VOLUME 5 NOMOR 2, OKTOBER 2016

ISSN 2089 - 1245

KILAT

JURNAL KAJIAN ILMU DAN TEKNOLOGI

ISSN 2089-1245

SEKOLAH TINGGI TEKNIK - PLN (STT-PLN)

KILAT	VOL.5	NO.2	HAL. 79 - 163	OKTOBER 2016	ISSN 2089 - 1245

APLIKASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA AES-128 (*ADVANCED ENCRYPTION STANDARD* -128) BERBASIS WEB PADA LABORATORIUM ICT TERPADU UNIVERSITAS BUDI LUHUR

[1)]Diana Permatasari, [2)]Safitri Juanita
[1), 2)] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
e-mail : dianapermatasariubl@gmail.com

Abstract

Document exam for midterm and final exam is one of the very important document because it is used by lecturers to evaluate the lecture material for Teaching and Learning Activities. ICT Laboratory Integrated Budi Luhur University as one of the operator of the test lab at the University of Budi Luhur who has responsibility for securing documents exams during the process of mid term and final exam, so in practice there is requiring an application to security documents such as Cryptography Web Based Application using algorithms AES-128 on Lab ICT Integrated Budi Luhur University. Method that is used to develop this application is using Waterfall model, this application used PHP with MySQL database. The research objective is to implement the algorithm AES-128 to encrypt and decrypt files exam on Lab ICT Integrated Budi Luhur University, securing document exam file that can not be read by anyone other than the owner of the file and the person who has access to the file. The conclusion of this study prove that the method algorithm AES-128 algorithm is excellent in secure files, as well as by the application of safeguards files, documents exams more awake, and confidential and the decryption process, the results of the file content decryption did not change from the original file.

Keywords: *cryptography, AES-128, Document Examination, Web-Based.*

Abstrak

Dokumen ujian merupakan salah satu data yang sangat penting karena digunakan oleh Dosen untuk mengevaluasi materi perkuliahan selama Kegiatan Belajar Mengajar (KBM). Lab ICT Terpadu Universitas Budi Luhur sebagai salah satu penyelenggara ujian praktikum di Universitas Budi Luhur yang memiliki tanggung jawab untuk mengamankan dokumen ujian selama proses UTS dan UAS berlangsung, sehingga dibutuhkan aplikasi pengamanan dokumen yaitu Aplikasi Kriptografi menggunakan Algoritma AES-128 Berbasis Web pada Lab ICT Terpadu Universitas Budi Luhur. Aplikasi ini dibangun menggunakan metode pengembangan sistem Waterfall, aplikasi ini dibangun menggunakan bahasa pemograman PHP dengan basis data MySQL. Tujuan penelitian adalah mengimplementasikan algoritma AES-128 untuk enkripsi dan dekripsi file soal ujian pada Lab ICT Terpadu Universitas Budi Luhur, mengamankan soal ujian dalam bentuk file dokumen agar tidak bisa dibaca oleh orang lain selain pemilik file tersebut dan orang yang memiliki hak akses terhadap file tersebut, serta memberikan kontribusi ilmu pengetahuan di bidang ilmu komputer khususnya topik keamanan komputer. Kesimpulan penelitian ini membuktikan bahwa metode Algoritma AES-128 adalah algoritma yang sangat baik dalam mengamankan file, serta dengan adanya aplikasi pengamanan file, dokumen ujian lebih terjaga kerahasiaanya dan pada proses dekripsi, hasil dari isi file dekripsi sama sekali tidak mengalami perubahan dari file asli.

Kata Kunci *: Kriptografi, AES-128, Dokumen Ujian, Web-Based.*

1. PENDAHULUAN

1.1 Latar Belakang

Laboratorium *Information Communication and Technology* (Laboratorium ICT) Terpadu Universitas Budi Luhur adalah organisasi yang termasuk dalam Badan Otonom di Universitas Budi Luhur. Saat penyelenggaraan Ujian Tengah Semester (UTS) dan Ujian Akhir Semester (UAS), beberapa dosen pengampu matakuliah praktikum akan memberikan dokumen penting dan rahasia berupa soal ujian ke Lab ICT Terpadu Universitas Budi Luhur berupa *softcopy* yang akan dibagi (*share)* ke Mahasiswa yang terdaftar pada kelas dosen yang mengampu mata kuliah praktikum dan berada pada jaringan yang ada di Laboratorium Universitas Budi Luhur. Sehingga soal berupa softcopy tersebut dapat dilihat oleh kepala lab dan *supervisor* yang memiliki akses ke sistem ujian. Dari masalah tersebut diperlukan sebuah aplikasi yang dapat mengamankan dokumen tersebut, yaitu "Aplikasi Kriptografi menggunakan Algoritma AES-128 (*Advanced Encryption Standard*-128) Berbasis Web pada Laboratorium ICT Terpadu Universitas Budi Luhur".

1.2 Masalah

Bagaimana menerapkan metode AES-128 (*Advanced Encryption Standard*-128) dalam Aplikasi Kriptografi Berbasis Web Pada Lab ICT Terpadu Universitas Budi Luhur ?, sehingga keamanan dokumen soal ujian dapat terjaga

1.3 Tujuan Penelitian

Mengimplementasikan algoritma AES-128 untuk enkripsi dan dekripsi *file* soal ujian pada Lab ICT Terpadu Universitas Budi Luhur.

2. KAJIAN TEORI

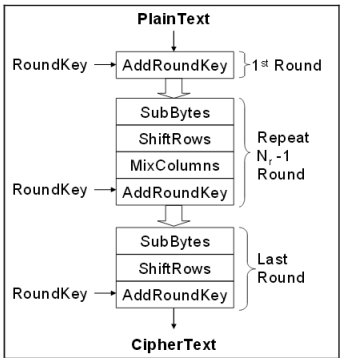
2.1 Algoritma AES

Menurut Daemen dan Rijmen [2] : AES atau *Advanced Encryption Standard* merupakan standar enkripsi kunci simetris yang pada awalnya diterbitkan dengan algoritma Rijndael. Algoritma ini dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen. AES termasuk dalam algoritma kriptografi yang sifatnya simetris dan *block cipher.* AES memiliki panjang kunci 128 bit, 192 bit, dan 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah *round* yang akan diimplementasikan pada algoritma AES ini. Di bawah ini adalah tabel yang memperlihatkan jumlah *round* (*Nr*) yang harus diimplementasikan pada masing-masing panjang kunci.

Tabel 1 : Perbandingan jumlah Round dan Key [2]

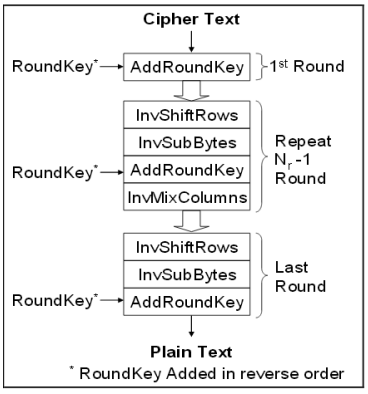
	Key Length *(Nk words)*	Block Size *(Nb words)*	Number of Rounds *(Nr)*
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Menurut Daemen dan Rijmen [4] : Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi *bytes*, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Pada awal proses enkripsi, *input* yang telah dikopikan kedalam *state* akan mengalami transformasi *byte AddRoundKey*. Setelah itu *state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns, and AddRoundKey* secara berulang-rulang sebanyak *Nr.* Proses ini dalam algoritma AES disebut sebagai *round function. Round* yang terakhir sedikit berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, *state* tidak mengalami transformasi *MixColumns.*



Gambar 1 : Diagram Alur Proses Enkripsi [8]

Menurut Daemen dan Rijmen [4] : Proses dekripsi pada algortima AES menggunakan transformasi yang berlawanan dari proses enkripsi.Transformasi yang berlawanan tersebut digunakan untuk menghasilkan *inverse cipher* sehingga cipherteks yang dikembalikan menjadi plainteks. Penjelasan lebih mendalam mengenai transformasi *InvShiftRows, InvSubBytes, InvMixColumns* dan *AddRoundKey*. Algoritma dekripsi dapat dilihat pada skema berikut ini :



Gambar 2 : Diagram Alur Proses Dekripsi [8]

2.2 Studi Literatur Penelitian Sebelumnya

a. Menurut Bendi dan S Aditya [1] tahun 2012 dalam penelitiannya yang berjudul Implementasi Algoritma Rijndael untuk Enkripsi dan Dekripsi pada Citra Digital mengatakan bahwa masalah keamanan dan kerahasiaan data dan informasi merupakan suatu hal yang penting. Salah satu cara menjaga keamanan dan kerahasiaan data dan informasi adalah dengan teknik enkripsi dan dekripsi. Salah satu algoritma kriptografi yang sering digunakan saat ini adalah Rijndael atau yang dikenal juga dengan AES (*Advanced*

Encryption Standard). Perangkat lunak ini akan dibangun dengan menggunakan metode Waterfall. Hasil dari pembangunan perangkat lunak ini telah dapat mengimplementasikan algoritma kriptografi Rijndael untuk menjaga keamanan dan kerahasiaan citra digital dengan format *file* citra bitmap.

b. Menurut Renaldy [6] tahun 2015 dalam penelitiannya yang berjudul Implementasi Kriptografi pada Diary Berbasis Mobile Android dengan Menggunakan Metode AES-128 (*Advanced Encryption Standard*-128) dan SHA-1 (Secure Hash Algorithm-1) mengatakan bahwa untuk menjaga keamanan privasi yang ditulis pada *diary*, penulis mencoba membuat aplikasi untuk menulis *diary* yang keamanannya dapat dijaga dengan cukup baik dan dapat digunakan dimana saja karena aplikasi ini menggunakan metode AES-128 dan SHA-1 serta dapat dijalankan pada *handphone* atau *smartphone* yang sudah sangat banyak digunakan masyarakat secara umum.

c. Menurut Hanifah [3] tahun 2012 dalam penelitiannya yang berjudul Aplikasi Algoritma Rijndael dalam Pengamanan Citra Digital mengatakan bahwa pengamanan data citra digital menjadi hal yang penting dan mendesak. Salah satu pengamanan bisa dilakukan dengan menerapkan algoritma enkripsi Rijndael. Empat proses utama algoritma ini terdiri dari satu proses permutasi (ShiftRows) dan tiga proses substitusi (SubBytes, MixColumns, dan AddRoundKey) dan juga proses penjadwalan kunci. Dalam penelitian ini akan dibahas tentang pengamanan data citra digital oleh algoritma Rijndael dan juga implementasi algoritma ini dalam mengamankan citra digital.

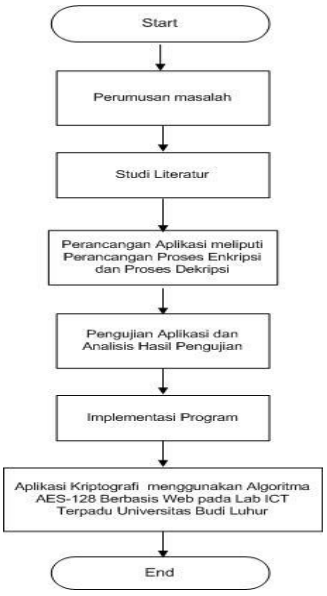
d. Menurut Ramdhansya et al**.** [7] tahun 2014 dalam penelitiannya yang berjudul Implementasi *Advanced Encryption Standard* (AES) pada Sistem Kunci Elektronik Kendaraan Berbasis Sistem Operasi Android dan Mikrokontroler Arduino mengatakan bahwa selama ini untuk menghidupkan kendaraan seseorang harus menggunakan sebuah kunci, sehingga untuk mengakses banyak kendaraan harus digunakan banyak kunci yang berbeda. Namun jika handphone dijadikan kunci elektronik, tentunya semua kunci tersebut tidak dibutuhkan lagi, karena satu handphone dapat mewakili kunci tersebut. Pada penelitian ini, sistem kunci elektronik menggunakan *handphone* sebagai kunci, dan sebuah mikrokontroler Arduino pada kendaraan sebagai penerima kontrol.. Oleh karena itu, penelitian ini dibuat untuk melengkapi aspek keamanan kunci elektronik dengan mengimplementasikan *Advanced Encryption Standard* (AES) dengan panjang kunci 128 bit, 192 bit, dan 256 bit. Hasil yang diperoleh dari penelitian ini adalah meningkatnya dukungan aspek keamanan yang diperoleh dari implementasi AES. Setelah dilakukan pengujian, total waktu eksekusi maksimum sistem kunci elektronik kendaraan yang telah dibuat sebesar 385 ms pada jarak 20 m. Lama waktu tersebut masih lebih rendah dibanding batas kenyamanan pengguna yaitu di bawah 1000 ms (Nielsen, 1993), sehingga sistem layak untuk diterapkan.

Perbedaan penelitian ini dengan 4 (empat) penelitian diatas adalah pada penelitian ini menggunakan kriptografi dengan algoritma AES-128 (*Advanced Encryption Standard*-128) untuk mengamankan *file* soal ujian, khususnya pada *file* dokumen word, excel dan pdf. Dan aplikasi ini bisa digunakan oleh banyak *user* atau *multi user* dengan berbasis web.

3. ANALISA DAN PERANCANGAN PROGRAM

3.1 Alur Pikir Penelitian

Alur pikir penelitian dimulai dengan merumuskan masalah penelitian, kemudian melakukan studi literatur dengan membaca hasil penelitian terdahulu dan beberapa buku yang mendukung penelitian serta dokumen lainnya. Tahap selanjutnya adalah pengumpulan data dengan wawancara dan observasi pada pihak instansi. Setelah melakukan pengumpulan data, tahap selanjutnya adalah melakukan perancangan aplikasi yang meliputi proses enkripsi dan proses dekripsi, tahap ini dilakukan untuk merancang aplikasi yang akan dibangun ke aplikasi kriptografi. Tahap selanjutnya adalah pengujian terhadap sistem dengan menggunakan *Black Box testing* serta hasil yang diberikan apakah sudah sesuai dengan konsep kriptografi menggunakan algoritma AES-128 (*Advanced Encryption Standard*-128) . Dan tahap selanjutnya yang harus dilakukan adalah implementasi program , pada tahap ini dilakukan dengan cara mengimplementasikan tahap alur pertama, kedua, ketiga dan keempat ke dalam sebuah program dengan membuat aplikasi sesuai kebutuhan sistem berdasarkan perancangan sistem yang telah dilakukan.

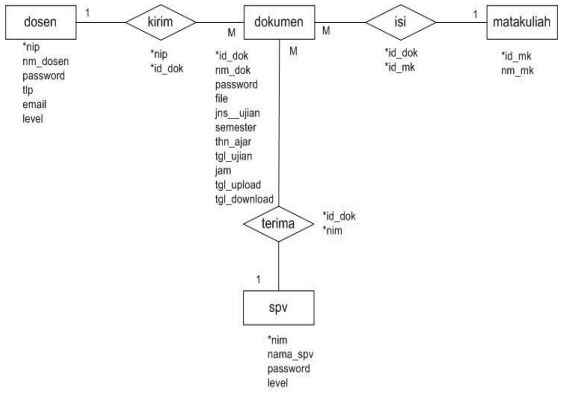


Gambar 3: Alur Pikir Penelitian

3.2 Rancangan Basis Data

a. ERD (*Entity Relationship Diagram*)

Berikut ini adalah ER-D pada aplikasi kriptografi menggunakan AES-128 berbasis web pada LAB ICT Terpadu. Pada ER-D ini memiliki 4 tabel yang terdiri dari tabel spv, dosen, dokumen dan mata kuliah.



Gambar 4 : ER-Diagram (Entity Relationship Diagram)

b. *Spesifikasi* Basis Data

Berikut adalah struktur tabel yang digunakan dalam pembuatan *database* untuk aplikasi ini :

1) Nama Tabel : spv
   Primary Key : nim
   Media : *Hard Disk*
   Isi : Data Supervisor

Tabel 2 : Spesifikasi Tabel Spv

Nama *Field*	Jenis	Panjang	Keterangan
nim	char	10	nim
nama_spv	varchar	50	nama
password	varchar	50	password
level	int	1	level

2) Nama Tabel : Dosen
   Primary Key : nip
   Media : *Hard Disk*
   Isi : Data Dosen

Tabel 3 : Spesifikasi Tabel Dosen

Nama *Field*	Jenis	Panjang	Keterangan
nip	char	10	nip
nm_dosen	varchar	50	nama dosen
password	varchar	50	password
tlp	varchar	15	telepon
email	varchar	50	email
level	varchar	1	level

3) Nama Tabel : MataKuliah
   Primary Key : id_mk
   Media : *Hard Disk*
   Isi : Data Mata Kuliah

Tabel 4 : Spesifikasi Tabel Matakuliah

Nama *Field*	Jenis	Panjang	Keterangan
id_mk	char	10	id matakuliah
nm_mk	varchar	50	Nama matakuliah

4) Nama Tabel : dokumen
   Primary Key : id_dok
   Foreign Key : nip, id_mk, nim
   Media : *Hard Disk*
   Isi : Data Dokumen

Tabel 5 : Spesifikasi Tabel Dokumen

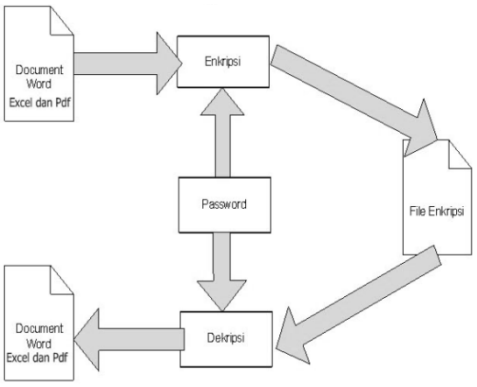
Nama *Field*	Jenis	Panjang	Keterangan
id_dok	int	4	id dokumen
nm_dok	varchar	50	nama dokumen
password	varchar	50	password dokumen
file	text	255	nama file enkripsi
jns_dok	varchar	3	jenis dokumen
semester	varchar	6	semester
tgl_ujian	datetime	10	tanggal ujian
jam	varchar	11	jam ujian
tgl_upload	datetime	20	tanggal upload
nip	char	10	nip
id_mk	char	6	id mata kuliah
nim	char	10	nim

3.3 Perancangan Program

Program yang dibuat terdiri dari 14 buah *form*, yang terdiri dari *Form Login Admin/Supervisor/*Dosen, *Form Dashboard Admin, Form* Entri *Supervisor*, *Form* Edit *Supervisor*, *Form* Entri Dosen, *Form* Edit Dosen, *Form* Entri Mata Kuliah, *Form Edit* Mata Kuliah, *Form* Dokumen, *Form* Dekripsi, *Form Dashboard* Dosen, *Form* Ganti *Password* , *Form* Enkripsi dan *Form Dashboard Supervisor*.

Untuk melakukan enkripsi isi *file*, *user* (Dosen) dapat memilih menu enkripsi. Pada menu ini, *user* (Dosen) diharuskan memilih *file* word,excel dan pdf terlebih dahulu, baru kemudian melakukan proses enkripsi, selanjutnya akan tampil *output* berupa informasi hasil enkripsi *file* tersebut.

Sedangkan untuk mengembalikan *file* yang sudah di enkripsi menjadi *file* asli, *user* (*Admin* dan *Supervisor*) dapat memilih menu dekripsi.

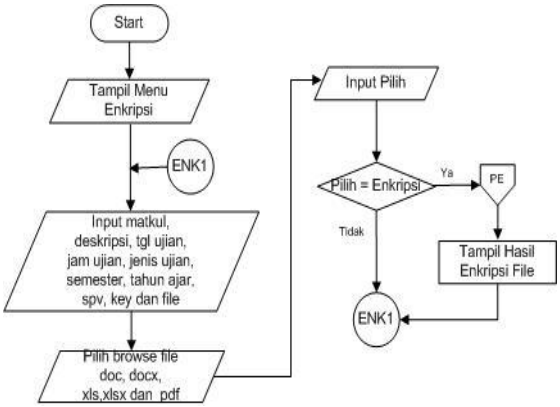


Gambar 5: Alur Program Enkripsi dan Dekripsi File

3.4 *Flowchart* Form Enkripsi

Pada *Flowchart Form* Enkripsi ini, Dosen akan memilih mata kuliah yang akan dipilih untuk meng*upload* soal ujian, tanggal ujian, jam ujian, jenis ujian, semester, tahun ajar, nama spv yang akan dipilih untuk mendekripsi soal ujian, *key* untuk keamanan enkripsi, dan pilih *browse* untuk mengambil *file* doc, docx, xls, xlsx dan pdf yang

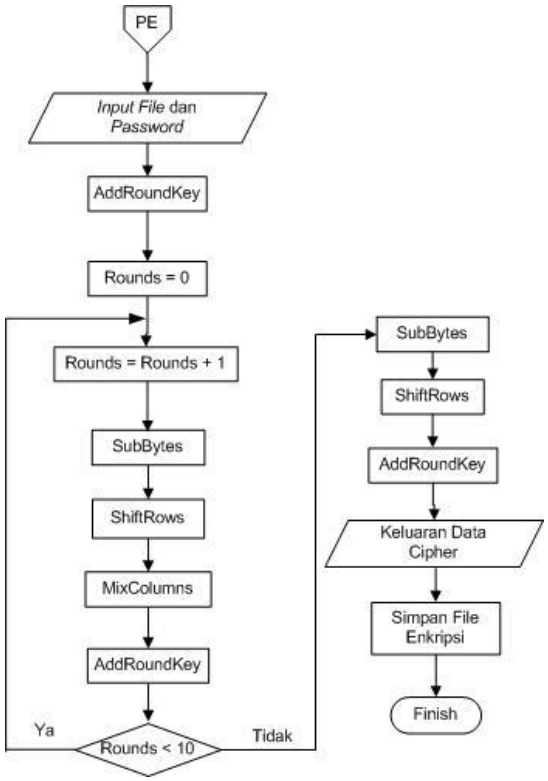
dipilih lalu klik enkripsi untuk menyimpan data inputan dan akan dikembalikan ke menu enkripsi.



Gambar 6 : Flowchart Form Enkripsi

3.5 Flowchart Proses Enkripsi AES-128

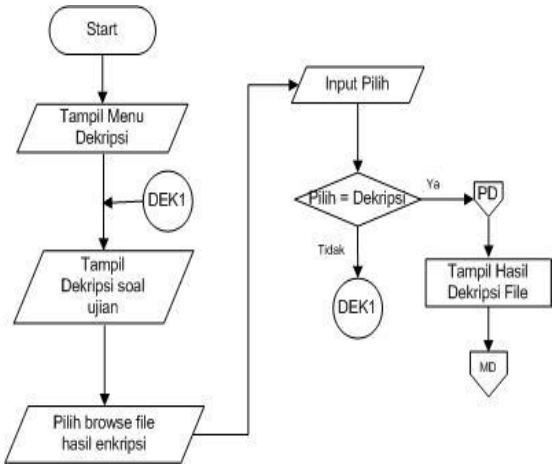
Flowchart ini merupakan alur jalannya proses enkripsi AES-128 sebuah *file* doc, docx, xls, xlsx dan pdf yang dipilih. *Flowchart* proses enkripsi dapat dilihat seperti Gambar 7 :



Gambar 7 : Flowchart Proses Enkripsi AES-128

3.6 *Flowchart Form* Dekripsi

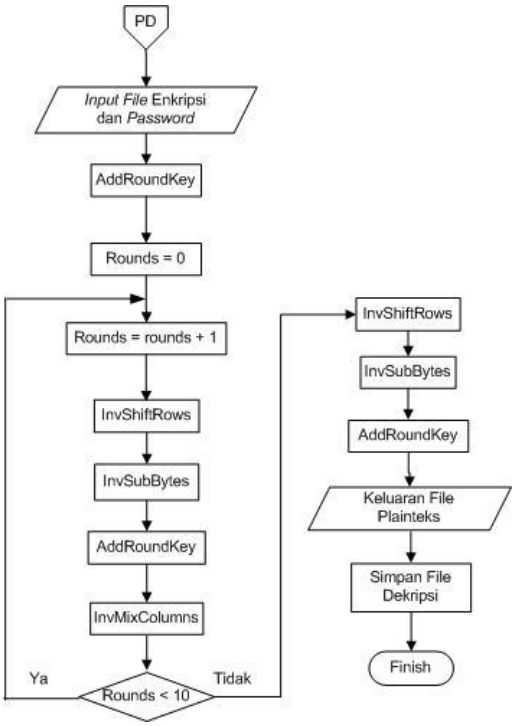
Pada *Flowchart Form* Dekripsi ini, ditampilkan menu Dekripsi, *Admin* atau *Supervisor* akan memilih *browse* untuk mengambil *file* soal ujian hasil proses enkripsi. Lalu pilih dekripsi untuk melakukakan proses dekripsi. Jika proses dekripsi *file* telah selesai akan kembali ke menu *Dashboard Admin* atau *Supervisor.*



Gambar 8 : Flowchart Form Dekripsi

3.7 *Flowchart* Proses Dekripsi AES-128

Flowchart ini merupakan alur jalannya proses dekripsi sebuah *file* doc, xls dan pdf yang sudah dipilih. *Flowchart* proses dekripsi dapat dilihat seperti Gambar 9 berikut :



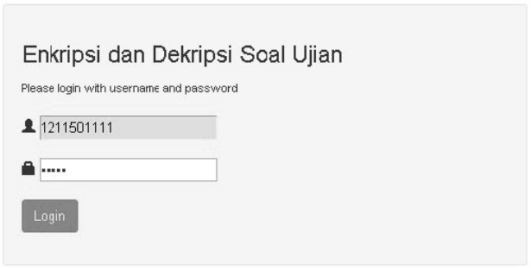
Gambar 9 : Flowchart Proses Dekripsi AES-128

4. IMPLEMENTASI DAN ANALISIS HASIL UJI COBA PROGRAM

4.1 Tampilan Layar

a. Tampilan Layar *Form Login*

Tampilan layar dari *Form Login* merupakan tampilan awal pada saat program pertama kali di akses atau dijalankan. Pada *Form Login* ini, *Admin* dan *User* memasukkan *username* dan *password* agar dapat masuk dan menggunakan aplikasi ini. Tampilan Layar *Form Login* dapat dilihat pada Gambar 10:



Gambar 10 : Tampilan Layar Form Login

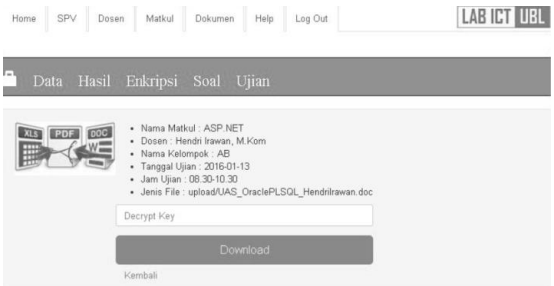
b. Tampilan Layar Menu *Dashboard* Admin

Tampilan layar dari Menu *Dashboard Admin* ini akan muncul setelah *Admin login*. *Admin* memiliki hak untuk menambah *Supervisor* pada Menu SPV , menambah Dosen pada Menu Dosen, menambah Mata Kuliah baru di lab pada Menu Mata Kuliah, Menu Dokumen untuk melihat *file* hasil enkripsi yang telah di *input* Dosen atau Menu *Help* untuk melihat penjelasan panduan aplikasi. Tampilan Layar Menu *Dashboard Admin* dapat dilihat pada Gambar 11 :

Gambar 11 : Tampilan Layar Menu Dashboard Admin

c. Tampilan Layar Menu Dekripsi

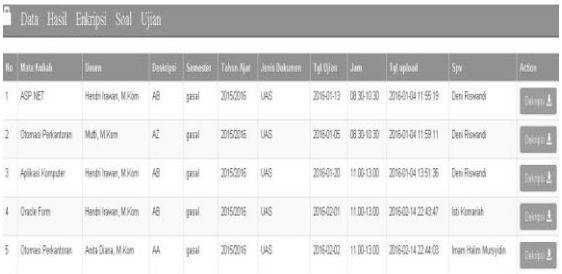
Pada tampilan Layar Menu Dekripsi ini, ditampilkan tahun ajaran, semester, Dosen, mata Kuliah, tanggal ujian, jam, *key* yang dipanggil dari *database*, dokumen yang akan *browse file* hasil enkripsi dan *button* dekripsi *file* nya.



Gambar 12 : Tampilan Layar Menu Dekripsi

d. Tampilan Layar Menu Dokumen Admin

Pada tampilan layar Menu Dokumen *Admin* ini ditampilkan *form* hasil dari enkripsi, *file* hasil enkripsi akan terdata sesuai nama dosen yang telah meng*upload file* soal ujian dan nama-nama *supervisor* yang telah diberikan hak akses oleh Dosen.



Gambar 13 : Tampilan Layar Menu Dokumen Admin

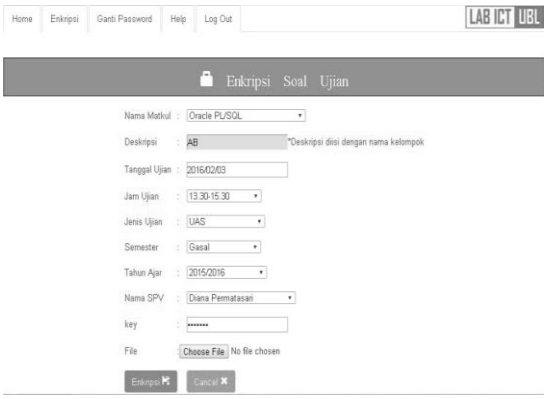
e. Tampilan Layar Menu Dashboard Dosen

Tampilan layar dari Menu *Dashboard* Dosen ini muncul setelah Dosen *login*. Dosen dapat memilih menu enkripsi untuk mengenkripsi soal ujian atau menu ganti *password* untuk mengubah *password.* Tampilan Layar Menu *Dashboard* Dosen dapat dilihat pada Gambar 14 :

Gambar 14 : Tampilan Layar Menu Dashboard Dosen

f. Tampilan Layar Menu Enkripsi

Pada tampilan layar Enkripsi ini, Dosen akan memilih mata kuliah yang akan dipilih untuk meng*upload* soal ujian, tanggal pelaksanaan ujian, jam ujian, jenis ujian, semester, tahun ajaran, nama *supervisor* yang diberikan hak akses untuk dapat mendekripsi soal ujian, key untuk keamanan enkripsi, dan pilih *browse* untuk mengambil *file* doc, docx, xls, xlsx dan pdf lalu klik enkripsi untuk menyimpan data inputan. Pada *form key* akan di *input* maksimal 16 karakter.



Gambar 15 : Tampilan Layar Menu Enkripsi

Jika proses enkripsi berhasil, maka akan tampil hasil enkripsi seperti pada Gambar 16 dibawah ini.

Gambar 16 : Tampilan Layar Data Enkripsi telah Berhasil

Jika data enkripsi telah berhasil, maka akan ditampilkan *list* dari tabel hasil enkripsi dan dapat dilihat pada Gambar 17. Dosen dapat memilih *action button* hapus untuk menghapus data enkripsi soal ujian jika terjadi salah *input*.

Gambar 17 : Tampilan Layar Data Hasil Enkripsi Soal Ujian

g. Tampilan Layar Menu Dashboard Supervisor

Tampilan layar dari Menu *Dashboard Supervisor* ini muncul setelah *Supervisor login*. *Supervisor* dapat memilih menu dekripsi untuk mengdekripsi soal ujian atau menu ganti *password* untuk mengubah *password.* Tampilan Layar Menu *Dashboard Supervisor* dapat dilihat pada Gambar 18:

Gambar 18 : Tampilan Layar Menu Dashboard Supervisor

h. Tampilan Layar Menu Dokumen Supervisor

Pada tampilan layar Menu Dokumen *Supervisor* ini ditampilkan *form* hasil enkripsi yang telah dilakukan oleh Dosen. Dan *file* hasil enkripsi pada dokumen *Supervisor* akan terdata sesuai dengan nama *Supervisor* yang telah diberikan hak akses oleh Dosen.

Gambar 19 : Tampilan Layar Menu Dokumen Supervisor

4.2 Tabel Pengujian

Dalam pengujian kali ini, akan dibahas perbandingan antara proses enkripsi dan dekripsi *file*. *File* word, excel dan pdf yang diuji meliputi jenis *file*, yaitu *file* doc, docx, xls, xlsx dan pdf. Pengujiannya yaitu antara lain ukuran *file*, panjang *password* yang diberikan, waktu proses enkripsi dan waktu proses dekripsi.

Tabel Enkripsi dan Dekripsi *File* DOC, DOCX, XLS, XLSX dan PDF.

Tabel 6 : Hasil Uji Coba Enkripsi dan Dekripsi File

No	Nama File	Password	Ukuran File (KB)	Waktu Enkripsi	Waktu Dekripsi
1	UAS_OraclePLSQL_HendrilRawan.doc	rahasia	164	18	32
2	UAS_OP_Anita.docx	secret	121	21	24
3	UAS_APLIKOM.xls	rahasia	62	12	13
4	UAS_PPDPA_Prita.xlsx	qwerty	12	3	4
5	UAS_PEMVIS_Windarto.pdf	qwerty123	102	12	14

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan rumusan masalah, implementasi, dan analisa sistem maka didapat kesimpulan sebagai berikut :

a. Berdasarkan hasil kuesioner yang telah diberikan ke 10 responden, membuktikan bahwa Algoritma AES-128 sangat baik digunakan untuk pengamanan *file*.
b. Dengan adanya proses enkripsi pada aplikasi pengamanan *file* dokumen, dokumen soal ujian dapat terjaga keamanan dan kerahasiaannya.
c. Pada proses dekripsi, hasil dari isi *file* dekripsi sama sekali tidak mengalami perubahan dari *file* asli.
d. Dari hasil penelitian yang telah dilakukan bahwa ukuran *file* hasil enkripsi tidak berubah dari *file* asli.
e. Waktu yang diperlukan untuk proses dekripsi pada penelitian yang telah dilakukan lebih lama dibandingkan dengan proses enkripsi, hal ini terjadi akibat proses *invers* memiliki efisiensi yang rendah dan menyebabkan dekripsi AES lebih lambat.
f. Aplikasi ini dirancang sesederhana mungkin agar mempermudah *user* untuk menggunakannya.
g. *File* yang telah terenkripsi tidak dapat dibuka atau dikembalikan seperti sedia kala tanpa *key* yang diinput saat enkripsi.
h. Aplikasi ini hanya digunakan pada *file* dokumen word, excel, dan pdf.
i. Semakin besar ukuran *file* nya maka semakin lama pula waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi.

6. DAFTAR PUSTAKA

[1]. Bendi, Kristoforus Jawa., S Aditya BP. 2012. Implementasi Algoritma Rijndael untuk Enkripsi dan Dekripsi pada Citra Digital. Seminar Nasional Aplikasi Teknologi Informasi 2012(SNATI 2012): 15–16 Juni 2012. Yogyakarta.

[2]. Federal Information Processing Standards Publication(FIPS)197. 2001. Announcing the advanced encryption standard (AES), Nasional Institute of Standards and Technology (NIST), pp. 1–51. [online]. available at : http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf. tgl.akses : 2/8/2016.

[3]. Hanifah, Fadhilah. 2012. Aplikasi Algoritma Rijndael dalam Pengamanan Citra Digital. Skripsi. Depok : Universitas Indonesia.

[4]. J. Daemen and V. Rijmen.2002. The Design of Rijndael : AES - The Advanced EncryptionStandard. Springer-Verlag.

[5]. Pressman, R.S. 2010. Software Engineering : a practitioner's approach. New York: McGraw-Hill.

[6]. Renaldy, Muammar. 2015. Implementasi Kriptografi pada Diary Berbasis Mobile Android dengan Menggunakan Metode AES-128 (Advanced Encryption Standard-128) dan SHA-1 (Secure Hash Algorithm-1). Skripsi. Jakarta : Universitas Budi Luhur.

[7]. Ramdhansya et al. 2014. Implementasi Advanced Encryption Standard (AES) pada Sistem Kunci Elektronik Kendaraan Berbasis Sistem Operasi Android dan Mikrokontroler Arduino. Seminar Nasional Informatika 2014 (semnasIF 2014) 12 Agustus 2014, pp. 92–98, Yogyakarta.

[8]. Staillings, W. 2005. Cryptography and Network Security Principles and Practice 4th Edition. Prentice Hall.