan hasil aplikasi yang dirancang adalah sebagai berikut:

1. Tampilan *Form* Login

Form login merupakan *interface* program kriptografi, dimana untuk menggunakan aplikasi kriptografi ini dapat melalui *interface form* login. dapat dilihat pada gambar 5 dibawah ini.



Gambar 5. Tampilan *Form* Login

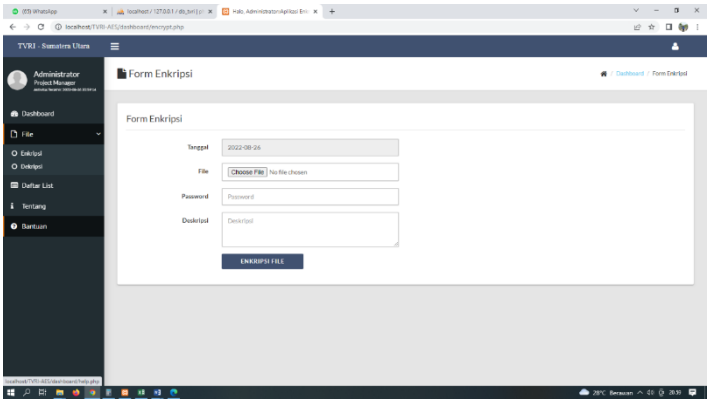
2. Tampilan *Form* Utama

Form utama merupakan *interface* program kriptografi secara keseluruhan, dimana untuk menggunakan aplikasi kriptografi ini dapat melalui *interface form* utama. Dalam *form* utama terdapat beberapa menu yaitu, menu *file* dan menu program. Untuk lebih jelasnya tampilan *form* utama dapat dilihat pada gambar 6 dibawah ini.

Gambar 6. Tampilan *Form* Utama

3. Tampilan *Form* Data Enkripsi

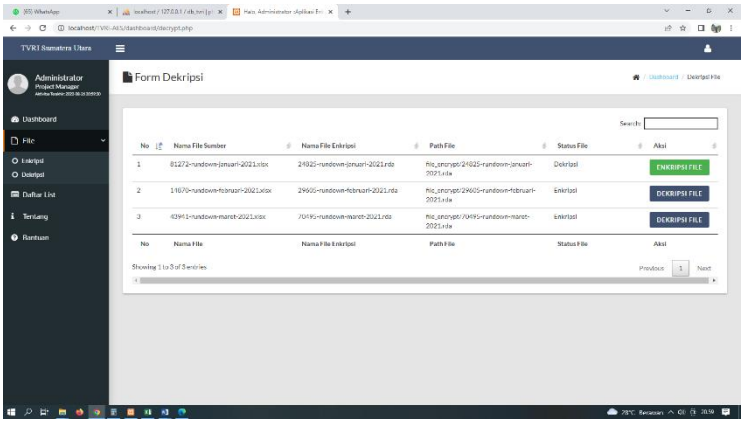
Form enkripsi ini berfungsi untuk merubah isi data *file* dalam bentuk *chipretext*, sehingga isi *plaintext* tidak dapat dikenali isi datanya dan hanya bisa dibuka dengan menggunakan kunci yang diberikan oleh *user* terhadap sistem. Ada beberapa hal yang bisa dilakukan didalam *form* data enkripsi seperti memasukkan data *file doc,* menyimpan hasil enkripsi (*chipertext*), dan keluardari *form* data enkripsi. Berikut ini tampilan *form* data enkripsi dapat dilihat pada gambar 7 berikut ini:



Gambar 7. Tampilan *Form* Data Enkripsi

4. Tampilan *Form* Dekripsi

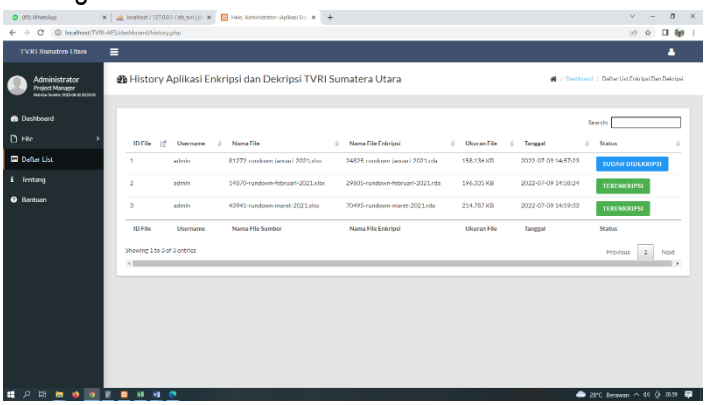
Form data dekripsi ini berfungsi untuk merubah isi data *chipertext* dalam bentuk *plaintext*, sehingga isi *chipertex t* dapat dikenali kembali isi datanya dan bisa dibuka dengan menggunakan kunci yang diberikan oleh *user* terhadap sistem. Ada beberapa hal yang bisa dilakukan didalam *form* data dekripsi, seperti memasukkan atau membuka data teks (*chipertext*), menyimpan hasil dekripsi (*plaintext*), dan keluardari *form* dekripsi.



Gambar 8. Tampilan *Form* Dekripsi

5. Tampilan *Form* Daftar List

Form Daftar list berfungsi untuk menampilkan data yang sudah terenkripsi pesan asli menjadi plainteks, dapat dilihat sebagai berikut ini:



Gambar 9. Tampilan *Form* Daftar List

KESIMPULAN

Berdasarkan hasil pambahasan dan uji coba yang telah dilakukan, dapat disimpulkan :

1. Aplikasi Telah dibangun dan dapat memanipulasi data file dan terhadap isi suatu *file* dengan system penyandian Aplikasi algoritma *AES*.
2. Sistem yang dibangun sudah mampu melakukan enkripsi dan dekripsi terhadap data Sehingga dapat Melindungi data-data Acara TV Pada TVRI Sumatera Utara Dengan Menggunakan Metode AES.
3. Sistem yang dibangun mempunyai tampilan yang sangat sederhana dan mudah digunakan oleh *user* .

SARAN

Untuk menyempurnakan aplikasi ini maka diberikan saran :

1. Diharapkan untuk dikembangkan agar dalam mengunakan kata kunci pada sistem yang dibangun, boleh ada huruf yang sama didalam kata kunci. Hal ini agar saat pemilihan kata kata kunci, *user* bebas membuat kata kunci sesuai dengan keinginan *user*.
2. Diharapakan untuk dikembangkan agar proses enkripsi (*chipertext*) dengan sistem yang dibuat dapat menghasilkan data yang berbeda.
3. Melakukan perkembangan performance aplikasi untuk membuat pengguna tidak bosan dalam penggunaan aplikasi

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah banyak memberikan masukkan dan saran dalam penyelesaian Penelitian ini.

DAFTAR PUSTAKA

Aditya Puji Nugroho 2020, “Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES” Jurnal Sistem Informasi Volume: 04, Number: 01, April 2020 ISSN 2579-5341

Ahmad Lutfi, 2017; 105 “SISTEM INFORMASI AKADEMIK MADRASAH ALIYAH SALAFIYAH SYAFI’IYAH

Aris (2017), “Implementasi Kriptografi Algoritma AES Serta Algoritma Kompresi Huffman Dengan Menggunakan Pemograman PHP” Konferensi Nasional Sistem & Informatika 2017 STMIK STIKOM Bali, 10 Agustus 2017.

Badrul Anwar, 2020, “Aplikasi Pengamanan Dokumen Penjualan Tiket Pesawat Di Pt. Benua Raya Jaya Tour And Travel Menggunakan Metode Advanced Encryption Standard (AES)”, Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD P:ISSN : 2621-8976 E-ISSN : 2615-5133 Vol.3, No.1, Januari 2020.

Jaka Prayudha, Saniman, Ishak (2019), “Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)” Sains dan Komputer (SAINTIKOM) Vol.18, No.2, Agustus 2019, pp. 119~129 P-ISSN: 1978-6603 E-ISSN : 2615-3475.

Lilik Asih Indrayani (2019), “Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document” JINACS: Volume 01 Nomor 01, 2019 (Journal of Informatics and Computer Science).

MENGGUNAKAN PHP DAN MYSQL” Volume 3 No. 2 / Oktober 2017