Volume 10 Number 1. Mei 2020 Page. 25-34
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i1

Article DOI : 10.36350/jbs.v10i1.74
Received: Maret; Accepted : April; Published : Mei

Penerapan Algoritma Advanced Encryption Standard (AES) untuk Pengamanan Berkas Soal Ujian

Binanda Wicaksana[1*], Ma'mun Setiawan[2]
[1]Teknik Informatika/STIKOM Binaniga
Email: binanda@stikombinaniaga.ac.id
[2] Teknik Informatika /STIKOM Binaniga
Email: m4munsetiawan@gmail.com

ABSTRACT

The development of technology at this time is developing rapidly, especially in the increasingly global exchange of information, the ability to access and exchange data or information is very fast, this also greatly affects criminality in the world of technology or also called hackers, namely a person or group intentionally retrieve important information without responsibility. Data security is very important to do especially in school exam questions that are stored on a computer without any special security, so that a method or method for the security process is carried out by applying an advanced encryption standard algorithm for the process of inserting or encrypting questions. So that the security of exam questions will be better protected from irresponsible parties. As a result, the data or exam questions will be more secure and can only be accessed by users who have access rights to the data.

Keywords*: advanced encryption standard; hacker; encryption; data security.*

ABSTRAK

Perkembangan teknologi pada saat ini sangat berkembang dengan pesat khususnya pada pertukaran informasi yang semakin global, kemampuan untuk mengakses serta bertukar data atau informasi sudah sangat cepat, hal ini juga sangat berpengaruh pada kriminalitas di dunia teknologi atau disebut juga hacker yaitu seseorang atau kelompok yang dengan sengaja mengambil informasi penting tanpa tanggung jawab. Pengamanan data sangat penting dilakukan khususnya pada soal-soal ujian di sekolah yang disimpan di komputer tanpa ada pengamanan yang khusus, sehingga dilakukan cara atau metode untuk proses keamanannya dengan cara menerapkan algoritma advanced encryption standard untuk proses penyisipan atau enkripsi soal. Sehingga keamanan soal ujian akan lebih terjaga dari pihak-pihak yang tidak bertanggung jawab. Hasilnya data atau soal ujian akan lebih terjaga kerahasiannya dan hanya dapat diakses oleh pengguna yang memiliki hak akses terhadap data tersebut.

Kata Kunci*: advanced encryption standard, hacker, enkripsi, pengamanan data.*

A. PENDAHULUAN

1. Latar Belakang

Tulisan atau data teks merupakan salah satu media komunikasi yang sering digunakan untuk menyampaikan pesan kepada manusia, dengan kepentingan atau tujuan tertentu seseorang

ingin mengirim pesan atau data yang isinya tidak ingin diketahui orang lain kecuali oleh penerima pesan yang dituju karena isi pesan atau data tersebut sangat rahasia dan pribadi. Kejahatan dalam dunia maya (internet) merupakan hal yang sangat merugikan bagi pengguna internet ataupun penyedia jasa internet tersebut, namun pada kenyataannya banyak kasus pencurian data atau penyadapan data yang sangat rahasia bisa dicuri oleh pihak yang sangat tidak bertanggung jawab yang biasa dikenal dengan sebutan *hacker*.

Untuk menjaga keamanan dan terutama bagi suatu perusahaan, lembaga, institusi atau organisasi yang memiliki data-data yang rahasia dan sangat penting, mereka mengamankan data atau dokumen tersebut agar terhindar dari gangguan orang lain, saat ini kebanyakan orang, instansi atau perusahaan menggunakan aplikasi Microsoft Word untuk membuat dokumen-dokumen penting tersebut, karna sebagian besar sudah terbiasa dengan aplikasi Microsoft Office yang sangat memudahkan siapa saja ketika menggunakan aplikasi ini, pengolah kata Microsoft Word begitu mudah digunakan sehingga siapapun yang menggunakannya akan merasa nyaman dengan pengolah kata ini. Dalam aplikasi Microsoft Office pengolah kata disimpan sebagai file Microsoft Word, pengolah angka sebagai file Microsoft Excel dan sebagainya, memang tidak ada yang aneh dalam sistem penyimpanan seperti ini karena memang sebagian besar di antara kita menggunakan semua aplikasi yang ada pada Microsoft Office. Soal Ujian merupakan salah satu data yang sangat dijaga kerahasiaannya jika belum memasuki waktu ujian. Berkas data yang disimpan di dalam komputer dapat dengan mudah dibuka oleh pihak yang tidak mempunyai wewenang untuk mengakses data tersebut. Untuk mengamankan data penting tersebut dibutuhkan suatu teknik keamanan data, salah satunya dengan menggunakan teknik kriptografi.

Kriptografi adalah sebuah cara untuk mengamankan data. Dalam ilmu kriptografi, ada istilah enkripsi dan dekripsi. Enkripsi adalah teknik merubah suatu data asli menjadi data yang hanya bisa dibaca oleh pembaca yang memiliki kunci (key). Sedangkan Dekripsi merupakan teknik mengembalikan data yang sudah terenkripsi menjadi data semula. Advanced Encryption Standard (AES) merupakan salah satu teknik di dalam ilmu kriptografi.

2. Permasalahan

Dari uraian latar belakang diatas, maka dapat diidentifikasikan masalah dalam penelitian ini adalah:

a. Belum optimalnya tingkat keamanan untuk menjaga kerahasiaan berkas soal ujian
b. Belum adanya aplikasi untuk mengamankan berkas soal ujian

3. Tujuan

Adapun tujuan dari penelitian ini adalah:

a. Meningkatkan keamanan untuk menjaga kerahasiaan berkas soal ujian
b. Merancang aplikasi keamanan data untuk mengamankan berkas soal ujian

4. Tinjauan Pustaka

a. Soal Ujian

Soal Ujian adalah suatu tolak ukur yang digunakan guru untuk mengukur atau mengetahui sejauh mana kemampuan siswanya.

b. Data

Data adalah catatan atas kumpulan fakta, yang berarti hasil pengukuran atau pengamatan suatu variabel yang bentuknya dapat berupa angka, kata-kata atau citra.

c. Kriptografi

Kriptografi adalah Ilmu atau seni untuk menyembunyikan suatu informasi dengan teknik penyandian atau informasi menjadi sandi-sandi yang tidak dimengerti oleh orang lain, selain pembuat dan penerimanya.

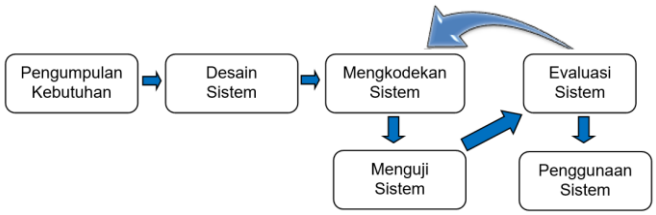
B. METODE

Metode yang digunakan dalam penelitian ini adalah metode eksperimen, dimana peneliti melakukan uji coba terhadap permasalahan tertentu dengan menggunakan teori tertentu dan menghasilkan jawaban yang tepat untuk permasalahan dengan teori yang digunakan.

1. Prosedur Pengembangan

Volume 10 Number 1. Mei 2020 Page. 25-34
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i1

Prosedur pengembangan merupakan langkah-langkah dari proses pengembangan yang dilakukan. Prosedur pengembangan digambarkan pada gambar 1.



Gambar 1. Prosedur Pengembangan

Pada gambar diatas dapat dijelaskan sebagai berikut:

a. Pengumpulan Kebutuhan, yaitu pengumpulan data-data yang diperlukan untuk digunakan sebagai dasar dari pengembangan sistem keamanan soal ujian sekolah.
b. Membangun Prototype, Membangun design prototyping dengan membuat perancangan sementara yang berfokus pada penyajian kepada pengguna.
c. Evaluasi Prototipe, Evaluasi ini dilakukan oleh pengguna, apakah prototyping yang sudah dibangun sudah sesuai dengan keinginan pengguna atau belum. jika sudah sesuai, maka langkah selanjutnya akan diambil jika belum maka akan kebali lagi pada tahap awal.
d. Mengkodekan Sistem, yaitu proses mengcoding untuk membuat suatu sistem.
e. Menguji Sistem, yaitu proses untuk menguji sistem apakah sudah berjalan dengan baik atau masih terdapat beberapa kesalahan pada codingan, lalu dilanjutkan pada langkah berikutnya yaitu evaluasi sistem.
f. Evalusasi Sistem, Pengguna mengevaluasi apakah sistem yang sudah jadi sudah sesuai dengan yang diharapkan . Jika ya, langkah (g) dilakukan; jika tidak, ulangi langkah (d).
g. Penggunaan Sistem, merupakan tahap terakhir dimana pengguna sudah merasa puas dengan sistem yang telah dibuat

2. Uji Coba Produk

Uji coba produk dilakukan dengan maksud untuk mengumpulkan data yang dapat digunakan sebagai dasar peniliaian terhadap tingkat kelayakan dari produk yang dihasilkan. Dalam bagian ini secara berurutan perlu dikemukakan uji coba layanan, subjek uji coba, jenis data, instrumen pengumpulan data dan teknik analisis data.

a. Uji Coba Layanan
   Desain uji coba dengan menggunakan kuesioner, kuesioner diisi oleh ahli IT yang ada di SMK Plus PGRI 1 Cibinong.
b. Subjek Uji Coba
   Subjek uji coba penelitian pengembangan ini yaitu uji coba ahli IT di SMK Plus PGRI 1 Cibinong sebanyak 2 orang yaitu Bapak Nirat, S.Kom sebagai Kepala Program TKJ dan Arga Prahara S.Kom sebagai Koordinator Laboratorium Komputer dan uji coba pengguna kepada para guru mata pelajaran sebanyak 57 guru aktif yang ada di SMK Plus PGRI 1 Cibinong.

3. Jenis Data

Adapun jenis data yang digunakan dalam penelitian ini adalah data kuantitatif yaitu jenis data yang dapat diukur atau dihitung secara langsung, yang berupa informasi atau penjelasan yang dinyatakan dengan bilangan atau berbentuk angka, dalam hal ini data kuantitatif yang diperlukan diantaranya jumlah guru yang aktif, jumlah ahli IT dan hasil angket sedangkan sumber data yang digunakan dalam penelitian ini adalah data primer yaitu data yang dibuat oleh peneliti untuk maksud khusus untuk menyelesaikan permasalahan yang ditanganinya, data dikumpulkan dan dihitung sendiri oleh peneliti dari sumber pertama atau tempat objek penelitian.

4. Instrumen Pengumpulan Data

Dalam pengumpulan data yang akan dilakukan dalam penelitian ini yaitu Kuesioner, Kuesioner merupakan pengumpulan data yang dilakukan dengan cara memberikan pertanyaan tertulis kepada responden untuk dijawabnya.

Volume 10 Number 1. Mei 2020 Page. 25-34
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i1

Teknik pengolahan data pada penelitian pengembangan ini menggunakan pengukuran skala likert. Skala Likert merupakan metode skala bipolar, yang menentukan positif atau negatif respon pada sebuah pernyataan. Skala Likert atau Likert Scale adalah skala penelitian yang digunakan untuk mengukur sikap dan pendapat. Dengan skala likert ini, responden diminta untuk melengkapi kuesioner yang mengharuskan mereka untuk menunjukkan tingkat persetujuannya terhadap serangkaian pertanyaan. Pertanyaan atau pernyataan yang digunakan dalam penelitian ini biasanya disebut dengan variabel penelitian dan ditetapkan secara spesifik oleh peneliti. Nama Skala ini diambil dari nama penciptanya yaitu Rensis Likert, seorang ahli psikologi sosial dari Amerika Serikat.
Tingkat persetujuan yang dimaksud dalam skala Likert ini terdiri dari 5 pilihan skala yang mempunyai gradasi dari Sangat Setuju (SS) hingga Sangat Tidak Setuju (STS). 5 pilihan tersebut diantaranya adalah :

Tabel 1. Tabel Skala Likert

No.	Kategori	Skor
1	Sangat Setuju (SS)	5
2	Setuju (S)	4
3	Ragu-ragu (RG)	3
4	Tidak Setuju (TS)	2
5	Sangat Tidak Setuju (STS)	1

Berikut tabel kuesioner yang digunakan peneliti untuk ahli IT dan Pengguna untuk pengamanan soal ujian di sekolah :

Tabel 2. Kuisoner Ahli IT

No.	**Aktivitas**	**Hasil Yang Diharapkan**	**Taraf Ketercapaian**	
			Ya	**Tidak**
1	User Interface	Tampil Halaman Awal Sistem		
2	Interaksi System	Sistem sangat mudah untuk dipergunakan.		
3	Prosedur Program	User dapat melihat hasil enkripsi dan dekripsi setelah memasukan kata kunci rahasia		
4	Logika Program	Setelah menekan tombol encrypt isi data otomatis terenkripsi.		
5	Ketepatan Informasi	Orang lain tidak dapat melihat isi data setelah di enkripsi		
6	Kekinian Informasi	Setelah data di enkripsi oleh pengguna maka data sudah tidak bisa dilihat secara kasat mata oleh orang lain.		
7	Waktu Respon	Kecepatan waktu yang cepat dalam proses enkripsi dan dekripsi		
8	Keluwesan System	Menu-menu berfungsi dengan baik dan mudah		
9	Keamanan Sistem	Sistem memiliki keamanan yang memadai.		

Tabel 3. Kuisoner Pengguna

No.	**Pertanyaan**	**Pilihan**				
		SS	**S**	**RG**	**TS**	**STS**
Kualitas Keamanan						
1	Saya merasa akan mendapatkan keamanan data yang cukup terjamin					
2	Saya merasa aman membagi data pribadi kepada orang lain.					
3	Saya merasa sistem ini akan memecahkan masalah dari *hackers.*					
4	Saya yakin sistem ini dapat menjaga data pribadi dan dapat diandalkan.					
Kualitas Sistem						
5	Saya merasa setiap menu/fitur berfungsi dengan baik.					
6	Saya merasa sistem ini mudah untuk dipergunakan.					
7	Saya merasa setiap proses membutuhkan waktu yang cepat.					
8	Saya merasa tidak terjadi eror dalam menjalankan sistem ini.					
9	Saya merasa bahasa dalam sistem ini mudah untuk					

	dimengerti.					
10	Saya merasa sistem ini sangat perlu untuk dipergunakan.					
Kualitas Layanan						
11	Saya merasa dengan menggunakan sistem ini akan menjamin data pribadi lebih aman.					
12	Saya merasa sistem ini yang dibutuhkan untuk keamanan data.					
Kemudahan Pengguna						
13	Saya belajar menggunakan sistem ini dengan baik dan cepat.					
14	Saya mudah mengingat menggunakan sistem ini.					
15	Saya merasa instruksi sistem ini jelas dan mudah dimengerti.					
Kepuasaan Pengguna						
16	Saya puas dengan sistem yang telah dibuat.					
17	Saya akan terus memakai sistem ini untuk selanjutnya.					
Keuntungan Pengguna						
18	Saya merasa setiap proses membutuhkan waktu yang singkat					
19	Saya merasa pengiriman data lebih epektif.					
20	Saya berharap menu dan fitur ditambah lagi.					

5. Teknik Analisa Data

Analisis data adalah proses mencari dan menyusun secara sistematis data yang diperoleh dari hasil wawancara, catatan lapangan, dan bahan-bahan lain, sehingga dapat mudah dipahami, dan temuannya dapat diinformasikan kepada orang lain (Bogdan dalam Sugiyono, 2013:244). Teknik analisis yang digunakan pada penelitian pengembangan ini disesuaikan dengan jenis i nstrumen yang dikumpulkan. Analisis data ini menggunakan teknik analisis deskriptif, data yang diperoleh melalui kuesioner dengan analisis deskriptif akan diuraikan secara naratif. Jenis data yang diperoleh dari hasil uji kelayakaan (Validasi) oleh pengguna yaitu data kuantitatif, data kuantitatif berupa angka-angka mulai dari 1 hingga 5 berdasarkan skala likert yang kemudian akan di presentasekan.

Teknik analisis data yang digunakan untuk menganalisis data hasil penilaian kelayakan adalah dengan teknik analisis deskriptif. Adapun teknik deskriptif presentase yang akan digunakan, dapat dituliskan sebagai berikut:

$$\textbf{Persentase kelayakan (\%)} = \frac{Skor\ yang\ diobservasi}{Skor\ yang\ diharapkan} x\ 100\ \%$$

Jenjang kualifikasi kriteria kelayakan untuk menyimpulkan hasil validasi adalah sebagai berikut :

Tabel 4. Konversi Tingkat Pencapaian

Tingkat Ketercapaian	Kualifikasi
90%-100%	Sangat Layak
75%-89%	Layak
65%-74%	Cukup Layak
55%-64%	Kurang Layak
0%-54%	Tidak Layak

C. HASIL DAN PEMBAHASAN

1. HASIL

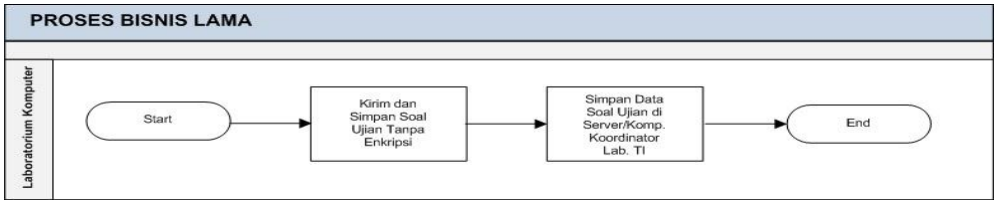
a. Pengumpulan Kebutuhan

Pengumpulan kebutuhan merupakan kegiatan yang dilakukan dalam rangka mengumpulkan kebutuhan-kebutuhan untuk mengembangkan sistem, berikut ini teknik pengumpulan data yang dilakukan :

1) Pengumpulan Dokumen
Pengumpulan dokumen dilakukan untuk memenuhi kebutuhan dalam mengidentifikasi sebuah sistem, dokumen-dokumen tersebut berasal dari bagian Wakil Kepala Sekolah bidang Kurikulum dan Koordinator Laboratorium IT SMK Plus PGRI 1 Cibinong.

Volume 10 Number 1. Mei 2020 Page. 25-34
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i1

2) Wawancara
Wawancara dilakukan dalam rangka mempelajari bagaimana proses pembuatan sistem dan proses pengiriman atau penyimpanan soal ujian siswa-siswi SMK Plus PGRI 1 Cibinong yang terjadi, wawancara dilakukan kepada Wakil Kepala Sekolah Bidang Kurikulum, Koordinator Laboratorium IT dan Guru Mata Pelajaran, adapun sistem yang sedang berjalan adalah sebagai berikut :



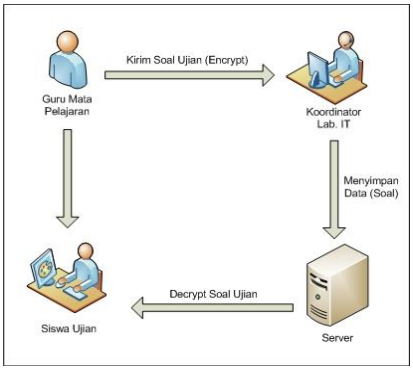
Gambar 2. Proses Bisnis Lama

Gambar 2. mendefinisikan bahwa proses pengiriman kepada koordinator laboratorium komputer dan penyimpanan soal ujian tanpa atau tidak menggunakan enkripsi sehingga tidak ada pengamanan apabila ada orang yang tidak bertanggunggung jawab mencuri soal ujian tersebut.

b. Perancangan

Perancangan merupakan proses penggambaran, perencanaan, dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh dan berfungsi sebagai perancangan sistem dapat dirancang dalam bentuk bagan alir system yang merupakan alat bentuk grafikyang dapat digunakan untuk menunjukan urutan-urutan proses dari sistem.

1) Proses Bisnis
Berikut adalah gambaran proses bisnis untuk sistem keamanan data untuk soal ujian di sekolah, dapat dilihat pada gambar berikut :



Gambar 3. Proses Bisnis Baru

Gambar 3 mendefinisikan bahwa proses bisnis baru diawali dengan seorang guru mata pelajaran yang sudah membuat soal untuk ujian maka soal tersebut dienkripsi dulu sebelum dikirimkan ke koordinator lab. IT, setelah dikirim ke koordinator lab. IT kemudian soal ujian divalidasi dan disimpan didalam server ujian, kemudian pada hari pelaksanaan ujian soal akan di dekripsi oleh koordinator lab. IT agar siswa-siswi bisa langsung melaksanakan ujian.

2) Prosedur enkripsi dan dekripsi dengan algoritma advanced encryption standard (AES)
Algoritma *Advanced Encryption Standard (*AES) adalah suatu algoritma *block chiper* dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi, Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (National Institute of Standard and Technology) sebagai pengganti algoritma DES (Data Encryption Standard) yang sudah berakhir masa penggunaannya. Algoritma AES adalah algoritma kriptografi yang dapat

mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit, Perbedaan dari ketiga urutan tersebut adalah panjang kunci yang mempengaruhi jumlah *round* (perputaran) yang dapat digambarkan dalam bentuk tabel.

Tabel 5. Urutan data Algoritma AES

	Panjang Kunci	Panjang Blok	Jumlah Putaran
AES 128	4	4	10
AES 192	6	4	12
AES 256	8	4	14

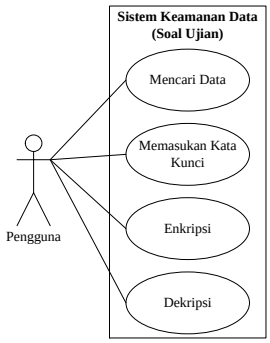
Tabel 5 mendefinisikan mengenai tipe dari algoritma AES dengan panjang kunci, panjang blok dan jumlah putaran yang berbeda-beda. Untuk penelitian ini digunakan AES-128 bit dengan jumlah putaran enkripsi sebanyak 10 kali.

Berikut langkah-langkah atau prosedur proses enkripsi algoritma aes 128 :

a) *Addroundkey* : Pada tahap ini pesan yang dikirim (*plain text*) akan di XOR kan dengan cipher key. Tahap ini disebut juga dengan *Initial round.*
b) *Round* : Selanjutnya akan dilakukan putran sebanyak Nr-1 kali.
c) Final Round : untuk putaran ke Nr, dilakukan tahap-tahap yang sama dengan *round* namun tidak melalui proses *Mixcolumns*.

3) Use Case Diagram

Use case atau diagram *use case* menggambarkan kelakuan (*behavior*) sistem informasi yang akan dibuat. *Use case* mendekripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat. Secara kasar, *use case* digunakan untuk mengetahui apa saja yang ada di dalam sebuah sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi itu (Sugiarti, 2013 : 41). Use case tidak menjelaskan secara detail tentang penggunaan usecase tetapi hanya memberikan gambaran singkat hubungan antara usecase, actor dan sistem. Aplikasi yang dikembangkan memiliki satu aktor yaitu guru mata pelajaran (user) seperti gambar berikut :

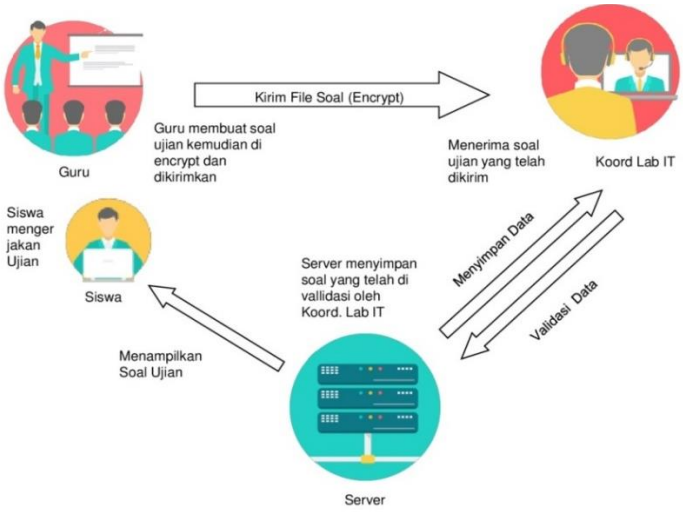


Gambar 4 Use Case Diagram

c. Membangun Prototyping

Membangun *prototyping* disini berfokus pada skema keamanan soal ujian, berikut ini merupakan contoh gambar skema keamanan soal ujian yang akan berjalan.

Volume 10 Number 1. Mei 2020 Page. 25-34
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i1



Gambar 6. Skema Keamanan Soal Ujian

Gambar 6 mendefinisikan bahwa pengamanan soal ujian pada penelitian ini bertujuan untuk memberikan kemanan soal ujian pada pengguna dalam mengirimkan atau menyimpan soal ujian tersebut, pengguna disini adalah guru mata pelajaran yang terdapat di SMK Plus PGRI 1 Cibinong, dengan menerapkan keamanan soal ujian guru mata pelajaran tidak perlu lagi untuk khawatir dengan keamanan soal ujiannya dalam mengirimkan atau menyimpan soal ujian tersebut, cukup dengan mengakses sistem kemanan data yang telah ada dengan key yang sangat rahasia maka soal ujian akan terenkrip dan soal ujian akan tidak akan mudah di lihat secara kasat mata dan tidak bisa digunakan.

Skema keamanan soal ujian di mulai dengan guru mata pelajaran mengakses sistem keamanan data untuk memulai proses enkripsi soal yang telah dibuat, berikut gambar aplikasi sistem keamanan data soal ujian :

Gambar 7. Sistem Keamanan Data

Gambar 8. Tampilan File Soal Yang Sudah Terenkripsi

Dalam prosesnya dan soal yang sudah terenkripsi tidak akan bisa dibaca secara kasat mata bahkan tidak akan bisa digunakan oleh penggunanya apabila belum di dekripsi kembali soal ujian tersebut, Gambar 8 merupakan tampilan soal ujian yang bertipe (doc) yang sudah di enkripsi menggunakan aplikasi keamanan data.

2. PEMBAHASAN

Data yang diperoleh melalui instrumen penelitian ini di uji dengan menggunakan statistik dekriptif kuantitatif dimaksudkan untuk menggambarkan karakteristik data pada masing-masing variabel. Hasil presentase digunakan sebagai jawaban atas kelayakan dari aspek-aspek yang diteliti dengan hasil angket dijumlahkan berdasarkan poin-poin jawaban lalu

Volume 10 Number 1. Mei 2020 Page. 25-34
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i1

dibandingkan dengan jumlah yang diharapkan untuk memperoleh presentase berikut hasil kelayakan presentase dalam penelitian ini.

Tabel 6 Hasil kuesioner Ahli IT

Item Pertanyaan	(%) Jawaban YA	(%) Jawaban TIDAK
P1	2	0
P2	1	1
P3	2	0
P4	2	0
P5	2	0
P6	2	0
P7	2	0
P8	1	1
P9	2	0
Total	**16**	**2**

Persentase kelayakan (%) = 16/18 x 100 % = 88,88 %
Dengan persentasi yang didapat sebesar = 88,88 % dikategorikan “Layak”

Tabel 7. Presentase kelayakan

Aspek penilaian	Skor observasi	Skor yang diharapkan	Kelayakan
Kualitas Keamanan	983	1140	86,22%
Kualitas Sistem	1470	1710	85,96%
Kualitas Layanan	485	570	85,08%
Kemudahan Pengguna	749	855	87,60%
Kepuasaan Pengguna	471	570	82,63%
Keuntungan Pengguna	728	855	85,14%
Total	4886	5700	85,71%

Pada Tabel diatas Persentase yang didapat sebesar 85,71%, maka Penelitian tentang keamanan data dapat dikategorikan **“Layak”**.

D. KESIMPULAN

Berdasarkan hasil dari mulai penelitian, perancangan sampai implementasi, kesimpulan yang bisa diuraikan antara lain :

1. Berdasarkan pada hasil penelitian yang telah dilakukan dapat disimpulkan bahwa penerapan algoritma advanced encryption standard untuk pengamanan soal ujian menjadi lebih aman, waktu yang dibutuhkan dalam proses enkripsi juga lebih cepat dan pengguna juga bisa menggunakan sistem ini dimanapun sehingga tidak perlu datang ke sekolah.
2. Dari hasil data kuesioner pengguna, penerapan algoritma advanced encryption standard pada keamanan soal ujian sekolah berfungsi dengan baik dan dinyatakan layak dengan nilai persentase kelayakan sebesar 85,71 %.
3. Berdasarkan uji coba yang telah dilakukan, aplikasi sistem keamanan data ini berhasil mengimplementasikan proses enkripsi dan dekripsi untuk mengamankan file. Hal ini dibuktikan melalui pengujian yang telah dilakukan bahwa semua file yang di emkripsi dengan sistem keamanan data dapat dikembalikan ke file semula dalam proses dekripsi dan file tidak mengalami perubahan serta berhasil untuk pengiriman maupun untuk diri sendiri.
4. Dari hasil data kuesioner ahli sistem informasi aplikasi keamanan data yang telah dibuat berjalan dengan baik dan dinyatakan layak dengan nilai persentase kelayakan sebesar 88,88 %.

E. DAFTAR RUJUKAN

[1] A. Permana And D. Nurnaningsih, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," Vol. 11, No. 2, 2018.

[2] Harbani, Arif, and Muhamad A. Fahreza. "Aplikasi Keamanan Data Gambar Menggunakan Algoritma RSA (Rivest Shamir Adleman) Berbasis Desktop." *Teknois*, vol. 9, no. 1, May. 2019, pp. 1-9, doi:10.36350/jbs.v9i1.1.

[3] J. I. Mulawarman Et Al., "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks , Isi File Dokumen , Dan File Dokumen Menggunakan Algoritma Advanced Encryption," Vol. 10, No. 1, 2015.

[4] Kriptografi Algoritma Advanced Encryption Standard Dan Pengecekan Error Detection Cyclic Redundancy Check," No. October 2015, 2016.

[5] M. Caesar, C. Dan, And O. Xor, "Perancangan Aplikasi Enkripsi Dekripsi Menggunakan Metode Caesar Chiper Dan Operasi Xor," Vol. 2, No. 1, Pp. 72–80, 2018.

[6] P. Handoko And M. Kom, "Keamanan Data Menggunakan Kriptografi Dengan Algoritma Vigenere Cipher Dan Steganografi Dengan Metode End Of File (Eof) Teknik," Pp. 1–7.

[7] S. Musirawas, "Implementasi Keamanan Data Menggunakan Algoritma," Vol. 8, No. 1, Pp. 251–264, 2017.

[8] S. Musirawas, "Penerapan Algoritma Asimetris Rsa Untuk Keamanan Data Pada Aplikasi Penjualan Cv . Sinergi Computer Lubuklinggau," Vol. 9, No. 2, 2018.

[9] Sajati, N. Dewi, J. T. Informatika, S. Tinggi, And T. Adisutjipto, "Penerapan Sistem Keamanan Menggunakan Cryptography Pada Aplikasi Chatting Dengan," Pp. 61–74.

[10] Sutisna, "Enkripsi Data Melalui Keamanan Model," Vol. 1, No. 2, Pp. 62–70,2016.

[11] T. J. Pattiasina And M. Kom, "Rancang Bangun Aplikasi Enkripsi Dan Dekripsi Email Dengan Menggunakan Algoritma Advanced Encryption Standard Dan Knapsack," Pp. 1–10.

[12] Wandani, M. A. Budiman, M. C. Sc, A. S. S. Si, And M. Kom, "Implementasi Sistem Keamanan Data Dengan Menggunakan Teknik Steganografi End Of File (Eof) Dan Rabin Public Key Cryptosystem."