4th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
27 Maret 2024 – Jakarta, Indonesia
Volume 3, Nomor 1, April 2024 - ISSN 2962-8628 (*online*)

APLIKASI KRIPTOGRAFI BERBASIS *WEB SYSTEM* MENGGUNAKAN ALGORITMA AES-128 UNTUK KEAMANAN FILE UJIAN SISWA SMK CENGKARENG 1 JAKARTA

Peri Rusyandi[1], Rizky Pradana[2*]

[1,2] Sistem Informasi, Fakultas Teknologi Informasi, Universitas Budi Luhur, Kota Tangerang, Indonesia
Email: [1]perirusyandi2@gmail.com,[2*]rizky.pradana@budiluhur.ac.id

Abstrak- Kemajuan teknologi informasi saat ini telah berkembang dengan pesat dan cepat, khususnya pada sektor pendidikan. SMK Cengkareng 1 Jakarta merupakan sekolah menengah kejuruan yang termasuk dalam bidang keahlian Bisnis Manajemen, Teknologi Informasi dan Seni & Ekonomi Kreatif. Dokumen soal ujian merupakan data yang dibuat oleh sekolah, data tersebut diperoleh dari guru mata pelajaran yang bertugas dalam membuat soal ujian, data soal ujian sangat dijaga kerahasiaannya, jika data tersebut diketahui oleh pihak yang tidak bertanggung jawab kemungkinan dapat terjadi penyadapan data, maka hal tersebut akan menyebabkan suatu masalah. Tujuan dari penelitian ini menerapkan teknik kriptografi yaitu menggambarkan suatu teknik untuk meningkatkan aspek keamanan suatu data atau informasi. Sehingga keamanan soal ujian akan lebih terjaga. File soal ujian disimpan didalam sebuah folder penyimpanan komputer tanpa adanya sistem pengamanan data, sehingga untuk mengamankan data soal ujian dibutuhkan suatu teknik keamanan data menggunakan teknik kriptografi. Metode dalam pengembangan sistem menggunakan *waterfall* yang terdiri atas *analysis, design, code* dan *test.* Penelitian ini bertujuan untuk mengamankan soal ujian di SMK Cengkareng 1 Jakarta dalam meningkatkan keamanan akses dokumen. Penelitian ini memberikan manafaat dalam melakukan pengamanan data yang dilakukan dengan cara menerapkan teknik kriptografi menggunakan algoritma Advanced Encryption Standard (AES)-128 untuk menjalankan proses enkripsi dan deskripsi file soal ujian atau proses menyembunyikan sebuah informasi. Kesimpulan pengujian proses enkripsi dan deskripsi pada aplikasi memberikan kesimpulan bahwa pengujian file soal ujian yang telah melalui proses enkripsi dan dekripsi dinyatakan berhasil mencapai 100% dari soal ujian yang diuji dan memberikan hasil yang efektif pada penelitian SMK Cengkareng 1 Jakarta dalam mengatasi keamanan dokumen soal ujian.

Kata Kunci: Soal Ujian, AES-128, *Waterfall*, Kriptografi

CRYPTOGRAPHY APPLICATIONS BASED OF WEB SYSTEM AN USING AES-128 ALGORITHM FOR EXAM FILE SECURITY STUDENTS AT SMK CENGKARENG 1 JAKARTA

Abstract- *Current advances in information technology have developed rapidly and rapidly, especially in the education sector. SMK Cengkareng 1 Jakarta is a vocational high school which includes areas of expertise in Business Management, Information Technology and Arts & Creative Economy. Exam question documents are data created by the school, this data is obtained from subject teachers who are in charge of creating exam questions, exam question data is strictly kept confidential, if the data is known by irresponsible parties there is a possibility of data interception, then this will cause a problem. The aim of this research is to apply cryptographic techniques, namely to describe a technique to improve the security aspects of data or information. So the security of the exam questions will be better maintained. Exam question files are stored in a computer storage folder without a data security system, so to secure exam question data a data security technique using cryptographic techniques is required. The system development method uses waterfall which consists of analysis, design, code and testing. This research aims to secure exam questions at SMK Cengkareng 1 Jakarta in order to increase document access security. This research provides benefits in securing data by applying cryptographic techniques using the Advanced Encryption Standard (AES)-128 algorithm to carry out the encryption process and description of exam question files or the process of hiding information. The conclusion of testing the encryption process and description of the application provides the conclusion that testing exam question files that have gone through the encryption and decryption process was declared successful in achieving 100% of the exam questions tested and gave good results in research at SMK Cengkareng 1 Jakarta in overcoming the security of exam question documents.*

Keywords*: Exam Questions, AES-128, Waterfall, Cryptography*

1. PENDAHULUAN

Teknologi telah unggul dalam suatu hal yang hampir dari seluruh manusia di muka bumi ini telah bergantung pada kecanggihan dari teknologi itu sendiri [1]. Membuat aktivitas manusia menjadi lebih sederhana dengan mencari data dengan lebih cepat. Bagaimanapun, tidak semua perbaikan dalam inovasi mempunyai dampak positif dan produktif. Penyadapan merupakan permasalahan yang paling ditakuti oleh para pengguna jaringan komunikasi, penyadapan memiliki dampak negatif dari kemajuan teknologi, karena komunikasi data jarak jauh tidak selalu memiliki jalur yang aman dari penyadapan, maka keamanan informasi menjadi bagian penting dalam dunia informasi itu sendiri [2]. Meski data telah tersimpan dengan rapi, namun semakin banyak orang yang mampu mengubahnya karena kemajuan teknologi komputer [3].

Sekolah Menengah Kejuruan (SMK) Cengkareng 1 Jakarta didirikan oleh Yayasan Pendidikan Cengkareng 1 (YPC1) pada tahun 1998 yang dipimpin Bapak Drs. H. Gijono MM. Sekolah ini berlokasi di Jl. Bambu Larangan No. 67, Kelurahan. Cengkareng Barat, Kecamatan. Cengkarang, Jakarta Barat. SMK Cengkareng 1 Jakarta adalah sekolah menengah kejuruan yang termasuk dalam bidang keahlian Bisnis Manajemen, Teknologi Informasi dan Seni & Ekonomi Kreatif. Sesuai dengan bidangnya, SMK Cengkareng 1 memiliki 5 Program Keahlian yaitu Administrasi Perkantoran, Akuntansi, *Broadcasting*, Pemasaran dan Teknik Komputer dan Jaringan.

Permasalahan pada penelitian berfokus pada media penyimpanan file-file data ujian siswa SMK Cengkareng 1 Jakarta yang disimpan didalam sebuah folder penyimpanan pada komputer sekolah tanpa adanya sistem pengaman data sehingga perlu dilakukan proses untuk menjaga kerahasiaan dokumen ujian yang bersifat rahasia agar tidak mudah diketahui oleh pihak yang tidak bertanggung jawab. Pada masing-masing folder terdapat beberapa file dokumen yaitu file ujian siswa kelas X, kelas XI dan kelas XII yang telah dipersiapkan pada setiap semester untuk melakukan evaluasi belajar terhadap siswa dan siswi serta mengukur tingkat kompetensi siswa dan siswi selama menempuh pembelajaran.

Soal Ujian menjadi hal yang sangat perlu diperhatikan karena dikhawatirkan apabila media penyimpanan pada beberapa file dokumen memiliki akses yang lemah dapat saja terjadi kecurangan sebelum memasuki waktu ujian. Salah satunya berkas data yang telah disimpan didalam komputer dalam bentuk folder dapat dengan mudah dibuka oleh pihak yang tidak berkepentingan untuk mengakses data tersebut.

Pada penelitian sebelumnya telah diusulkan proses dalam melakukan pengamanan dokumen pada tahun 2020, 2021 dan 2022. Untuk penelitian di tahun 2020 dilakukan oleh [4] dengan judul "Keamanan Dokumen Menggunakan Algoritma *Advanced Encryption Standard* (AES) menghasilkan kesimpulan penelitian yaitu file yang melalui uji coba enkripsi akan berubah bentuk menjadi file yang tak bisa dibaca, file dapat kembali kebentuk asli jika melalui proses dekripsi dengan menggunakan kunci yang sama saat enkripsi dan dari hasil penelitian telah dibuktikan bahwa isi file awal yang mengalami proses enkripsi, kemudian mengalami proses dekripsi, maka akan kembali seperti file awal semula.

Lalu untuk penelitian di tahun 2021 dilakukan oleh [5] dengan judul "Meningkatkan Keamanan *Web* Menggunakan Algoritma *Advanced Encryption Standard* (AES) Terhadap Serangan *Cross Site Scripting"* yang menghasilkan penelitian bahwa dengan menerapkan Algoritma AES, dimana sebelumnya terdapat 2 (dua) kerentanan kategori *hight* dengan nama serangan XSS, setelah implementasi Algoritma AES maka kerentanan serangan XSS tersebut tidak ditemukan lagi. Berdasarkan hasil yang diperoleh dalam penelitian dapat disimpulkan bahwa Implementasi Algoritma AES pada token dapat meningkatkan keamanan *website* dari serangan XSS

Lalu penelitian berikutnya yang berjudul "Penerapan *Algoritma Advanced Encryption* Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem *E-Marketplace*" pada tahun 2022 oleh [6] menunjukkan keamanan data pada sistem pembayaran menggunakan algoritma kriptografi AES yang berfungsi untuk mengenkripsi data transaksi pembayaran agar rekaman data yang tersimpan di dalam *database* tidak mudah dibaca dan menghindari penyalahgunaan data oleh pihak yang tidak memiliki hak akses. Metode ini sangat cocok diterapkan dalam pengembangan perangkat lunak dengan sumber daya yang minim sehingga dapat mempercepat proses iterasi setiap tahapan pengembangan dan tetap memperhatikan masukan dari calon pengguna sistem.

Dari permasalahan yang terdapat pada SMK Cengkareng 1 Jakarta untuk meningkatkan keamanan media penyimpanan dokumen yang sifatnya sangat rahasia dalam mengurangi resiko pencurian data yang mungkin saja dapat terjadi. Maka, untuk bisa mengamankan data penting tersebut perlu suatu teknik keamanan data menggunakan teknik kriptografi. Salah satu metode yang digunakan untuk meningkatkan keamanan data atau informasi menggunakan metode kriptografi menggunakan algoritma AES [7].

Kriptografi [8] merupakan ilmu dan seni untuk menjaga kerahasiaan suatu pesan atau informasi. Proses enkripsi dan dekripsi memerlukan sebuah kode dalam penggunaanya yang disebut dengan kunci.. Kriptografi [10] telah menjadi bagian dari ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Teknik penyandian data (kriptografi) yang diterapkan pada data maupun informasi, dilakukan dengan mengkodekan atau menyembunyikan data aslinya [11]. Dalam hal ini sistem keamanan sangat diperlukan untuk mengamankan suatu file yang dianggap penting. Dalam ilmu kriptografi, ada istilah enkripsi dan

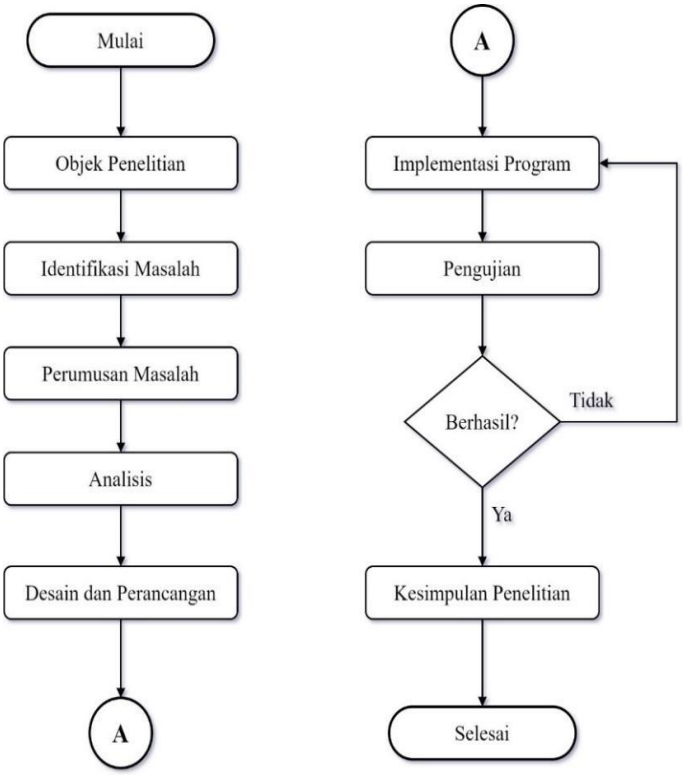
dekripsi [12]. Enkripsi adalah teknik merubah suatu data asli menjadi data yang hanya bisa dibaca oleh pembaca yang memiliki kunci (*key*) [13]. Sedangkan Dekripsi merupakan teknik mengembalikan data yang sudah terenkripsi menjadi data semula [14].

Berdasarkan uraian yang telah dipaparkan pada latar belakang diatas. Penelitian dilakukan untuk mengimplementasikan sebuah aplikasi pada bidang Teknologi dan Informatika yang kemudian diberi judul "Aplikasi Kriptografi Berbasis *Web System* Menggunakan Algoritma AES-128 Untuk Keamanan File Ujian Siswa SMK Cengkareng 1 Jakarta.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Pada tahapan penelitian dibawah ini menggambarkan tahapan-tahapan penelitian dari awal hingga akhir yang direpresentasikan pada bagan diagram alir sebagai berikut yang diperlihatkan pada Gambar 1.



Gambar 1. Tahapan Penelitian

2.2 Penerapan Metode

Pada penelitian ini menggunakan metode *waterfall* dalam pengembangan sistem yang terdiri atas *analysis, design, code* dan *test*. Berikut tahapan-tahapan penelitian dari awal hingga akhir yang terdiri sebagai berikut:

a. Pengumpulan Data
   Proses observasi dan wawancara seputar data soal ujian di lakukan secarang langsung kepada Tata Usaha Sekolah Menengah Kejuruan (SMK) Cengkareng 1 Jakarta untuk mendapatkan infromasi soal ujian kelas X, XI dan XII.
b. Analisis Kebutuhan
   Pada tahap ini melakukan analisis secara berurutan, mulai dari analisis data masukan, analisis penerapan algoritma dan analisis terhadap sistem keluaran yang akan dibuat. Melakukan analisis data masukan terkait file ujian siswa yang bersifat rahasia yang nantinya data file tersebut akan diolah sebagai data masukan. Proses enkripsi dan dekripsi data menggunakan algoritma AES (*Advanced Encryption Standard*)-128 dilakukan pada saat proses sistem berjalan menggunakan teknik penyisipan kunci. Beberapa rancangan akan dibuat sesuai dengan proses kriptografi pada program seperti proses enkripsi dan proses dekripsi sehingga dapat dilihat hasil keluaran pada sistem.

2.3 Kriptografi

Teknik kriptografi menjadi salah satu teknik yang digunakan dalam mengamankan data yang bersifat rahasia. Pengamanan data menggunakan teknik kriptografi dilakukan dengan merubah pesan *plaintext* menjadi sandi (*ciphertext*). Proses untuk mengkonversi *plaintext* menjadi *ciphertext* disebut dengan proses enkripsi sedangkan proses yang dilakukan untuk mengembalikan *ciphertext* menjadi *plaintext* disebut deskripsi. Proses enkripsi dan dekripsi memerlukan sebuah kode dalam penggunaanya yang disebut dengan kunci. Kunci (key) harus bersifat rahasia (private) dan tidak boleih diberitahukan kepada orang lain yang tidak berhak untuk menerima pesan [9].

2.4 *Advanced Encryption Standard* (AES)

Advanced Encryption Standard [15] atau umumnya disingkat AES [12] merupakan algoritma *cryptographic* yang dapat digunkan untuk mengamakan data. Algoritma AES adalah blok *chipertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut *ciphertext*, sebaliknya dekripsi adalah merubah *ciphertext* data menjadi bentuk semula yang kita kenal sebagai *plaintext*. Algoritma AES menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan mendekrip data. Perbedaan panjang kunci tersebut nantinya mempengaruhi jumlah putaran pada algoritma AES.

2.5 Rancangan Basis Data

Pada rancangan basis data, menerangkan tentang *Entity Relationship Diagram* (ERD), *Logical Record Structure* (LRS) serta spesifikasi data tabel atau *database* yang digunakan pada pembuatan aplikasi ini, antara lain:

a. Entity Relationship Diagram (ERD)
   Entity Relationship Diagram ini berisi komponen-komponen himpunan entitas dan himpunan relasi. Masing-masing dilengkapi dengan atribut-atribut yang mewakili seluruh data yang ada.
b. Logical Record Structure (LRS)
   Logical Record Structure yang terdapat di dalam basis data yang digunakan serta teknik untuk menggambarkan hubungan basis data berupa relasi antar tabel.

2.6 Pengujian Sistem

Pada pengujian sistem menjelaskan tentang tahap-tahap yang akan dilakukan oleh terkait beberapa hasil dari pembuatan aplikasi kriptografi. Pengujian sistem yang akan dilakukan oleh terdiri dari 2 tahap, antara lain:

a. Parameter Pengujian Fungsional
   Pengujian akan dilakukan dari sisi fungsional sistem dengan menggunakan teknik pengujian *black box testing*. Berikut parameter pengujian fungsional dapat dilihat pada Tabel 1 dibawah ini.

Tabel 1. Parameiteir Peinguijian Fuingsional Fituir Meinui

No	Kelas Uji	Butir Uji	Teknik Pengujian
1	Fitur *Login*	Akses Masuk Sistem	*Black Box Testing*
2	Fitur *Dashboard*	Menjalankan Halaman Utama dan Fungsi	*Black Box Testing*
3	Fitur Menu Enkripsi	Menjalankan Proses Enkripsi	*Black Box Testing*
4	Fitur Menu Dekripsi	Menjalankan Proses Dekripsi	*Black Box Testing*

b. Parameter Pengujian Data Enkripsi dan Dekripsi
   Pengujian akan dilakukan dari data yang telah disiapkan berupa file berekstensi docx, xlsx, txt, jpeg, png, pptx dan pdf. Pada proses pengujian sistem menggunakan Algoritma AES (Advanced Encryption Standard)-128 pada penentuan kunci enkripsi dan dekripsi.

2.7 Spesifikasi *Database*

Berikut Ini adalah struktur file yang terdapat di dalam basis data yang digunakan. Tabel dalam basis data ini akan menyimpan record-record yang telah dimanipulasi oleh program sesuai spesifikasinya masing-masing. Berikut Tabel User dan Table File dapat dilihat pada Table 2 dan Table 3 dibawah ini.

a. Tabel User

Nama Tabel : users
Media : SSD
Primary Key : username
Foreign Key : -

Tabel 2. Tabeil Uiseir

No.	Nama Field	Tipe Data	Panjang/Nilai	Keterangan
1	username	varchar	15	*Primary Key*
2	password	varchar	100	Kata Sandi
3	fullname	varchar	50	Nama Asli
4	job_title	varchar	50	Jabatan Pengguna
5	join_date	timestamp	-	Tanggal Mendaftar
6	last_activity	timestamp	-	Aktifitas Terakahir
7	status	enum	(‘1’, ‘2’)	Status Pengguna

b. Tabel File

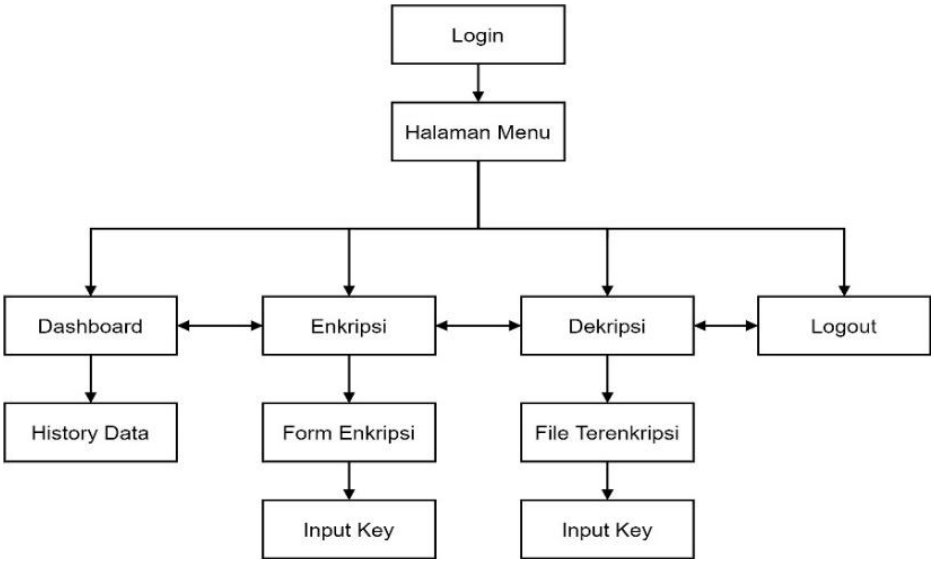
Nama Tabel : file
Media : SSD
Primary Key : id_file
Foreign Key : username

Tabel 3. Tabeil Filei

No.	Nama Field	Tipe Data	Panjang/Nilai	Keterangan
1	id_file	int	11	*Primary Key*
2	username	varchar	15	*Foreign Key*
3	file_name_source	varchar	255	Nama File Asli
4	file_name_finish	varchar	255	Nama Hasil File
5	file_url	varchar	255	Lokasi Penyimpanan
6	file_size	float	-	Ukuran File
7	password	varchar	16	Kata Sandi
8	tgl_upload	timestamp	-	Tanggal Upload
9	status	enum	(‘1’, ‘2’)	Status Pengguna
10	keterangan	varchar	255	Keterangan File

2.8 Rancangan Menu

Pada rancangan menu merupakan bagian utama dalam pengembangan sistem dengan tujuan agar dapat menjadi sebuah sistem yang baik. Karena struktur menu ini merupakan perkembangan bagaimana informasi, proses dan hasil berjalan secara efisien. Berikut rancangan menu dapat dilihat pada Gambar 2 dibawah ini.



Gambar 2. Rancangan Menu

Rancangan menu memberikan struktur untuk mengidentifikasi elemen-elemen kerangka kerja dan menekankan fungsi yang harus diselesaikan oleh program, dibandingkan dengan menampilkan penjelasan program yang digunakan untuk menyelesaikan fungsi tersebut.

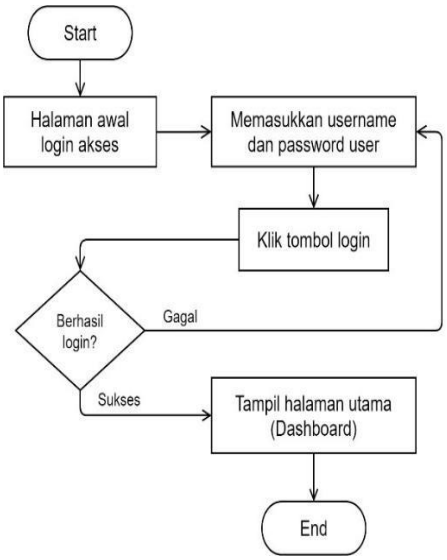
3. HASIL DAN PEMBAHASAN

3.1 *Flowchart*

Flowchart merupakan rancangan aktivitas kerja yang bertujuan untuk menjelaskan rangkaian aktivitas, proses dan pengulangan yang terjadi. Berikut adalah *flowchart* yang dibuat berdasarkan hasil rancangan sistem.

3.1.1 *Flowchart* Proses *Login*

Rancangan pada *flowchart* proses *login* menjelaskan validasi *username* dan *password* pengguna untuk mengakses halaman utama sistem. Berikut *flowchart* proses *login* dapat dilihat pada Gambar 3 dibawah ini.

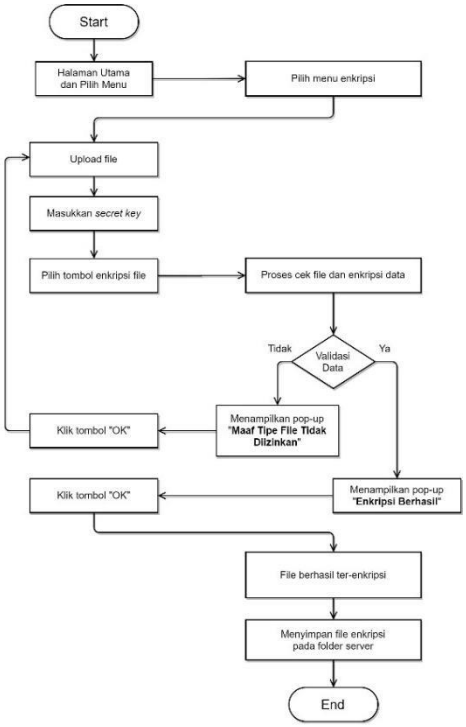


Gambar 3. *Flowchart* Proseis *Login*

3.1.2 *Flowchart* Proses Enkripsi

File yang dapat dienkripsi beberapa file yang berekstensi .docx, .xlsx, .pptx dan .pdf. Apabila file memenuhi syarat dalam tahap proses validasi, maka dinyatakan proses enkripsi berhasil dan sebaliknya apabila

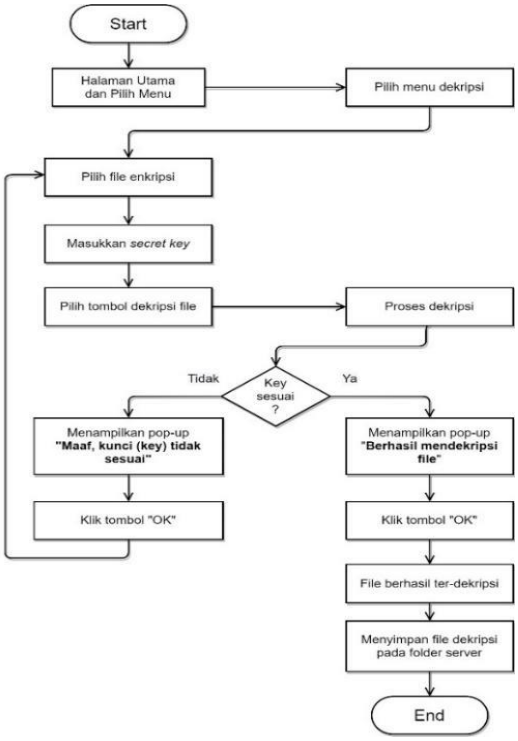
proses validasi pada enkripsi tidak memenuhi syarat terhadap file yang tidak mendukung ekstensi, maka akan terjadi proses *looping* pada sistem program tersebut dan kembali pada tahap sebelumnya. Berikut Gambar 4 dibawah ini menjelaskan tentang *flowchart* proses enkripsi file.



Gambar 4. *Flowchart* Proseis Einkripsi

3.1.3 *Flowchart* Proses Dekripsi

Rancangan pada *flowchart* proses dekripsi menjelaskan bahwa file yang telah terenkripsi hanya dapat didekripsi oleh sistem ini. Berikut rancangan *flowchart* proses dekripsi file dapat dilihat pada Gambar 5 dibawah ini.



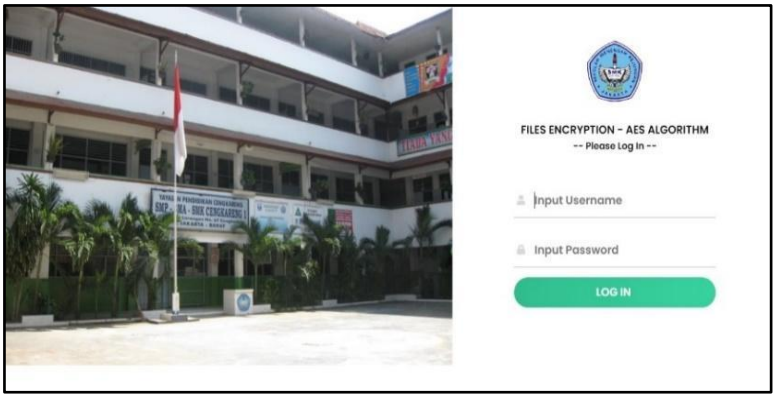
Gambar 5. *Flowchart* Proseis Deikripsi

3.2 Tampilan Layar Aplikasi

Pada tampilan layar pada aplikasi. Aplikas telah selesai dibuat, yang dimana sistem yang dibuat ini untuk memenuhi kebutuhan penyimpanan data saat terjadinya distribusi file atau dokumen terkait data soal ujian yang terdapat pada SMK Cengkareng 1 Jakarta.

3.2.1 Tampilan Layar Halaman Login

Halaman *login* pada aplikasi menampilkan halaman dimana terdapat kolom *username* dan *password* yang harus di *input* untuk masuk ke halaman utama sistem. Berikut tampilan *login* dapat dilihat pada Gambar 6 dibawah ini.



Gambar 6. Tampilan *Login* Aplikasi

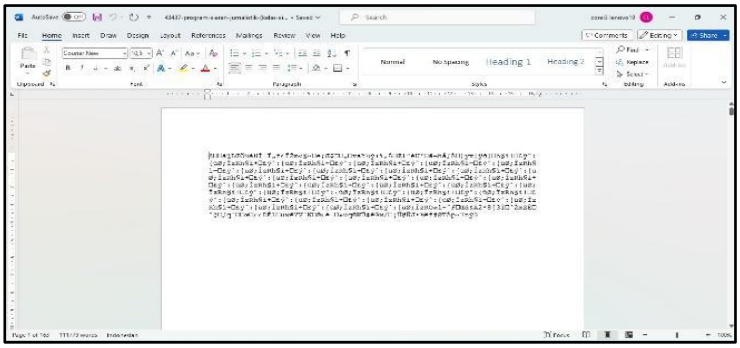
3.2.2 Tampilan Layar Halaman Utama (Dashboard)

Pada halaman utama aplikasi memberikan tampilan menu-menu pada layar dan untuk tampilan *dashboard* menampilkan data *users*, data enkripsi *file* dan dekripsi *file*. Berikut tampilan layar aplikasi pada halaman utama dapat dilihat pada Gambar 7 dibawah ini.

Gambar 7. Tampilan Halaman Uitama (*Dashboard*)

3.2.3 Tampilan Layar Hasil Proses Enkripsi

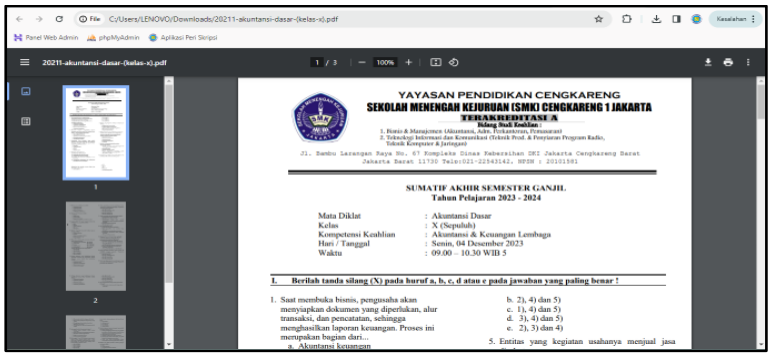
Proses enkripsi dilakukan dengan menerapkan algoritma AES-128 menggunakan enkripsi simetris, yang berarti menggunakan kunci yang sama pada algoritma ini untuk mengenkripsi dan mendekripsi file. Kunci ini harus memiliki panjang 128 bit (16 *byte*) dan hanya diketahui oleh Admin pada sistem yang dibuat ini pada saat mengenkripsi dan mendekripsi file. Berikut dapat dilihat pada Gambar 8 adalah hasil dari proses file atau dokumen yang telah dilakukan proses enkripsi.



Gambar 8. Tampilan Hasil Proses Enkripsi

3.2.4 Tampilan Layar Hasil Proses Dekripsi

Berikut tampilan aplikasi hasil proses dekripsi file, untuk dapat mendekripsi file perlu memasukkan kunci publik yang telah dibuat sebelumnya agar dapat mengembalikan file yang telah dienkripsi. File tidak dapat dikembalikan seperti semula apabila salah dalam memasukkan kunci. Untuk file dokumen yang telah berhasil dilakukan dekripsi dapat dilihat pada Gambar 9 dibawah ini.



Gambar 9. Tampilan Hasil Proses Dekripsi

3.3 Hasil Pengujian Enkripsi dan Dekripsi

Berikut ini pengujian hasil enkripsi dan dekripsi yang dilakukan pada fitur menu pada proses melakukan enkripsi dan dekripsi file dokumen soal ujian seperti ditampilkan pada Tabel 3 dan Tabel 4 dibawah ini.

Tabel 3. Pengujian Hasil Enkripsi File

No.	Nama File	Ekstensi File	Ukuran File (Asli)	Hasil Enkripsi	Ukuran File (Terenkripsi)
1	Administrasi Umum (Kelas X)	.pdf	495 KB	Berhasil	494.434 KB
2	Agama Kristen (Kelas X)	.pdf	492 KB	Berhasil	491.13 KB
3	Akuntansi Dasar (Kelas X)	.pdf	486 KB	Berhasil	485.841 KB
4	Administrasi Jaringan (Kelas XI)	.pdf	220 KB	Berhasil	219.155 KB
5	Administrasi Pajak (Kelas XI)	.pdf	474 KB	Berhasil	473.754 KB
6	Bahasa Indonesia (Kelas XI)	.pdf	268 KB	Berhasil	267.48 KB
7	Program Siaran Artistik - Kelas XII	.docx	2.187 KB	Berhasil	2186.61 KB
8	Teknologi Layanan Jaringan - Kelas XII	.docx	204 KB	Berhasil	203.017 KB
9	Adm Sistem Jaringan - Kelas XII	.docx	205 KB	Berhasil	204.564 KB
10	Komputer Akuntansi - Kelas XII	.docx	2.054 KB	Berhasil	2053.87 KB

Dari hasil pengujian enkripsi file soal ujian berekstensi .docx dan .pdf menunjukkan hasil pengujian sesuai dengan tahap perancangan, dimana aplikasi sistem ini dapat melakukan enkripsi yang kapasitas file dapat mencapai lebih dari 5 MB.

Tabel 4. Pengujian Hasil Dekripsi File

No.	Nama File	Ekstensi File	Ukuran File (Asli)	Hasil Enkripsi	Ukuran File (Terenkripsi)
1	53879-administrasi-umum-(kelas-x).encryption-aes	.pdf	494.434 KB	Berhasil	495 KB
2	79910-agama-kristen-(kelas-x).encryption-aes	.pdf	491.13 KB	Berhasil	492 KB
3	35681-akuntansi-dasar-(kelas-x).encryption-aes	.pdf	485.841 KB	Berhasil	486 KB
4	36076-administrasi-jaringan-(kelas-xi).encryption-aes	.pdf	219.155 KB	Berhasil	220 KB
5	80555-administrasi-pajak-(kelas-xi).encryption-aes	.pdf	473.754 KB	Berhasil	474 KB
6	79065-bahasa-indonesia-(kelas-xi).encryption-aes	.pdf	267.48 KB	Berhasil	268 KB
7	16977-program-siaran-artistik---kelas-xii.encryption-aes	.docx	2186.61 KB	Berhasil	2.187 KB
8	96211-teknologi-layanan-jaringan---kelas-xii.encryption-aes	.docx	203.017 KB	Berhasil	204 KB
9	16736-adm-sistem-jaringan---kelas-xii.encryption-aes	.docx	204.564 KB	Berhasil	205 KB
10	27093-komputer-akuntansi---kelas-xii.encryption-aes	.docx	2053.87 KB	Berhasil	2.054 KB

Dari hasil pengujian enkripsi file soal ujian berekstensi .docx dan .pdf berhasil melakukan proses dekripsi file. Serta hasil dari semua pengujian proses dekripsi mencapai tingkat keberhasilan 100% pada soal ujian yang diuji.

4. KESIMPULAN

Berdasarkan penjelasan yang telah diuraikan pada penelitian ini, maka dapat disimpulkan bahwa algoritma *Advanced Encryption Standard* - 128 berhasil diimplementasikan kedalam aplikasi yang dibuat dengan tingkat keberhasilan dari proses enkripsi dan dekripsi mencapai 100%, sehingga memberikan hasil yang efektif dalam

mengamankan soal ujian SMK Cengkareng 1 Jakarta dari pihak yang tidak bertanggung jawab. Aplikasi dapat melakukan enkripsi dan dekripsi pada file soal ujian yang berekstensi docx, xlsx, txt, jpeg, png, pptx dan pdf. Pada proses enkripsi soal ujian, aplikasi yang dibuat menggunakan kunci rahasia atau kunci simetris, sehingga proses dekripsi hanya bisa dilakukan apabila pengguna mengetahui kuncinya. Waktu proses untuk enkripsi dan dekripsi berpengaruh lambat atau cepatnya menyesuaikan size atau ukuran file tersebut, untuk batasan ukuran file saat menjalankan proses enkripsi dan dekripsi file dapat mencapai ukuran file hingga 5 MB yang dapat diuji, sehingga aplikasi tidak bisa memproses file yang lebih besar dari 5 MB. Dari batasan ukuran file aplikasi tersebut, diharapkan pada penelitian selanjutnya dapat mengenkripsi file yang lebih besar.

1. UCAPAN TERIMA KASIH

Semoga penelitian ini dapat bermanfaat pada masa yang akan datang. Maka, dari itu rasa terima kasih diucapkan kepada seluruh pihak-pihak terkait yang telah berkontribusi secara langsung maupun tidak langsung atas terlaksananya dan terselesaikannya penelitian ini tepat pada waktunya.

2. DAFTAR PUSTAKA

[1] F. Damanik, I. Gunawan, Z. M. Nasution, Sumarno, and I. O. Kirana, "Pemanfaatan Algoritma AES Untuk Keamanan Data Karyawan PT. Telkom Indonesia Pematangsiantar," *STORAGE J. Ilm. Tek. dan Ilmu Komput.*, vol. 1, no. 1, pp. 32–37, 2022, doi: 10.55123.

[2] D. Widyawan and Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode AES-128 Berbasis Web Di Komite," *SKANIKA*, vol. 4, no. 1, pp. 15–22, 2021.

[3] Y. Suharya and H. Widia, "Implementasi Digital Signature Menggunakan Algoritma Kriftografi RSA Untuk Pengamanan Data Di SMK Wirakarya 1 Ciparay," *J. Inform.*, vol. 07, no. 01, pp. 20–29, 2020.

[4] J. Handoyo and Y. M. Subakti, "Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (AES)," *J. SITECH Sist. Inf. dan Teknol.*, vol. 3, no. 2, pp. 143–152, 2020, doi: 10.24176/sitech.v3i2.5865.

[5] Y. Putra, Y. Yuhandri, and S. Sumijan, "Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting," *J. Sistim Inf. dan Teknol.*, vol. 03, no. 02, pp. 56–63, 2021, doi: 10.37034/jsisfotek.v3i2.44.

[6] M. Riyan Andriyanto and P. Sukmasetya, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace," *J. Comput. Syst. Informatics*, vol. 4, no. 1, pp. 179–187, 2022, doi: 10.47065/josyc.v4i1.2451.

[7] S. Widyastuti, W. Ariandi, and V. Sulistiono, "Implementasi Kriptografi AES Dalam Pengamanan Data Seleksi Peserta JAMKESMAS," *J. Ilm. Intech Inf. Technol. J. UMUS*, vol. 1, no. 02, pp. 13–22, 2019, doi: 10.46772/intech.v1i02.66.

[8] N. Taliasih and I. Afrianto, "Sistem Keamanan Basis Data Klien PT. INFOKES Menggunakan Kriptografi Kombinasi RC4 Dan Base64," *J. Nas. Teknol. dan Sist. Inf.*, vol. 06, no. 01, pp. 009–018, 2020.

[9] N. Sinaga, S. Aini, and B. Gulo, "Penerapan Algoritma Skipjack Untuk Menyandikan Short Message Service," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 2, no. 1, p. 33, 2018, doi: 10.30645/j-sakti.v2i1.54.

[10] A. Z. F. Rangkuti and H. Fahmi, "Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, pp. 170–175, 2020, doi: 10.32672/jnkti.v3i2.2384.

[11] Y. Wiharto and Mufti, "Implementasi Advanced Encryption Standard 128 Sebagai Pengamanan Basis Data Obat-obatan Apotek," *J. Tek. Inform. dan Sist. Inf.*, vol. 8, no. 2, pp. 335–350, 2022, doi: 10.28932/jutisi.v8i2.4817.

[12] D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018, doi: 10.15408/jti.v11i2.7811.

[13] F. Fadlullah, M. Tahir, B. P. Bintari, M. L. Dewi, and M. F. Ilmy, "Implementasi Algoritma AES pada Autentikasi Login Sistem Informasi," *J. Bintang Pendidik. Indones.*, vol. 1, no. 2, pp. 251–263, 2023.

[14] B. Wicaksana and M. Setiawan, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Pengamanan Berkas Soal Ujian," *Teknois J. Ilm. Teknol. Inf. dan Sains*, vol. 10, no. 1, pp. 25–34, 2020, doi: 10.36350/jbs.v10i1.74.

[15] D. Widyawan and Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode AES -128 Berbasis Web Di Komite," *SKANIKA*, vol. 4, no. 1, pp. 15–22, 2021.