APLIKASI KRIFTOGRAFI UNTUK KEAMANAN DATA AUDIT MENGGUNAKAN METODE RIJNDAEL PADA PT. SERBA MULIA AUTO

M.Irwan Ukkas [1)], Asep Nurhuda [2)], Jeri Yules[3)]

[1]Sistem Informasi, STMIK Widya Cipta Dharma
[2]Sistem Informasi, STMIK Widya Cipta Dharma
[3]Sistem Informasi, STMIK Widya Cipta Dharma
[1,2,3]Jl. M. Yamin No.25, Samarinda, 75123
E-mail : Irwan212@yahoo.com [1)], [2)], efraimjerry@gmail.com[3)]

ABSTRAK

Penerapan Metode *Rijndael* pada Enkripsi dan Dekripsi Data Audit dengan Menggunakan Metode *Rijndael*, merupakan bentuk penelitian untuk membuktikan bahwa algoritma *Rijndael* dapat digunakan untuk pencarian solusi, khususnya pada permasalahan keamanan data.

Penelitian ini dilakukan pada PT. Serba Mulia Auto khususnya pada lingkup kerja audit internal. Metode pengumpulan data yang digunakan yaitu dengan wawancara yang mengajukan pertanyaan-pertanyaan yang berkaitan dengan data-data audit. Dengan cara observasi, yaitu mengadakan pengamatan seca langung ke PT. Serba Mulia Auto.

Tujuan dari penelitian ini adalah merancang dan membangun sebuah aplikasi yang dapat menyelesaikan masalah enkripsi data untuk merahasiakan sebuah data dengan mengacak nilai dari *Byte* yang terdapat pada data dengan menggunakan bahasa pemrograman *Microsoft Visual Studio 2012*. Dalam penelitian ini, teknik pengumpulan data yang digunakan adalah studi pustaka. Metode pengujian yang digunakan adalah dengan pengujian *White-Box*.

Hasil dari penelitian ini adalah dibuatnya aplikasi Kriftografi yang dapat mengacak *byte* yang terdapat pada data agar terjadi pengacakan *byte* pada data yang dienkripsi.Pengguna dapat menentukan kunci yang digunakan dalam melakukan proses enkripsi dan kemudian proses enkripsi menggunakan metode *Rijndael*. Setelah Proses enkripsi maka data yang telah terenkripsi dapat disimpan.

.

Kata Kunci: Keamanan Data Audit dengan metode *Rijndael*

1. PENDAHULUAN

Teknologi komputer pada masa ini sangat membantu hampir seluruh kegiatan manusia. Tetapi dengan perkembangan teknologi komputer yang pesat penyalahgunaan pemakaian komputer juga semakin meningkat. Salah satu faktor yang perlu diperhatikan seiring dengan kemajuan teknologi komputer adalah masalah keamanan komputer. Keamanan pada komputer terlebih mengarah kepada keamanan data yang tersimpan didalam komputer tersebut. Salah satu cara untuk mengamankan data komputer adalah melakukan enkripsi pada sebuah data atau file yang kita anggap penting. Teknik enkripsi adalah teknik untuk merubah bentuk data sehingga orang lain tidak mengetahui bentuk asli dari data tersebut.

Kriptografi adalah ilmu yang berguna untuk mengacak (kata yang lebih tepat adalah Masking) data sedemikan rupa sehingga tidak bisa dibaca oleh pihak ke tiga. Tentu saja data yang diacak harus bisa dikembalikan ke bentuk semula oleh pihak yang berwenang.

Data yang ingin diacak biasanya disebut Plainteks *(Plaintext).* Data diacak menggunakan kunci Enkripsi *(Encryption Key)* Proses pengacakan itu sendiri disebut Enkripsi (*Encryption).* Plainteks yang telah diacak disebut Cipherteks (*Chipertext*) Kemudian proses untuk mengembalikan Cipherteks ke Plainteks disebut Dekripsi (*Decryption).* Kunci yang digunakan pada tahap Dekripsi disebut kunci Dekripsi (*Decryption Key).*

Dalam penelitian ini teknik enkripsi yang digunakan untuk mengenkripsi sebuah data adalah dengan metode Rijndael yang lebih menekankan proses matematika untuk menghasilkan kunci rahasia yang dapat disebarkan secara luas tanpa harus khwatir karena kunci rahasia yang dapat disebarkan secara luas tanpa harus khawatir karena kunci rahasia tersebut hanya dapat di dekripsi hanya oleh pengirim dan penerima.

Maka dalam penelitian ini akan dilakukan penelitian dalam mengenkripsi data menggunakan metode Rinjdael. Algoritma kriptografi bernama Rinjdael yang dideasin oleh Vincent Rijmen dan John Daemen asal belgia sebagai pemenang konter algoritma kriptografi pengganti DES yang diadakan oleh NIST *(National Institutes Of Standards and Technology)* milik pemerintah Amerika Serikat pada 26 November 2001. Algoritma Rinjdael inilah yang kemudian dikenal dengan *Advanced*

Encryption Standard (AES). Setelah mengalami beberapa proses standardisasi oleh NIST. Rinjdael kemudian diadopsi menjadi standard algoritma kriptografi secara resmi pada 22 Mei 2002.

2. RUANG LINGKUP PENELITIAN

1. Cakupan Permasalahan

Berdasarkan uraian latar belakang masalah diatas, maka dapat diambil rumusan masalah dari penelitian ini adalah, "Bagaimana membuat Aplikasi Kriftografi untuk kemananan data Audit dengan Metode Rijndael pada PT. Serba Mulia Auto ?"

2. Batasan masalah pada penelitian ini Batasan masalah pada penelitian ini adalah :

Tidak dibatasi karakter kunci, inputan file berupa data-data audit pada PT. Serba Mulia Auto, Menggunakan algoritma rinjdael untuk proses enkripsi dan dekripsi file, Dalam perancangan dan menerapkan algoritma Rijndael dengan menggunakan bahasa pemrograman Visual Basic.NET

3. Tujuan penyusunan penelitian ini adalah untuk

Melakukan Enkripsi Data Audit menggunakan metode Rijndael sehingga diharapkan mampu menyembunyikan informasi penting dari sebuah data dan mampu menjaga privasi kerahasian dari data tersebut.

3. BAHAN DAN METODE

3.1 Teori Dasar Kriftografi

Menurut Dony (2008), Kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata *Crypto* dan *Graphia* yang berarti penulisan rahasia. Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. *Ciphertext* inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, ciphertext tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali. Proses tranformasi dari plaintext menjadi ciphertext disebut proses *Encipherment* atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali ciphertext menjadi plaintext disebut proses dekripsi (*decryption*). Untuk mengenkripsi dan mendekripsi data.

Kriptografi menggunakan suatu algoritma (*cipher*) dan kunci (*key*). *Cipher* adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi data. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data.

Menurut Dony (2008),Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tidak semua aspek keamanan informasi ditangani oleh kriptografi.

Kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat dan mata-mata. Namun pada saat ini kriptografi lebih dari sekedar *privacy*, tetapi juga tujuan data *integrity, authentication* dan *non repudation*

Algoritma kriptografi modern tidak lagi mengandalkan keamanannya pada kerahasiaan algoritma tetapi kerahasiaan kunci. Plaintext yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan *ciphertext* yang berbeda pula. Dengan demikian algoritma kriptografi dapat bersifat umum dan boleh diketahui oleh siapa saja, akan tetapi tanpa pengetahuan tentang kunci, data tersandi tetap saja tidak dapat terpecahkan. Ada 4 (empat) tujuan mendasar dari ilmu kriftografi ini yang juga merupakan aspek keamanan informasi yaitu:

Kerahasiaan (*confidentiality)*, adalah layanan yang ditunjukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak. Di dalam kriptografi, layanan ini direalisasikan dengan menyandikan pesan menjadi cipherteks. Integritas data (*data integrity)*, adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: "apakah pesan yang diterima masih asli atai tidak mengalami perubahan?" untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubstitusian data lain ke dalam pesan yang sebenarnya.

Otentikasi (*authentication)*, adalah layanan yang berhubungan dengan identifikasi, baik mengindentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authencation)* maupun mengindentifikasi kebenaran sumber pesan (*data origin authencation).* Pihak yang saling bekomunikasi harus dapat mengotentikasi satu sama lain sehingga dapat memastikan sumber pesan. Pesan yang dikirim melalu saluran komunikasi juga harus diotentikasi asalnyya. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan : " Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar?"

Nirpenyangkal (*non-repudiation)*, adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

3.2 Rijndael

Menurut Munir (2006) dalam bukunya "Kriptografi", Rijndael menggunakan substitusi dan permutasi, dan sejumlah putaran (cipher berulang) setiap putaran menggunakan kunci internal yang berbeda (kunci setiap putaran disebut round key). Joan Daemen & Vincent Rijmen, dalam artikel yang berjudul A

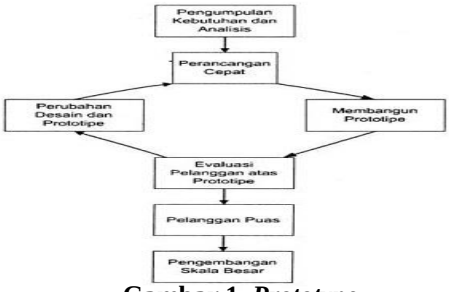
Specification for Rijndael, the AES Algorithm, menjelaskan input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi chipertext. Chiper keydari AES terdiri dari keydengan panjang 128 bit, 192 bit, atau 256 bit. *pattern* ditemukan.

3.3 Kriptografi

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tidak semua aspek keamanan informasi ditangani oleh kriptografi. (Dony ,2008)

4. Metode Pengembangan Sistem

Dalam pengembangan sistem paradigma yang digunakan adalah prototipe dengan alasan prototipe perlu digunakan untuk pembuatan suatu proyek, karena sering terjadinya seorang pengguna hanya mendefinisikan secara umum apa yang dikehendakinya tanpa menyebutkan secara detail *output* apa saja yang di butuhkan, pemrosesan dan data-data apa saja yang dibutuhkan. Sebaliknya disisi pengembang kurang memperhatikan efesiensi algoritma, kemampuan sistem operasi dan interface yang menghubungkan manusia dengan komputer. Untuk dapat mengatasi ketidakserasian antara pengguna dan pengembang itu, maka harus dibutuhkan suatu prototipe untuk menimbulkan kerjasama yang baik diantara keduanya, sehingga pengembang akan mengetahui dengan benar apa yang diinginkan pengguna dengan tidak mengesampingkan segi-segi teknis dan pengguna akan mengetahui proses-proses dalam menyelesaikan sistem yang diinginkan.



Gambar 1. *Prototype*

5. IMPLEMENTASI

5.1 Implementasi Rancangan Sistem

Desain program diterjemahkan ke dalam kode-kode dengan menggunakan bahasa pemrograman Visual Basic.Net 2012 dan menggunakan Aplikasi Visual Basic.Net 2012. Program yang dibangun langsung diuji secara unit, apakah sudah bekerja dengan baik. Adapun bagian-bagian yang dibangun dalam aplikasi ini adalah Tampilan *Form.*

5.1.1 Proses Rijndael

Simulasi proses perhitungan manual algoritma rijndael dapat dilihat pada contoh berikut :

Plaint Text :STIMIKWICIDA2016
Chiper Key :MAHASISWAWCD2016
Round 1
Masukan ke kolom 4x4

S	T	I	M	M	A	H	A
I	K	W	I	S	I	S	W
C	I	D	A	A	W	C	D
2	0	1	6	2	0	1	6

.

Konversi teks menggunakan kode ASCII ke heksadesimal

53	54	49	4D
49	4B	57	49
43	49	44	41
32	30	31	36

4D	41	48	41
53	49	53	57
41	57	43	44
32	30	31	36

0E	15	01	0C
1A	02	04	1E
02	1E	07	05
00	00	00	00

Proses Sub-Bytes

0E	15	01	0C
1A	02	04	1E
02	1E	07	05
00	00	00	00

AB	59	7C	FE
A2	77	F2	72
77	72	C5	6B
63	63	63	63

Proses Shift-Row

AB	59	7C	FE
A2	77	F2	72
77	72	C5	6B
63	63	63	63

AB	59	7C	FE
A2	77	F2	72
77	72	C5	6B
63	63	63	63

AB	59	7C	FE
77	F2	72	A2
77	72	C5	6B
63	63	63	63

AB	59	7C	FE
77	F2	72	A2
77	72	C5	6B
63	63	63	63

AB	59	7C	FE	AB	59	7C	FE
77	F2	72	A2	77	F2	72	A2
C5	6B	77	72	C5	6B	77	72
63	63	63	63	63	63	63	63

Mix Column

69	C7	6A	0B
69	63	62	EE
55	6E	E3	BB
89	B4	47	96

Proses putaran kunci

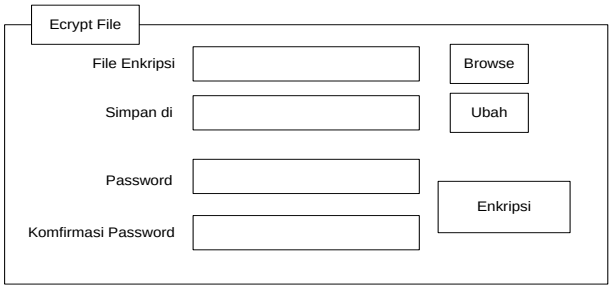
4D	41	48	41	17	56	1E	5F
53	49	53	57	48	01	52	05
41	57	43	44	44	13	50	14
32	30	31	36	B1	81	B0	86

Hasil keseluruhan Proses Rinjdael/Chipertext

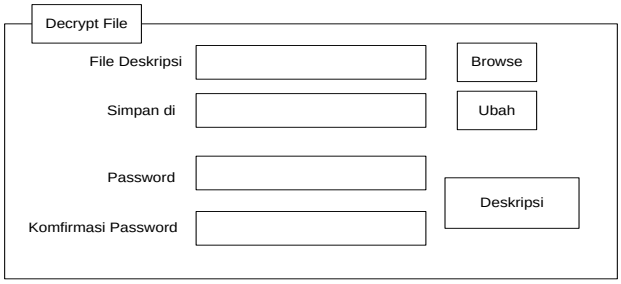
1F	98	8D	25
DD	2C	C1	E6
4E	F5	25	6D
D3	67	6C	0E

5.1.2 Perancangan Antar Muka

Di bawah ini adalah tahapan perancangan antar muka penerapan aplikasi kriptografi untuk kemanan data audit menggunakan metode *rinjdael* pada PT. Serba Mulia Auto :



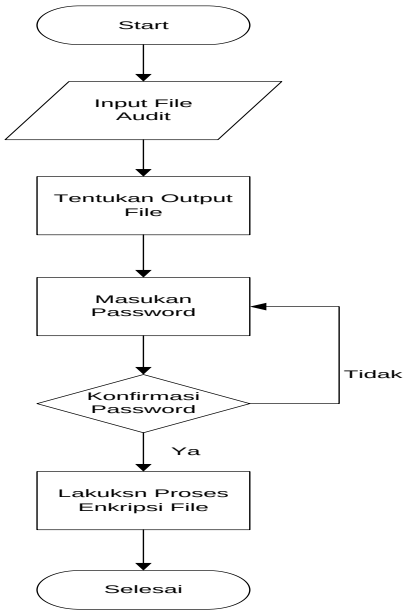
Gambar 2 Perancangan Antar Muka Aplikasi Kriptografi untuk keamanan data audit



Gambar 3 Perancangan Antar Muka Aplikasi Kriptografi untuk keamanan data audit

5.1.3 Flowchart Proses Enkripsi

Di bawah ini adalah tahapan flowchart penerapan enkripsi data audit pada PT. Serba Mulia Auto :

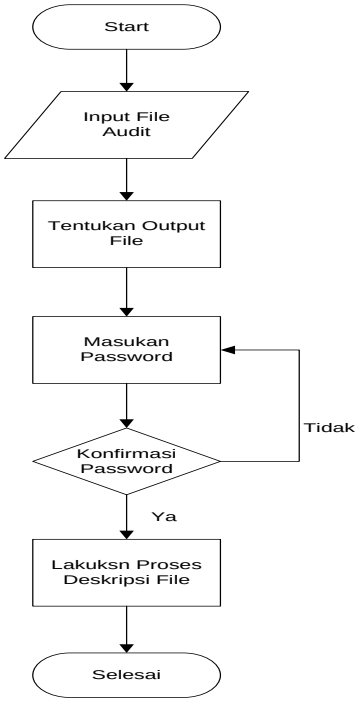


Gambar 4 *Flowchart* Proses Ekripsi data Audit

Flowchart proses enkripsi Rijndael merupakan suatu rancangan sistem yang digunakan untuk memperlihatkan alur dari kinerja sistem untuk melakukan proses dekripsi pada aplikasi enkripsi.

5.1.4 Flowchart Proses Dekripsi

Pada gambar di bawah ini adalah *flowchart* desain algoritma enkripsi data keuangan :



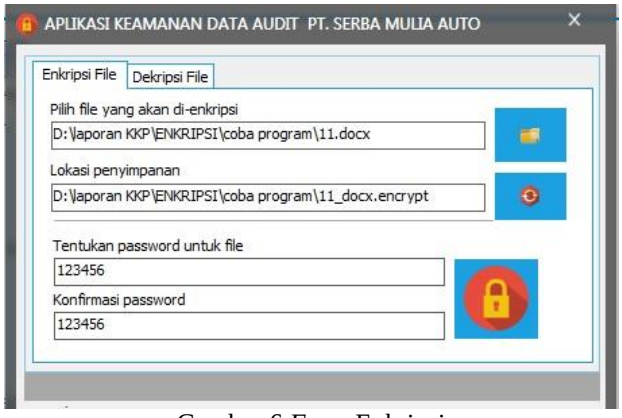
Gambar 5 *Flowchart* Proses Dekripsi data Audit

Flowchart proses dekripsi rijndael merupakan suatu rancangan sistem yang digunakan untuk memperlihatkan alur dari kinerja sistem untuk melakukan proses enkripsi pada aplikasi enkripsi alogritma rijndael.

5.2 Membangung *prototype*

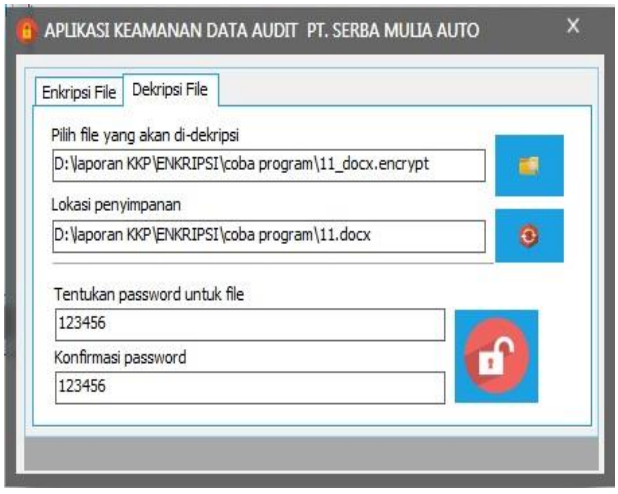
Membangung *prototype* merupakan tahapan yang bertujuan mengubah hasil dari rancangan sistem menjadi bentuk nyata. Pada saat pertama kali aplikasi dijalankan maka akan muncul sebuah tampilan seperti gambar di bawah ini :

5.2.1 *Form* Enkripsi



Gambar 6 *Form* Enkripsi

5.2.2 *Form* Dekripsi



Gambar 7 *Form* Dekripsi

5.3Evaluasi *Prototype*

Unit program atau program individual diintegrasikan dan diuji sebagai sistem yang lengkap untuk menjamin bahwa persyaratan sistem telah terpenuhi.

Pengujian perangkat lunak merupakan salah satu proses rangkaian dari pengembangan perangkat lunak dan pengujian yang dilakukan disini dengan *White Box*.

6. KESIMPULAN

Dengan adanya hasil penelitian yang dilakukan dan berdasarkan uraian-uraian yang dibahas dalam bab-bab sebelumnya yang telah dikemukakan mengenai aplikasi kriptografi untuk keamanan data audit menggunakan metode rijndael pada PT. Serba Mulia Auto, maka dapat ditarik kesimpulan bahwa :

1. Algoritma yang digunakan pada sistem ini adalah algoritma rijndael yang dapat berfungsi dengan baik untuk enkripsi dan dekripsi pada aplikasi ini.
2. Aplikasi ini dapat membantu mengamankan data-data audit khususnya audit pada PT. Serba Mulia Auto.

5.1 Saran

Aplikasi ini masih dapat dikembangkan lebih lanjut sesuai kebutuhan pengguna. Sebagai bahan pertimbangan dalam upaya menyesuaikan kinerja dan mengembangkan aplikasi kriftografi untuk kemanan data audit dimasa yang akan datang maka :

1. Dalam Pemrosesan Enkripsi dan Dekripsi kunci yang digunakan harus lebih variatif lagi maka lebih baik lagi untuk kunci di enkripsikan menggunakan metode yang berbeda.
2. Aplikasi dapat di kembangkan ke system operasi *mobile* seperti android , windows phone dan ios.
3. Kunci yang digunakan dalam implementasi masih tergolong lemah maka diharapkan untuk penelitian yang lebih lanjut ada metode pembangkitan karakter.

8. DAFTAR PUSTAKA

Prayudi Yudi & Idham Halik. 2006. *Studi Analisis Algoritma Rivest Code 6 (RC6) Dalam Enkripsi/Dekripsi Data*. Seminar Nasional Aplikasi Teknologi Informasi 2006 (SNATI 2006), Yogyakarta.

Ariyus Dony. 2008. *Pengantar Ilmu Kriptografi*. Penerbit : ANDI. Yogyakarta.

Satria Eko. 2009, *Studi Algoritma Rijndael dalam Sistem Keamanan Data, Universitas Sumatera Utara*

Munir Rinaldi. 2006, *Kriptografi*, Informatika, Bandung

Kristanto Andri 2007, *Perancangan sistem informasi dan aplikasinya* , Yogyakarta: Gava Media, 2007

Mulyanto Agus. 2009. *Sistem Informasi Konsep dan Aplikasi*. Pustaka Pelajar.

Kadir Abdul, 2009. *Pengenalan Sistem Informasi*. Andi Offset:Yogyakarta

Jogiyanto. 2007. *Analisis dan Desain Sistem Informasi*. Yogyakarta: Penerbit Andi.

Tripton Harold F. 2007. *Information Security Management*, Penerbit CRC Press

Agoes,Sukrisno (2011). *Petunjuk Praktis Pemeriksaan Akuntan oleh Akuntan Publik.* Jakarta : Salemba Empat

Tugiman 2006 , *Standart Profesional Audit Internal.* Penerbit Kanisius.

Wahana Kompuer 2013, shourt course :*visual basic 2012 programing* Yogyakarta: Andi.

Simarmata. Janner (2010), *RekayasaPerangkatLunak*, Andi Offset, Yogyakarta.

Nugroho Adi. *Rekayasa Perangkat Lunak Berorientasi Objek DenganMetode USDP*. Yogyakarta: Andi, 2010

Thad Van den Bosch. "Encrypt/Decrypt File in VB.Net (Using Rijndael). https://www.codeproject.com/Articles/12092/Encrypt-Decrypt-Files-in-VB-NET-Using-Rinjdael.html. Diakses 10 Oktober 2015.