Jurnal CyberTech

Vol.3. No.11, November 2020, pp. 1673~1681
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Implementasi Algoritma AES(Advanced Encryption Standard) Untuk Mengamankan File Soal Ujian Sekolah Dengan Kunci Algoritma 3Des (Triple DES)

ANGGA SYAHPUTRA *, Jaka Prayudha, **, Tugiono, **

* Program Studi Mahasiswa, STMIK Triguna Dharma
** Program Studi Dosen Pembimbing, STMIK Triguna Dharma

Article Info

Article history:
Received Nov 12th, 2020
Revised Nov 20th, 2020
Accepted Nov 29th, 2020

Keyword:
Soal Ujian
Implementasi
kriptografi

ABSTRACT

Soal ujian sekolah adalah data yang dibuat dan dikeluarkan oleh sekolah dimana data tersebut diperoleh dari guru mata pelajaran yang bertugas dalam membuat soal ujian, jika data tersebut diketahui oleh orang yang tidak bertanggung jawab dan menyebarkan nya kepada khalayak umum maka hal tersebut akan menyebabkan suatu masalah. Implementasi merupakan sebuah tahapan penting pada suatu program yang telah ditetapkan agar tercapainya tujuan yang diinginkan serta dapat dirasakan dampaknya.Secara etimologi, menurut Kamus Webster yang dikutip oleh Solichin Abdul Wahab tentang pengertian implementasi yang berasal dari bahasa inggris yakni *to implement.* Dalam kamus besar Webster menyatakan bahwa *to implement* (mengimplementasikan) itu berarti menyediakan sarana untuk melaksanakan sesuatu (*to provide the means for carrying out),* untuk menimbulkan dampak/akibat terhadap sesuatu *(to give practical effect to).* Kriptografi adalah ilmu yang mempelajari tentang teknik-teknik pada matematika yang berhubungan dengan aspek keamanan data berupa kerahasiaan, integritas, serta otentikasi suatu data.

Corresponding Author:
Nama : ANGGA SYAHPUTRA
Program Studi : Sistem Informasi STMIK Triguna Dharma
Email : anggasyahputra050896@gmail.com

1. PENDAHULUAN

UJian merupakan salah satu bentuk alat ukur yang terdiri dari butir-butir pertanyaan untuk mengukur kemampuan siswa dalam mencapai tujuan pembelajaran yang telah dilakukan. Penilaian dilakukan berdasarkan poin-poin hasil pengukuran. Data hasil pengukuran kemudian dianalisis melalui sebuah prosedur yang sistematis, selanjutnya diinterpretasikan untuk membuat sebuah kesimpulan.[1]

Ada berbagai macam algoritma kriptografi yang dapat diimplementasikan untuk pengamanan data yaitu algoritma kriptografi *Advance Encryption Standart dan Triple Data Encryption Standart.* AES termasuk kepada algoritma kriptografi modern yaitu sistem penyandian blok yang bersifat *non-Feistel* karena AES menggunakan komponen yang selalu memiliki *invers* dengan panjang blok 128 *bit.* Kunci *Advanced Encryption Standard* (AES) dapat memiliki panjang kunci *bit* 128, 192, dan 256 *bit.* Penyandian *Advanced Encryption Standard* (AES) menggunakan proses yang berulang yang disebut dengan ronde[2]. 3DES merupakan salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan suatu data berupa pesan teks. Proses yang dilakukan dalam penyandian pesan teksnya, yaitu proses enkripsi dan proses

dekripsi, prosesnya adalah mengulang algoritma DES sebanyak tiga kali, sesuai dengan pemilihan kuncinya dan urutan proses yang dipilih. Algoritma triple DES termasuk kedalam kriptografi modern, karena penyandian modern berorientasi pada mode *bit*. [3]

Berdasarkan latar belakang tersebut maka diangkat judul yaitu **"IMPLEMENTASI ALGORITMA AES (ADVANCED ENCRYPTION STANDARD) UNTUK MENGAMANKAN FILE SOAL UJIAN SEKOLAH DI MA. RAUDHATUSSALAM DENGAN KUNCI ALGORITMA 3DES (TRIPLE DES)".**

2. METODE PENELITIAN

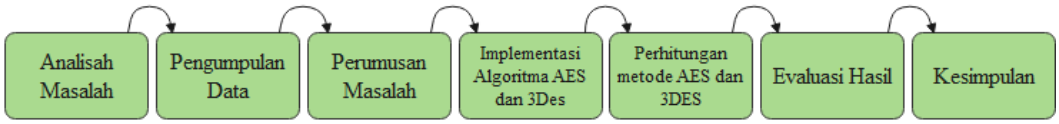
Di dalam melakukan risert atau penelitian terdapat beberapa cara dalam pengambilan data dengan cara sebagai berikut:

1. Pengumpulan Data (Data Collecting)

Dalam teknik pengumpulan data terdapat beberapa yang dilakukan yaitu dengan cara observasi dan wawancara. Pada bagian observasi ini merupakan pencarian atau pengumpulan data dengan melakukan tinjauan langsung ke MA. Raudhatussalam Riau. Dimana untuk melakukan kegiatan observasi pra-riset terlebih dahulu, bertujaun untuk mencari tahu masalah dan kendala seperti apa yang dialami serta sejauh apa dampak yang terjadi dengan keamanan data di instansi terkait. Berdasarkan observasi tersebut ditemukan masalah terkait keamanan data pada soal ujian di instansi tersebut. Melakukan wawancara ini sebaiknya dilakukan dengan kepala sekolah atau pun pihak-pihak yang mengelolah data tersebut.

2. Studi Literatur

Dari komposisi yang ada dengan jumlah literatur yang digunakan sebanyak 23 sumber referensi. Diharapkan dengan literatur tersebut dapat membantu peneliti dalam menyelesaikan permasalahan pengamanan data yang terjadi pada soal ujian sekolah. Dikarenakan dalam penelitian ini menggunakan konsep pendekatan eksperimental, maka dibawah ini merupakan gambar yang mampu menjelaskan bagaimana tahap - tahap dalam melakukan penelitian ini, yaitu :



Gambar 1 Metode Penelitian

3. ANALISA DAN HASIL

3.1 Algoritma Sistem

Algoritma sistem merupakan penjelasan dari langkah - langkah dalam penyelesaian masalah saat perancangan sistem keamanan soal ujian sekolah dengan menggunakan algorithma AES dan 3DES. Hal ini dilakukan untuk meningkatkan keamanan data soal ujian sekolah tersebut.

Pada algoritma 3DES terdapat 4 proses yang harus dilalui, yaitu sebagai berikut [4]:

1. Permutasi awal
2. Pembangkitan kunci internal
3. Proses enkripsi
4. Proses dekripsi

Sedangkan pada algoritma AES terdapat 3 proses utama, yaitu sebagai berikut [5]:

1. Proses pembangkitan/ekspansi kunci (*Roundkey*).
2. Proses enkripsi (*Subbyte, Shiftrow, Mixcolumn, Addroudkey*).
3. Proses dekripsi (*Invshiftrow, invsubbyte, invmixcolumn, addroundkey*).

Tahapan proses yang terjadi yaitu kunci dari algoritma AES terlebih dahulu di enkripsi menggunakankan algoritma 3DES, hasil dari proses tersebut akan menjadi key input untuk algoritma AES.

3.2 Enkripsi 3DES

Tabel 1 Konversi Plaintext dan Key ke Biner

	HEXA	BINER							
M	4D	0	1	0	0	1	1	0	1
D	44	0	1	0	0	0	1	0	0
N	4E	0	1	0	0	1	1	1	0

	HEXA	BINER							
A	41	0	1	0	0	0	0	0	1
N	4E	0	1	0	0	1	1	1	0
G	47	0	1	0	0	0	1	1	1
G	47	0	1	0	0	0	1	1	1
A	41	0	1	0	0	0	0	0	1
S	53	0	1	0	1	0	0	1	1
Y	59	0	1	0	1	1	0	0	1
A	41	0	1	0	0	0	0	0	1
H	48	0	1	0	0	1	0	0	0
P	50	0	1	0	1	0	0	0	0
U	55	0	1	0	1	0	1	0	1
T	54	0	1	0	1	0	1	0	0

T	54	0	1	0	1	0	1	0	0
G	47	0	1	0	0	0	1	1	1
D	44	0	1	0	0	0	1	0	0
I	49	0	1	0	0	1	0	0	1
N	4E	0	1	0	0	1	1	1	0
2	32	0	0	1	1	0	0	1	0
0	30	0	0	1	1	0	0	0	0
1	31	0	0	1	1	0	0	0	1
6	36	0	0	1	1	0	1	1	0
0	30	0	0	1	1	0	0	0	0
2	32	0	0	1	1	0	0	1	0
0	30	0	0	1	1	0	0	0	0
3	33	0	0	1	1	0	0	1	1

Initial Permutasi pada *bit plaintext* menggunakan tabel IP untuk mencari nilai L0R0.

Tabel 2 Initial Permutasi (IP)

Tabel IP							
1	2	3	4	5	6	7	8
58	50	42	34	26	18	10	02
9	10	11	12	13	14	15	16
60	52	44	36	28	20	12	04
17	18	19	20	21	22	23	24
62	54	46	38	30	22	14	06
25	26	27	28	29	30	31	32
64	56	48	40	32	24	16	08
33	34	35	36	37	38	39	40
57	49	41	33	25	17	09	01
41	42	43	44	45	46	47	48
59	51	43	35	27	19	11	03
49	50	51	52	53	54	55	56
61	53	45	37	29	21	13	05
57	58	59	60	61	62	63	64
63	55	47	39	31	23	15	07

Generate kunci yang akan digunakan untuk mengenkripsi *plaintext* menggunanakan tabel permutasi kompresi, pada langkah ini terjadi kompresi dengan membuang 1 bit masing - masing blok kunci dari 64 bit menjadi 56 bit

Tabel 3 Permutasi Kompresi

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

$CD(k)$ = 0000000 0111111 1100000 0000000 1001010 0101111 11110000 1011000

Pecah $CD(k)$ menjadi 2 bagian, kanan dan kiri yaitu:

C0 = 0000000 0111111 1100000 0000000

D0 = 1001010 0101111 1111000 1011000

Lakukan pergeseran ke kiri (*left shift*) pada C0 dan D0 sebanyak 1 atau 2 kali berdasarkan table *left shift*.

Tabel 4 *Left Shift*

Rounde ke - i	**Jumlah Pergeseran**
1	1
2	1
3	2
4	2

5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Berikut Output nya :
C0 = 0000000 0111111 1100000 0000000
D0 = 1001010 0101111 1111000 1011000
C1 = 0000000 1111111 1000000 0000000
D1 = 0010100 1011111 1110001 0110001
Begitu seterusnya hingga mendapatkan C_{16} dan D_{16}

Setiap putaran C dan D digabung kembali menjadi C_iD_i dan di input kedalam tabel *permutation compression* (PC-2) dan terjadi kompresi data C_iD_i 56 bit menjadi C_iD_i 48 bit.

Tabel 5 PC-2

14	17	11	24	01	05
03	28	15	06	21	10
23	19	12	04	26	08
16	07	27	20	13	02
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Proses dilakukan sebanyak tiga kali, sehingga mendapatkan hasil sebagai berikut :
10111000 11101001 11101100 01000110 01011011 10111100 11000001 01110101 01000010 10110010 00100001 11111110 00010100 11101100 11101101 11001011
Atau diubah kedalam bentuk karakter menjadi : ¸éìF[¼ÁuB²!þìíË
Atau diubah kedalam bentuk hexadecimal menjadi : B8 E9 EC 46 5B BC C1 75 42 B2 21 FE 14 EC ED CB

3.3 Enkripsi AES

proses enkripsi menggunakan algorithma AES, panjang teks yang akan di enkripsi sama dengan panjang kunci, karena panjang kunci yang digunakan adalah 128 bit, maka karakter yang akan di enkripsi adalah 16 karakter pertama, kemudian dilanjutkan dengan 16 karakter berikutnya sampai seluruh karakter selesai di enkripsi. Jika teks terakhir tidak mencukupi 16 karakter maka ditambahkan padding 00

Plaintext : ANGGASYAHPUTRAAB
Key : B8 E9 EC 46 5B BC C1 75 42 B2 21 FE 14 EC ED CB
Konversi kedalam bentuk heksadesima :
Plaintext: 41 4E 47 47 41 53 59 41 48 50 55 54 52 41 41 42
Key : B8 E9 EC 46 5B BC C1 75 42 B2 21 FE 14 EC ED CB

Langkah dalam proses enkripsi AES sebagai berikut :
1. Ekspansi Kunci

Sebelum masuk dalam tahapan enkripsi maka dilakukan terlebih dahulu ekspansi kunci yang akan digunakan pada setiap putaran pada algorithma AES. Kunci yang digunakan akan dibagi menjadi beberapa blok, jika kunci 128 bit, maka panjang kunci (Nk) dibagi 32. 128/32=4, maka pengisian baris dan kolom adalah berdasarkan kolom, maka :

W0 = B8 E9 EC 46 W2 = 42 B2 21 FE
W1 = 5B BC C1 75 W3 = 14 EC ED CB

Untuk mencari kolom pertama pada setiap ronde dengan cara :
W3 = RotWord(W3)
Rotword adalah memindahkan bit teratas menjadi bit terbawah
14 EC ED CB = EC ED CB 14
Selanjutnya melakukan transformasi Sub*Byte* dengan S-Box
EC ED CB 14 = CE 55 1F FA
Melakukan XOR dengan kolom pertama
CE 55 1F FA ⊕ B8 E9 EC 46 = 76 BC F3 BC
Selanjutnya melakukan XOR dengan Rcon
76 BC F3 BC⊕ 01 00 00 00 = 77 BC F3 BC

Tabel 6 Roundkey Enkripsi AES

Roundkey 0				**Roundkey 1**				**Roundkey 2**			
B8	5B	42	14	77	2C	6E	7A	2D	01	6F	15
E9	BC	B2	EC	BC	00	B2	5E	07	07	B5	EB
EC	C1	21	ED	F3	32	13	FE	43	71	62	9C
46	75	FE	CB	BC	C9	37	FC	66	AF	98	64
Roundkey 3				**Roundkey 4**				**Roundkey 5**			
C0	C1	AE	BB	05	C4	6A	D1	CE	0A	60	B1
D9	DE	6B	80	AA	74	1F	9F	D0	A4	BB	24
00	71	13	8F	50	21	32	BD	AD	8C	BE	03
3F	90	08	6C	D5	45	4D	21	EB	AE	E3	C2
Roundkey 6				**Roundkey 7**				**Roundkey 8**			
D8	D2	B2	03	F8	2A	98	9B	8E	A4	3C	A7
AB	0F	B4	90	FD	F2	46	D6	8F	7D	3B	ED
88	04	BA	B9	19	1D	A7	1E	E9	F4	53	4D
23	8D	6E	AC	58	D5	BB	17	4C	99	22	35
Roundkey 9				**Roundkey 10**							
C0	64	58	FF	30	54	0C	F3				
6C	11	2A	C7	46	57	7D	BA				
7F	8B	D8	95	74	FF	27	B2				
10	89	AB	9E	06	8F	24	BA				

2. Melakukan XOR antara *Plainteks* dengan *Key*

Plaintext (input)					Key (input)					AddRoundKey			
41	41	48	52		B8	5B	42	14		F9	1A	0A	46
4E	53	50	41	⊕	E9	BC	B2	EC	=	A7	EF	E2	AD
47	59	55	41		EC	C1	21	ED		AB	98	74	AC
47	41	54	42		46	75	FE	CB		01	34	AA	89

3. Subbyte

99	A2	67	5A
5C	DF	98	95
62	46	92	91
7C	18	AC	A7

4. Shiftrow

99	A2	67	5A
DF	98	95	5C
92	91	62	46
A7	7C	18	AC

5. Mixcolumn

$S'(x) = a(x) \otimes S(x)$

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,0} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,0} \end{bmatrix} \Rightarrow \begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,0} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 99 \\ df \\ 92 \\ a7 \end{bmatrix}$$

$S'_{0,c} = (\{02\} \bullet 99) \oplus (\{03\} \bullet df) \oplus 92 \oplus a7$

$= (\{10\} \bullet 10011001) \oplus (\{11\} \bullet 11011111) \oplus 10010010 \oplus 10100111$

= 00110010 ⊕ 01100001 ⊕ 10010010 ⊕ 10100111
= 01100110 => **'66'**
Untuk mencari kolom selanjutnya dilakukan cara yang sama seperti diatas sehingga menghasilkan seluruh kolom sebagai berikut:

$$\begin{bmatrix} 66 & 01 & 10 & BA \\ 36 & 5D & E8 & 84 \\ 8B & 87 & 1E & 65 \\ A8 & 06 & 6E & B7 \end{bmatrix}$$

6. Addroundkey

Mixcolumn			
66	01	10	BA
36	5D	E8	84
8B	87	1E	65
A8	0C	6E	B7

⊕

Roundkey 1			
77	2C	6E	7A
BC	00	B2	5E
F3	32	13	FE
BC	C9	37	FC

=

AddRoundKey			
11	2D	7E	C0
8A	5D	5A	DA
78	B5	0D	9B
14	C5	59	4B

Tabel 7 Hasil Enkripsi AES

Round 1				Round 2				Round 3				Round 4			
11	2D	7E	C0	82	9D	71	E6	40	38	C6	61	7F	E0	47	3D
8A	5D	5A	DA	CC	7E	91	2	DF	B6	0E	49	81	0	82	3
78	B5	0D	9B	F6	2A	54	AF	23	AB	6A	AF	C0	BB	AE	5
14	C5	59	4B	1D	99	2A	97	D2	D9	4	9A	E9	EF	FD	8
Round 5				Round 6				Round 7				Round 8			
0	93	D3	55	43	96	16	FC	3B	BA	4A	71	AB	B6	E0	FE
C3	C0	E7	6A	8D	E5	15	A2	80	28	A4	E6	65	32	E3	23
9F	8A	70	1B	83	23	B7	A7	E1	48	0	4F	AD	83	CE	A9
61	D2	7C	E5	C4	0C	6C	C3	5A	43	43	7	B7	34	1	60
Round 9				Round 10											
3A	B1	66	D5	B0	9C	3F	F0								
1E	BA	3B	B5	B2	B5	A8	C8								
58	89	6	24	1B	C9	4D	15								
A5	D0	10	11	84	89	54	70								

3.4 Proses Dekripsi 3DES

1. Melakukan Permutasi *Chiperteks* dengan table IP
   Cipher dalam biner = 10111000 11101001 11101100 01000110 01011011 10111100 11000001 01110101 01000010 10110010 00100001 11111110 00010100 11101100 11101101 11001011
   Atau dalam Hexa = B8 E9 EC 46 5B BC C1 75 42 B2 21 FE 14 EC ED CB
   sehingga di dapatkan hasil sebagai berikut :
   L0 = 11011110 10110001 10101100 11010010
   R0 = 01100111 10100111 00110111 00011000
2. Untuk proses selanjutnya dilakukan langkah yang sama pada saat proses enkripsi.
   P(B16) = 11110010 11011111 10111111 00011101
   L15 = 11011110 10110001 10101100 11010010
   ---------- XOR
   R16 = 00101100 01101110 00010011 11001111
3. Langkah diatas diulang sampai iterasi Ke 1, sehingga mendapatkan hasil sebagai berikut :
   R1 = 10110010 10100010 01011001 01111010
   L1 = 10100000 01101010 00011001 01111110
4. selanjutnya melakukan permutasi R1 dan L1 dengan tabel *inverse initial permutation*, sehingga menghasilkan nilai dekripsi pertama, yaitu sebagai berikut :
   10001101 01010011 10101010 00101101 11000111 01111011 10100101 01111000
5. Proses diulang sebanyak tiga kali hingga mendapatkan hasil dekripsi sebagai berikut :

01000001 01001110 01000111 01000111 01000001 01010011 01011001 01000001 01001000 01010000 01010101 01010100 01010010 01000001 01000001 01000010, atau dalam bentuk hexadesimal sebagai berikut : 41 4E 47 47 41 53 59 41 48 50 55 54 52 41 41 42.

3.5 Proses Dekripsi AES

Tahapan proses Dekripsi AES sama seperti pada saat proses Enkripsi, hanya saja pada saat ini merupakan proses kebalikan nya yaitu sebagai berikut :

1. *Transformasi AddRoundkey*
   a. Meng-XOR-kan ciphertext dengan kunci putaran kesepuluh.

Ciphertext			
B0	9C	3F	F0
B2	B5	A8	C8
1B	C9	4D	15
84	89	54	70

⊕

Roundkey 10			
30	54	0C	F3
46	57	7D	BA
74	FF	27	B2
06	8F	24	BA

=

Inv AddRoundKey			
80	C8	33	03
F4	E2	D5	72
6F	36	6A	A7
82	06	70	CA

   b. Inverse ShiftRow

80	C8	33	03
F4	E2	D5	72
6F	36	6A	A7
82	06	70	CA

80	C8	33	03			
	F4	E2	D5	72		
		6F	36	6A	A7	
			82	06	70	CA

80	C8	33	03
72	F4	E2	D5
6A	A7	6F	36
06	70	CA	82

   c. Inverse SubByte

Inv ShiftRow			
80	C8	33	03
72	F4	E2	D5
6A	A7	6F	36
06	70	CA	82

InvSubByte			
3A	B1	66	D5
1E	BA	3B	B5
58	89	06	24
A5	D0	10	11

2. *Round*

Pada tahapan ini proses yang dilakukan adalah trasformasi *inverse addroundkey, inverse mixcolumn, inverse shiftrow*, dan *inverse subbyte*. Berikut ini Hasil dari setiap *roundnya*:

Round 2				Round 3				Round 4			
AB	B6	E0	FE	3B	BA	4A	71	43	96	16	FC
65	32	E3	23	80	28	A4	E6	8D	E5	15	A2
AD	83	CE	A9	E1	48	00	4F	83	23	B7	A7
B7	34	01	60	5A	43	43	07	C4	0C	6C	C3

Round 5				Round 6				Round 7			
00	93	D3	55	7F	E0	47	3D	40	38	C6	61
C3	C0	E7	6A	81	00	82	03	DF	B6	0E	49
9F	8A	70	1B	C0	BB	AE	05	23	AB	6A	AF
61	D2	7C	E5	E9	EF	FD	08	D2	D9	04	9A

Round 8				Round 9				Round 10			
82	9D	71	E6	11	2D	7E	C0	F9	1A	0A	46
CC	7E	91	02	8A	5D	5A	DA	A7	EF	E2	AD
F6	2A	54	AF	78	B5	0D	9B	AB	98	74	AC
1D	99	2A	97	14	C5	59	4B	01	34	AA	89

3. *Final Round*

Round 10			
F9	1A	0A	46
A7	EF	E2	AD
AB	98	74	AC
01	34	AA	89

⊕

Key			
B8	5B	42	14
E9	BC	B2	EC
EC	C1	21	ED
46	75	FE	CB

=

Plaintext			
41	41	48	52
4E	53	50	41
47	59	55	41
47	41	54	42

Maka *Plaintext* yang dihasilkan adalah : **41 4E 47 47 41 53 59 41 48 50 55 54 54 41 41 42**
Karakter = **ANGGASYAHPUTRAAB**

4. KESIMPULAN

Berdasarkan penelitian yang telah dilalui dalam setiap tahapan perancangan keamanan data pada laporan hasil pengujian dengan menggunakan metode AES dan 3DES maka dapat disimpulkan bahwa :

1. Untuk mengamankan file soal ujian sekolah di MA. Raudhatussalam menggunakan metode AES dan 3DES sebagai kuncinya sebab file soal ujian sekolah ini bersifat rahasia.
2. Berdasarkan pemodelan dan perancangan sistem, metode Algoritma AES dan 3DES sebagai Algoritma kunci dapat diaplikasikan ke dalam pengimplementasian kriptografi pada file soal ujian sekolah. Dimana algoritma AES dan 3DES ini merupakan pengamanan data yang cukup terbilang rumit, karena

didalamnya perhitungannya memerlukan ketelitian dan logika yang kuat. Sehingga algoritma AES dan 3DES ini sangat membantu dalam mengurangi resiko penyalahgunaan pada file soal ujian tadi. Dengan pengamanan data berbasis website yang telah dibangun, sehingga dapat memudahkan admin dalam menginput data secara aman.

UCAPAN TERIMA KASIH

Terima kasih kepada dosen pembimbing Bapak Jaka Prayudha, S.Kom., M.KOM. dan Bapak Tugiono, S.Kom., M.Kom beserta pihak–pihak lainnya yang mendukung penyelesaian jurnal skripsi ini.

REFERENSI

[1] M. Elvira and S. Hadi, "Karakteristik Butir Soal Ujian Semester dan Kemampuan Siswa SMA di Kabupaten Muaro Jambi," *J. Eval. Pendidik.*, vol. 4, no. 1, pp. 58–68, 2016.

[2] E. D. Saragih, N. A. Hasibuan, and E. Bu'ulolo, "Implemantasi Algoritma Triple DES Dan Algoritma Advanced Encryption Standard dalam Penyandian File," *Maj. Ilm. INTI*, vol. 13, no. 3, pp. 263–269, 2018.

[3] N. Siregar, "Perancangan Aplikasi Keamanan Pesan Teks dengan Menggunakan Algoritma Triple DES," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 11–17, 2019.

[4] O. K. Sulaiman, M. Ihwani, and S. F. Rizki, "Model Keamanan Informasi Berbasis Tanda Tangan Digital Dengan Data Encryption Standard (Des) Algorithm," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 14–19, 2016, doi: 10.30743/infotekjar.v1i1.82.

[5] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *J. Mat. UNISBA*, vol. 15, no. 1, pp. 7–14, 2016.

BIBLIOGRAFI PENULIS

<table>
<tr><td>  </td><td>Data Diri
Nama : ANGGA SYAHPUTRA
Tempat/Tanggal Lahir : MAHATO, 05 AGUSTUS 1996
Jenis Kelamin : Laki-Laki
Agama : Islam
Status : Belum Menikah
Pendidikan Terakhir : Sekolah Menengah Atas
Kewarganegaraan : Indonesia
E-mail : anggasyahputra050896@gmail.com
Pendidikan Formal
1. Tahun 2002 - 2008 : SDN 016
2. Tahun 2008 - 2011 : MTs Al-Husna Bagan Batu
3. Tahun 2011 - 2014 : MAS Raudhatussalam Mahato
4. Tahun 2016 - 2021 : STMIK Triguna Dharma</td></tr>
<tr><td></td><td></td></tr>
<tr><td>  </td><td>NIDN : 0120059201
Program Studi : Sistem Komputer
Deskripsi : Dosen tetap Stmik triguna dharma yang aktif mengajar dan meneliti yang berfokus pada bidang keilmuan Robotics, Computer Vision, Software Enginner dan Artificial Intellegence
Prestasi : -</td></tr>
<tr><td></td><td></td></tr>
<tr><td>  </td><td>NIDN : 0111068302
E-mail: tugix.line@gmail.com
Program Studi : Sistem Informasi
Deskripsi : Dosen Tetap STMIK Triguna Dharma yang aktif mengajar dan fokus pada bidang keilmuan Pemrograman Visual, Sistem Pendukung Keputusan dan Sistem Manajemen Basis Data.</td></tr>
</table>