

## **Implementasi Algoritma Kriptografi AES (*Advanced Encryption Standard*) 128 Bit Untuk Pengamanan Dokumen Shipping**

**Rivian Nuari <sup>1</sup>, Niki Ratama <sup>2</sup>**

<sup>1</sup>Jurusan Teknik Informatika, Fakultas Teknik, Universitas Pamulang, Jl. Surya Kencana No. 1, Pamulang – Tangerang Selatan, 15417,

Indonesiae-mail:

<sup>1</sup>[rivian3221@gmail.com](mailto:rivian3221@gmail.com)

### **Abstract**

In the shipping document data storage is stored just like that without any special safeguards. to overcome the problem above, we need a way to secure the data with a fast time, so it is not misused. The researcher's goal is to use a description-encryption technique with the 128-bit AES algorithm into a system because it has a level of resistance to all types of attacks to avoid loss and theft and reduce the risk of damage to data / files. The process of encrypting and describing document files using the AES 128 bit (*Advanced Encryption Standard*) algorithm. In data / files, the encryption process (1 block) of plaintext is first converted to ASCII code in hexadecimal numbers and formed as a 4x4 byte matrix called state. The encryption process in AES 128 is a transformation of the state repeatedly in 10 rounds. Data processed in each round is binary data. Each AES round requires one key generation key result and uses 4 basic transformations namely subbytes, shiftrows, mixcolumns, and addroundkey. Whereas the decryption process has transformations in the order of invshiftrows, invsubbytes, addroundkey, and invmixcolumns. In document files that have been confirmed to have a number of characters more than 16 characters the encryption and decryption process will be performed every 128 bits or 16 characters. So that the AES encryption and decryption process is done in parallel. Whereas for text files with less than 16 characters, padding will be performed. Padding is the use of null ASCII characters to fill in the number of characters that are lacking in order to be processed and will not affect the results of encryption or decryption.

**Keywords:** AES (*Advanced Cryption Standard*) Crittography Algorithm 128 bits, SDLC

### **1. Pendahuluan**

Dokumen merupakan file atau data yang sangat penting karena sumber informasi yang diperlukan oleh suatu perusahaan. Tanpa dokumen perusahaan akan kehilangan data yang diperlukan untuk kegiatan dimasa mendatang. Pada penyimpanan data dokumen shipping di simpan begitu saja tanpa ada pengamanan khusus. Dengan adanya dampak negatif dari perkembangan teknologi maka keamanan data dalam penyimpanan file atau data menjadi sangat penting. Belum tentu dalam penyimpanan data dapat lebih aman dari pencurian file atau data, sehingga keamanan informasi atau data menjadi bagian penting dalam perkembangan teknologi. Untuk mengatasi masalah diatas maka diperlukan cara untuk mengamankan data tersebut agar data tersebut tidak disalah gunakan. Dengan

menggunakan teknik kriptografi/enkripsi. Kriptografi adalah ilmu matematika yang sangat berhubungan dengan transformasi data artinya tidak bisa dipahami. mencegahnya dari perubahan tanpa izin, atau tidak sah. kriptografi juga bisa

diartikan sebagai proses untuk mengamankan data dalam mengubah data yang sebelumnya tidak bisa di pahami dan dapat dipahami kembali dengan datayang terenkripsi. kriptografi (encryption/decryption) yang akan proses untuk men-enkripsi data dokumen shipping pada masalah diatas adalah dengan menggunakan metode AES (Advanced Encryption Standard). Dimana metode AES adalah algoritma chipher blok menggunakan teknik substitusi, pemutasian dan sejumlah putaran pada setiap blok yang akan di enkripsi dan deskripsi.

Dipilihnya algoritma AES (Advanced Encryption Standard) karena dirancang khusus untuk keamanan tingkat tinggi serta ketahanan terhadap berbagai jenis serangan, bahkan kesederhanaan rancangan, kekompakan kode dan kecepatan men- enkripsi dan deskripsi setiap file atau data.

Metode perancangan dan pembangunan aplikasi ini merupakan metode SDLC. Metode SDLC adalah metode pengembangan sistem dimana memberikan sebuah model pengembangan

yang meliputi perencanaan permodelan, pembangunan dan penyebaran.

## 2. Penelitian Terkait

Adapun peneliti terkait menggunakan kriptografi AES 128 bit untuk mengamankan shipping dokumen. Dalam penulisan, peneliti menggunakan referensi tinjauan pustaka yang berhubungan dengan kegiatan ini. Referensi yang digunakan sebagai sumber informasi peneliti ini didapat dari materi kuliah, jurnal, beberapa penulisan dan karya ilmiah yang berkaitan dengan pembahasan pada penelitian ini adalah "Implementasi Algoritma Kriptografi AES (Advance encryption standard) 128 bit untuk pengamanan dokumen shipping". Adapun referensi atau jurnal pendukung sebagai berikut :

Penelitian ini dilakukan oleh Fricles Ariswisanto sianturi (STMIK Budi darma Medan, 2013) yang berjudul **"Perancangan Aplikasi Pengamanan Data Dengan Kriptografi Advanced Encrription Standart (AES"**, yang membahas tentang pengamanan berkas teks menggunakan metode kriptografi AES dengan tujuan mempermudah dalam mengeonglah data baik admin ataupun penggunaanya ( *ISSN : 2303- 0755 Vol. 4 NO. 3 juli 2013*).

Penelitian ini dilakukan oleh Vina Noviatnty (Sekolah Tinggi Teknologi Garut, 2015) yang berjudul **"Mengamankan Basis Data Keuaangan Koperasi Dengan Menggunakan Kriptografi Advanced Encrription Standart"** yang membahas pengamanan Basis Data Keuangan Koperasi Dengan Menggunakan Kriptografi Advance Encrription Standart ,Dengan tujuan untuk pengamanan file dan berkas-berkas keuangan dalam basis data koperasi. (*ISSN : 2302-7339 Vol. 12 No.1 2015*).

Penelitian ini dilakukan oleh Aditia Rahmat Tulloh (Universitas Islam Bandung ,2016). Yang berjudul **"Kriptografi Advanced Encrription Standard (AES) Untuk Penyandian File Dokumen"** yang membahas tentang bagaimana proses penyandian dengan Advanced Encrription Standard (AES)?, dengan tujuan merancang dan menggunakan program pengamanan data teks metode kriptografi AES dengan menggunakan Graphical User Interface (GUI) MATLAB. (*ISSN : 1412-5050 Vol.15 No.1 Mei 2016*).

## 3. Metode Penelitian

Metodologi yang digunakan adalah metode penelitian studi literatur pada buku-buku dan sumber-sumber lain yang relevandengan topik penulisan, yaitu buku-buku serta jurnal referensi

dan sumber-sumber lain yang terdapat pada daftar pustaka.

a. Pengumpulan Data

Pengumpulan data diambil dari sumber buku dan jurnal serta sumber-sumber lain yang tercantum pada daftar pustaka

b. Wawancara

Melakukan proses wawancara untuk mengetahui permasalahan yang sedang dialami serta dibutuhkan oleh PT. Lion Air untuk dapat menunjang keamanan dokumen shipping

c. Analisa sistem berjalan

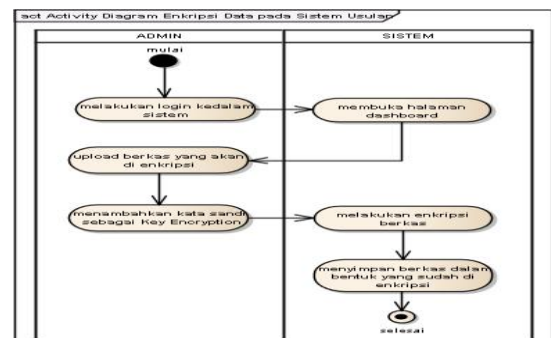
- Staf menghandel dan mengirim dokumen melalui pesawat dan di catat no shipping nya di report shift.
- Setiap dokumen di cek kembali di ruangan di sesuaikan dengan catatan repot shift.
- Setelah sudah cocok dokumen di data kembali di komputer.
- Dokumen di data dengan lengkap (flight number ,no shipping , nama pengirim ,alamat pengirim, penerima, alamat penerima, waktu ,dan isi dokumen ) di power point. Setelah selesai dokumen di simpan di folder yang sudah di buat.

d. Analisa sistem usulan

- Berkas yang tersimpan akan di enkripsi oleh sistem dengan metode AES 128 bit
- Ekstensi berkas akan diubah menjadi .rda
- Berkas tidak dapat diunduh setelah di enkripsi ke dalam sistem jika berkas belum di deskripsi kembali
- Berkas tidak dapat dibaca walaupun admin mengambil berkas tersebut dari *root system* ataupun merubah ekstensinya secara manual
- User yang dapat mengakses aplikasi ini ada 1 (satu) yaitu admin

Di bawah ini adalah gambaran sistem usulan yang akan kita implementasikan pada proses enkripsi data yang akan diterapkan di PT Lion Air Indonesia:

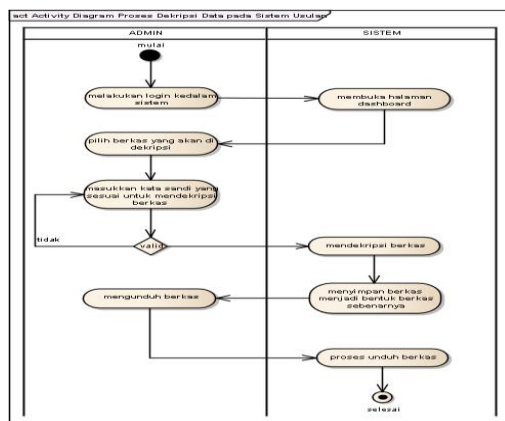
a. Sistem Usulan Proses Enkripsi Berkas



Keterangan :

Gambar diatas menjelaskan aktivitas diagram proses enkripsi berkas pada aplikasi yang akan dibuat. Dimulai oleh admin yang melakukan login kepada aplikasi, lalu admin akan melakukan *upload* berkas ke dalam sistem dan menambahkan kata sandi sebagai *key encryption*. Lalu sistem akan merubah berkas kedalam bentuk enkripsi dengan metode *encryption* AES 128 Bit dan merubah ekstensi berkas menjadi .rda.

#### b. Sistem Usulan Proses Dekripsi Berkas



**Gambar 3.1 Sistem Usulan Dekripsi Berkas**

Keterangan:

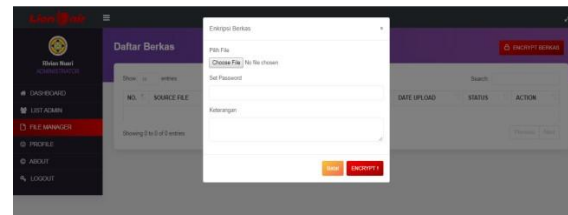
Gambar diatas menjelaskan aktivitas diagram proses Deskripsi berkas pada aplikasi yang akan dibuat. Dimulai oleh admin yang melakukan login kepada aplikasi, lalu admin memilih berkas yang akan di deskripsi dan memasukkan kata sandi yang sesuai. Jika kata sandi salah maka sistem akan menampilkan pesan kesalahan, jika kata sandi benar, maka sistem akan melakukan proses deskripsi pada berkas dan merubah ekstensi .rda ke dalam ekstensi yang sebenarnya. Setelah berkas berhasil di deskripsi, maka admin dapat mengunduh berkas tersebut dari sistem dan menyimpannya pada komputer lokal.

#### 4. Hasil Dan Pembahasan

Dari hasil penelitian di hasilkan dan pembahasan nya adalah sebagai berikut :

##### A. Hasil tampilan dan pembahasan

##### a. Tampilan Enkripsi Berkas

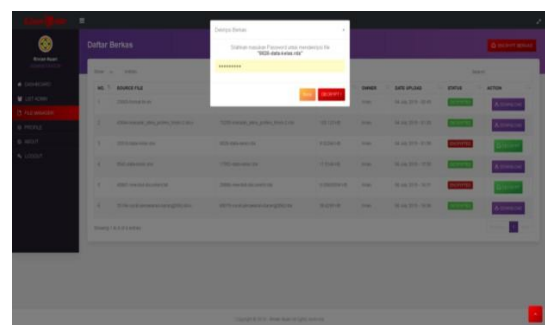


**Gambar 3 Tampilan Enkripsi Berkas**

Gambar di atas adalah tampilan enkripsi berkas, pengguna atau admin menekan tombol encrypt berkas setelah itu pilih file atau dokumen yang pengguna ingin

enkripsi, masukan password atau key, isi keterangan dan tekan tombol Encrypt. Dokumen atau file berhasil di enkripsi. Jika file tidak mendukung contohnya file gambar maka enkripsi gagal. Karena aplikasi ini hanya bisa mengenkripsi file seperti doc, docx, pdf, ppt, pptx, txt, xls, xlsx.

##### b. Tampilan Dekripsi Berkas



**Gambar 4 Tampilan Dekripsi Berkas**

Gambar di atas adalah tampilan deskripsi berkas, penggunaan atau admin bisa langsung mendeskripsi berkas yang sudah di enkripsi sebelumnya, tekan tombol deskripsi dan masukan password sesuai pada saat pengguna mengenkripsi berkas jika password valid maka deskripsi berkas akan berhasil dan jika tidak pengguna harus memasukkan ulang password dengan benar.

**a) Enkripsi**

- a. Pengujian men-enkripsi file doc,docx, pdf, ppt,pptx, txt, xls, xlsx.

**Tabel 1. men-enkripsi file doc,docx, pdf,ppt,pptx, txt, xls, xlsx**

Skenario pengujian	Hasil pengujian
Langkah yang dilakukan	Pilih file manager , tekan tombol encrypt, pilih file ,masukan password dan keterangan, lalu tekan tombol

Pengamatan	encrypt. Sistem memproses file doc, docx, pdf, ppt, pptx, txt, xls, xlsx.
Kesimpulan	Sukses

b. Hasil enkripsi file docx

**Tabel 2. Hasil enkripsi file docx**

Skenario pengujian	Hasil pengujian
Langkah yang dilakukan	Pilih file manajer, tekan tombol encrypt, pilih file, masukan password dan keterangan, lalu tekan tombol encrypt.
Pengamatan	Bila dibuka dengan Notepad, maka isi, Docx yang sudah dienkripsi, seperti terlihat pada Gambar.
Kesimpulan	Sukses

c. Hasil enkripsi file ppt.

**Tabel 3. Hasil enkripsi file ppt**

Skenario pengujian	Hasil pengujian
Langkah yang dilakukan	Pilih file manajer, tekan tombol encrypt, pilih file, masukan password dan keterangan, lalu tekan tombol encrypt.
Pengamatan	Bila dibuka dengan Notepad, maka isi ppt. yang sudah dienkripsi, seperti terlihat pada Gambar

Kesimpulan	Sukses
------------	--------

d. Hasil enkripsi file xlsx.

**Tabel 4. Hasil enkripsi file xlsx**

Skenario pengujian	Hasil pengujian
Langkah yang dilakukan	Tekan tombol deskripsi pada dokumen yang sudah di encrypt, masukan password sesuai ketika men-encrypt berkas sebelum nya.
Pengamatan	Bila dibuka dengan Notepad, maka perbedaan isi xlsx. yang sudah dienkripsi, seperti terlihat pada Gambar.
Kesimpulan	Sukses

e. Hasil enkripsi file pdf

**Tabel 5. Hasil enkripsi file pdf**

Skenario pengujian	Hasil pengujian
Langkah yang dilakukan	Tekan tombol deskripsi pada dokumen yang sudah di encrypt, masukan password sesuai ketika men-encrypt berkas sebelum nya.
Pengamatan	Bila dibuka dengan Notepad, maka isi pdf. yang sudah dienkripsi, seperti terlihat pada Gambar.



<p>Kesimpulan</p>	<p>Sukses</p>
-------------------	---------------

f. Hasil enkripsi file text.

Tabel 6. Hasil enkripsi file text

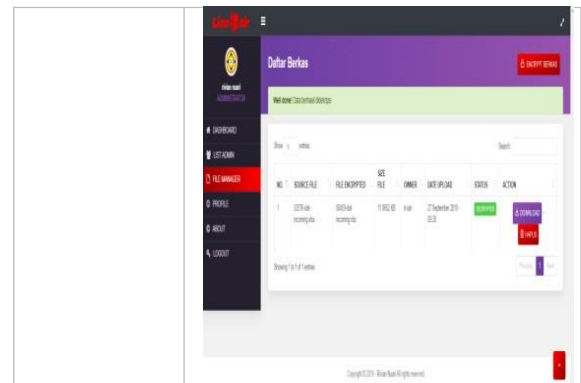
Skenario pengujian	Hasil pengujian
Langkah yang dilakukan	Tekan tombol deskripsi pada dokumen yang sudah di encrypt, masukan password sesuai ketika men-enkripsi berkas sebelum nya .
Pengamatan	Bila dibuka dengan Notepad, maka isi text. yang sudah dienkripsi, seperti terlihat pada Gambar.
Kesimpulan	Sukses

## b) Pengujian Deskripsi

a. Pengujian men-deskripsi berkas.

Tabel 7. Pengujian men-deskripsi

Skenario pengujian	Hasil pengujian
Langkah yang dilakukan	Tekan tombol deskripsi pada dokumen yang sudah di encrypt, masukan password sesuai ketika men-enkripsi berkas sebelum nya .
Langkah yang dilakukan	System memproses deskripsi berkas dengan memberi keterangan weel done!data berhasil deskripsi .
Kesimpulan	Sukses



Kesimpulan	Sukses
Pengamatan	System memproses deskripsi
	berkas file doc,docx, pdf,
	ppt,pptx, txt, xls, xlsx,dengan
	membri keterangan weel
	done!data berhasil deskripsi .
Kesimpulan	Sukses

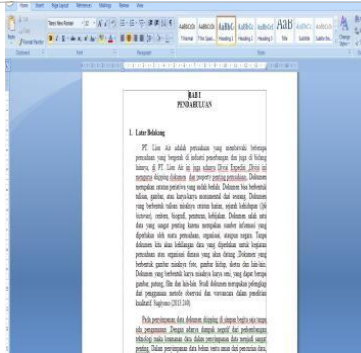
c. Tampilan hasil dekripsi file docx.

Tabel 4.9.Tampilan hasil dekripsi file docx


Skenario pengujian	Hasil pengujian
--------------------	-----------------



Langkah yang dilakuka n	Tekan tombol deskripsi ,dan masukan password salah
Pengamatan	memperlihatkan tampilan <i>file</i> docx yang telah di deskripsi


	
Kesimpulan	Sukses

d. Tampilan hasil deskripsi file pdf.  
**Tabel 10. Tampilan hasil deskripsi file pdf**


Skenario pengujian	Hasil pengujian
Langkah yang dilakukan	Tekan tombol deskripsi ,dan masukan password salah
Pengamatan	memperlihatkan tampilan file pdf yang telah di deskripsi
	
Kesimpulan	Sukses

e. Tampilan hasil deskripsi file xlsx.  
**Tabel 11. Tampilan hasil dekripsi file**


Skenario pengujian	Hasil pengujian
Langkah yang dilakukan	Tekan tombol deskripsi ,dan masukan password salah
Pengamatan	memperlihatkan tampilan file xlsx yang telah di deskripsi

	
Kesimpulan	Sukses

f. Tampilan hasil deskripsi file text.  
**Tabel 12. Tampilan hasil deskripsi file text.**

Skenario pengujian	Hasil pengujian
Langkah yang dilakukan	Tekan tombol deskripsi ,dan masukan password salah
Pengamatan	memperlihatkan tampilan file txt yang telah di deskripsi
	
Kesimpulan	Sukses

g. Tampilan hasil deskripsi file ppt.  
**Tabel 13. Tampilan hasil deskripsi file ppt.**

Skenario pengujian	Hasil pengujian
Langkah yang dilakukan	Tekan tombol deskripsi ,dan masukan password salah
Pengamatan	memperlihatkan tampilan file ppt yang telah di deskripsi
	
Kesimpulan	Sukses

### C. Hasil Kuisisioner

Tabel 14 Pengujian Tampilan dengan Kuisisioner

Tampilan						
Pernyataan	SS	S	CS	ST	STS	Frekuensi
Pertanyaan 1	14	4	2	0	0	30
Pertanyaan 2	11	13	6	0	0	30
Pertanyaan 3	10	12	8	0	0	30
Pertanyaan 4	7	20	3	0	0	30
Pertanyaan 5	11	18	1	0	0	30
Pertanyaan 6	13	11	6	0	0	30
Total	66	78	26	0	0	180
Persentasi	39%	46%	15%	0%	0%	100%

Tabel 15 Pengujian Kemudahan Pengoperasian dengan kuisisioner

Tampilan						
Pernyataan	SS	S	CS	ST	STS	Frekuensi
Pertanyaan 1	18	11	1	0	0	30
Pertanyaan 2	13	16	1	0	0	30
Pertanyaan 3	19	11	0	0	0	30
Pertanyaan 4	12	15	3	0	0	30
Pertanyaan 5	18	12	0	0	0	30
Pertanyaan 6	3	23	4	0	0	30
Total	83	88	9	0	0	180
Persentasi	46%	49%	5%	0%	0%	100%

Tabel 16. Pengujian Efektivitas dengan Kuesioner

Tampilan						
Pernyataan	SS	S	CS	ST	STS	Frekuensi
Pertanyaan 1	14	11	5	0	0	30
Pertanyaan 2	14	15	1	0	0	30
Pertanyaan 3	6	15	9	0	0	30
Total	34	41	15	0	0	90
Persentasi	38%	45%	17%	0%	0%	100%

Tabel 17. Pengujian Efisiensi dengan kuisisioner

Tampilan						
Pernyataan	SS	S	CS	ST	STS	Frekuensi
Pertanyaan 1	15	14	1	0	0	30
Pertanyaan 2	9	14	7	0	0	30
Pertanyaan 3	9	13	8	0	0	30
Total	33	41	16	0	0	90
Persentasi	37%	45%	18%	0%	0%	100%

Tabel 18. Pengujian kepuasan

Tampilan						
Pernyataan	SS	S	CS	ST	STS	Frekuensi
Pertanyaan 1	16	12	2	0	0	30
Pertanyaan 2	12	13	5	0	0	30
Pertanyaan 3	11	18	1	0	0	30
Total	39	43	8	0	0	90
Persentasi	43%	48%	9%	0%	0%	100%

### 5. Kesimpulan

Dari hasil studi pustaka, merancang aplikasi pengimplementasian dan pengujian memperoleh poin poin untuk menjawab masalah- masalah yang ada pada PT.Lion (ekspedisi shipping dokumen) , berikut adalah kesimpulan dari peneliti yang peneliti lakukan.

- Untuk meningkatkan dan memaksimalkan dalam mengamankan data ,peneliti merancang dan membangun sebuah perancangan aplikasi pengamanan data menggunakan algoritma kriptografi AES (ADVANCED ENCRPTION STANDART) 128 bit berbasis web dengan metode SDLC. Aplikasi ini dapat diakses melalui web dan tentunya pengguna harus terdaftar dulu menjadi admin.
- Untuk mengurangi resiko kehilangan dan kerusakan data , setelah adanya aplikasi data akan lebih terhindar dari resiko-resiko kehilangan dan kerusakan data .Hal ini di perkuat dari hasil pengumpulan data menggunakan dengan kuesioner dengan 30 responden diperoleh data sebagai berikut :
- Kecepatan waktu ketika melakukan proses enkripsi dan deskripsi tergantung besar kecilnya file yang akan diproses ,semakin kecil file yang akan diproses maka kecepatan waktunya semakin cepat sebaliknya semakin besar file , maka kecepatan waktunya akan lebih lama.

### DAFTAR PUSTAKA

- Achmad, Solihin (2016). *Pemrograman Web Dengan PHP dan MySQL*. Jakarta :Universitas Budi Luhur.
- Aditia Rahmat Tulloh (,2016). *Kriptografi Advanced Enciption Standard (AES) Untuk Penyandian File Dokumen*,Bandung :Universitas Islam.
- Angga Aditya Permana (2018).*Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Enciption Standard (AES)* Tangerang :UniversitasMuhamadyah
- Andi, Sunyoto. (2007). *AJAX Membangun Web Dengan Teknologi Asynchrone Javascript & XML*.Yogyakarta :Andi
- AndriKristanto. (2018). *Perancangan Sistem Informasi dan Aplikasinya*.Yogyakarta : GAVA Media
- Anhar .(2010). *Panduan Menguasai PHP & MySQL*



- Al-Bahra bin Ladjamudin. (2005). *Analisis dan Desain Sistem Informasi*. Yogyakarta :Graha Ilmu.
- Arjana, P.H. et al. (2012). *Implementasi Enkripsi Data dengan Algoritma Vigenere Chiper*. Sentika, (ISSN: 2089-9815).
- Budi, Kurniawan. (2008). *Desain Web Praktis Dengan CSS*. Jakarta : PT. Elex Media Komputindo.
- Connolly, T., Begg, C. (2010). *Database System : a practical approach to design, implementation, and management*. 5<sup>th</sup> Edition. America: Pearson Education.
- Elisabeth, Yunaeti & Rita, Irvani. (2017). *Pengantar Sistem Informasi*. Yogyakarta : Andi.
- Hans, Limantara. (2009). *Jelajah Dunia Maya Dengan Cepat dan Mudah*. Jakarta : PT. Elex Media Komputindo.
- Jubilee, Enterprise. (2014). *MySQL Untuk Pemula*. Jakarta : PT Elex Media Komputindo.
- Luminita Defta (2010). Yang berjudul. *AES Algorithm Implementation In Programming Languages* University Of Pitesti, ISSN : 1596-2490
- Mazmanian dan Sabatier (2013). *Implementasi Teknik Informatika*. Surabaya.
- Muhammad Taufiqur Rahman (2017). *Perbandingan Performansi Algoritma Kriptografi Advanced Encryption Standard (AES) Dan Blowfish Pada Teks di Platform Android*. Universitas Brawijaya ISSN : 2548-964
- Marwah K. Hussein, (2017). *Encryption of Stereo Image After Compression by Advanced Encryption Standard (AES)*. Iraq : University of Basrah.
- Pressman, R.S. (2010). *Rekayasa Perangkat Lunak : Pendekatan Praktisi Buku 1*. Yogyakarta : Andi.
- Pressman, R.S. (2010). *Software Engineering : a practitioner's approach*, McGraw – Hill, New York.
- Ridwan S., Onno W. (2002). *Membuat Aplikasi W@P Dengan PHP*. Jakarta : PT. Elex Media Komputindo
- Sri Mulyani. (2016). *Metode Analisis dan Perancangan Sistem*. Bandung: Abdi Sistematika
- Sianturi, F.A., (2013). *Perancangan Aplikasi Pengamanan Data Dengan Kriptografi Advanced Encryption Standard ( AES )*. , (ISSN: 2301-9425)
- Sitinjak, S. & Fauziah, Y., 2010. *Aplikasi Kriptografi File Menggunakan Algoritma Blowfish*. , 2010 (ISSN: 1979-2328), pp.78–86.
- Sugiyono (2013). *Apa itu Dokumen Dan Dasar Dokumen*. Yogyakarta .
- Vina Noviatnity (2015) *Mengamankan Basis Data Keuangan Koperasi Dengan Menggunakan Kriptografi Advanced Encryption Standard*. Garut : Sekolah Tinggi Teknologi.
- Oppliger, ( 2005). *Ilmu Matematika Tentang Kriptografi (encryption/decryption) AES (Advanced Encryption Standard)* . Bandung.
- Wardana. (2016). *Aplikasi Website Profesional dengan PHP dan JQuery*. Jakarta : PT. Elex Media Komputindo.
- Winarno, A. et al., (2012). *Polynomial Functions dan Implementasinya dalam Algoritma AES pada Database Accounting*. Yogyakarta.
- Yuhafizar. (2008). *10 Jam Menguasai Internet : Teknologi dan Aplikasinya*. Jakarta : PT. Elex Media Komputindo.