LAPORAN PRAKTIK SISTEM KEAMANAN DATA

ALGORITMA DES

KELOMPOK 3

DISUSUN OLEH

Bagas Aditya pramudana	(V3920012)
Dion Aji cahyono	(V3920018)
~~Isnan Nur Ahmad Wijayakusuma~~	~~(V3920029)~~
Ivan Fausta Dinata	(V3920030)
Kreshna Putra Adi Wicaksana	(V3920032)

PROGRAM STUDI D-III TEKNIK INFORMATIKA

FAKULTAS SEKOLAH VOKASI

UNIVERSITAS SEBELAS MARET SURAKARTA

2021/2022

JURNAL 1

❖ **Implementasi algoritma advanced encryption standard pada aplikasi chatting berbasis android**

❖ **Latar Belakang**

Dalam perkembangan teknologi yang begitu cepat, komunikasi manusia sudah mengalami berbagai perubahan. Dalam bertukar informasi saat ini sudah tidak dibatasi oleh jarak, sekarang dalam komunikasi manusia dalam melakukan pertukaran pesan, telepon, maupun melalui internet. Saat ini internet merupakan teknologi yang paling sering digunakan dalam komunikasi antar manusia. 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. Pada penelitian ini dirancang sebuah aplikasi pesan instan yang melakukan enkripsi pesan yang akan dikirim dengan kunci yang ditentukan pengirim. Aplikasi ini mengirimkan pesan yang terenkripsi sehingga pesan ini aman saat melalui jaringan internet sehingga mencegah terjadinya pembajakan pesan yang terkirim. Aplikasi chatting ini menggunakan enkripsi Algoritma AES. Algoritma AES digunakan untuk enkripsi pesan yang akan dikirim dan dekripsi pesan yang diterima agar dapat dibaca oleh pengguna.

❖ **Tujuan Penelitian**

Tujuan penelitian ini adalah untuk merancang dan membangun sebuah aplikasi chatting dengan mengimplementasikan algoritma AES untuk sebuah keamanan pada pesan dengan melakukan analisis pada pesan yang di enkripsi dan dekripsi untuk memastikan pesan yang diterima oleh user atau pengguna aman dan dapat di dekripsi

❖ **Algoritma yang dipakai beserta alur penelitiannya**

Menggunakan Algoritma Rijndael

Algoritma Rijndael 128 secara spesifik memiliki panjang state dan panjang kunci sebesar 128 bit. State merupakan blok plaintext yang akan dienkripsi atau didekripsi. 128 bit data pada state dan kunci tersebut dipecah menjadi 16 bagian. Setiap bagian berisi masing-masing 1 byte data (8 bit data). Tiap byte data pada state dan kunci tersebut masing-masing dimasukkan ke dalam 16 byte matriks berukuran 4 x 4 dalam notasi heksadesimal.

Alur penelitian:

1. **Kriptografi**

   Digunakan untuk menjaga pesan dari orang yang tidak berhak melihat isi dari konten pesan

2. **Advanced Encryption Standard (AES)**

   Standar Enkripsi Lanjutan disingkat AES merupakan standar enkripsi dengan kunci simetris yang diadopsi oleh Pemerintah Amerika Serikat. Standar ini terdiri dari tiga penyandian blok, yaitu AES-128, AES-192, dan AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai **Rijndael**. Tiap-tiap penyandian memiliki ukuran blok 128 bit dengan ukuran kunci masing-masing 128, 192, dan 256 bit. AES telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya, Standar Enkripsi Data (DES).

   AES adalah variasi dari Rijndael dengan ukuran blok tetap 128 bit dan ukuran kunci 128, 192, atau 256 bit. Sebaliknya, Rijndael sendiri didesain dengan ukuran blok dan kunci kelipatan 32 bit dengan minimum 128 bit dan maksimum 256 bit. AES menggunakan matriks 4 × 4 dengan urutan bita sesuai kolom-lalu-baris (ke bawah, lalu ke kanan). Matriks ini disebut "status" (state).

3. **Struktur Advanced Encryption Standard**

   Advanced Encryption Standard menyusun dan membangun blok yang didesain berdasarkan sebuah standar yang diketahui sebagai substitution-transformation diatur dengan ukuran blok 128 bits, dan sebuah kunci berukuran 128, 192, atau 256 bits dan memiliki kecepatan yang tinggi dalam software dan hardware. setiap operasi memiliki 4 kesamaan tetapi stage yang berbeda, termasuk yang bergantung pada kunci enkripsi itu sendiri. Setiap stage itu adalah ByteSub, ShiftRows, MixColumn and addRoundKey

4. **Proses Data**

   Pesan tersebut apabila ingin dibaca maka terlebih dahulu pesan tersebut dekripsi menggunakan algoritma metode AES sehingga menghasilkan pesan asli

5. **Aplikasi Chatting**

   Suatu fasilitas dalam internet untuk berkomunikasi sesama pengguna internet yang sedang online. Komunikasi dapat berupa teks

6. **Android**

   Sistem operasi menggunakan masukan sentuhan untuk memanipulasi objek pada layar, dan sebuah keyboard virtual yang didukung oleh berbagai alat pengembangan pihak ketiga.

7. **Kotlin**

   Sebuah bahasa pemrograman pengetikan statis yang berjalan pada Java Virtual Machine dan juga dapat dikompilasikan dalam bentuk kode sumber Javascript atau menggunakan infrastruktur kompilasi LLVM

8. **Cloud Computing**

   Bentuk teknologi informasi yang digunakan pada bidang jaringan komputer atau internet. dalam cloud computing ada tiga layanan yang disediakan antara lain (SaaS) Software as a Service, (PaaS) Platform as a Service, dan (IaaS) Infrastructure as a Service.

❖ **Hasil penelitian pada jurnal tersebut dan kesimpulannya**

Kesimpulan dan hasil penelitian pada implementasi algoritma AES pada aplikasi chatting berbasis android ini bahwa pada pengimplementasiannya pada sebuah aplikasi chatting ini diperlukannya pesan kunci yang dimana kunci ini harus diketahui oleh si penerima untuk melakukan sebuah dekripsi pesan yang dimana pesan yang disimpan dalam firebase realtime database ini adalah berbentuk heksadesimal karena pada algoritma AES membutuhkan pesan dan kunci diubah kedalam bentuk heksadesimal

❖ **Kelebihan dan kekurangan masing-masing jurnal**

- **Kelebihan**
  - Memberikan percontohan dari aplikasi yang ingin dikembangkan, sehingga pembaca dapat memiliki bayangan yang lebih jelas tentang aplikasi yang ingin dikembangkan.

- **Kekurangan**
  - Tidak menjabarkan secara detail dari desain sistem yang akan dibuat, sehingga pembaca tidak dapat memahami desain sistem persebut secara menyeluruh seperti yang dimaksudkan oleh penelitinya. Dari aplikasi chatting ini key harus terlebih dahulu diketahui oleh penerima terlebih dahulu agar dapat melakukan dekripsi. Sehingga jika kita menggunakan kunci lain maka harus memberikan kunci terlebih dahulu.

JURNAL 2

❖ **Implementasi Kriptografi Dengan Algoritma Advanced Encryption Standard (AES) 128 Bit Dan Steganografi Menggunakan Metode End Of File (EOF) Berbasis Java Desktop Pada Dinas Pendidikan Kabupaten Tangerang**

❖ **Latar Belakang**

Seiring dengan perkembangan dunia digital saat ini membuat lalu lintas pengiriman data elektronik semakin ramai dan sensitif. Dengan adanya perkembangan tersebut, kejahatan teknologi komunikasi dan informasi juga turut berkembang. Dengan adanya pencurian data maka aspek keamanan dalam pertukaran informasi serta penyimpanan data dianggap penting, karena suatu komunikasi data jarak jauh, belum tentu memiliki jalur transmisi yang aman dari penyadapan, serta penyimpanan data belum tentu aman dari pencurian sehingga keamanan informasi menjadi bagian penting dalam dunia informasi. Keamanan data di Dinas Pendidikan Kabupaten Tangerang selama ini, hanya melakukan pengamanan data secara sederhana dan tidak terlalu memperhatikan tingkat keamanan. Padahal sebuah instansi pemerintah yang pasti memiliki banyak data yang tidak boleh diketahui oleh masyarakat umum. Seperti contohnya data Instrumen Seleksi Calon Kepala Sekolah dan Pengawas, Hasil seleksi yang belum waktunya diumumkan, SPJ (Surat Pertanggung Jawaban) keuangan yang belum diperiksa oleh pemeriksa internal dan eksternal, dan masih banyak lagi data yang bersifat rahasia lainnya. Dengan demikian aplikasi keamanan terhadap data atau file sangat diperlukan untuk menghindari tindakan-tindakan tertentu yang dapat merugikan. Sehingga perlu dilakukan pengamanan data dengan menggunakan metode Advanced Encryption Standard (AES) 128 bit.

❖ **Tujuan Penelitian**

Tujuan dari penelitian ini adalah mengimplementasikan algoritma kriptografi advanced encryption standard (AES) dan juga metode steganografi End Of File (EOF) untuk mengamankan sebuah file atau informasi dengan membuat sebuah aplikasi pengamanan data berbasis desktop yang dimana hal ini menghasilkan proses enkripsi dan dekripsi data dan juga penyisipan data secara optimal tanpa adanya data yang rusak pada proses ini. Hasil datanya inipun berupa gambar

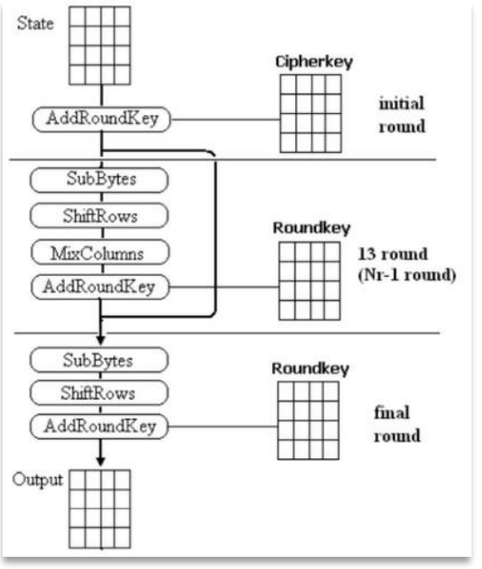
❖ **Algoritma yang dipakai beserta alur penelitiannya**

A. Kriptografi Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai plaintext (teks biasa). Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja

B. Algoritma AES (Advanced Encryption Standard) Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi ciphertext. Cipher key dari AES terdiri dari key dengan panjang 128bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah round yang akan diimplementasikan pada algoritma AES ini.

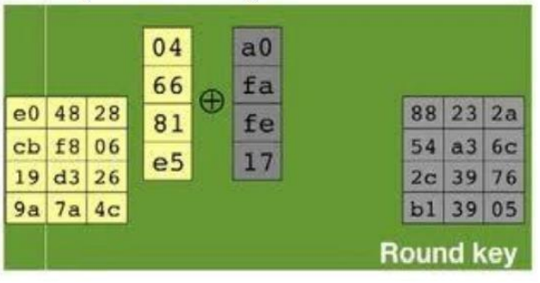
a) Proses Enkripsi AES

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dicopykan ke dalam state akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai round function. Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns. Berikut ilustrasi AES 256 Bit:



1) Add Round Key

Pada proses enkripsi dan dekripsi AES proses AddRoundKey sama, sebuah round key ditambahkan pada state dengan operasi XOR. Setiap round key terdiri dari Nb word dimana tiap word tersebut akan dijumlahkan dengan word atau kolom yang bersesuaian dari state. Transformasi AddRoundKey pada proses enkripsi pertama kali pada round = 0 untuk round selanjutnya round = round + 1, pada proses dekripsi pertama kali pada round = 14 untuk round selanjutnya round = round - 1. Pada gambar dibawah ini yang sebelah kiri adalah ciphertext dan sebelah kanan adalah roundkeynya. XOR dilakukan perkolom yaitu kolom-1 ciphertext di XOR dengan kolom-1 roundkey dan seterusnya.

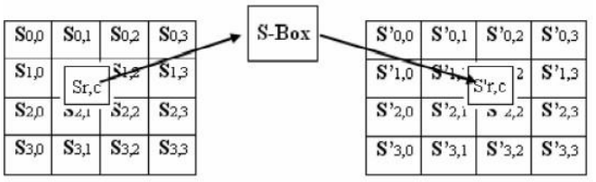


2) Sub Bytes

SubBytes merupakan transformasi byte dimana setiap elemen pada state akan dipetakan dengan menggunakan sebuah tabel subtitusi (S-Box). Tabel subtitusi S-Box akan dipaparkan dalam tabel dibawah.

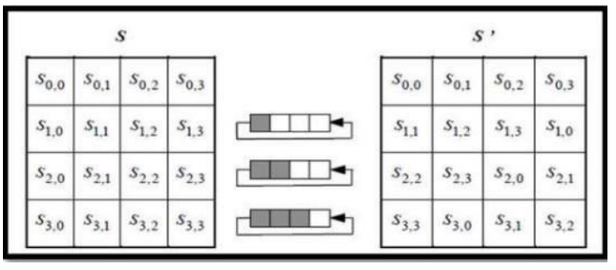
	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Untuk setiap byte pada array state, misalkan S[r,c]=xy, yang dalam hal ini xy adalah digit heksadesimal dari nilai S[r,c], maka nilai subtitusinya, dinyatakan dengan S[r,c], adalah elemen didalam tabel subtitusi yang merupakan pengaruh pemetaan byte pada setiap byte dan state. Pengaruh Pemetaan pada setiap byte dalam state:



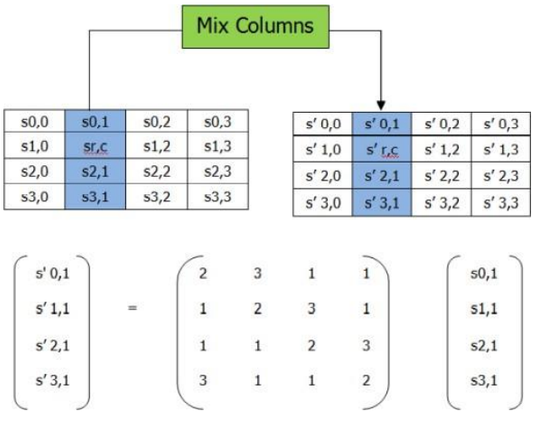
3) ShiftRows

Transformasi Shiftrows pada dasarnya adalah proses pergeseran bit dimana bit paling kiri akan dipindahkan menjadi bit paling kanan (rotasi bit). Proses pergeseran Shiftrow ditunjukkan dalam gambar berikut:



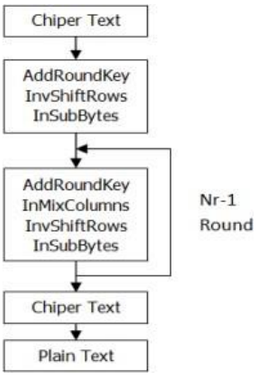
4) Mix Columns

MixColumn adalah mengalikan tiap elemen dari blokcipher dengan matriks oleh table yang sudah ditentukan dan siap dipakai. Pengalian dilakukan dengan perkalian matriks biasa yaitu menggunakan dot product lalu perkalian keduanya dimasukkan ke dalam sebuah blokcipher baru, berikut perkaliannya:



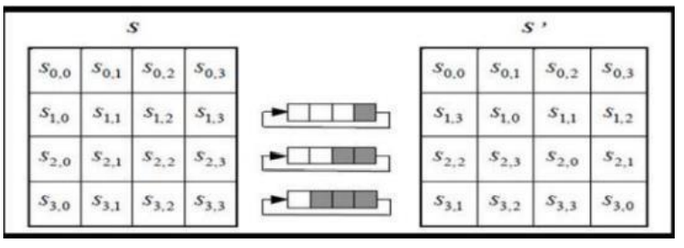
b) Proses Dekripsi AES

Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Algoritma dekripsi dapat dilihat pada skema berikut ini :



1) InvShiftRows

InvShiftRows adalah transformasi byte yang berkebalikan dengan transformasi ShiftRows. Pada transformasi InvShiftRows, dilakukan pergeseran bit ke kanan sedangkan pada ShiftRows dilakukan pergeseran bit ke kiri.



2) InvSubBytes

InvSubBytes juga merupakan transformasi bytes yang berkebalikan dengan transformasi SubBytes. Pada InvSubBytes, tiap elemen pada state dipetakan dengan menggunakan tabel Inverse S-Box. Tabel Inverse S-Box akan ditunjukkan dalam tabel berikut:

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	f
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	c
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	2
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	9
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	8
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	0
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	7
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	e
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	6
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7

3) InvMixColumns

Setiap kolom dalam state dikalikan dengan matrik perkalian dalam AES.

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

C. Steganografi

Steganografi (steganography) adalah ilmu dan seni menyembunyikan pesan rahasia(hiding message) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Sebuah pesan steganografi (plaintext), dienkripsikan dengan beberapa arti tradisional, yang menghasilkan ciphertext.

Kemudian, covertext dimodifikasi dalam beberapa cara sehingga berisi ciphertext, yang menghasilkan stegotext. Contohnya: ukuran huruf, ukuran spasi, jenis huruf, atau karakteristik covertext lainnya dapat dimanipulasi untuk membawa pesan tersembunyi. Hanya penerima yang mengetahui tekniknya yang dapat membuka pesan dan mendekripsikannya. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video

D. Metode End Of File (EOF)

Dalam metode ini pesan disisipkan diakhir berkas. Pesan yang disisipkan dengan metode ini jumlahnya tidak terbatas. Kekurangannya adalah ukuran berkas menjadi lebih besar dari ukuran semula. Ukuran berkas yang terlalu besar dari yang seharusnya, tentu akan menimbulkan kecurigaan bagi yang mengetahuinya.

❖ **Hasil penelitian pada jurnal tersebut dan kesimpulannya**

Hasil penelitian dan kesimpulan pada jurnal ini adalah proses penyimpanan dan pertukaran informasi yang terjadi ini menjadi lebih aman, kemudian tindakan pembobolan file yang terenkripsi akan berkurang karena adanya keamanan atau security ganda yang menggunakan steganografi. Selanjutnya tindakan penyalahgunaan data ini tidak akan terjadi. Selanjutnya proses dekripsi dengan dengan kunci yang asli akan mengembalikan file menjadi file semula tanpa adanya perubahan. Waktu yang digunakan dalam proses enkripsi dan dekripsi ini berbanding lurus dengan ukuran file yang di proses dan yang terakhir proses penyisipan file dan media covernya ini sangat cepat sehingga tidak memakan waktu yang lama

❖ **Kelebihan dan kekurangan masing-masing jurnal**

- **Kelebihan**
  - Menjabarkan proses enkripsi dan dekripsi AES secara lengkap
  - Pada bagian kesimpulan ini dijabarkan juga apa saja yang didapat dari proses pengimplementasiannya
  - Pesan tidak terdeteksi oleh indera manusia karena data dimarkan, sehingga sulit dideteksi dan sangat melidungi terhadap data tersebut

- **Kekurangan**
  - Tidak memberikan bagaimana contoh halaman atau contoh dari memasukkan file pada web untuk melakukan enkripsi dokumen tersebut, sehingga pembaca tidak memiliki bayangan cara file tersebut diproses di dalam website enkripsi tersebut.
  - Ukuran file menjadi lebih besar dari aslinya