SKANIKA: Sistem Komputer dan Teknik Informatika
Volume 6, Nomor 1, Januari 2023, Halaman 22-31 E-ISSN: 2721-4788

Implementasi Kriptografi dengan Metode AES-128 untuk Pengamanan File Berbasis Web pada SMP Yapipa

Isra Priambudi[1*], Mufti[2]
[1,2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta Selatan, Indonesia
Email: [1*]israpriambudi16@gmail.com, [2]mufti@budiluhur.ac.id
(* : corresponding author)

Abstrak

Secara khusus, perkembangan teknologi sistem keamanan data untuk menjaga keamanan data sudah berkembang pesat. Dan sekolah zaman sekarang mencatat file-file penting seperti file soal ujian secara sistematis dan terkomputerisasi, karna file soal ujian bersifat internal dimana hanya pihak sekolah yang terkait saja yang memiliki wewenang untuk mengetahui file soal ujian tersebut. Masalahannya di sekolah ini tidak memiliki sistem untuk pengamanan file terutama dibagian soal ujian yang cukup penting bagi sekolah. Sebagai solusi dari masalah tersebut, maka penelitian ini merancang sebuah aplikasi yang dapat melindungi file agar tidak dapat dibaca/dipahami oleh orang lain. Penelitian ini akan mengimplementasikan kriptografi menggunakan algoritme AES-128 untuk proses enkripsi dan dekripsi file dokumen yang berformat PDF, XLS, DOC, dan TXT. Hasil yang diperoleh setelah melakukan beberapa percobaan dari penerapan enkripsi dan dekripsi menggunakan AES-128, maka diperoleh hasil bahwa isi file soal ujian asli (*plaintext*) yang dienkripsi menggunakan AES-128 dapat terenkripsi dengan baik, hal ini terbukti dari isi file soal ujian yang hasilkan tidak dapat dimengerti oleh pengguna, kemudian setelah isi file soal ujian tersebut dideskripsi, maka akan kembali seperti data awal yang diinputkan. Waktu dari hasil uji enkripsi dan dekripsi dari sembilan file soal uji menunjukkan bahwa rata-rata waktu enkripsi adalah 1,3108 detik dan waktu dekripsi rata-rata 1,5532 detik, dengan ukuran file kurang dari 3MB relatif cepat yaitu kurang dari 4 detik. Ukuran file juga mempengaruhi berapa lama proses enkripsi dan dekripsi berjalan, tetapi ukuran file setelah dienkripsi maupun didekripsi kembali ke ukuran file awal. Kesimpulannya algoritme AES-128 bit ini berhasil diterapkan pada pengamanan file SMP YAPIPA, untuk pengamanan file yang dilakukan dengan cara enkripsi sehingga hanya orang yang mengetahui kunci yang dapat mendekripsi file agar file tersebut dapat kembali seperti semula dan file tidak dapat dipahami oleh pihak yang tidak berhak atau yang tidak memiliki kunci.

Kata Kunci: keamanan, kriptografi, *advanced encryption standart* (AES), enkripsi, dekripsi, file soal ujian.

Abstract

In particular, the development of data security system technology to maintain data security has grown rapidly. And today's schools record important files such as exam question files systematically and computerized because the exam question files are internal and only the school concerned has the authority to know the exam question files. The problem is that this school does not have a system for securing files, especially in the exam questions section which is quite important for the school. As a solution to this problem, this research designs an application that can protect files from being read/understood by others. This study will implement cryptography using the AES-128 algorithm for the encryption and decryption process of document files in PDF, XLS, DOC, and TXT formats. The results obtained after carrying out several experiments from the application of encryption and decryption using AES-128, the results obtained that the contents of the original exam file (plaintext) encrypted using AES-128 can be well encrypted, this is evident from the contents of the exam question files that are generated. cannot be understood by the user, then after the contents of the exam question file are described, it will return to the initial data entered. The time encryption and decryption test results from the nine test files shows that the average encryption time is 1.3108 seconds and the average decryption time is 1.5532 seconds, with a file size of less than 3MB which is relatively fast, which is less than 4 seconds. The file size also affects how long the encryption and decryption process takes, but the file size after being encrypted or decrypted returns to the initial file size. In conclusion, the AES-128 bit algorithm was successfully applied to the YAPIPA SMP file security, for file security which is carried out by encryption so that only people who know the key can decrypt the file so that the file can return to its original state and the file cannot be understood by unauthorized parties. or who don't have a key.

***Keywords**: security, cryptography, advanced encryption standart (AES), encryption, description, exam question files.*

1. PENDAHULUAN

Dengan perkembangan teknologi yang semakin pesat, setiap orang menggunakan teknologi untuk banyak kegiatan, terutama pengelolaan data. Data sensitif serta data umum [1]. Kerahasiaan data atau informasi adalah layanan menyeluruh untuk mencegah informasi yang disimpan tidak mudah dibaca atau dipahami oleh orang yang tidak berwenang. [2]. Contoh file yang dijaga kerahasiaanya pada SMP YAPIPA adalah file soal ujian. File tidak dapat dilihat atau dibuka oleh sembarang orang, hanya orang tertentu yang dapat mengakses dokumen [3].

SMP YAPIPA merupakan sekolah yang berlokasi di kecamatan serpong utara, kota tangerang selatan. Layaknya seperti sekolah lain, SMP YAPIPA setiap semester akan dilaksanakan ujian, karna file soal ujian bersifat internal dimana hanya pihak sekolah yang terkait saja yang memiliki wewenang untuk mengetahui file soal ujian tersebut. Masalahannya di sekolah ini tidak memiliki sistem untuk pengamanan file terutama dibagian soal ujian yang cukup penting bagi sekolah. Karna SMP YAPIPA menyimpan file yang cukup penting yaitu file soal ujian secara sistematis dan terkomputerisasi di dalam satu folder pada komputer sekolah tanpa adanya sistem pengamanan file.

Berdasarkan hal tersebut, SMP YAPIPA memerlukan sebuah aplikasi pengamanan file berbasis web yang dapat melindungi file soal ujian dari kebocoran file. Penelitian ini akan mengimplementasikan kriptografi menggunakan algoritme AES-128 untuk proses enkripsi dan dekripsi file dokumen yang berformat PDF, XLS, DOC, dan TXT.

Banyak penelitian sebelumnya telah menerapkan kriptografi untuk keamanan data. Salah satunya adalah penggunaan enkripsi untuk keamanan data pada aplikasi berbasiskan desktop. [2] Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. Kelemahan dari aplikasi berbasis desktop adalah bahwa mereka harus diinstal atau dikonfigurasi pada setiap komputer yang menggunakannya. Sama halnya dengan penerapan kriptografi pengamanan data pada aplikasi berbasiskan mobile [4] Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android. Kekurangan aplikasi berbasiskan mobile juga harus menginstall terlebih dahulu pada smartphone yang ingin digunakan.

Penelitian sebelumnya juga banyak penerapan kriptografi pengamanan data pada aplikasi berbasiskan web [5] Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman. Salah satu kelebihan aplikasi keamanan data berbasis web adalah pengguna hanya perlu menggunakan browser untuk mengakses alamat web server.

Selain berbeda basis ada juga penelitian penerapan kriptografi yang berbeda algoritme, contohnya seperti penelitian sebelumnya [6] Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES. Kekurangan pengamanan data algoritme DES adalah algoritme tersebut sudah dianggap kuno dan mudah dibobol [7].

Sama seperti penelitian ini, penelitian sebelumnya juga sudah banyak yang menggunakan algoritme AES [8] Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Hal ini dikarenakan, penelitian sebelumnya menunjukkan bahwa kecepatan enkripsi dan dekripsi AES masih lebih unggul daripada algoritme lain. [9], [10].

2. METODE PENELITIAN

Tahapan penelitian yang dilakukan pada penelitian ini adalah sebagai berikut:

a. Studi Literatur

Studi juga dilakukan dengan mempelajari berbagai jenis buku, kuliah, jurnal, dan makalah akademik yang terkait dengan topik yang sedang dibahas yaitu kriptografi, khususnya algoritme *Advanced Encryption Standard* (AES), sehingga penulis mendapatkan dasar-dasar referensi yang kuat dan benar untuk memecahkan masalah yang sedang diteliti.

b. Studi Lapangan

Pada tahap ini akan dilakukan studi kasus dalam pengamanan file di SMP YAPIPA untuk menemukan permasalahan yang ada dan merumuskannya dalam rumusan masalah.

c. Perumusan Masalah

Pada tahap ini diidentifikasi masalah yang akan dipecahkan dalam investigasi ini: tidak adanya keamanan pada file soal ujian SMP YAPIPA.

d. Pengumpulan Data

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

1) Wawancara (*interview*)

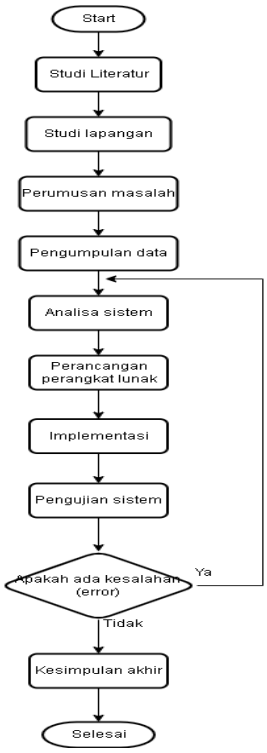
Wawancara adalah proses tatap muka bertanya dan mengumpulkan data tentang pengamanan file soal ujian yang dilakukan pada kepala sekolah sebagai pihak yang berwenang untuk membuat aplikasi kriptografi pengamanan file. Dari wawancara tersebut, penulis juga mendapatkan file soal-soal ujian yang akan digunakan dalam pengembangan sistem kriptorafi pengamanan file.

2) Observasi

Kegiatan ini dilakukan untuk mengamati secara langsung masalah-masalah yang berkaitan dengan sistem keamanan file kriptografi pengamanan file sekaligus sebagai masukan dalam penelitian ini.

3) Studi Pustaka

Kegiatan ini dilakukan dengan membaca majalah, *e-book*, dan referensi terkait teori kriptografi, teori pengamanan file, teori *Advanced Encryption Standard* (AES), dan teori lain yang terkait dengan pembuatan kriptografi pengamanan file ini.



Gambar 1. Tahapan Penelitian

e. Analisis Sistem

Menerapkan keamanan pada sistem adalah proses enkripsi isi file. Enkripsi dilakukan untuk mengamankan isi file yang bersifat rahasia/penting (hanya pihak berwenang yang bisa akses). Maka dari itu peneliti membutuhkan modul untuk mengenkripsi data. Modul pengenkripsi ditempatkan pada aplikasi yang akan dipanggil ketika user ingin mengamankan isi file. Sedangkan modul pendekripsi dipanggil ketika user ingin melihat isi file.

f. Perancangan Perangkat Lunak

Pada tahap ini dilakukan perancangan sesuai dengan hasil analisis sistem, khususnya perancangan modul enkripsi dan dekripsi serta modul pendukung lainnya yang terintegrasi ke dalam aplikasi, dan perancangan antarmuka.

g. Implementasi

Dalam proses implementasi ini, modul yang dirancang dalam tahap perancangan diimplementasikan dalam bahasa pemrograman tertentu. Dalam hal ini aplikasi yang digunakan:

1) *Software* yang akan digunakan dalam implementasi pengamanan file menggunakan bahasa pemrograman PHP dan DBMS menggunakan MySQL.
2) Dan *hardware* akan menggunakan *Processor Intel Pentium* G4400, Memori RAM HYNIX 4GB DDR3, *Hardisk Seagate* 250GB Slim.

h. Pengujian Sistem

Tahap pengujian dilakukan dengan tujuan untuk memastikan bahwa sistem yang dibuat sudah sesuai dengan hasil analisis dan rancangan, sehingga menghasilkan kesimpulan apakah sistem tersebut memenuhi harapan. Untuk itu diperlukan suatu metode pengujian yang merupakan suatu ukuran atau parameter yang dengannya peneliti dapat menyimpulkan bahwa sistem tersebut memang telah bekerja sesuai dengan tujuannya.

i. Kesimpulan

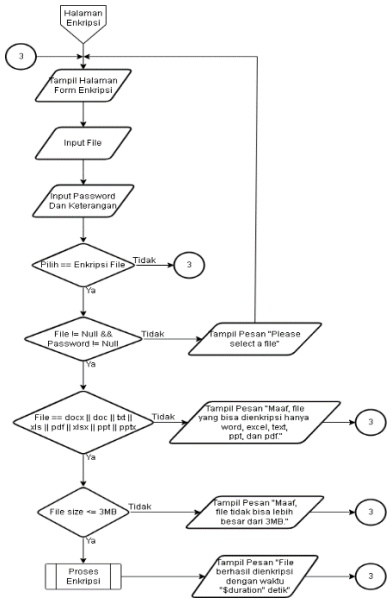
Pada tahap ini, kesimpulan akhir mengenai penerapan kriptografi *Advanced Encryption Standard* (AES) untuk pengamanan file soal ujian pada SMP YAPIPA adalah untuk menentukan apakah implementasi *Advanced Encryption Standard* (AES) sudah diterapkan berdasarkan hasil pengujian yang dilakukan isi file tidak dapat dipahami oleh sembarang orang, itu artinya sistem ini dapat melakukan pengamanan terhadap isi file dengan baik.

3. HASIL DAN PEMBAHASAN

3.1 *Flowchart*

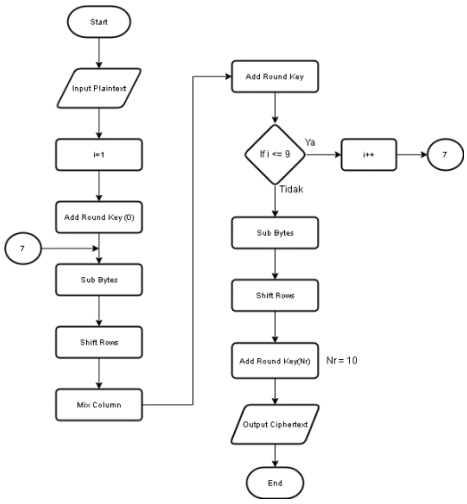
Berikut ini adalah flowchart atau gambaran alur algoritme aplikasi enkripsi dan dekripsi file ini dalam bentuk diagram, yang menyatakan alur arah aplikasi enkripsi dan dekripsi tersebut. Berikut adalah flowchart alur sistem dari aplikasi enkripsi dan dekripsi file.

Berikut adalah *flowchart* dari halaman *form* enkripsi, dimana *flowchart* ini menjelaskan tentang melakukan enkripsi file, dalam mengenkripsi admin *user* harus memasukkan *password*, setelah itu program akan memproses enkripsi. Dapat dilihat pada Gambar 2.



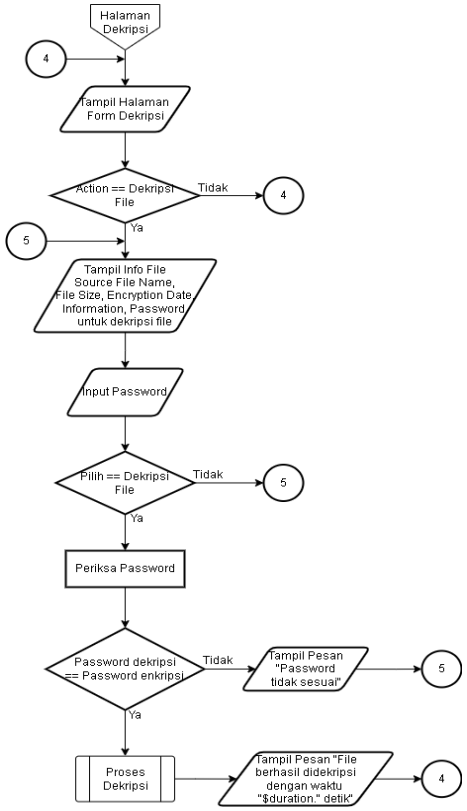
Gambar 2. *Flowchart Form* Enkripsi

Berikut adalah *flowchart* dari proses enkripsi AES. Menjelaskan alur proses apa saja yang terjadi pada enkripsi menggunakan AES-128. Dapat dilihat pada Gambar 3 berikut:



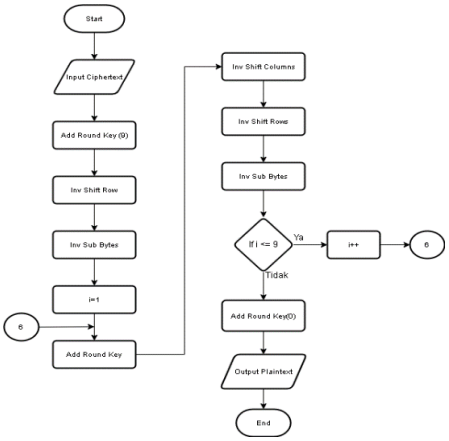
Gambar 3. *Flowchart* Enkripsi AES-128

Berikut adalah *flowchart* dari halaman *form* dekripsi, dimana *flowchart* ini menjelaskan tentang melakukan dekripsi file, dalam dekripsi file admin *user* harus memasukkan *password* yang sesuai dengan *password* enkripsi, setelah itu program akan memproses dekripsi. Dapat dilihat pada Gambar 4.



Gambar 4. *Flowchart Form* Dekripsi

Berikut adalah *flowchart* dari proses dekripsi AES. Menjelaskan alur proses yang terjadi pada algoritme AES-128 untuk mendekripsi *ciphertext.* Dapat dilihat pada Gambar 5.



Gambar 5. *Flowchart* Dekripsi AES-128

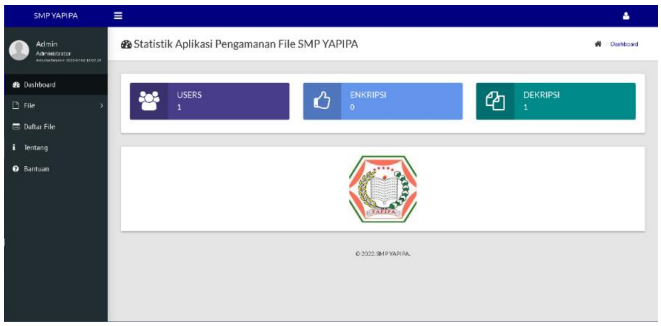
3.2 Tampilan Layar

Tampilan layar program aplikasi dapat membantu *user* mengetahui apakah aplikasi yang dibuat bekerja dengan baik dan optimal atau apakah menimbulkan kesalahan-kesalahan yang tidak diinginkan. Selain itu tampilan layar juga menjadi bahan evaluasi program yang dibuat oleh peneliti. Berikut ini adalah tampilan layar program aplikasi dan penjelasan tentang penggunaannya di setiap tampilan aplikasi pengamanan file menggunakan algoritme AES-128 bit.

Berikut adalah tampilan layar *login*, untuk dapat masuk kedalam halaman beranda, admin *user* harus memasukkan *username* dan *password* seperti pada Gambar 6. Berikut:

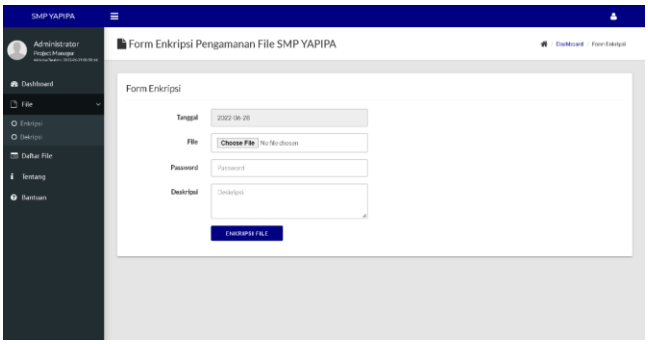
Gambar 6. Tampilan Layar *Login*

Ketika admin *user* berhasil *login* dan sistem mengenali admin *user* yang terdaftar pada database, maka akan ditampilkan halaman beranda seperti yang terlihat pada gambar 7. Pada halaman beranda, berisi informasi jumlah *user* yang terdaftar, jumlah file yang telah terenkripsi dan terdekripsi, dan juga berisi menu-menu. Terdapat menu *form* enkripsi, *form* dekripsi, dan *form* daftar file.



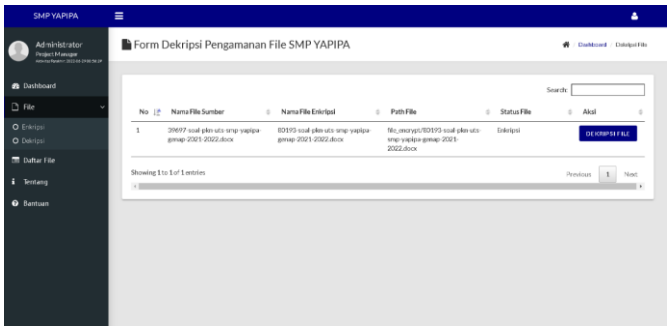
Gambar 7. Tampilan Layar Halaman Beranda

Ketika admin *user* memilih menu enkripsi, maka sistem akan menampilkan halaman *form* enkripsi seperti yang terlihat pada gambar 8. Pada halaman *form* enkripsi, admin *user* dapat melakukan enkripsi file.



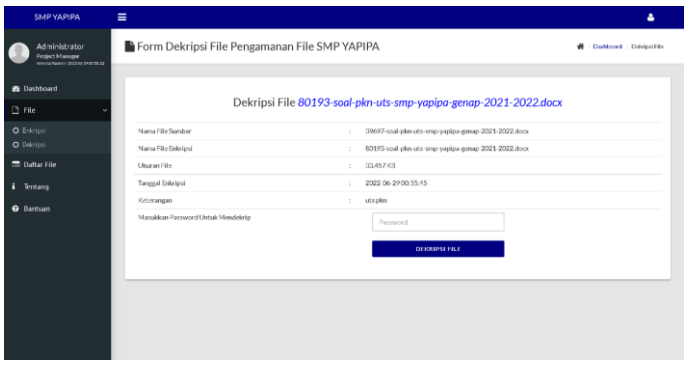
Gambar 8. Tampilan Layar *Form* Enkripsi

Ketika admin *user* memilih menu dekripsi, maka sistem akan menampilkan halaman *form* dekripsi seperti yang terlihat pada gambar 9. Pada halaman *form* dekripsi, admin *user* dapat memilih file yang terenkripsi dan menekan tombol dekripsi file untuk melakukan dekirpsi file.



Gambar 9. Tampilan Layar *List* File Dekripsi

Ketika admin *user* menekan tombol dekripsi file, maka sistem akan menampilkan halaman *form* dekripsi file seperti yang terlihat pada gambar 10. Pada halaman *form* dekripsi file, untuk melakukan proses dekripsi admin *user* harus memasukkan *password* yang sesuai dengan *password* enkripsi.



Gambar 10. Tampilan Layar *Form* Dekripsi

3.3 Pengujian

Setelah dibuatnya aplikasi, kemudian pengujian dilakukan dan berikut ini adalah hasil pengujian file yang asli dengan file yang telah dienkripsi dan sebaliknya. Penggunaan aplikasi ini dapat berjalan dengan persyaratan yang terpenuhi, baik spesifikasi perangkat lunak dan perangkat keras.

Berikut ini adalah tabel hasil dari proses enkripsi file dan dekripsi file yang dikerjakan oleh sistem dengan menggunakan aplikasi ini.

a. Tabel Proses Enkripsi

Tabel ini berisi proses pengujian enkripsi yang dikerjakan oleh sistem.

Tabel 1. Proses Enkripsi

No	Nama Sebelum Enkripsi	Ukuran File Sebelum Enkripsi (KB)	Waktu Enkripsi (Detik)	Nama Sesudah Enkripsi	Ukuran File Sesudah Enkripsi (KB)
1.	Soal UTS Bahasa Indonesia Kelas 9 SMP YAPIPA.docx	63,7 KB	1.0226 Detik	46048-soal-uts-bahasa-indonesia-kelas-9-smp-yapipa.docx	63,7 KB
2.	Soal Bahasa Inggris Kelas 9 SMP YAPIPA.docx	58,5 KB	0.9289 Detik	73219-soal-uts-bahasa-inggris-kelas-9-smp-yapipa.docx	58,5 KB
3.	Soal UTS IPA Kelas 9 SMP YAPIPA.docx	83,4 KB	1.3952 Detik	53279-soal-uts-ipa-kelas-9-smp-yapipa.docx	83,4 KB
4.	Soal UTS IPS Kelas 9 SMP YAPIPA.docx	87,8 KB	1.4594 Detik	36316-soal-uts-ips-kelas-9-smp-yapipa.docx	87,8 KB
5.	Soal UTS Matematika Kelas 9 SMP YAPIPA.docx	189 KB	3.1532 Detik	8173-soal-uts-matematika-kelas-9-smp-yapipa.docx	189 KB
6.	Soal UTS PAI Kelas 9 SMP YAPIPA.docx	55,9 KB	0.9436 Detik	70322-soal-uts-pai-kelas-9-smp-yapipa.docx	55,9 KB
7.	Soal UTS Penjaskes Kelas 9 SMP YAPIPA.docx	57,6 KB	0.9767 Detik	63223-soal-uts-penjaskes-kelas-9-smp-yapipa.docx	57,6 KB
8.	Soal UTS PKn Kelas 9 SMP YAPIPA.docx	56,4 KB	0.9371 Detik	82623-soal-uts-pkn-kelas-9-smp-yapipa.docx	56,4 KB
9.	Soal UTS Seni Budaya Kelas 9 SMP YAPIPA.docx	60,1 KB	0.9812 Detik	46478-soal-uts-seni-budaya-kelas-9-smp-yapipa.docx	60,1 KB

b. Proses Dekripsi

Tabel ini berisi proses pengujian dekripsi yang dikerjakan oleh sistem.

Tabel 2. Proses Dekripsi

No	Nama Sebelum Dekripsi	Ukuran File Sebelum Dekripsi (KB)	Waktu Dekripsi (Detik)	Nama Sesudah Dekripsi	Ukuran File Sesudah Dekripsi (KB)
1.	46048-soal-uts-bahasa-indonesia-kelas-9-smp-yapipa.docx	63,7 KB	1.0884 Detik	77858-soal-uts-bahasa-indonesia-kelas-9-smp-yapipa.docx	63,7 KB
2.	73219-soal-uts-bahasa-inggris-	58,5 KB	1.7034 Detik	32076-soal-uts-bahasa-inggris-kelas-	58,5 KB

	kelas-9-smp-yapipa.docx			9-smp-yapipa.docx	
3.	53279-soal-uts-ipa-kelas-9-smp-yapipa.docx	83,4 KB	1.4908 Detik	19736-soal-uts-ipa-kelas-9-smp-yapipa.docx	83,4 KB
4.	36316-soal-uts-ips-kelas-9-smp-yapipa.docx	87,8 KB	2.6086 Detik	30724-soal-uts-ips-kelas-9-smp-yapipa.docx	87,8 KB
5.	8173-soal-uts-matematika-kelas-9-smp-yapipa.docx	189 KB	3.2024 Detik	67256-soal-uts-matematika-kelas-9-smp-yapipa.docx	189 KB
6.	70322-soal-uts-pai-kelas-9-smp-yapipa.docx	55,9 KB	0.9824 Detik	88534-soal-uts-pai-kelas-9-smp-yapipa.docx	55,9 KB
7.	63223-soal-uts-penjaskes-kelas-9-smp-yapipa.docx	57,6 KB	0.9303 Detik	88127-soal-uts-penjaskes-kelas-9-smp-yapipa.docx	57,6 KB
8.	82623-soal-uts-pkn-kelas-9-smp-yapipa.docx	56,4 KB	0.9783 Detik	65443-soal-uts-pkn-kelas-9-smp-yapipa.docx	56,4 KB
9.	46478-soal-uts-seni-budaya-kelas-9-smp-yapipa.docx	60,1 KB	0.9945 Detik	33447-soal-uts-seni-budaya-kelas-9-smp-yapipa.docx	60,1 KB

Waktu dari hasil uji enkripsi dan dekripsi dari sembilan file soal uji menunjukkan bahwa rata-rata waktu enkripsi adalah 1,3108 detik dan waktu dekripsi rata-rata 1,5532 detik, dengan ukuran file kurang dari 3MB relatif cepat yaitu kurang dari 4 detik. Ukuran file juga mempengaruhi berapa lama proses enkripsi dan dekripsi berjalan, tetapi ukuran file setelah dienkripsi maupun didekripsi kembali ke ukuran file awal.

4. KESIMPULAN

Sesuai dengan pembahasan mengenai aplikasi enkripsi menggunakan metode AES-128 bit, maka kesimpulan yang dapat diambil dari penelitian ini adalah sebagai berikut:

a. Algoritme AES-128 bit berhasil diterapkan pada pengamanan file SMP YAPIPA.
b. Untuk pengamanan file dilakukan enkripsi sehingga hanya orang yang mengetahui kunci yang dapat mendekripsi file agar file tersebut dapat kembali asli dan file tidak dapat dipahami oleh pihak yang tidak berhak atau yang tidak memiliki kunci.
c. Kecepatan waktu ketika melakukan proses enkripsi dan dekripsi tergantung besar/kecilnya file yang akan diproses, semakin kecil file yang akan diproses maka kecepatan waktunya semakin cepat sebaliknya semakin besar file yang akan diproses maka kecepatan waktunya akan semakin lama.

DAFTAR PUSTAKA

[1] A. Ignasius and D. V. Shaka Yudha Sakti, “Penerapan Algoritma Aes (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi,” *Skanika*, vol. 5,

no. 1, pp. 1–10, 2022, doi: 10.36080/skanika.v5i1.2118.

[2] A. Prameshwari and 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.

[3] D. Darwis, R. Prabowo, and N. Hotimah, "Kombinasi Gifshuffle, Enkripsi AES dan Kompresi Data Huffman untuk Meningkatkan Keamanan Data," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 4, p. 389, 2018, doi: 10.25126/jtiik.201854727.

[4] Y. Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 29–37, 2019.

[5] W. Pramusinto, N. Wizaksono, and A. Saputro, "Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman," *J. Bit*, vol. 17, no. 2, pp. 46–52, 2020.

[6] W. R. Maya, A. Azanuddin, and E. Elfitriani, "Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 21, no. 1, p. 1, 2022, doi: 10.53513/jis.v21i1.4764.

[7] R. Laia, "Implementasi Algoritma Aes 256 Bit Dan Lsb Untik Pengamanan Dan Penyisipan Pesan Teks Pada File Audio," *Pelita Inform. Inf. dan Inform.*, vol. 8, no. April, pp. 467–469, 2020.

[8] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[9] M. A. Muin, A. Setyanto, and Sudarmawan, "Perbandingan Algoritma AES256 dan Blowfish," *J. Transform. (Informasi Pengemb. Iptek)*, vol. 14, no. 1, pp. 84–91, 2018.

[10] Donzilio Antonio Meko, "Jurnal Teknologi Terpadu Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , STIMIK Kupang Jurnal Teknologi Terpadu," *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 8–15, 2018.