Penerapan Kriptografi Menggunakan Advanced Encryption Standard 128 Untuk Pengamanan File Pada SMK Muhammadiyah 4

by Hari Soetanto

Submission date: 28-Aug-2023 09:28AM (UTC+0700)
Submission ID: 2152410841
File name: n_Standard_128_Untuk_Pengamanan_File_Pada_SMK_Muhammadiyah_4.pdf (820.59K)
Word count: 3732
Character count: 23681

PENERAPAN KRIPTOGRAFI MENGGUNAKAN *ADVANCED ENCRYPTION STANDARD* 128 UNTUK PENGAMANAN FILE PADA SMK MUHAMMADIYAH 4

Romi Ramadhan[1*], Hari Soetanto[2]

[1.2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta Selatan, Indonesia
Email: [1*]romiramadhann@gmail.com, [2]hari.soetanto@budiluhur.ac.id
(* : corresponding author)

Abstrak-Perkembangan teknologi pada masa kini sangat berkembang pesat, terlebih pada pertukaran informasi yang kian luas. Pada SMK Muhammadiyah 4 Jakarta data-data penting yang ada dalam sekolah tersebut masih berupa teks asli, yang dapat dibaca tanpa adanya pengamanan. Terkait dengan data penting yang dimana hanya pihak sekolah yang memiliki wewenang untuk mengetahui file-file tersebut karena file tersebut bersifat rahasia. Hal ini dapat menimbulkan masalah karena sekolah SMK Muhammadiyah 4 Jakarta mencatat file-file penting seperti file soal ujian secara sistematis dan terkomputerisasi. Karena data dan informasi yang penting dan juga rahasia yang masih rentan terhadap penyalahgunaan oleh pihak tertentu dikarenakan tidak adanya pengamanan, dan dapat menyebabkan pencurian hingga dapat mengakibatkan kerugian yang cukup besar. Maka dari masalah tersebut maka sebagai pencegahan direncanakan penelitian ini untuk diimplementasikan penyandian isi data file soal ujian menggunakan kriptografi. Dengan menggunakan metode yang cukup handal adalah *Advanced Encryption Standard*. Penelitian ini akan menggunakan kriptografi algoritme AES-128 untuk pengamanan file. khususnya adalah file dengan ukuran <=3 Mb yang bertipe doc, docx, txt, xlsx, pdf, dan pptx. Berdasarkan dengan melakukan perbaan dengan penerapan enkripsi dan dekripsi AES-128 maka didapatkan hasil, bahwa isi file asli yang dienkripsi dengan AES-128 dapat terenkripsi dengan baik, hal tersebut terbukti dari isi file yang dihasilkan tidak dapat terbaca oleh pengguna, kemudian setelah file tersebut didekripsi, maka file tersebut dapat kembali seperti file awal. Waktu yang didapat dari hasil percobaan proses enkripsi dan dekripsi dari sembilan file soal ujian, menunjukan rata-rata waktu pengenkripsian yaitu 33. 183 detik dan rata rata waktu dekripsi yaitu 35.700 detik, dengan ukuran file kurang dari 3Mb. Ukuran file setelah dienkripsi maupun didekripsi kembali ke ukuran file awal, tetapi ukuran file juga ikut mempengaruhi waktu pada saat melakukan proses enkripsi dan dekripsi.

Kata Kunci: keamanan, kriptografi, *advanced encryption standard*, *file*.

APPLICATION OF CRYPTOGRAPHY ADVANCED ENCRYPTION STANDARD-128 METHOD FOR FILE SECURITY AT SMK MUHAMMADIYAH 4

Abstract-*Technology developments are currently growing rapidly, especially in the increasingly widespread exchange of information At SMK Muhammadiyah 4, important data in the school is still in the form of original text, which can be read without any security. Associated with important data where only the school has the authority to know the files because the files are confidential. This can cause problems because the SMK Muhammadiyah 4 records important files such as exam questions in a systematic and computerized manner. Because important and confidential data and information are still vulnerable to misuse by certain parties due to the absence of security, and can cause theft to result in considerable losses. So from this problem, as a prevention, this research is planned to implement encoding the contents of the exam question file data using cryptography. With a fairly reliable method is the Advanced Encryption Standard. This research will use the AES-128 algorithm cryptography for file security. in particular are files with a size of <=3 Mb of type doc, docx, txt, xlsx, pdf, and pptx. Based on experiments with the application of AES-128 encryption and decryption, the results obtained, that the contents of the original file encrypted with AES-128 can be encrypted properly, this is evident from the contents of the resulting file cannot be read by the user, then after the file is decrypted , then the file can return to the original file. The time obtained from the experimental results of encryption and decryption process of nine test question files, shows average encryption time is 33, 183 seconds and average decryption time is 35,700 seconds, with a file size of less than 3Mb. The file size after being encrypted or decrypted returns to the initial file size, but the file size also affects time during encryption and decryption process.*

Keywords*: cryptography, security, advanced encryption standards, files.*

1. PENDAHULUAN

Pada era perkembangan teknologi informasi masa ini, pengiriman informasi selalu terjadi sehingga membuat unsur keamanan informasi menjadi nilai sangat penting [1]. Keamanan merupakan indikator yang bernilai penting pada penyimpanan dan pengiriman data atau pesan [2]. Pada institusi atau lembaga sangat membutuhkan sistem

keamanan teknologi informasi yang kuat untuk mengamankan aset terpenting mereka seperti sistem keamanan informasi dan komunikasi dari berbagai macam serangan di masa depan [3]. Hal ini tentu saja menimbulkan risiko jika informasi yang sensitif dan berharga dapat diakses oleh orang yang tidak berwenang dan tidak bertanggung jawab [4].

Pendidikan di Indonesia pada masa ini telah masuk era teknologi, yang dimana hampir setiap sesuatunya dilakukan menggunakan gadget dan komputasi. Pada SMK Muhammadiyah 4 Jakarta data-data penting yang ada dalam sekolah tersebut masih berupa teks asli, yang dapat dibaca tanpa adanya pengamanan. Terkait dengan data penting yang dimana hanya pihak sekolah yang memiliki wewenang untuk mengetahui file-file tersebut karena file tersebut bersifat rahasia.

Hal ini dapat menimbulkan masalah karena sekolah SMK Muhammadiyah 4 Jakarta mencatat file-file penting seperti file soal ujian secara sistematis dan terkomputerisasi. Karena data dan informasi yang penting dan juga rahasia yang masih rentan terhadap penyalahgunaan oleh pihak tertentu dikarenakan tidak adanya pengamanan, dan dapat menyebabkan pencurian hingga dapat mengakibatkan kerugian yang cukup besar.

Terkait dari masalah tersebut sebagai langkah pengamanan, maka diimplementasikan penyandian isi data file-file penting dan file soal ujian dengan menggunakan kriptografi. Pada penelitian ini memakai kriptografi dengan algoritme *Advanced Encryption Standard* 128 untuk pengamanan file. Khususnya adalah file dengan ukuran <=3 Mb yang bertipe *doc, docx, txt, xlsx, pdf,* dan *pptx*.

Sumber refrensi terkait metode yang diambil berasal dari penelitian sebelumnya [5] yang dibuat untuk keamanan aplikasi *mobile BluCampus* dengan menggunakan metode *Advanced Encryption Standard* dan *Affine Cipher* pada Universitas Budi Luhur. keamanan data karena pada proses pengiriman dan penerimaan data harus melalui jaringan internet yang rawan terhadap penyadapan, pencurian data, pemalsuan informasi oleh pihak yang tidak bertanggung jawab.

Penelitian lainnya oleh [6] Menerapkan Algoritme *Advanced Encryption Standard* (AES) pada *QR-Code* untuk mengamankan identitas tiket yang telah terjual dan memudahkan petugas tiket untuk melakukan verifikasi tiket. Penerapan Algoritme Kriptografi AES (*Advanced Encryption Standard*) pada *QR-Code* sebagai tiket, dapat digunakan untuk keamanan data dan proses verifikasi tiket yang belum dapat mengetahui apakah tiket tersebut (asli) valid atau (palsu) tidak valid. Sehingga petugas dapat melakukan proses verifikasi lebih mudah dan cepat. Dengan adanya data yang telah terenkripsi oleh algoritme AES pada *QR-Code*.

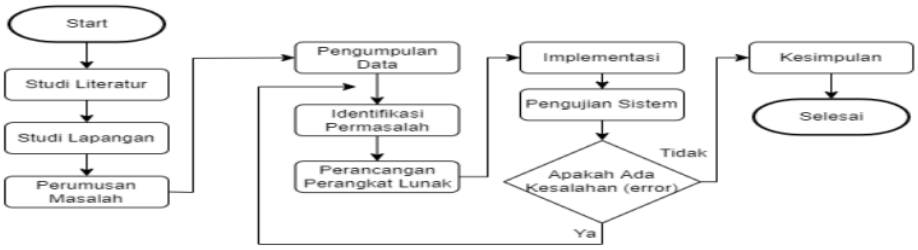
Banyak juga penelitian sebelumnya yang sudah mempergunakan kriptografi untuk pengamanan data. Contohnya penerapan kriptografi pada pengamanan data berbasiskan *smartphone* [7] Rancang Bangun Aplikasi Keamanan Data Menggunakan Metode AES Pada *Smartphone*. Kekurangan aplikasi berbasis *smartphone* harus melakukan instalasi pada *smartphone* yang digunakan. *desktop* adalah harus dilakukan install atau dikonfigurasi pada setiap komputer yang akan menggunakannya. Sama halnya dengan diantaranya penerapan kriptografi untuk pengamanan data pada aplikasi berbasiskan *desktop* [8] Implementasi Algoritme *Advanced Encryption Standard* (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. Kekurangan aplikasi *desktop* adalah harus dilakukan instalasi atau konfigurasi di setiap komputer yang akan menggunakan aplikasinya.

Selain berbeda basis pengaplikasian ada juga penelitian penerapan kriptografi yang menggunakan algoritme berbeda, contohnya seperti penelitian sebelumnya [9] Aplikasi *Quiz* Psikologis Berbasis *Website* Dengan Pengaplikasian Algoritma DES. Kekurangan pengamanan data algoritme DES adalah algoritme tersebut sudah dianggap kuno dan mudah dibobol [10].

Sama seperti penelitian ini, penelitian sebelumnya juga sudah banyak yang menggunakan algoritme *Advanced Encryption Standard* Penerapan Algoritma AES pada QR CODE untuk Keamanan Verifikasi Tiket. Karena menurut penelitian sebelumnya hasil *Advanced Encryption Standard* lebih efektif dan ideal dalam pengkodean bit data dengan peningkatan 13,085% dalam kinerja dekripsi dalam hal waktu, kecepatan dan hasil [11].

2. METODE PENELITIAN

Metode penelitian digunakan sebagai pedoman dalam melakukan penelitian agar hasil yang dicapai tidak menyimpang dari tujuan. Gambar 1 menyajikan tahapan yang dilakukan dalam tahapan penelitian yang akan dilakukan dalam penelitian ini.



Gambar 1. Tahapan Penelitian

a. Studi literatur

Studi literatur dilakukan menggunakan cara mengumpulkan penelitian-penelitian sebelumnya untuk dijadikan refrensi. Dan mempelajari berbagai macam diktat kuliah, jurnal dan karya ilmiah yang berhubungan dengan masalah penelitian yang akan diulas adalah kriptografi dengan metode *Advanced Encryption Standard*.

b. Studi Lapangan

Studi kasus untuk mengetahui permasalahan yang ada di SMK Muhammadiyah 4 Jakarta

c. Perumusan masalah

Pada tahap ini ditemukan masalah yang akan diselesaikan dalam penelitian ini, yaitu pengamanan file-file yang bersifat penting pada sekolah SMK Muhammadiyah 4 Jakarta dengan menggunakan kriptografi metode AES-128.

d. Pengumpulan Data

Pada tahap ini dilakukan pengumpulan data yang telah disebutkan diatas. Semua tahap pada proses pengumpulan data tersebut diperoleh dari wawancara dan observasi.

1) Wawancara (*interview*)

Wawancara merupakan pengumpulan data dengan mengajukan pertanyaan yang berhubungan dengan pengamanan file yang dilakukan pada wakil hubungan distribusi sebagai bagian yang berwenang untuk membuat aplikasi/piranti kriptografi pengamanan file. Dari wawancara tersebut, peneliti juga mendapatkan file-file yang akan digunakan dalam pengembangan sistem kriptografi pengamanan file.

2) Observasi

Observasi merupakan kegiatan mengumpulkan data melalui investigasi langsung dengan hal-hal yang berhubungan dengan sistem kriptografi pengamanan file sekaligus sebagai masukan dalam penelitian ini.

e. Identifikasi Permasalahan

Setelah melakukan tahap sebelumnya, langkah selanjutnya adalah mengidentifikasi permasalahan sistem yang akan diterapkan sesuai dengan batasan-batasan yang ada. Pada tahap ini, analisis yang dibutuhkan dalam penyelesaian untuk masalah dalam penelitian ini akan dilakukan dalam beberapa tahapan. Tahapan yang dilakukan antara lain:

1) Analisis Data

Analisis data merupakan salah satu tahap untuk penyelesaian permasalahan keamanan ini, dalam analisis data dilakukan :

a) Pengumpulan data yang berfungsi untuk memperoleh data yang diperlukan dalam perancangan program.
b) Pendeskripsian data untuk menentukan langkah selanjutnya yang harus diambil untuk membangun aplikasi yang memiliki tampilan yang *user friendly* agar mudah dipahami.

2) Analisis Penerapan Algoritme

Setelah melakukan tahap analisis data, langkah selanjutnya adalah analisis penerapan algoritme. Analisis penerapan algoritme menjelaskan tahap untuk menerapkan metode kriptografi *Advanced Encryption Standard* (AES) pada proses pengamanan file. Pada tahapan ini dilakukan :

a) Menentukan kunci yang akan digunakan untuk proses enkripsi dan dekripsi file.
b) Proses enkripsi file menggunakan kunci enkripsi, yaitu proses mengubah isi data file yang akan dienkripsi menjadi *ciphertext* yang tidak dapat terbaca dengan menggunakan kunci enkripsi tersebut.
c) Proses dekripsi *ciphertext* menggunakan kunci dekripsi yang sama dengan kunci enkripsi, yaitu proses mengubah *ciphertext* menjadi isi data file yang dapat terbaca kembali (*plaintext*).

3) Analisis Sistem

Implementasi pengamanan pada sistem adalah proses enkripsi isi file. Enkripsi dilakukan untuk mengamankan isi file yang bersifat rahasia/penting (hanya pihak berwenang yang bisa akses). Karena itu

membutuhkan modul untuk melakukan enkripsi data tersebut. Modul pengenkripsi ditempatkan pada aplikasi yang akan dipanggil ketika pengguna ingin mengamankan isi file. Sedangkan modul pendekripsi dipanggil ketika user ingin melihat isi file.

f. Perancangan Perangkat Lunak

Pada bagian ini dilakukan perancangan sesuai dengan hasil sistem terutama perancangan modul enkripsi dan dekripsi, dan modul pendukung lainnya yang akan diimplementasikan pada aplikasi, serta analisis antarmuka. Dalam tahap pengembangan perangkat lunak akan digunakan dengan menggunakan metode *Waterfall*. Model ini membutuhkan penyelesaian suatu tahap secara menyeluruh sebelum melanjutkan ke tahap berikutnya.

g. Implementasi

Pada proses implementasi ini dilakukan pembuatan modul-modul yang telah dirancang dalam tahap perancangan ke dalam bahasa pemrograman tertentu. Dalam hal ini aplikasi ini akan digunakan :

1) Perangkat lunak yang digunakan dalam penerapan pengamanan file menggunakan bahasa pemrograman *PHP* dan *DBMS* menggunakan *MySQL*.
2) Perangkat keras yang akan digunakan *Processor Intel Core i3, RAM 4 GB, Harddisk 1 TB*.

h. Pengujian Sistem

Tahap pengujian dilakukan dengan maksud tujuan untuk menjamin sistem yang sesuai dengan hasil analisis dan perancangan serta menghasilkan satu kesimpulan apakah sistem tersebut sesuai dengan yang diharapkan. Untuk itu diperlukan suatu metode pengujian yang menjadi ukuran atau parameter sehingga dapat disimpulkan bahwa sistem memang telah berjalan sesuai dengan tujuannya. Metode pengujian yang digunakan adalah *blackbox*, yaitu sebuah metode yang digunakan untuk menemukan kesalahan dan mendemonstrasikan fungsional aplikasi saat dioperasikan, apakah input diterima dengan benar dan output yang dihasilkan telah sesuai dengan yang diharapkan.

i. Kesimpulan

Pada tahap ini didapatkan kesimpulan akhir pada penerapan kriptografi dari metode *Advanced Encryption* Standard (AES) untuk pengamanan isi file pada SMK Muhammadiyah 4 Jakarta, menurut dengan hasil pengujian yang sudah dilakukan, untuk mengetahui apakah implementasi metode *Advanced Encryption Standard* (AES) yang sudah dilakukan dapat melakukan pengamanan terhadap isi file dengan baik. Pada kesimpulan ini juga diberikan saran untuk perbaikan pada pengembangan sistem.

2.1 *Advanced Encryption Standard*

a. Algoritme Enkripsi AES-128

Ringkasan algoritme Rijndael yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut (selain proses pembuatan *addround key*):

1) *AddRoundKey* Melakukan *XOR* antara *state awal* (*plaintext*) dengan *cipher key*, tahapan ini disebut juga *initial round*.
2) Putaran sebanyak Nr – 1. Proses yang dilakukan pada setiap putaran adalah.
   a) *SubBytes* subtitusi *byte* dengan menggunakan tabel subtitusi (*S-box*).
   b) *ShiftRows* pergeseran baris-baris *array state* secara *wrapping*.
   c) *MixColumns* mengacak data di masing-masing kolom *array state*.
   d) *AddRoundKey* melakukan *XOR* antara *state* sekarang dengan *round key*.
3) Final Round atau proses untuk putaran terakhir
   a) *SubBytes*
   b) *ShiftRows*
   c) *AddRoundKey*

b. Algoritme Dekripsi AES-128

Proses dekripsi adalah kebalikan dari proses enkripsi, dengan beberapa tahap pemrosesan dan komputasi yang sama berikut langkah-langkahnya.

1) *AddRoundKey*: melakukan *XOR* antara *state awal* (*ciphertext*) dengan *cipher key*. Tahap ini disebut juga *initial round*.
2) Putaran sebanyak Nr-1 kali. Proses yang dilakukan pada setiap putaran adalah.
   a) *Inverse InverseShiftRows*: pergeseran baris-baris *array state* secara *wrapping* kebalikan dari *ShiftRows*.
   b) *InverseSubBytes*: subtitusi *byte* dengan menggunakan tabel *invers* subtitusi (*invers S-box*).
   c) *AddRoundKey*: melakukan *XOR* antara *state* sekarang dengan *round key*.
   d) *InverseMixColumns*: membalikkan operasi *MixColumns*.
3) *Final round*: proses untuk putaran terakhir

a) *InverseShiftRows*
b) *InverseSubBytes*
c) *AddRoundKey*

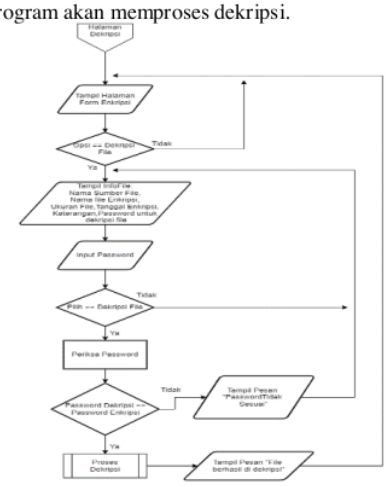
3. HASIL DAN PEMBAHASAN

3.1. *Flowchart*

Gambar 2 menyajikan *flowchart* dari halaman enkripsi file. Yang dimana *flowchart* ini menjelaskan tentang melakukan enkripsi file, dalam mengenkripsi pengguna harus memasukkan *password*, setelah itu program akan memproses enkripsi.

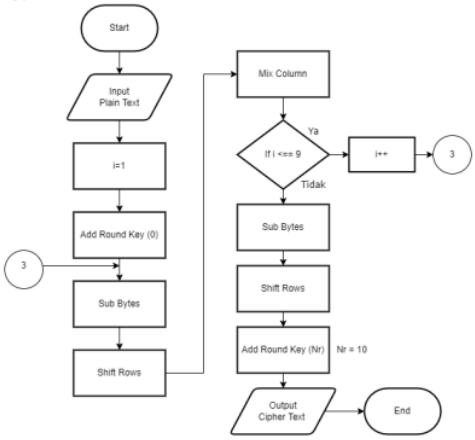
Gambar 2. *Flowchart* Halaman Enkripsi File

Gambar 3 menyajikan *flowchart* dari halaman dekripsi file. Yang dimana *flowchart* ini menjelaskan tentang melakukan dekripsi file, dalam mendekripsi file pengguna harus memasukkan *password* yang sesuai dengan *password* enkripsi file, setelah itu program akan memproses dekripsi.



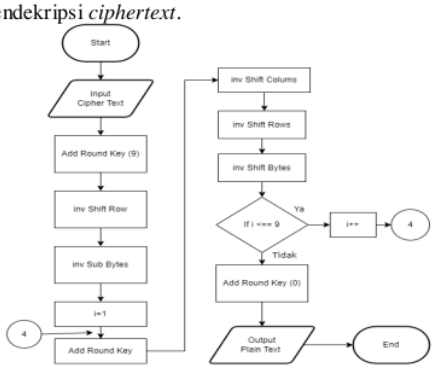
Gambar 3. *Flowchart* Halaman Dekripsi File

Gambar 4 menyajikan *flowchart* dari proses enkripsi AES. Menjelaskan alur proses yang terjadi pada enkripsi menggunakan algoritme AES-128.



Gambar 4. *Flowchart* Proses Enkripsi

Gambar 5 menyajikan *flowchart* dari proses dekripsi AES. Menjelaskan alur proses apa saja yang terjadi pada algoritme AES-128 untuk mendekripsi *ciphertext*.



Gambar 5. *Flowchart* Proses Dekripsi

3.2. Tampilan Layar

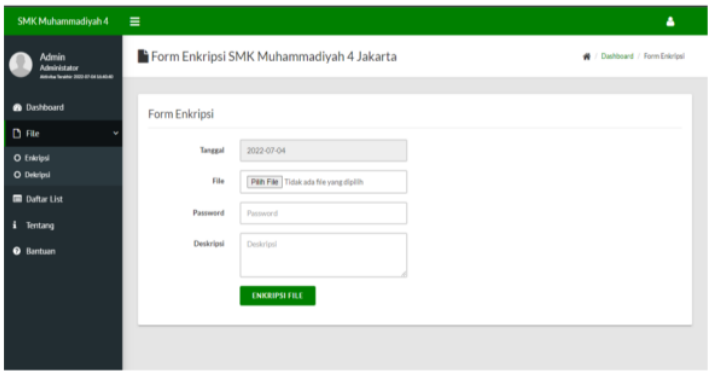
Setelah program dirancang, berikutnya dibuat sesuai dengan yang dirancang, dibuatlah program berbasis web. Gambar 6 menyajikan tampilan halaman *login*, untuk bisa masuk kedalam halaman beranda, pengguna harus memasukkan *username* dan *password* dengan sesuai.

Gambar 6. Tampilan Layar *Login*

Tampilan Layar Halaman Beranda Ketika pengguna berhasil *login* dan sistem mengenali pengguna yang terdaftar pada *database*, maka akan ditampilkan halaman beranda seperti yang disajikan pada gambar 7. Pada halaman beranda, terdapat menu-menu file. Terdapat 2 *submenu* dari file yang isinya adalah enkripsi, dekripsi. Lalu terdapat menu Daftar list, Tentang dan Bantuan. Dan di dalam halaman beranda terdapat beberapa fitur yang dapat menampilkan jumlah user, jumlah file enkripsi, dan jumlah file dekripsi.

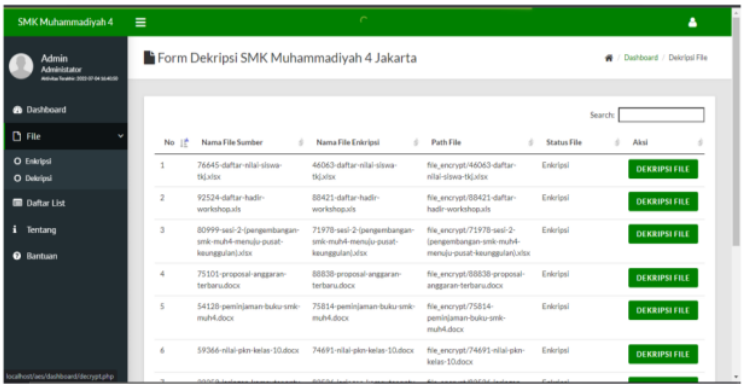
Gambar 7. Tampilan Layar Beranda

Tampilan Layar Halaman File Enkripsi Ketika sistem mengenali pengguna, maka akan ditampilkan halaman file enkripsi seperti yang disajikan pada gambar 8. Pada halaman file enkripsi, pengguna dapat melakukan enkripsi file.



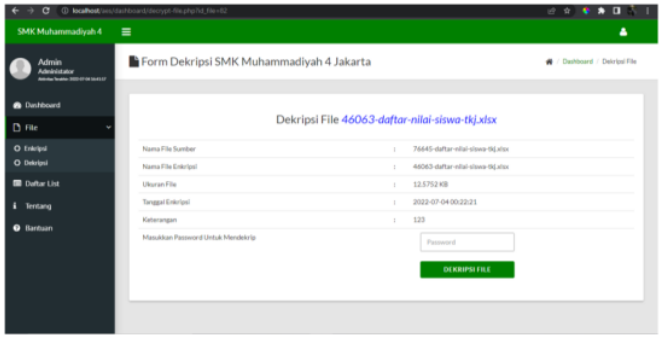
Gambar 8. Halaman Enkripsi File

Tampilan Layar Halaman File Tabel Dekripsi Ketika sistem mengenali pengguna, maka akan ditampilkan halaman file dekripsi seperti yang disajikan pada gambar 9. Pada halaman file dekripsi, pengguna dapat memilih file yang terenkripsi dan menekan *button* dekripsi file untuk melakukan dekripsi file.



Gambar 9 Tampilan Layar Tabel Dekripsi

Ketika sistem mengenali pengguna, maka akan ditampilkan halaman dekripsi file seperti yang disajikan pada gambar 10. Pada halaman form dekripsi, untuk melakukan proses dekripsi pengguna harus memasukkan *password* yang sesuai dengan *password* enkripsi.



Gambar 10. Tampilan Layar Dekripsi

3.3. Pengujian

Berikut adalah hasil dari pengujian file yang asli dengan file yang telah terenkripsi menggunakan aplikasi ini dengan kebutuhan yang telah terpenuhi baik spesifikasi *software* maupun spesifikasi *hardware*. File yang akan dicoba meliputi dengan format **.doc*, **.docx*, **.txt*, dan **.pdf*.

Pada tabel 1 menyajikan hasil proses enkripsi file dan tabel 2 menyajikan hasil dekripsi file yang dikerjakan oleh sistem dengan menggunakan aplikasi ini.

Tabel 1. Hasil Proses Enkripsi File

No	Nama Sebelum Enkripsi	Ukuran *File* Sebelum Enkripsi (Kb)	Waktu Enkripsi (Detik)	Nama Sesudah Enkripsi	Ukuran *File* Sesudah Enkripsi (Kb)
1.	Soal Instalasi Jaringan Wide Area Network XII.doc	2520	63.162	76268-soal-instalasi-jaringan-wide-area-network-xii.doc	2520
2.	SOAL MENDIAGNOSIS XI.doc	2511.5	60.290	14930-soal-mendiagnosis-xi.doc	2511.5
3.	Soal PAT Komputer Dan Jaringan Dasar 2021-2022 Genap.pdf	1981.46	47.726	15361-soal-pat-komputer-dan-jaringan-dasar-2021-2022-genap.pdf	1981.46
4.	Soal PAT Teknologi Layanan Jaringan 2021-2022 Genap.pdf	226.571	5.319	66657-soal-pat-teknologi-layanan-jaringan-2021-2022-genap.pdf	226.571

5.	SOAL UAS PANCASILA KLS 122021.txt	2.639	0.073	26995-soal-uas-pancasila-kls-122021.txt	2.639
6.	SOAL Ujian Sistem Komputer Kelas X .doc	2503.5	58.874	33342-soal-ujian-sistem-komputer-kelas-x-.doc	2503.5
7.	Soal Ujian Sistem Komputer Kelas XI GANJIL.doc	2516.5	58.528	85003-soal-ujian-sistem-komputer-kelas-xi-ganjil.doc	2516.5
8.	Soal UKK Etika Profesi Kelas X AK.docx	100.883	2.332	72483-soal-ukk-etika-profesi-kelas-x--ak.docx	100.883
9.	XI PKN PTS Genap.pdf	98.659	2.351	5567xi-pkn-pts-genap.pdf	98.659

Tabel 2. Hasil Proses Dekripsi File

No	Nama Sebelum Dekripsi	Ukuran *File* Sebelum Dekripsi (Kb)	Waktu Dekripsi (Detik)	Nama Sesudah Dekripsi	Ukuran *File* Sesudah Dekripsi (Kb)
1.	76268-soal-instalasi-jaringan-wide-area-network-xii.doc	2520	61.415	31752-soal-instalasi-jaringan-wide-area-network-xii.doc	2520
2.	14930-soal-mendiagnosis-xi.doc	2511.5	67.084	89535-soal-mendiagnosis-xi.doc	2511.5
3.	15361-soal-pat-komputer-dan-jaringan-dasar-2021-2022-genap.pdf	1981.46	48.395	81565-soal-pat-komputer-dan-jaringan-dasar-2021-2022-genap.pdf	1981.46
4.	66657-soal-pat-teknologi-layanan-jaringan-2021-2022-genap.pdf	226.571	6.169	69961-soal-pat-teknologi-layanan-jaringan-2021-2022-genap.pdf	226.571
5.	26995-soal-uas-pancasila-kls-122021.txt	2.639	0.087	34098-soal-uas-pancasila-kls-122021.txt	2.639
6.	33342-soal-ujian-sistem-komputer-kelas-x-.doc	2503.5	66.123	60809-soal-ujian-sistem-komputer-kelas-x-.doc	2503.5
7.	85003-soal-ujian-sistem-komputer-kelas-xi-ganjil.doc	2516.5	66.600	50629-soal-ujian-sistem-komputer-kelas-xi-ganjil.doc	2516.5
8.	72483-soal-ukk-etika-profesi-kelas-x--ak.docx	100.883	2.970	61361-soal-ukk-etika-profesi-kelas-x--ak.docx	100.883
9.	5567-xi_pkn_pts_genap.pdf	98.659	2.460	84229-xi_pkn_pts_genap.pdf	98.659

Waktu yang didapat dari hasil percobaan proses enkripsi dan dekripsi dari sembilan file soal ujian, menunjukan rata-rata waktu pengenkripsian yaitu 33. 183 detik dan rata rata waktu dekripsi yaitu 35.700 detik, dengan ukuran file kurang dari 3Mb. Ukuran file setelah dienkripsi maupun didekripsi kembali ke ukuran file awal, tetapi ukuran file juga ikut mempengaruhi waktu pada saat melakukan proses enkripsi dan dekripsi.

4. KESIMPULAN

Sesuai dengan pembahasan mengenai pengamanan file menggunakan metode AES-128 bit, maka dapat disimpulkan yaitu:

a. Algoritme AES-128 bit berhasil diterapkan pada pengamanan file SMK Muhammadiyah 4 Jakarta.
b. Waktu yang didapat dari hasil percobaan proses enkripsi dan dekripsi dari sembilan file soal ujian, menunjukan rata-rata waktu pengenkripsian yaitu 33.183 detik dan rata rata waktu dekripsi yaitu 35.700 detik.
c. Untuk mengamankan file dilakukan enkripsi sehingga hanya pengguna yang mengetahui kunci yang bisa mendekripsi file agar file yang terenkripsi dapat kembali asli.
d. Dapat mengenkripsi file dari Word, Excel, PowerPoint, Text, dan Pdf.

DAFTAR PUSTAKA

[1] A. Prayitno dan N. Nurdin, "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia," *J. Elektron. Sist. Inf. dan Komput.*, vol. 3, no. 1, pp. 1–11, 2017, [Online]. Available: nnurdin69@gmail.com.

[2] T. H. Saputro, N. H. Hidayati, dan E. I. H. Ujianto, "Survei Tentang Algoritma Kriptografi Asimetris," *J. Inform. Polinema*, vol. 6, no. 2, pp. 67–72, 2020, doi: 10.33795/jip.v6i2.345.
[3] O. Dakhi, M. Masril, R. Novalinda, J. Jufrinaldi, dan A. Ambiyar, "Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher," *INVOTEK J. Inov. Vokasional dan Teknol.*, vol. 20, no. 1, pp. 27–36, 2020, doi: 10.24036/invotek.v20i1.647.
[4] D. Nurnaningsih dan 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.
[5] L. A. Putri dan A. Solichin, "Pengamanan Aplikasi Mobile BluCampus dengan Algoritma AES-128 dan Affine Cipher : Studi Kasus Universitas Budi Luhur," vol. 1, no. MARET, 2018.
[6] A. Pariddudin dan F. Syauqi, "Penerapan Algoritma AES pada QR CODE untuk Keamanan Verifikasi Tiket," *Teknois J. Ilm. Teknol. Inf. dan Sains*, vol. 10, no. 2, pp. 43–52, 2020, doi: 10.36350/jbs.v10i2.87.
[7] A. M. Hasibuan, "Rancang Bangun Aplikasi Keamanan Data Menggunakan Metode AES Pada Smartphone," *MEANS (Media Inf. Anal. dan Sist.*, vol. 2, no. 1, pp. 29–35, 2017, doi: 10.54367/means.v2i1.20.
[8] A. Prameshwari dan N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Inform.*, vol. 8, no. 1, p. 52, 2018, doi: 10.30864/eksplora.v8i1.139.
[9] A. K. W. F. D. N. M. Kusnawi, "Aplikasi Quiz Psikologis Berbasis Website Dengan Pengaplikasian Algoritma Des," *Semin. Nas. Teknol. Inf. dan Multimed. 2017*, pp. 43–48, 2017.
[10] S. Rahmawati, I. Taufik, dan G. Sandi, "Implementasi Algoritma AES (Advanced Encryption Standard) 256 Bit Dan Kompresi Menggunakan Algoritma Huffman Pada Aplikasi Voice Recorder," *Prosiding-Seminar Nas. Tek. Elektro UIN Sunan Gunung Djati Bandung*, pp. 91–99, 2018.
[11] C. Saefudin, G. Abdillah, dan A. Maspupah, "Pengamanan Source Code Program Menggunakan Algoritma Advanced Encryption Standard Danalgoritma Base64," *Semin. Nas. Apl. Teknol. Inf.*, pp. 9–18, 2019.

Penerapan Kriptografi Menggunakan Advanced Encryption Standard 128 Untuk Pengamanan File Pada SMK Muhammadiyah 4

ORIGINALITY REPORT

13%	%	7%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Southern Mississippi Student Paper	5%
2	Submitted to Universitas Muria Kudus Student Paper	4%
3	Submitted to UIN Sultan Syarif Kasim Riau Student Paper	2%
4	Asri Prameshwari, Nyoman Putra Sastra. "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen", Eksplora Informatika, 2018 Publication	1%
5	Adhika Pramita Widyassari, Teguh Yuwono. "Sistem Pendukung Keputusan Pemilihan Rumah di Kawasan Cepu Menggunakan Analytical Hierarchy Process", INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi, 2019	1%

Publication

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		