IMPLEMENTASI ALGORITMA ENKRIPSI AES 256 DAN VIGENERE CIPHER UNTUK MENGAMANKAN DOKUMEN DIGITAL PADA APLIKASI PENYIMPAN DAN BERBAGI DOKUMEN DIGITAL BERBASIS WEB

Muhammad Rahman Saleh[1)], Windarto[2)]
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan, 12260
Telp. (021)5853753, Fax. (021)5866369
E-mail : rahman9600@gmail.com [1)], windarto@budiluhur.ac.id [2)]

ABSTRAK

Salah satu kegiatan menggunakan teknologi yang sering digunakan saat ini adalah laptop atau personal computer oleh guru untuk proses belajar dan dalam berbagai format antara lain microsoft word, microsoft power point atau pdf dan disimpan dalam media penyimpanan laptop atau personal computer. Namun jika seorang guru memerlukan materi pembelajaran terbaru akan tetapi guru tersebut tidak memilikinya, maka proses belajar mengajar menjadi terhambat. Selain itu dengan menyimpan dalam media penyimpanan laptop atau personal computer dapat terjadi pencurian atau pengaksesan dokumen oleh pihak yang bertujuan kurang baik. Oleh karena itu, untuk menyelesaikan permasalahan guru tersebut dapat digunakan teknologi cloud sebagai media berbagi pakai materi pembelajaran dan untuk menyimpan berbagai dokumen milik guru tersebut. Untuk meningkatkan keamanan file dan data yang disimpan dalam cloud dapat digunakan teknik kriptografi. Dalam teknik kriptografi beberapa algoritma yang dapat digunakan dalam penelitian ini yaitu algoritma AES 256 dan algoritma Vigenere Cipher. Algoritma AES 256 akan digunakan untuk mengamankan dokumen-dokumen yang disimpan dan Vigenere Cipher akan digunakan untuk mengamakan data-data dan log dari guru ketika menggunakan aplikasi cloud ini. Dengan adanya aplikasi cloud ini diharapkan dapat membantu guru untuk saling berbagi pakai materi pembelajaran dan dapat membantu mengamakan dokumen-dokumen mililk guru dari pihak yang memiliki tujuan kurang baik.

Kata Kunci : Cloud, Berbagi Pakai, Penyimpanan, AES 256, Vigenere Cipher

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin pesat dan semakin canggih memunculkan banyak ide-ide baru yang sebelumnya tidak terbayangkan. Salah satunya adalah teknologi cloud atau komputasi awan yang digunakan untuk menyimpan file digital baik program, surat, foto, video, audio, chat dan lain-lain. Disebut cloud dikarenakan sifat awan yang flexibel dan dapat bergerak kemana saja. Dengan adanya cloud maka dapat menyimpan file baru atau mengakses file yang tersimpan dimana saja dengan berbagai perangkat baik smartphone, tablet, laptop, atau personal computer

SMK Muhammadiyah 2 Tangerang merupakan Sekolah Menengah Kejuruan yang mengembangkan keahlian dalam bidang Teknologi Informasi. Untuk kegiatan belajar mengajar, salah satu metode yang digunakan guru pada SMK Muhammadiyah 2 Tangerang adalah menggunakan materi berbentuk digital yang disimpan dalam format Microsoft Word, Microsoft Power Point atau PDF dan disimpan dalam media penyimpanan pribadi. Permasalahan yang timbul adalah jika guru memerlukan materi pembelajaran terbaru untuk kegiatan belajar mengajar yang tidak dimiliki guru tersebut, maka proses belajar mengajar menjadi terhambat. Selain itu dengan metode penyimpanan tersebut dapat terjadi pencurian atau pengaksesan dokumen yang disimpan pada media penyimpanan pribadi seperti soal UTS yang belum saatnya dibagikan atau kunci jawaban UTS oleh pihak yang bertujuan kurang baik.

Teknologi yang mampu menyimpan file baru,mampu memberikan akses file yang telah tersimpan dimana saja dengan berbagai perangkat dapat digunakan sebagai media berbagi dokumen materi pembelajaran terbaru antar guru dan media untuk menyimpan dokumen seperti soal UTS atau kunci jawaban UTS milik guru. Namun keamanan terhadap dokumen yang disimpan didalam cloud rentan masih dapat dibobol oleh pihak yang memiliki pemahaman mengenai cloud diatas rata-rata namun memiliki tujuan yang kurang baik. Maka digunakan teknik kriptografi untuk mengamankan dokumen tersebut. Untuk semakin menigkatkan keamanan data guru dan log guru yang disimpan di dalam cloud. Maka digunakan kembali teknik kriptografi untuk mengamakan data guru dan log guru.

Dalam penelitian ini teknik kriptografi pertama yang akan digunakan adalah teknik AES 256 dan untuk teknik kriptografi kedua adalah Vigenere Cipher. Kriptografi dibagi menjadi 2 proses yaitu proses enkripsi dan dekripsi. Dengan menggunakan kunci yang unik dan perhitungan

aritmatika yang rumit dalam proses enkripsi, maka tingkat kesulitan untuk memecah kerahasiaan dari suatu teknik kriptografi akan semakin tinggi.

1.2 Masalah

Berdasarkan latar belakang diatas, maka dapat disimpulkan permasalahan dalam penelitian tugas akhir ini sebagai berikut:

a. Belum terdapatnya media penyimpanan terpusat untuk berbagi pakai materi pembelajaran pada SMK Muhammadiyah 2 Tangerang.
b. Ancaman pencurian atau pengaksesan terhadap dokumen milik guru seperti soal UTS yang belum saatnya dibagikan atau kunci jawaban yang disimpan dalam media penyimpanan pribadi guru oleh pihak yang tidak berhak mengakses dokumen tersebut.

1.3 Tujuan Penelitian

Berdasarkan permasalahan yang didapat sebelumnya, maka tujuan yang akan diharapkan dari penelitian tugas akhir sebagai berikut:

a. Membangun aplikasi yang dapat digunakan oleh guru untuk saling berbagi pakai dokumen digital dengan lebih mudah.
b. Menerapkan algoritma enkripsi yang dapat mengamankan dokumen digital milik guru yang akan disimpan dalam aplikasi seperti soal UTS yang belum saatnya dibagikan atau kunci jawaban dari pihak yang bertujuan kurang baik.

1.4 Batasan Masalah

Adapun batasan masalah pada penelitian tugas akhir ini adalah:

a. Aplikasi yang dikembangkan hanya dapat diakses oleh Guru dan Kepala Sekolah.
b. Aplikasi yang dikembangkan hanya dapat menyimpan dokumen dengan format dokumen adalah .txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx dan .pdf.
c. Aplikasi yang dikembangkan hanya dapat menyimpan dokumen berukuran kurang dari 1 MB.
d. Aplikasi yang dikembangkan mengimplementasikan algoritma Kriptografi AES 256 dan Vigenere Cipher.
e. Aplikasi yang dikembangkan memerlukan koneksi internet sebagai media perantara dengan pengguna.

2. DASAR TEORI

2.1 Kriptografi

a. Pengertian Kriptografi

Istilah kriptografi berasal dari bahasa yunani, yaitu kata *Crypto* dan *Grapho* yang masing-masing berarti rahasia dan menulis. Secara umum kriptografi dapat diartikan yakni ilmu/teknik/seni yang menjaga suatu tulisan/informasi. Namum kriptografi lebih dari sekedar menulis rahasia namum kearah teknik-teknik bagaimana merahasiakan tulisan tersebut.

Tentu apabila sebuah tulisan dirahasiakan diperlukan suatu teknik yang mengembalikan tulisan rahasia menjadi tulisan asli kembali.

Istilah yang paling sering disebut dalam teknik bagaimana merahasiakan tulisan disebut proses enkripsi sedangkan teknik bagaimana mengembalikan tulisan rahasia menjadi tulisan aslinya ialah proses dekripsi.

b. Kriptografi simetris

Salah satu teknik proses enkripsi ialah menggunakan suatu kunci. Kriptografi simetris menggunakan kunci yang sama dalam proses enkripsi dan dekripsi.

Menurut Massandy [2] Keuntungan teknik ini adalah pada kuncinya tersebut semakin rumit kuncinya maka akan semakin sulit dipecahkan oleh pihak lain. Namun kekurangannya ialah pada kuncinya sendiri, apabila kunci dapat diterka oleh pihak lain maka kerahasiaan tulisan dapat terancam

c. Kriptografi asimetris

Algoritma asimetris menggunakan kunci yang berbeda pada proses enkripsi dan dekripsi. Hal ini merupakan pengembangan dari teknik kriptografi simetris. Kunci yang digunakan dalam proses enkripsi disebut kunci publik (*public key*). Sedangkan kunci yang digunakan dalam proses dekripsi adalah kunci rahasia (*private key*).

Secara garis besar teori yang dapat ditarik adalah hanya pihak yang benar-benar tertuju yang dapat mengembalikan tulisan rahasia menjadi tulisan asli.

d. Algoritma transposisi

Menurut Munir [3] dalam kriptografi transposisi *plaintext* tetaplah sama akan tetapi urutannya berubah. Teknik ini hanya mengubah urutannya. Keuntungan kriptografi ialah tidak menggunakan kunci dalam proses enkripsi dan dekripsinya.

e. Algoritma substitusi

Teknik yang digunakan dengan mengganti / menyulin / mensubstitusi setiap karakter dengan karakterlain dalam susunan abjad / alfabet. [3]

Berdasarkan hasil enkripsinya, algoritma substitusi dibagi kembali menjadi 3 bagian yaitu:

1) Monoalphabetic Substitusion Cipher

Tenik satu karakter di diganti *plaintext* dengan satu karakter yang bersesuaian. Kesimpulannya ialah

fungsi enkripsinya adalah fungsi satu ke satu

2) Homophonic Substitusion Cipher

Menurut Munir [3] *Homophonic Substitusion* Cipher atau cipher substitusi homofinik seperti cipher abjad tunggal,kecuali bahwa setiap karakter dalam dapat plaintext dipetakan kedalam salah satu dari karakter yang mungkin.

3) Polyalphabetic Substitusion Cipher

Menurut Munir [3] *Polyalphabetic Substitusion* Cipher atau cipher abjad majemuk adalah bentuk cipher yang melibatkan penggunaan kunci yang berbeda-beda tergantung pada suatu periode.

Periode yang dimaksudkan baik itu putaran kunci yang sesuai dengan jadwal. Keuntungan kriptografi ini adalah penggunaan periode pada kunci yang menyebabkan kunci lebih sulit diterka oleh pihak lain.

2.2 AES 256

a. Pengertian AES 256

Ukuran data yang dapat masuk dalam algoritma AES adalah sebesar 128 *bit* yang disebut sebagai *state*. Sedangkan panjang kunci yang digunakan berkisar dari 128 bit, 192 bit atau 256 bit.

Masing-masing panjang kunci akan mempengaruhi terhadap banyaknya putaran yang akan dilalui oleh *state* tersebut.

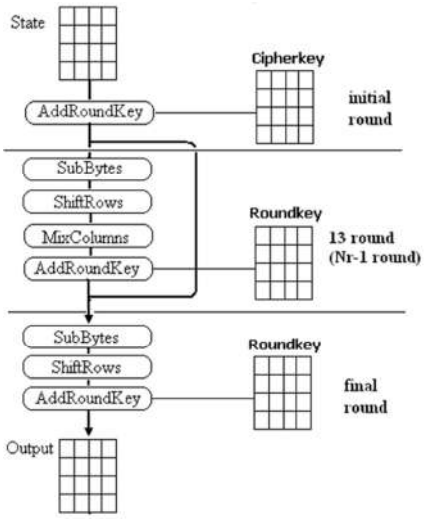
Tabel 1 : Putaran Terhadap State Pada Algoritma Aes [1]

Tipe	Panjang Kunci	Panjang Blok Input	Jumlah Putaran
AES-128	128 bit	128 bit	10
AES-192	192 bit	128 bit	12
AES-256	256 bit	128 bit	14

b. Enkripsi AES 256

Untuk proses enkripsi AES terdiri dari 4 bagian yaitu *SubByte*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Sebelum masuk tahap putaran, *state* akan melalui tahap *AddRoundKey* lalu masuk kedalam tahap putaran yaitu *SubByte*, *ShiftRows*, *MixColums*, dan *AddroundKey* lagi sebanyak jumlah putaran.

Proses putaran ini disebut *Round Function*. Pada putaran terakhir tidak dilakukan tahap *MixColums* . [1].



Gambar 1 : Proses enkripsi aes [1]

1) AddRoundKey

Sebelum masuk kedalam putaran atau putaran pertama, transformasi *AddRoundKey* akan dilakukan dengan kunci utama. Sedangkan dalam putaran yang lain menggunakan kunci putaran (*RoundKey*).

Proses *AddRoundKey* didefinisikan sebagai operasi XOR antara *state*/*array* dengan kunci/*round key*. Operasi XOR dilakukan pada tiap-tiap *byte* dalam state sehingga menghasilkan *byte* baru yang mengganti *byte* lama. Maka pada *state* tidak akan terjadi perubahan ukuran yakni tetap digambarkan 4x4.

2) SubBytes

Transformasi *SubByte* mengganti/mensubstitusi pada *byte-byte* dari *state* dengan *byte* pada tabel S-Box. Tabel S-Box dapat dilihat pada gambar 2.5.

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

Gambar 2 : S-box [1]

Cara pensubstitusinya adalah memecah byte menjadi 2 bagian

misal a dan 9. Perpotongan nilai a dan 9 yang akan digunakan sebagai substitusi pada *byte* dalam *state*..

3) ShiftRows

Transformasi *ShiftRows* dilakukan dengan melakukan pergeseran searah dan memutar pada state. Jumlah pergeseran bergantung kepada nilai baris(r).

4) MixColumns

Transformasi *MixColumns* merupakan kekuatan utama dari AES dan tahap yang paling sulit diantara tahap-tahap lainnya.

Prinsip *MixColumns* adalah difusi atau prinsip menyebarkan pengaruh satu bit *plaintext*/kunci sebanyak mungkin terhadap *ciphertext*.

Teknik *MixColumns* ialah mengalikan setiap kolom dari *array*/*state* dengan polinom a(x) mod (x4+1). Setiap kolom diperlakukan sebagai polinom 4 suku pada GF(28). Polinom a(x) yang ditetapkan pada persamaan 1.

a (x) = {03}x3 + {01} x2 + {01} x + {02} (1)

c. Dekripsi AES 256

Pada proses dekripsi AES dilakukan dengan metode terbalik pada tiap-tiap tahapnya dibandingkan pada proses enkripsi AES. Masing-masing tahap pada proses dekipsi AES adalah *InvSubBytes*, *InvShiftRows*, *InvMixColumns*, dan *AddRoundKey*.

2.3 Vigenere Cipher

Proses enkripsi dan dekripsi pada Vigenere Cipher dilakukan per karakter. Apabila suatu pesan yang dimasukkan lebih panjang daripada panjang kuncinya maka penggunaan kunci akan diperulang sampai seluruh pesan mendapatkan huruf kunci. Sebelum dilakukan enkripsi dan dekripsi, setiap karakter akan dikonversi menjadi angka dengan ketentuan dari tabel ASCII *(American Standart Code for Information Interchange*).

Secara matematis, proses enkripsi pada Vigenere Cipher adalah :

Ci = (Pi + Ki)mod 26

Sedangkan untuk proses dekripsi adalah :

Pi = (Ci – Ki)mod26 jika Ci-Ki > 0

Pi = ((Ci - Ki)+26)mod26 jika Ci-Ki < 0

Keterangan :

C = *Ciphertext* (Pesan yang telah disandikan)

P = *Plaintext* (Pesan yang belum disandikan / pesan asli)

K = Kunci

3. ANALISA MASALAH DAN RANCANGAN PROGRAM

3.1 Analisa Permasalahan

Salah satu kelebihan menggunakan materi pembelajaran digital adalah dapat dipresentasikan dalam berbagai bentuk. Soal Ujian Tengah Semester (UTS) dapat pula dibangun dalam bentuk digital sehingga mempermudah guru dalam mengedit soal. Kelebihan lainnya yaitu dapat disimpan dalam berbagai media penyimpanan pribadi milik guru baik laptop atau *personal computer* atau perangkat lain seperti *smartphone*.

Namun permasalahan yang timbul adalah jika guru memerlukan materi pembelajaran terbaru untuk kegiatan belajar mengajar yang tidak dimiliki guru tersebut menyebabkan proses belajar mengajar menjadi terhambat. Selain itu dengan menyimpan pada media penyimpanan pribadi, soal UTS yang belum saatnya dibagikan atau kunci jawaban UTS dapat dimungkinkan terjadinya pencurian atau pengaksesan oleh pihak yang bertujuan kurang baik.

3.2 Penyelesaian Masalah

Untuk menyelesaikan permasalahan yang telah diuraikan, diperlukan teknologi yang mampu menyimpan file baru, mampu memberikan akses file yang telah tersimpan dimana saja dengan berbagai perangkat dapat digunakan sebagai media berbagi pakai dokumen materi pembelajaran terbaru antar guru dan media untuk menyimpan dokumen seperti soal UTS atau kunci jawaban UTS milik guru.

Namun keamanan terhadap dokumen yang disimpan didalam *cloud* rentan dicuri oleh pihak yang memiliki pemahaman mengenai *cloud* diatas rata-rata dan memiliki tujuan yang kurang baik. Untuk mengamankan dokumen tersebut, digunakan teknik kriptografi dan digunakan pula teknik kriptografi untuk mengamankan data guru dan *log* guru yang disimpan di dalam *cloud*.

3.3 Perancangan Aplikasi

Aplikasi yang akan dikembangkan adalah sistem penyimpanan dan berbagi materi pembelajaran dengan teknologi cloud dengan mengimplementasikan algoritma kriptografi AES 256 terhadap dokumen yang akan masuk ataupun keluar dalam sistem cloud. Untuk data guru yaitu Nomor Induk Pegawai (NIP), nama, hint dan log guru yakni reference materi tersimpan, nama materi dan yang lainnya akan dienkripsi dengan algortima Vigenere Cipher sebelum akan disimpan dalam database.

Aplikasi yang dikembangkan akan mendukung guru untuk menyimpan

menyimpan dokumen baru serta mengubah, menghapus atau mengunduh kembali dokumen yang telah disimpan sebelumnya. Untuk membagikan dokumen dengan kehendak guru sebagai pemilik dokumen, maka sistem akan menyalin data informasi dokumen yang akan dibagikan sehingga dokumen tersebut dapat dilhat dan diunduh oleh pengguna lain.

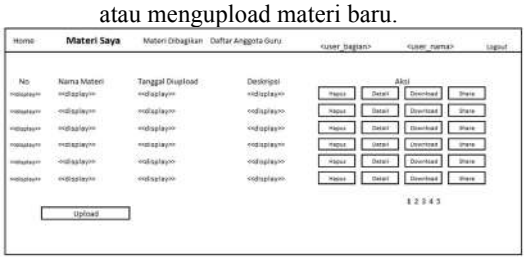
Dengan menerapkan algoritma kriptografi AES 256 pada aplikasi cloud meskipun pihak yang memiliki pemahaman mengenai cloud diatas rata-rata dan tujuan kurang baik dapat mengambil dokumen penting milik guru akan tetapi tidak dapat dimengerti isi dari dokumen tersebut karena telah terenkripsi. Hal yang sama dapat terjadi terhadap data guru dan log dari guru yang akan disimpan dalam database.

Aplikasi yang dikembangkan berbasis web dan akan disimpan dalam sebuah hosting sehingga tidak perlu diinstall. Aplikasi dikembangkan menggunakan bahasa pemrograman PHP dan menggunakan database MYSQL.

3.4 Rancangan Layar

a. Rancangan Layar Form Materi Saya

Form Materi saya menampilkan materi-materi yang telah diupload oleh user. Dalam form ini user dapat melakukan hapus,ubah,download materi yang telah diupload ke dalam aplikasi atau mengupload materi baru.



Gambar 3 : Rancangan Layar Form Materi Saya

b. Rancangan Layar Form Upload Materi Baru

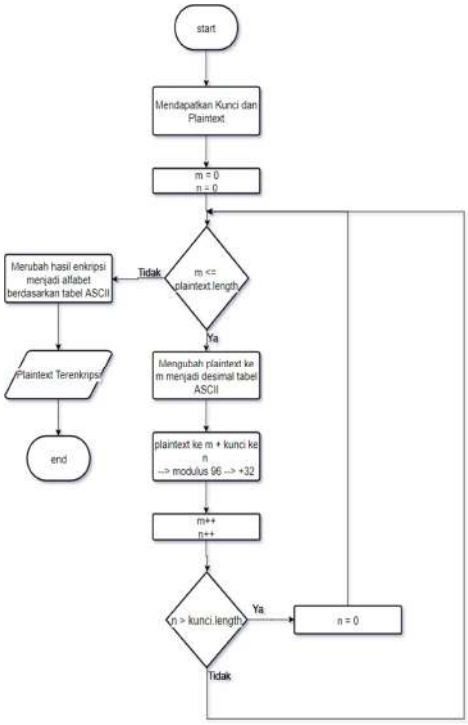
Form Upload Materi digunakan untuk mengupload materi baru untuk guru. Materi yang disimpan bersifat pribadi dan hanya dapat diakses oleh guru yang bersangkutan.

Gambar 4 : Rancangan Layar Form Upload Materi Baru

3.5 Flowchart

a. Flowchart enkripsi Vigenere Cipher

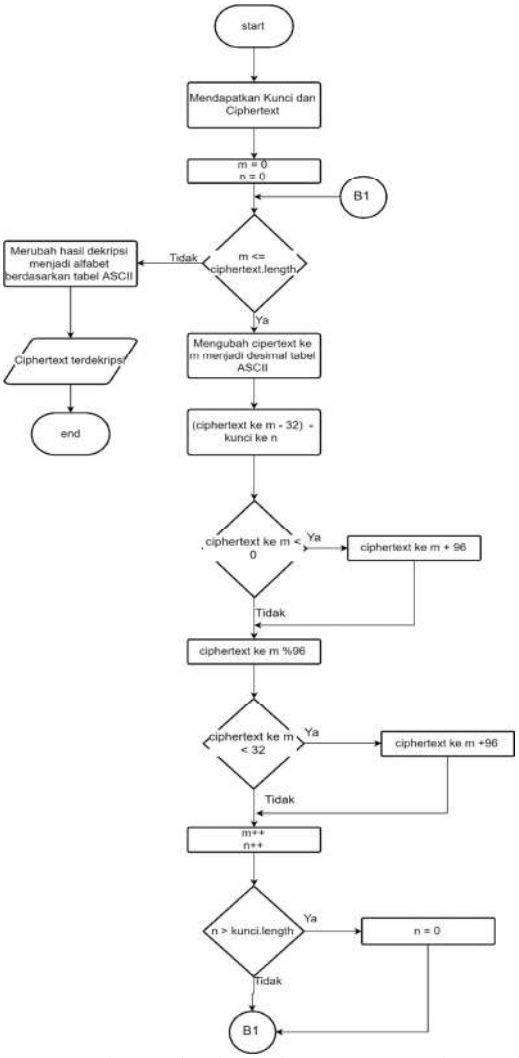
Berikut *flowchart* yang digunakan untuk mengenkripsi informasi yang akan disimpan dalam database.



Gambar 5 : Flowchart Enkripsi Vigenere Cipher

b. Flowchart Dekripsi Vigenere Cipher

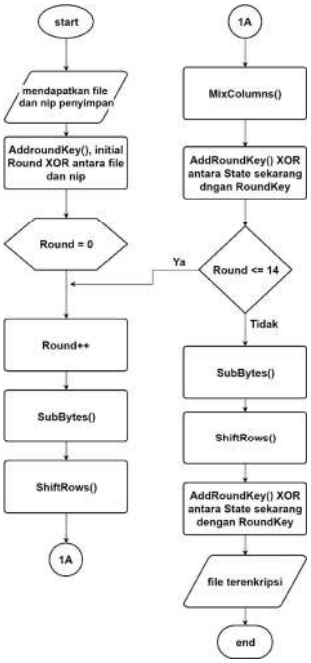
Berikut *flowchart* yang digunakan untuk mendekripsi informasi yang akan dibaca dari dalam database.



Gambar 6 : Flowchart Dekripisi Vigenere Cipher

c. Flowchart Enkripsi AES 256

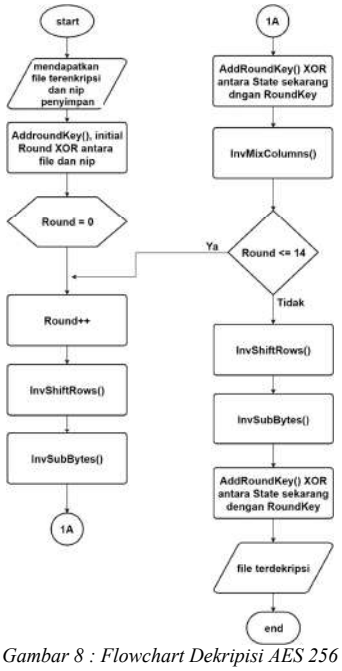
Berikut ini merupakan *flowchart* dari proses enkripsi AES 256 yang digunakan untuk mengenkripsi isi materi yang akan disimpan. Dengan menambahkan nip penyimpan materi sebagai *cipher key* nya.



Gambar 7 : Flowchart Enkripsi AES 256

d. Flowchart dekripsi AES 256

Berikut ini merupakan *flowchart* dari proses dekripsi AES 256 yang digunakan untuk mendekripsi isi materi yang akan didownload. Dengan menambahkan nip penyimpan materi sebagai *cipher key* nya.



Gambar 8 : Flowchart Dekripisi AES 256

4. IMPLEMENTASI DAN ANALISIS HASIL UJI COBA PROGRAM

4.1 Implementasi Program

Pada proses membangun Aplikasi Penyimpanan Dan Berbagi Pakai Materi ini

digunakan hardware dan software sebagai berikut:

a. Spesifikasi Hardaware
   1) Prosessor : Intel® Core i5-6200U CPU @2.30GHz 2.40GHz
   2) RAM : 8 GB
   3) Hardosk : 500 GB

b. Spesifikasi Software
   1) Microsoft Windows 10
   2) Netbeans IDE 8.2
   3) XAMPP v3.2.1

4.2 Tampilan Layar

a. Tampilan Layar Form Materi Saya

Form materi saya menampilan dokumen-dokumen pribadi milik user.

Gambar 9 : Tampilan Layar Form Materi Saya

b. Tampilan Layar Form Materi Dibagikan

Form materi dibagikan menampilkan dokumen-dokumen yang dibagikan untuk seluruh user.

Gambar 10 : Tampilan Layar Form Materi Dibagikan

c. Tampilan Layar Form Uplad Materi Baru

Form upload materi baru digunakan user untuk mengupload dokumen baru.

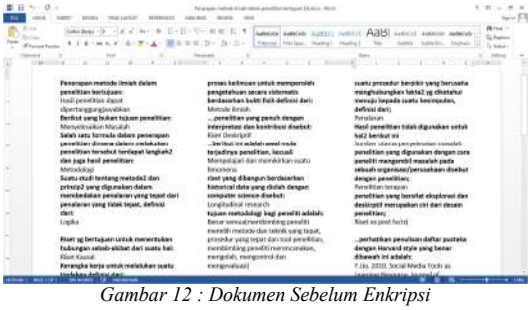
Gambar 11 : Tampilan Layar Form Upload Materi Baru

4.3 Pengujian Program

Pengujian program dilakukan untuk mencari kesalahan-kesalahan pada program dan menjamin fitur utama dapat bekerja sebagaimana mestinya.

a. Dokumen sebelum enkripsi

Dokumen yang sebelum disimpan akan dapat terbaca oleh user dan setelah diunduh maka akan tetap terbaca oleh user.



Gambar 12 : Dokumen Sebelum Enkripsi

b. Dokumen setelah enkripsi

Dokumen yang disimpan dalam aplikasi akan dienkripsi maka tidak dapat dibaca kecuali diunduh oleh user.

Gambar 13 : Dokumen Setelah Enkripsi

4.4 Analisa Hasil Uji Coba Program

Tabel 2 : Nama File Yang Diujicoba

No	Id File	Nama File Asli	Kunci	Nama File Terenkripsi
1	F1	Quis-1411502147-muhammad rahman saleh.xlsx	1nibuk4nkunc1	BCJ5b\{_\j^U"%en/J3U;862CcR6N#CKg/7:6Qi]AY
2	F2	sidang.pptx	1nibuk4nkunc1	d7E#C2">;IF
3	F3	PANDUAN-PENULISAN-SKRIPSI-Gasal-2017-2018.pdf	1nibuk4nkunc1	Ao/f*lB[{z|x=:!"pb~?t%!!~8/T#AX&^\[U!"fo291
4	F4	Soal Kuis untuk 15 januari.docx	1nibuk4nkunc1	D=B.Uvi7>UC1ef9aSjK^/9J/5Z□2P%M
5	F5	mari mengenal kalkulus.txt	1nibuk4nkunc1	^/S+U8Y<2:<$]q9B.@@`C>cB;e

Tabel 3 : Tabel Pengujian

No	Id file	UA	K	UE	DE	DD
1	F1	15 KB	14115021477777777777777777777	20 KB	0.519s	0.456s
2	F2	5312 KB	12345678917777777777777777777	7082 KB	166.732s	167.578s
3	F3	963 KB	97531246807777777777777777777	1284 KB	28.467s	29.451s
4	F4	11 KB	09821327317777777777777777777	15 KB	0.331s	0.437s
5	F5	1 KB	82169163137777777777777777777	1 KB	0.007s	0.004s

Keterangan nama kolom :

1. UA = Ukuran asli file sebelum proses enkripisi
2. UE = Ukuran enkrip file setelah porses enkripsi
3. K = Kunci yang digunakan untuk proses enkripsi dekripsi File

4. DE = Durasi proses enkripsi
5. DD = Durasi proses dekripsi

4.5 Kelebihan dan kekurangan program

a. Kelebihan Program
   1) Mempermudah guru untuk saling berbagi pakai materi pembelajaran.
   2) Melindungi dokumen milik guru seperti soal UTS yang belum saatnya dibagikan atau kunci jawaban dari ancaman pencurian dan pengaksesan dari pihak tidak bertanggung jawab.
   3) Aplikasi Penyimpanan dan Berbagi Pakai Materi ini memiliki interface yang sederhana, bersih dan cukup mudah digunakan.
   4) Aplikasi Penyimpanan dan Berbagi Pakai Materi ini berbasis web sehinga tidak perlu diinstal pada perangkat dan hanya memerlukan konektifitas internet dan browser.
   5) Tidak terjadi perubahan terhadap isi content meskipun melewati proses enkripsi dan dekripsi.

b. Kekurangan Program
   1) Tidak tersedianya fitur pencarian dalam Aplikasi Penyimpanan dan Berbagi Pakai Materi ini sehingga untuk mencari suatu dokumen atau materi tertentu cukup sulit.
   2) Hanya dapat mengunggah satu materi dalam satu waktu.
   3) Tidak dapat berbagi pakai hanya dengan guru tertentu.
   4) Ukuran dokumen yang dapat disimpan hanya 1 MB untuk mempercepat durasi enkripsi dan dekripsi dokumen.
   5) Ekstensi dokumen yang dapat disimpan masih terbatas.
   6) Tidak tersedianya foto profil sebagai identitas pengguna (guru).
   7) Fitur Lupa Password masih sederhana dan tidak dapat mengirim verifikasi menggunakan email.

5. PENUTUP

5.1 Kesimpulan

a. Dengan adanya aplikasi ini, guru-guru pada SMK Muhammadiyah 2 tangerang dapat berbagi pakai materi pembelajaran dengan lebih mudah.
b. Dengan diimplementasikannya algoritma AES 256 pada aplikasi ini, maka dokumen milik guru pada SMK Muhammadiyah 2 Tangerang seperti soal UTS yang belum saatnya dibagikan atau kunci jawaban dapat disimpan lebih aman dan terhindar dari pihak yang memiliki tujuan kurang baik.
c. Proses enkripsi dan dekripsi yang terjadi pada dokumen yang disimpan dalam aplikasi tidak menyebabkan perubahan pada isi dokumen tersebut.

5.2 Saran

Aplikasi Penyimpanan dan Berbagi Pakai ini masih belum sempurna dan masih perlu perbaikan-perbaikan untuk meningkatkan kualitas dari aplikasi ini. Beberapa saran yang penulis dapat diberikan untuk pengembangan berikutnya adalah sebagai berikut:

a. Diharapkan dapat ditambahkan fitur pencarian , sehingga dapat mempermudah pengguna mencari dokumen atau materi tertentu.
b. Diharapkan aplikasi mampu mengunggah beberapa materi dalam satu waktu.
c. Ukuran materi yang dapat disimpan dapat lebih besar dari 1 MB dan tidak ada batasan ekstensi dokumen.
d. Diharapkan aplikasi dapat menambahkan foto profil sebagai identitas pengguna (guru).
e. Diharapkan fitur lupa password pada aplikasi dapat melakukan verifikasi melalui email.

DAFTAR PUSTAKA

[1] Bhaudhayana, G. W. and Widiartha, I. M. (2015) 'Implementasi algoritma kriptografi aes 256 dan metode steganografi lsb pada gambar bitmap', *Jurnal ilmu komputer Universitas Udayana*, 8(2), pp. 15–25.
[2] Massandy, D. T. (2009) 'Algoritma elgamal dalam pengamanan pesan rahasia', *Institut Teknologi Bandung*, pp. 1–5. Available at: www.informatika.stei.itb.ac.id (Accessed : 15 November 2017).
[3] Munir, R. (2004b) 'Algoritma Kriptografi Klasik', in *Kriptografi*, pp. 0–18. Available at: http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/ (Accessed : 15 November 2017).
[4] Roikhatul, H. (2014) *Kriptologi Komputer*, *Hanif Roikhatul J*. Available at: http://hanif-roikhatul-fst12.web.unair.ac.id/artikel_detail-116340-PROKOM 2014-KRIPTOLOGI KOMPUTER.html (Accessed: 25 October 2017).