Journal Global Tecnology Computer
Vol 2, No. 2, April, 2023, Hal 75 - 86
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

Perancangan Aplikasi Audit Internal Dengan Menerapkan Algoritma AES 128 Bit Untuk Pengamanan Data

Haris Amanda Sagala

Program Studi Teknik Informatika, Fakultas Ilmu Komputer & Teknologi Informasi, Universitas Budi Darma, Medan, Indonesia
Jl. Sisingamangaraja No.338, Siti Rejo I, Kec. Medan Kota, Kota Medan, Sumatera Utara, Indonesia
Email: harissagala@gmail.com

Abstrak-Internal audit adalah proses pemeriksaan data internal suatu perusahaan dengan tujuan menganalisis, menilai dan mengajukan saran terhadap aktivitas perusahaan yang diperiksa, dengan demikian resiko yang dihadapi bisa diketahui dan diminimalisir. Dalam perkembangan teknologi saat ini masalah keamanan dan kerahasiaan data merupakan satu hal yang sangat penting untuk diperhatikan. Data laporan internal audit adalah rahasia perusahaan yang tidak boleh diketahui oleh pihak luar, karena akan sangat fatal akibatnya jika ada pihak yang tidak bertanggung jawab mengetahui hal tersebut. Ada banyak cara yang bisa dilakukan untuk mengamankan data, salah satunya adalah dengan memanfaatkan teknik kriptografi atau penyandian data sehingga data tersebut tidak dapat dibaca dan dipahami, kriptografi dapat diimplementasikan terhadap berbagai jenis file. Salah satu algoritma kriptografi yang sering digunakan adalah Advance Encryption Standard (AES) karena teruji ketahanannya terhadap segala jenis serangan terhadap data. Tidak hanya mampu mengenkripsi atau menyandikan data, tetapi algoritma AES juga mampu mendekripsi atau mengembalikan data yang telah terenkripsi sehingga data tersebut dapat dibaca atau dipahami kembali. Sehingga algoritma AES sangat tepat digunakan untuk mengamankan data.

Kata Kunci : Internal Audit, Kriptografi, AES, Enkripsi, dan Dekripsi

Abstract-Internal audit is the process of examining a company's internal data with the aim of analyzing, assessing and submitting suggestions on the activities of the company being examined, thus the risks faced can be identified and minimized. In the current development of technology, the issue of data security and confidentiality is a very important thing to pay attention to. Internal audit report data is a company secret that should not be known by outsiders, because it will be very fatal if an irresponsible party finds out about it. There are many ways that can be done to secure data, one of which is by utilizing cryptographic techniques or data encryption so that the data cannot be read and understood, cryptography can be implemented on various types of files. One of the cryptographic algorithms that is often used is the Advanced Encryption Standard (AES) because it has been tested for its resistance to all kinds of attacks on data. Not only is it able to encrypt or encode data, but the AES algorithm is also able to decrypt or restore encrypted data so that the data can be read or understood again. So the AES algorithm is very appropriate to use to secure data.

Keywords: Internal Audit, Cryptography, AES, Encryption and Decryption

1. PENDAHULUAN

Keamanan data adalah perlindungan data terhadap otoritas tidak sah, modifikasi atau perusakan. Keamanan biasanya digambarkan sebagai kebebasan dari bahaya atau sebagai kondisi keselamatan. Keamanan komputer, secara rinci adalah perlindungan data di dalam suatu sistem melawan terhadap otorisasi tidak sah, modifikasi, atau perusakan dan perlindungan sistem komputer terhadap penggunaan tidak sah atau modifikasi[1]**.** Internal Audit adalah proses pemeriksanaan data internal suatu perusahaan, proses ini bertujuan untuk menganalisis, menilai dan mengajukan saran terhadap aktivitas perusahaan yang diperiksa, dengan demikian resiko yang dihadapi perusahaan bisa diketahui dan diminimalisir. Internal perusahaan yang handal menjaga kekayaandan kinerja perusahaan[2].

Data internal audit pada Sekolahmerupakan rahasia yang hanya boleh diketahui oleh pihak yang diberi wewenang. Di Sekolah, Internal Auditor atau pihak yang bersifat independen merupakan pihak yang bertanggung jawab untuk memeriksa kebenaran data laporan yang telah dibuat. Laporan internal audit disediakan atau dibuat dengan tujuan mengetahui dan meminimalisir resiko yang akan dihadapi oleh sekolah dengan demikian pimpinan sekolah tidak akan mengambil keputusan yang tidak tepat.

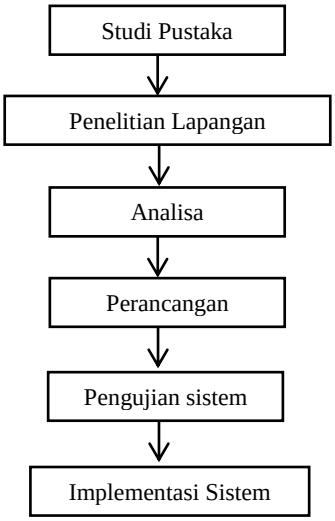
Pada jurnal *Ris. J. Akunt.*, vol. 1, no. 1, pp. 22–28, 2017, yang berjudul "Pengaruh peran audit internal dan pengendalian intern terhadap pencegahan fraud,". Disimpulkan bahwa Audit Internal berpengaruh terhadap pencegahan fraud atau tindakan yang dapat merugikan orang lain secara tidak jujur dengan tujuan mengambil keutungan pribadi maupun kelompok dan golongannya. Namun tidak adanya pengamanan data yang telah diperoleh dari Auditor. Dengan kelemahan tersebut dibutuhkan pengamanan data yang telah diperoleh auditor "[2].

Pada jurnal *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. April, pp. 67–74, 2016 yang berjudul "Aplikasi Pengamanan Daata Menggunakan Algoritma Steganografi Discrete Cosine Transform dan Kriptografi AES 128 BIT pad SMK PGRI 15 Jakarta. Disimpulkan bahwa Metode Steganografi DCT dan teknik Kriptografi AES 128 bit sangat membantu dalam menjaga kerahasiaan pesan agar tidak mudah dibaca oleh orang yang tidak memiliki kepentingan[3]

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Adapun tahapan-tahapan yang dilakukan pada penelitian ini dapat dijelaskan seperti gambar di bawah ini:



Gambar 1. Tahapan Penelitian

Ada beberapa metode yang dilakukan pada penelitian ini, diantaranya adalah sebagai berikut:

a. Studi Pustaka
   Metode ini dilakukan dengan cara mengumpulkan data dengan melakukan studi kepustakaan melalui buku-buku referensi untuk mendapatkan data yang berhubungan dengan topik penelitian.
b. Penelitian Lapangan
   Yaitu melakukan riset lapangan untuk mengetahui secara jelas dan terperinci permasalahan yang sedang dihadapi serta dapat menghasilkan data-data yang diperlukan. Dalam penelitian lapangan dilakukan beberapa hal yang dianggap perlu diantarany Wawancara (*interview)* dan Pengamatan (*observation)*
c. Analisa
   Menganalisa permasalahan di sekolah dan hal hal yang diperlukan dalam pembuatan sistem
d. Perancangan
   merancang hal-hal yang diperlukan dalam pembuatan sistem.
e. Pengujian Sistem
   Metode ini bertujuan untuk menguji sistem yang telah dibuat apakah sudah maksimal atau masih ada kekurangan yang harus diatasi dan melakukan evaluasi terhadap sistem.
f. Implementasi Sistem
   Mengimplementasikan metode *Advance Encryption Standard* dengan panjang kunci 128 bit ke dalam sistem keamanan data internal audit .

2.2 Kriptografi

Keamanan data adalah perlindungan data terhadap otoritas tidak sah, modifikasi atau perusakan. Keamanan komputer, secara rinci adalah perlindungan data di dalam suatu sistem melawan terhadap otorisasi tidak sah, modifikasi, atau perusakan dan perlindungan sistem komputer terhadap penggunaan tidak sah atau modifikasi [1]-[4]**.**

Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan yang bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak berkepentingan. Untuk menjamin keamanan dan keutuhan dari suatu data, dibutuhkan suatu proses penyandian, proses ini akan merubah suatu data asal menjadi data rahasia yang tidak dapat dibaca, sementara itu proses dekripsi dilakukan oleh penerima data yang dikirim tersebut. Denga cara penyandian tadi, maka data asli tidak akan terbaca oleh pihak yang tidak berkepentingan [5].

Pada dasarnya kriptografi terdiri dari 2 proses yaitu proses enkripsi dan deskripsi. Dalam kriptografi ada beberapa unsur diantaranya adalah :

a. Enkripsi, ini adalah proses penguncian informasi dengan cara merubah teks asli menggunakan kode tertentu.
b. Dekripsi, merupakan proses menguraikan informasi yang telah terenkripsi menggunakan menggunakan teknik atau kunci tertentu.
c. Kunci, merupakan sebuah kode rahasia seperti kata sandi yang digunakan untuk mengenkripsi dan mendekripsi informasi.

2.3 Algoritma *Advance Encryption Standard* (AES)

AES atau Advanced Encryption Standard merupakan standar enkripsi kunci simetri yang pada awalnya diterbitkan dengan algoritma Rijndael. Algoritma ini dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen. Advanced Encryption Standard (AES) dipublikasikan oleh NIST (National Institute of Standard and

Journal Global Tecnology Computer
Vol 2, No. 2, April, 2023, Hal 75 - 86
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

Technology) pada tahun 2001. AES merupakan blok kode simetris untuk menggantikan DES (Data Encryption Standard). Algoritma AES merupakan algoritma simetris yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe : AES-128, AES-192, dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu round key untuk setiap putaran [6].

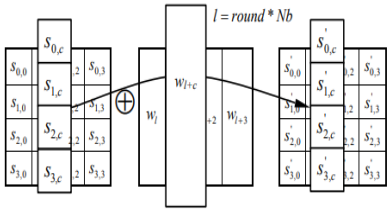
Proses putaran enkripsi dari masing-masing tipe berbeda, AES-128 dikerjakan sebanyak 10 kali *round*, AES-192 sebanyak 12 kali *round*, dan AES-256 dikerjakan sebanyak 14 kali *round* [7]-[8].

2.3.1 Proses Enkripsi AES-128 bit

AES merupakan enkripsi yang memiliki kunci yang lebih besar dibanding DES yaitu 128 bit, 192 bit, atau 256 bit. Proses enkripsi AES dengan panjang kunci 128 bit terdiri dari 4 tahapan yaitu *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns*. Karena adanya beberapa tahapan dalam proses enkripsi maka diperlukan subkey-subkey yang akan dipakai pada tiap tahap. Untuk melakukan pengembangan jumlah kunci yang akan dipakai dari kunci utama maka dilakukan key schedule [9]-[10].

a. *Key Schedule*
Untuk mendapatkan *sub key-sub key* dari kunci utama agar cukup untuk proses enkripsi dan deskripsi maka diperlukan proses *key schedule*. Berikut ini beberapa proses dalam key schedule antara lain adalah :
1. Rotate, adalah proses rotasi perputaran 8 bit pada 32 bit dari kunci.
2. Operasi *SubBytes*, pada operasi ini 8 bit dari subkey disubstitusikan dengan nilai dari *S-Box*.
3. Operasi Rconn, yaitu operasi yang diterjemahkan sebagai operasi pangkat 2 nilai tertentu dari user . pada operasi ini digunakan nilai-nilai dalam galois field. Kemudian nilai dari Rconn akan di-XOR dengan hasil operasi *SubBytes*.
4. Operasi XOR dengan w[i-Nk] yaitu *word* yang berada pada Nk sebelumnya.

b. *AddRoundKey*
Pada proses ini dilakukan XOR antara cipher text yang sudah ada dengan cipher key.

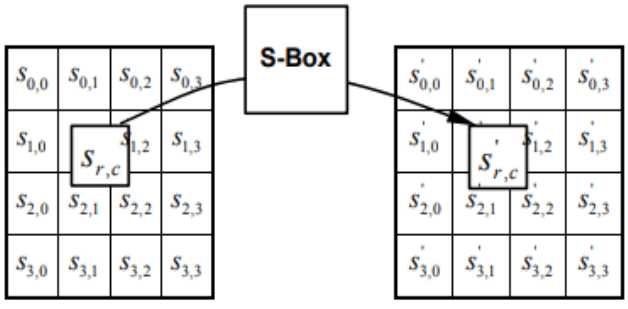


Gambar 2. Proses *AddRoundKey*

c. *SubBytes*
SubBytes adalah proses operasi yang akan melakukan substitusi linear dengan cara mengganti setiap byte state dengan byte pada sebuah tabel yang dinamakan tabel S-Box.

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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	5f	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

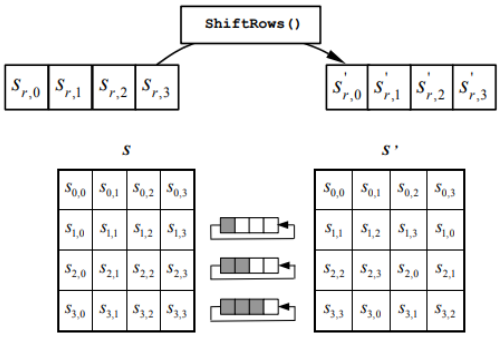
Gambar 3. *S-Box*



Gambar 4. Proses *SubBytes*

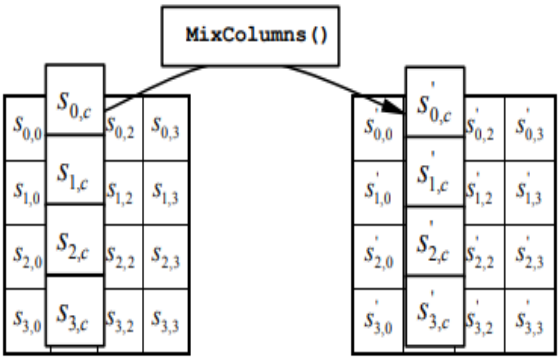
Journal Global Tecnology Computer
Vol 2, No. 2, April, 2023, Hal 75 - 86
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

d. *ShiftRows*
Proses ini bekerja dengan cara memutar byte-byte pada 3 baris terakhir dengan jumlah putaran yang berbeda. Baris kedua akan diputar sebanyak 1 kali, baris ketiga sebanyak 2 kali, baris keempat sebanyak 3 kali, sedangkan baris pertama tidak akan diputar.

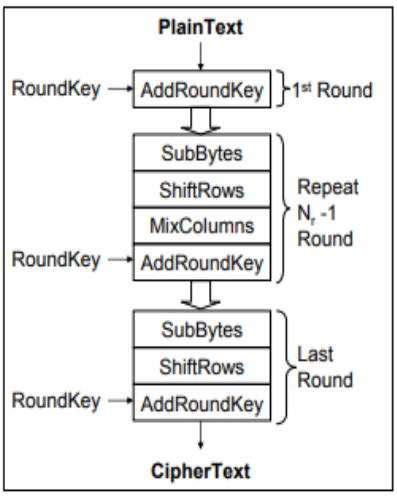


Gambar 5. Proses *ShiftRows*

e. *MixColums*
Proses ini mengalikan tiap elemen dari blok *cipher* dengan matriks yang sudah ditentukan dan siap pakai. Perkalian dilakukan seperti perkalian matriks biasa, lalu perkalian keduanya dimasukkan ke dalam sebuah blok chiper baru.



Gambar 6. Proses *MixColumns*

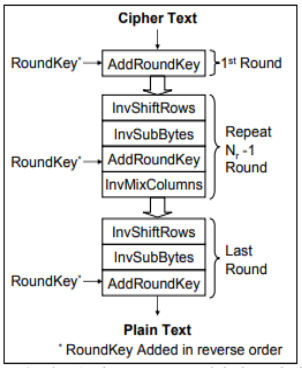


Gambar 7. Proses Enkripsi AES

2.3.2 Proses Deskripsi AES 128 bit

Proses deskripsi merupakan proses kebalikan dari proses enkripsi, diantaranya adalah *AddRoundKey*, *InvShiftRows*, *InvSubBytes*, dan *InvMixColumns*, dengan kunci round yang sama dengan proses enkripsi [11]. Proses dekripsi adalah proses untuk mengembalikan data yang telah terenkripsi (*ciphertext)* data semula yang dapat kembali di baca (*plaintext*). Proses transformasi pada dekripsi hampir sama dengan transformasi pada enkripsi, perbedaannya terletak pada proses *InvSubBytes*, pada proses ini state akan ditukar nilainya dengan tabel *Invers S-Box*, Lalu

InvShiftRows proses ini menggeser ke kanan 3 baris terakhir pada state, dan yang terakhir adalah *InvMixColumns*, proses ini mengalikan matriks yang disediakan dengan state hasil *AddRoundKey* [12].



Gambar 8. Proses Deskripsi AES

2.4 *Internal Audit*

Audit internal atau disebut juga dengan internal audit yakni sebuah penilaian terhadap keyanikan, independe, obyektif dan kegiatan konsultasi yang dibuat sebagai penambah nilai dan peningkatan operasi organisasi. Audit internal ini bisa sebagai pendukung suatu organisasi untuk mencapai tujuannya dengan membawa pendekatan yang sistematis dan disiplin dalam evaluasi dan peningkatan efektivitas proses manajemen risiko, pengendalian dan tatat kelola. Pengertian internal audit menurut para ahli memiliki beragam pengertian yang pada intinya memiliki makna yang sama [13].

Audit internal merupakan pengawasan manajerial yang fungsinya mengukur dan mengevaluasi sistem pengendalian dengan tujuan membantu semua anggota manajemen dalam mengelola secara efektif pertanggungjawabannya dengan cara menyediakan analisis, penilaian, rekomendasi, dan komentar-komentar yang berhubungan dengan kegiatankegiatan yang ditelaah [13].

Data internal audit pada Balai Wilayah Sungai Sumatera II merupakan rahasia yang hanya boleh diketahui oleh pihak yang diberi wewenang. Di Sekolah, *Internal Auditor* atau pihak yang bersifat independen merupakan pihak yang bertanggung jawab untuk memeriksa kebenaran data yang telah dibuat. laporan internal audit disediakan atau dibuat oleh pihak yang melaksanakan pekerjaannya. Pengamanan data internal audit bertujuan agar terhindar dari ancaman pencurian data atau diketahuinya rahasia instansi oleh pihak lain yang tidak bertanggung jawab.

Ancaman terhadap data internal audit ini dapat berasal dari mana saja, oleh karena itu untuk mengatasi ancaman kebocoran data dibutuhkan suatu sistem keamanan data dengan cara mengenkripsi data *internal audit* dengan teknik kriptografi menggunakan algoritma *Advance Encryption Standard* (AES) [11].

3. HASIL DAN PEMBAHASAN

3.1 Analisa

Data merupakan hal yang sangat penting bagi perusahaan, adanya ancaman pencurian atau kebocoran data merupakan suatu ancaman yang besar. Data internal audit merupakan data yang sangat penting karena mencakup informasi yang berisi resiko, kondisi dan saran untuk kemajuan perusahaan, dan jika data tersebut jatuh atau diketahui oleh pihak yang tidak bertanggung jawab maka akan menimbulkan kerugian yang besar Dengan perkembangnya teknologi yang sangat cepat, ancaman keamanan data bisa datang dari mana saja, baik dari dalam perusahaan maupun dari luar perusahaan. Untuk itu diperlukan sebuah sistem keamanan terhadap data agar data tidak sembarangan bisa diakses atau diketahui. ada banyak cara yang dapat dilakukan untuk mengamankan data terutama dari kejahatan cyber, salah satunya adalah dengan memanfaatkan teknik kriptografi, dimana metode yang digunakan adalah Advance Encryption Standard dengan panjang kunci 128 bit. Algoritma ini adalah algoritma kunci simetris yang artinya kunci yang digunakan adalah sama, namun algoritma ini digunakan karena tingkat kemamanannya yang sangat tinggi. Teknik kriptografi bisa menyandikan data internal audit sehingga tidak bisa sembarangan dibaca, namun tidak hanya bisa menyandikan tetapi metode ini bisa juga mengembalikan data seperti semula agar bisa kembali dibaca atau dipahami.

3.1.1 Algoritma Sistem

Advance Encryption Standard merupakan satu dari banyak algoritma kriptografi. Advance Encryption Standard menggunakan 4 tahapan dalam proses penyandian data, antara lain adalah *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey*. Proses penyandian dilakukan berulang atau bisa disebut dengan ronde. Banyaknya ronde pada Advance Encryption Standard dengan panjang kunci 128 bit adalah 10 ronde. Plaintext yang akan disandikan akan diurutkan dan

Journal Global Tecnology Computer
Vol 2, No. 2, April, 2023, Hal 75 - 86
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

dimasukkan ke dalam state 4 x 4. Plaintext yang telah dimasukkan ke dalam state akan diproses 4 kali transformasi dan akan di XOR-kan dengan masing-masing kunci yang berbeda setiap rondenya (*RoundKey*).

3.1.2 Ekspansi Kunci

Proses ekspansi kunci dibutuhkan untuk proses *AddRoundKey*. Jumlah kunci dari proses ekspansi kunci yang dibutuhkan algoritma AES 128 Bit adalah 10 kunci. Kunci yang akan digunakan pada kasus ini adalah "YPI.SMP.HIKMATUL.". Berikut ini adalah proses ekspansi kunci Advance Encryption Standard:

a. Urutkan plaintext kunci ke dalam blok berukuran 128 Bit (16 Kode ASCII), setelah itu kunci akan diubah ke dalam bentuk *Hexadecimal*.

Y	P	I	.	S	M	P	.	H	I	K	M	A	T	U	L
59	50	49	2E	53	4D	50	2E	48	49	4B	4D	41	54	55	4C

b. Setelah itu susun kunci yang telah diubah ke dalam *state* berukuran 4 x 4 seperti berikut :

59	50	49	2E
53	4D	50	2E
48	49	4B	4D
41	54	55	4C

→ Kunci Ronde ke-0

c. Setelah itu langkah pertama untuk menghasilkan kunci ke-1 adalah melakukan fungsi *RotWord*, yaitu dengan menggeser setiap bit pada kolom ke 4 ke atas 1 kali dari kunci ronke ke-0.

2E	⇨	2E	
2E		4D	
4D		4C	
4C		2E	

d. Lalu substitusikan hasik dari *RotWord* dengan nilai pada tabel *S-Box* (*SubBytes*).

Tabel 1. Tabel *S-Box*

		Y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
	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
X	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	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

2E	→	31
4D	→	E3
4C	→	29
2E	→	31

→ Hasil substitusi *RotWord* dengan nilai pada tabel *X-Box*

e. Tahap akhir untuk mendapatkan kolom pertama kunci ronde ke-1 adalah proses XOR antara kolom pertama dari kunci ronde ke-0 dan hasil dari *SubBytes* lalu di XOR-kan dengan RCon.

Journal Global Tecnology Computer
Vol 2, No. 2, April, 2023, Hal 75 - 86
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

Tabel 2. 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

59		31		01		69	→	Kolom pertama kunci ronde ke-1 (wi)
53	⊕	E3	⊕	00	=	B0		
48		29		00		61		
41		31		00		70		

f. Lalu untuk mendapatkan kolom kedua dilakukan XOR antara kolom pertama (wi) dengan kolom kedua dari kunci ronde ke-0, setelah itu lakukan proses seperti kolom kedua untuk mendapatkan kolom berikutnya.

50		69		39	→	Kolom kedua
4D	⊕	B0	=	FD		
49		61		28		
54		70		24		

49		4E		70	→	Kolom ketiga
50	⊕	E3	=	AD		
4B		2C		63		
55		4B		71		

2E		07		5E	→	Kolom keempat
2E	⊕	B3	=	83		
4D		67		2E		
4C		1E		3D		

g. Dengan demikian, dari seluruh proses di atas maka dihasilkan kunci untuk ronde ke-1, yaitu :

69	39	70	5E
B0	FD	AD	83
61	28	63	2E
70	24	71	3D

Proses diatas akan diulang sebanyak 10 kali untuk mendapatkan kunci ronde ke-2 sampai kunci ronde ke-10. Kunci dari setiap rondenya akan digunakan untuk proses enkripsi dan deskripsi, berikut ini adalah hasil seluruh ekspansi *key*:

69	39	70	5E
B0	FD	AD	83
61	28	63	2E
70	24	71	3D

Kunci Ronde Ke-1

87	BE	CE	90
81	7C	D1	52
46	6E	0D	23
28	0C	7D	40

Kunci Ronde Ke-2

83	3D	F3	63
A7	DB	0A	58
4F	21	2C	0F
48	44	39	79

Kunci Ronde Ke-3

E1	DC	2F	4C
D1	0A	00	58
F9	D8	F4	FB
B3	F7	CE	B7

Kunci Ronde Ke-4

9B	47	68	24
DE	D4	D4	8C
50	88	7C	87
9A	6D	A3	14

Kunci Ronde Ke-5

DF	98	F0	D4
C9	1D	C9	45
AA	22	5E	D9
AC	C1	62	76

Kunci Ronde Ke-6

F1	69	99	4D
FC	E1	28	6D
92	B0	EE	37
E4	25	47	31

Kunci Ronde Ke-7

4D	24	BD	F0
66	87	AF	C2
55	E5	0B	3C
07	22	65	54

Kunci Ronde Ke-8

73	57	EA	1A
8D	0A	A5	67
75	90	9B	A7
8B	A9	CC	98

Kunci Ronde Ke-9

Journal Global Tecnology Computer
Vol 2, No. 2, April, 2023, Hal 75 - 86
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

C0	97	7D	67
D1	DB	7E	19
33	A3	38	9F
29	80	4C	D4

Kunci Ronde Ke-10

3.1.3 Enkripsi

Pada proses ini dilakukan penyandian terhadap data internal audit Sekolah. *Plaintext* yang akan dienkripsi adalah "AUDIT ATAS LAPOR", dan berikut ini adalah proses enkripsinya:

a. Urutkan *plaintext* ke dalam blok lalu ubah ke bentuk bilangan *hexadecimal*.

A	U	D	I	T		A	T	A	S		L	A	P	O	R
41	55	44	49	54	20	41	54	41	53	20	4C	41	50	4F	52

b. Susun 16 byte pertama dari *plaintext* yang sudah diubah ke bentuk bilangan *hexadecimal* ke dalam *state* 4 x 4.

41	54	41	41
55	20	53	50
44	41	20	4F
49	54	4C	52

c. Lalu masuk ke proses *AddRoundKey*, pada proses ini XOR-kan *plaintext* di atas dengan kunci ronde ke-0.

41	54	41	41
55	20	53	50
44	41	20	4F
49	54	4C	52

⊕

42	53	54	2e
57	55	45	44
53	4D	52	55
2E	41	41	41

=

03	07	15	6F
02	75	16	14
17	0C	72	1A
67	15	0D	13

d. Setelah itu hasil dari *AddRoundKey* di atas akan menjadi ronde ke-1 yang akan diproses lagi dengan 4 transformasi, yaitu *SubBytes, ShiftRows, MixColumns* dan *AddRoundKey*.

Ronde 1

a. Transformasi pertama yaitu *SubBytes*, pada proses ini setiap *byte* akan ditukar dengan nilai pada tabel *S-Box*.

03	07	15	6F
02	75	16	14
17	0C	72	1A
67	15	0D	13

SubBytes →

7B	C5	59	A8
77	9D	47	FA
F0	FE	40	A2
85	59	D7	7D

b. Setelah itu dilakukan proses *ShiftRows*, dengan cara menggeser setiap baris kecuali baris pertama pada *state*, baris kedua digeser 1 *byte* ke kiri, baris ketiga digeser 2 *byte* ke kiri, dan baris keempat digeser 3 *byte* ke kiri, untuk lebih jelasnya seperti di bawah ini :

7B	C5	59	A8
77	9D	47	FA
F0	FE	40	A2
85	59	D7	7D

=

7B	C5	59	A8
9D	47	FA	77
40	A2	F0	FE
7D	85	59	D7

c. Proses Selanjutnya adalah *MixColumns*, pada proses ini dilakukan proses perkalian antar *polinominal* tetap dengan *state* hasil *ShiftRows*.

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

X

7B	C5	59	A8
9D	47	FA	77
40	A2	F0	FE
7D	85	59	D7

Proses perhitungan untuk mencari baris pertama mmenggunakan operator polinominal, dengan aturran 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 1B (0001 1011) jika MSB = 1, dan jika dikali 03 maka dilakukan operasi dikali 02 dan XOR dengan bilangan hexadecimal hasil ShiftRows itu sendiri. Langkah terakhir dari ronde ke-1 adalah *AddRoundKey*, proses ini sama dengan yang sebelumnya tetapi *state* hasil proses *MixColumns* di-XOR-kan dengan kunci ronde ke-1

3.1.4 Dekripsi

Dekripsi adalah proses pengembalian data yang telah ter-enkripsi menjadi *plaintext* kembali. Proses *transformasi*

Journal Global Tecnology Computer
Vol 2, No. 2, April, 2023, Hal 75 - 86
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

dekripsi pada metode *Advance Encryption Standard* adalah *InvSubBytes*, *InvShiftRows*, *InvMixColumns*, dan *AddRoundKey*. berikut ini adalah proses dekripsi dari hasil *ciphertext* ronde ke-10 yang telah didapatkan sebelumnya:

a. Lakukan proses XOR antara *ciphertext* yang telah diperoleh dari proses enkripsi dengan *RoundKey* ke-10.

EE	92	1D	38	⊕	21	D4	23	A7	=	B5	41	18	20
F8	5A	8A	73		83	44	3D	D0		DD	D7	6A	62
A5	42	AD	A1		0E	11	23	04		CE	D3	EE	24
01	46	91	47		82	F1	10	86		13	A6	F3	EC

b. Pada ronde ke-1 sampai ronde ke-9 proses dekripsi dilakukan *transformasi InvShiftRows*, *InvSubBytes*, *InvMixColumns*,*dan AddRoundKey.*
Ronde ke-1
InvShiftRows

B5	41	18	20												
→ DD	D7	6A	62												
→ CE	D3	EE	24						=	B5	41	18	20
→ 13	A6	F3	EC							62	DD	D7	6A
										EE	24	CE	DE
										A6	F3	EC	13

c. Selanjutnya lakukan proses *InvSubBytes.* Cara kerja proses *InvSubBytes* dan *SubBytes* hampir sama, hanya saja nilai pada *S-Box* untuk *InvSubBytes* ini berbeda dengan nilai pada S-*Box* untuk *SubBytes* karena telah dilakukan operasi *invers*. Berikut ini adalah prosesnya:

Tabel 3. *Invers S-Box*

x \ 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

B5	41	18	20			D2	F8	34	54
62	DD	D7	6A	*InvSubBytes* →		AB	C9	0D	58
EE	24	CE	DE			99	A6	EC	9C
A6	F3	EC	13			C5	7E	83	82

d. Lalu lakukan operasi XOR antara hasil *InvSubBytes* dengan *RoundKey* 9 untuk melakukan transfirmasi *AddRoundKey*.

D2	F8	34	54	⊕	42	F5	F7	84	=	90	0D	C3	D0
AB	C9	0D	58		4F	C7	79	ED		E5	0E	74	B5
99	A6	EC	9C		9E	1F	32	27		07	B9	DE	BB
C5	7E	83	82		DD	73	E1	96		18	0D	62	14

e. Kemudian lakukan proses transformasi *InvMixColumns* dari hasil *AddRoundKey* di atas dengan aturan *irreducible polynomial.*

0E	0B	0D	09	X	90	0D	C3	D0
09	0E	0B	0D		E5	0E	74	B5
0D	09	0E	0B		07	B9	DE	BB
0B	0D	09	0E		18	0D	62	14

Proses perhitungan di atas dapat dilakukan dengan mengubah bilangan *hexadecimal* ke bilangan *biner*, kemudian diubah ke bilangan *Polynomial*, berikut ini adalah rincian perhitungannya :
Ronde 2

InvShiftRows

17	95	09	90
59	FF	F3	E0
8A	E0	2A	36
77	FB	E5	41

InvSubBytes

87	AD	40	96
15	7D	7E	A0
CF	A0	95	24
02	63	2A	F8

RoundKey 8

7B	B7	02	73
16	88	BE	94
6B	81	2D	15
52	AE	92	77

AddRoundKey

2B	55	86	07
B3	5E	45	EF
8A	A2	C1	DE
07	FA	4F	C9

InvMixColumns

2F	41	90	D3
BA	4F	65	C0
88	CE	FF	CF
EA	2C	E7	9C

Ronde 3

InvShiftRows

2F	41	90	D3
C0	BA	4F	65
FF	CF	88	CE
2C	E7	9C	EA

InvSubSytes

4E	F8	96	A9
1F	C0	92	BC
7D	5F	97	EC
42	B0	1C	BB

RoundKey 7

1E	CC	B5	71
11	9E	36	2A
B2	EA	AC	38
F1	FC	3C	E5

AddRoundKey

F0	AD	A9	FE
5D	45	8A	C8
18	18	C1	42
1C	2D	E0	EF

InvMixColumns

31	F4	2B	95
5E	0B	89	58
8B	DF	38	52
B4	EA	E8	8D

Ronde 4

InvShiftRows

31	F4	2B	95
58	5E	0B	89
38	52	8B	DF
EA	E8	8D	B4

InvSubBytes

2E	BA	0B	AD
5E	9D	9E	F2
76	48	CE	EF
BB	C8	B4	C6

RoundKey 6

C2	D2	79	C4
33	8F	A8	1C
87	58	46	94
ED	0D	C0	D9

AddRoundKey

80	62	60	C5
5D	5A	03	9E
D1	6A	DF	17
A0	0B	D5	6E

InvMixColumns

CF	25	07	3F
BC	8A	1E	33
D7	2F	B0	E0
C2	61	F3	C3

Ronde 5

InvShiftRows

CF	25	07	3F
33	BC	8A	1E
B0	E0	D7	2F
61	F3	C3	C2

InvSubBytes

5F	C2	38	25
66	78	CF	E9
FC	A0	0D	4E
D8	7E	33	A8

RoundKey 5

6F	10	AB	BD
86	BC	27	B4
53	DF	1E	D2
97	E0	CD	19

AddRoundKey

90	54	8B	26
0C	BC	95	18
86	25	3E	AA
B8	A6	91	61

InvMixColumns

22	4B	07	40
9C	87	B2	84
4A	F9	AB	19
83	AF	DF	0D

Ronde 6

InvShiftRows

22	4B	07	40
85	9C	87	B2
AB	19	4A	F9
AF	DF	0D	83

InvSubBytes

94	CC	38	72
67	1C	EA	3E
0E	8E	5C	69
1B	EF	F3	41

RoundKey 4

A3	7F	BB	16
CD	3A	9B	93
1B	8C	C1	CC
D0	77	2D	D4

AddRoundKey

29	95	1D	C2
03	B2	74	95
0B	71	EA	8E
9C	57	89	2A

InvMixColumns

DD	6B	64	69
7F	F1	53	55
94	09	9C	C8
A5	D2	35	31

Journal Global Tecnology Computer
Vol 2, No. 2, April, 2023, Hal 75 - 86
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

Ronde 7

InvShiftRows

DD	6B	64	69
55	7F	F1	53
9C	C8	94	09
D2	35	31	A5

InvSubBytes

C9	05	8C	E4
ED	6B	2B	50
1C	B1	E7	40
7F	D9	2E	29

RoundKey 3

9B	DC	C4	AD
1A	F7	A1	08
82	97	4D	0D
45	A7	5A	F9

AddRoundKey

EA	E1	F0	71
66	A1	1B	65
9B	4B	AE	21
D2	E6	EC	38

InvMixColumns

FC	4C	E3	E7
E6	8D	0E	E7
C5	AD	90	2D
B7	34	20	28

Ronde 8

InvShiftRows

FC	4C	B3	E7
E7	E6	8D	0E
90	2D	C5	AD
34	20	28	B7

InvSubBytes

55	5D	4B	B0
B0	F5	B4	D7
96	FA	07	18
28	54	EE	20

RoundKey 2

4C	47	18	69
13	ED	56	A9
88	15	DA	40
BC	E2	FD	A3

AddRoundKey

19	9A	D3	59
0F	B4	4E	D2
77	87	B4	30
94	C6	13	F3

InvMixColumns

92	A8	04	21
A5	3B	3E	37
9D	63	97	E8
DB	03	B2	D0

AddRoundKey

2C	64	6F	0A
19	D7	F2	2E
55	55	BB	9B
CA	10	0F	B1

InvMixColumns

34	5A	59	22
6D	F6	40	CF
22	38	8F	C3
F1	DE	B6	EC

Ronde 9

InvShiftRows

92	A8	04	21
37	A5	3B	3E
97	E8	9D	63
03	B2	D0	DB

InvSubBytes

74	6F	30	7B
B2	29	49	D1
85	C8	75	00
D5	3E	60	9F

RoundKey 1

58	0B	5F	71
AB	FE	BB	FF
D0	9D	CF	9A
1F	5E	1F	5E

Ronde 10

InvShiftRows

34	5A	59	22
CF	6D	F6	40
8F	C3	22	38
DE	B6	EC	F1

InvSubBytes

28	46	15	94
5F	B3	D6	72
73	33	94	76
9C	79	83	2B

RoundKey 0

42	53	54	2E
57	55	45	44
53	4D	52	55
2E	41	41	41

AddRoundKey

41	54	41	41
55	20	53	50
44	41	20	2F
49	54	4C	52

Dari semua proses diatas maka didapatkan hasil " 41 55 44 49 54 20 41 54 41 53 20 4C 41 50 2F 52". State AddRoundKey pada ronde ke 10 tersebut dikonversikan ke karakter sehingga di dapatkan Plaintext "AUDIT ATAS LAPOR".

4. KESIMPULAN

Berdasarkan rumusan masalah dan pembahasan pada bab-bab sebelumya maka dapat dibuat kesimpulan bahwa Algoritma *Advance Encryption Standard* digunakan untuk mengamankan data *internal audit* karena sangat sulit untuk memecah sandi dan ciphertext yang telah mengalami beberapa proses transformasi sehingga sangat tepat digunakan untuk menyandikan atau mengamankan data. Dan Langkah-langkah untuk mengimplementasikan algoritma *Advance*

Encryption Standard (AES) 128 bit dalam mengamankan data *internal audit* adalah dengan memasukkan perhitungan AES 128 bit ke dalam sistem sehingga dapat memberikan solusi mengamankan data *internal audit.*

REFERENCE

[1] J. N. A. Am, “Pengamanan File Data,” *Maj. Ilm.*, pp. 1–10, 2002.
[2] Suginam, “Pengaruh peran audit internal dan pengendalian intern terhadap pencegahan fraud,” *Ris. J. Akunt.*, vol. 1, no. 1, pp. 22–28, 2017.
[3] R. Rahmawati and D. Rahardjo, “Aplikasi Pengamanan Data Menggunakan Algoritma Steganografi Discrete Cosine Transform dan Kriptografi grafi AES 128 BIT pada SMK PGRI 15 Jakarta,” *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. April, pp. 67–74, 2016.
[4] A. Pariddudin and F. Syauqi, “Penerapan Algoritma AES pada QR CODE untuk Keamanan Verifikasi Tiket,” *Teknois J. Ilm. Teknol. Inf. dan Sains*, vol. 10, no. 2, pp. 43–52, 2020.
[5] N. Fajar, “No Titleسی رر باطب ارتیوه شی زندگی تلا وابه برت ریت تئوآرت اسدرزنان درزنان ومردان سالمند,” □□ □□□□□□, vol. 1, no. 4, p. 53, 2015.
[6] A. Arif and P. Mandarani, “Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Advanced Encryption Standard (AES) 128 Bit Pada Sistem Keamanan Short Message Service (SMS) Berbasis Android,” *Teknoif*, vol. 4, no. 1, pp. 1–10, 2016.
[7] T. Bin Tahir, M. Apriyadi, M. Rais, and I. Syarif, “Sistem Informasi Encrypt Dan Decrypt Dengan Algoritma AES Menggunakan Framework Laravel,” *Patria Artha Technol. J.*, vol. 4, no. 1, pp. 41–46, 2020.
[8] R. Amalia, “Implementasi Algoritma AES dan Algoritma XOR pada Aplikasi Enkripsi dan Dekripsi Teks Berbasis Android,” *Fakt. Exacta*, vol. 11, no. 4, pp. 370–379, 2018.
[9] A. Ignasius and D. V. S. Y. Sakti, “Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi,” *SKANIKA*, vol. 5, no. 1, pp. 1–10, 2022.
[10] D. Surian, “Algoritma Kriptografi AES Rijndael,” *TESLA J. Tek. Elektro UNTAR*, vol. 8, no. 2, p. pp-97, 2009.
[11] D. Q. P. A. Paramarta, A. Kusyanti, and M. Data, “Implementasi Algoritme Advance Encryption Standard (AES) pada Enkripsi dan Dekripsi QR-Code,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 12, pp. 6729–6736, 2018.
[12] Z. Musliyana, T. Y. Arif, and R. Munadi, “Peningkatan sistem keamanan autentikasi single sign on (sso) menggunakan algoritma aes dan one-time password studi kasus: sso universitas ubudiyah indonesia,” *J. Rekayasa Elektr.*, vol. 12, no. 1, pp. 21–29, 2016.
[13] D. S. Jasi, R. O. Bura, and J. Jupriyanto, “MODEL KONSEPTUAL AUDIT TEKNOLOGI ALAT UTAMA SISTEM SENJATA (STUDI KASUS RUDAL C-705),” *Ind. Pertahanan*, vol. 3, no. 1, pp. 28–47, 2021.