

PENERAPAN ALGORITMA AES-128 UNTUK PENGAMANAN FILE PADA SMK PGRI 31 LEGOK

Kaliyana Tantri Rukmana^{1*}, Pipin Farida Ariyani²

^{1,2}Fakultas Teknologi Informasi, Teknik Informatika, Universita Budi Luhur, Jakarta, Indonesia

Email: ^{1*}kaliyanatantrirukmana31@gmail.com, ²pipin.faridaariyani@budiluhur.ac.id
(* : corresponding author)

Abstrak- Sekolah SMK PGRI 31 Legok memiliki banyak file-file yang tercatat secara sistematis dan terkomputerisasi. File nilai uas dan file data siswa tersebut bersifat internal dimana hanya pihak sekolah yang terkait saja yang memiliki wewenang untuk mengetahui file-file tersebut. Untuk pihak yang tidak memiliki wewenang mengetahui file tersebut akan menimbulkan kebocoran data, untuk mempertimbangkan hal itu perlu pengamanan data lebih lanjut. Maka dalam penelitian ini akan direncanakan untuk mengimplementasikan konsep pengamanan isi file dengan menggunakan kriptografi. Kriptografi merupakan salah satu solusi atau metode untuk melindungi dokumen, yang tepat untuk menjaga kerahasiaan dan keaslian dokumen, serta dapat meningkatkan aspek keamanan dokumen atau informasi. Salah satu metode kriptografi untuk mengamankan informasi adalah *Advanced Encryption Standard (AES)*. Penelitian ini bertujuan untuk membuat sebuah sistem keamanan data berbasis web menggunakan bahasa pemrograman *PHP* dan *MySQL* sebagai *Database Management System* dengan mengimplementasikan kriptografi enkripsi pada isi file data dengan menggunakan algoritma *Advanced Encryption Standard (AES)*. Sehingga file asli tidak dapat dibaca sehingga diperlukan proses dekripsi menggunakan *key* atau *password* yang sama pada saat melakukan enkripsi file tersebut agar isi file akan kembali ke asli. Ukuran file mempengaruhi berapa lama waktu yang dibutuhkan selama proses enkripsi dan dekripsi. Hasil dari percobaan dua file yang berbeda saat dienkripsi dan dekripsi dengan ukuran yang beda akan mempengaruhi berapa lama waktu enkripsi dan dekripsi. File yang berukuran 42.496 bytes waktu enkripsinya adalah 1.4714 milisecond dan file yang berukuran 22.176 bytes waktu enkripsinya adalah 0.7903 milisecond. Dari hasil implementasi dapat disimpulkan bahwa *algoritma kriptografi AES* dapat diimplementasikan dalam menjaga keamanan isi file.

Kata Kunci: keamanan, *kriptografi*, *advanced encryption standard (AES)*, *enkripsi*, *dekripsi*, file dokumen

APPLICATION OF AES-128 ALGORITMA FOR FILE SECURITY AT SMK PGRI 31 LEGOK

Abstract- PGRI 31 Legok Vocational School has many files that are recorded systematically and computerized. The final grade files and student data files are internal, where only the school concerned has the authority to find out about these files. For parties who do not have the authority to know that the file will cause data leakage, to consider this further data security is needed. So in this study it will be planned to implement the concept of securing file contents using cryptography. Cryptography is one solution or method to protect documents, which is appropriate to maintain the confidentiality and authenticity of documents, and can improve the security aspects of documents or information. One of the cryptographic methods for securing information is the *Advanced Encryption Standard (AES)*. This study aims to create a web-based data security system using the *PHP* programming language and *MySQL* as a *Database Management System* by implementing encryption cryptography on the contents of data files using the *Advanced Encryption Standard (AES)* algorithm. So that the original file cannot be read so that the decryption process is required using the same key or password when encrypting the file so that the contents of the file will return to the original. File size affects how long it takes during the encryption and decryption process. The results of the experiment of two different files when encrypted and decrypted with different sizes will affect how long the encryption and decryption time. The file size is 42,496 bytes the encryption time is 1.4714 milliseconds and the file size is 22,176 bytes the encryption time is 0.7903 millisecond. From the implementation results, it can be concluded that the *AES* cryptographic algorithm can be implemented in maintaining the security of file contents..

Keywords: security, cryptography, advanced encryption standard (AES), encryption, decryption, document files.

1. PENDAHULUAN

Keamanan data di sekolah SMK PGRI 31 Legok selama ini telah menerapkan teknologi informasi untuk pengelolaan data, namun data-data yang ada dalam sekolah tersebut masih berupa teks asli, yang dapat dengan mudah di baca. Hal ini dapat menimbulkan masalah karena sekolah SMK PGRI 31 Legok memiliki banyak file-file yang tercatat secara *sistematis* dan *terkomputerisasi*. File nilai uas dan file data siswa tersebut bersifat internal dimana hanya pihak sekolah yang terkait saja yang memiliki wewenang untuk mengetahui file-file tersebut karena

file tersebut bersifat penting. Untuk pihak yang tidak memiliki wewenang mengetahui file tersebut akan menimbulkan kebocoran data, untuk mempertimbangkan hal itu perlu pengamanan data lebih lanjut.

Terikat dengan masalah yang ada dan pentingnya pengamanan file maka dalam penelitian ini akan direncanakan untuk mengimplementasikan konsep pengamanan isi file yang digunakan untuk melindungi file nilai uas, file data siswa dan informasi penting demi menjaga kerahasiaan informasi file tersebut. Ilmu yang mempelajari konsep pengamanan isi file disebut dengan istilah kriptografi.

Dalam kriptografi terdapat metode yang bisa digunakan dalam kasus pengamanan file. Pada dasarnya file yang akan diamankan dilakukan penyandian atau pengacakan kode. Data file tidak bisa dibaca karena telah tersandi. Apabila file ingin dapat dibaca, maka harus melakukan pengembalian data yang telah tersandi tersebut ke data aslinya.

Kriptografi adalah teknologi keamanan informasi yang memproses informasi awal (*plaintext*) menggunakan metode *enkripsi* tertentu dengan kunci tertentu untuk menghasilkan informasi baru (*ciphertext*) yang tidak dapat dibaca. *Ciphertext* dapat dikembalikan ke informasi aslinya (*plaintext*) dengan proses *dekripsi*.

Algoritma AES (*Advanced Encryption Standard*) adalah pengembangan lebih lanjut dari algoritma *enkripsi standard DES (Data Encryption Standard)* yang telah dihentikan karena alasan keamanan. Kecepatan komputer yang sangat tinggi dianggap terlalu berbahaya bagi algoritma *DES*, sehingga pada tanggal 2 Maret 2001, algoritma baru *Rijndael* yang diberi nama *Advanced Encryption Standard (AES)*. Kriteria pemilihan untuk *AES* didasarkan pada tiga kriteria utama yaitu keamanan, harga, dan karakteristik algoritma beserta implementasinya.

Penelitian sebelumnya [1] enkripsi dalam pengamanan file data karyawan dengan metode *DES (data encryption standard)* pada cv. Sinergi Infomasi Global pada penelitian ini menggunakan algoritma *DES* untuk pengamanan file data karyawan.

Penelitian selanjutnya [2] pengamanan file menggunakan kriptografi dengan metode *AES-128* di komite nasional keselamatan transportasi. Pada penelitian ini mengamankan file data yang bersifat rahasia.

2. METODE PENELITIAN

2.1 Pengumpulan data

Tahapan ini dilakukan pengumpulan data-data yang dibutuhkan dalam perancangan sistem, adapun beberapa pendekatan yang dilakukan di antaranya seperti wawancara, *observasi* dan studi pustaka.

a. Wawancara

Proses ini dilakukan melalui wawancara atau sesi tanya jawab langsung dengan para pemangku kepentingan yang terlibat dalam pengembangan aplikasi dan program untuk mendapatkan informasi tentang aplikasi dan keamanan yang ada.

b. Observasi

Observasi dilakukan di SMK PGRI 31 Legok untuk mengetahui keadaan objek penelitian yang sebenarnya. Hal ini dimaksudkan untuk memberikan gambaran tentang data dan informasi yang diperlukan untuk penelitian.

c. Studi Pustaka

Studi Pustaka ini dilakukan dengan membaca jurnal dan *e-book*, materi-materi yang berkaitan dengan teori kriptografi keamanan file, menggunakan metode *Advanced Encryption Standard (AES)*, dan teori-teori lain yang berkaitan dengan pembuatan *kriptografi* keamanan file ini.

2.2 Advanced Encryption Standard (AES)

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 *chiprterkey*, tahapan ini disebut juga *initial round*.
2. Putaran sebanyak $Nr - 1X$. Proses yang dilakukan pada setiap putaran adalah.
 - a) *SubBytes* substitusi byte dengan menggunakan tabel substitusi (*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) *InverseInverseShiftRows* : pergeseran baris-baris *array state* secara *wrapping* kebalikan dari *ShiftRows*.
 - b) *InverseSubBytes* : substitusi *byte* dengan menggunakan tabel *invers* substitusi (*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*

2.3 Perancangan Perangkat Lunak

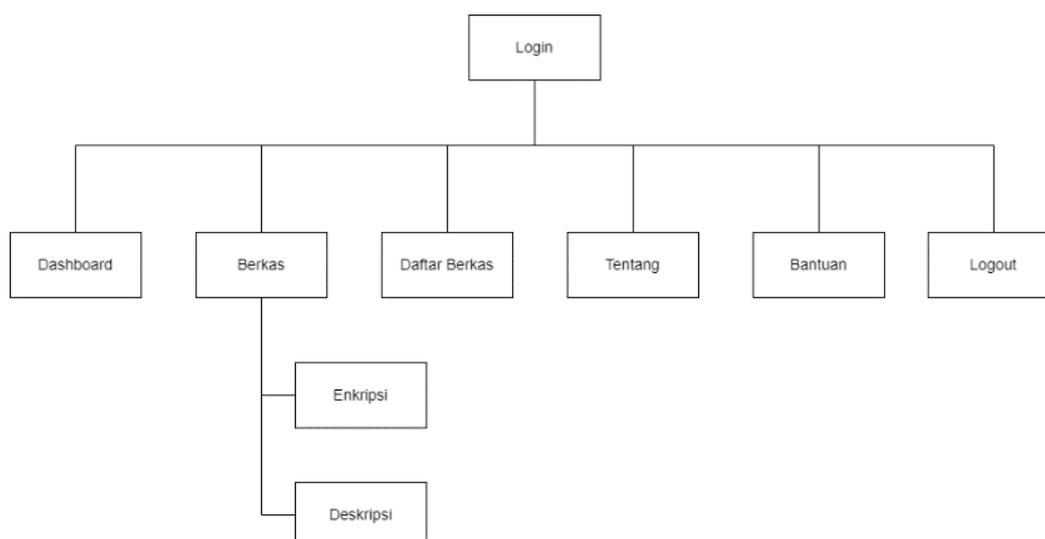
Tahapan ini dilakukan perancangan berdasarkan hasil analisis sistem, khususnya perancangan enkripsi dan dekripsi. Selain itu, dukungan tambahan dibangun ke dalam aplikasi dan desain antarmuka. Pengembangan sistem dengan metode waterfall. Model harus diselesaikan secara berurutan sebelum melanjutkan ke tahap berikutnya dan hasil dari setiap tahap harus didokumentasikan dengan baik.

2.4 Rancangan Pengujian

Selama tahap pengujian ini, pengujian dilakukan dengan tujuan untuk memverifikasi apakah sistem yang dibuat sesuai dengan hasil analisis dan desain. apakah aplikasi sesuai dengan yang diharapkan. Untuk mengetahui apakah suatu sistem berperilaku seperti yang diharapkan, diperlukan suatu metode pengujian yang merupakan ukuran atau parameter untuk pengujian sistem. Metode pengujian yang digunakan adalah pengujian *black box*. Ini adalah teknik yang digunakan untuk menguji aplikasi untuk menemukan *bug* dan menjalankan eksperimen pada aplikasi fungsional saat runtime untuk melihat apakah aplikasi menerima *input* dan menghasilkan *output* yang diinginkan. Aplikasi itu seperti yang diharapkan.

2.5 Rancangan Menu

Gambar 1 Menunjukkan Rancangan menu pada aplikasi yang akan dibuat terdiri dari beberapa tampilan menu yaitu dashboard, berkas, daftar berkas, tentang dan bantuan di menu berkas terdapat pilihan untuk enkripsi file dan dekripsi file.



Gambar 1. Rancangan Menu

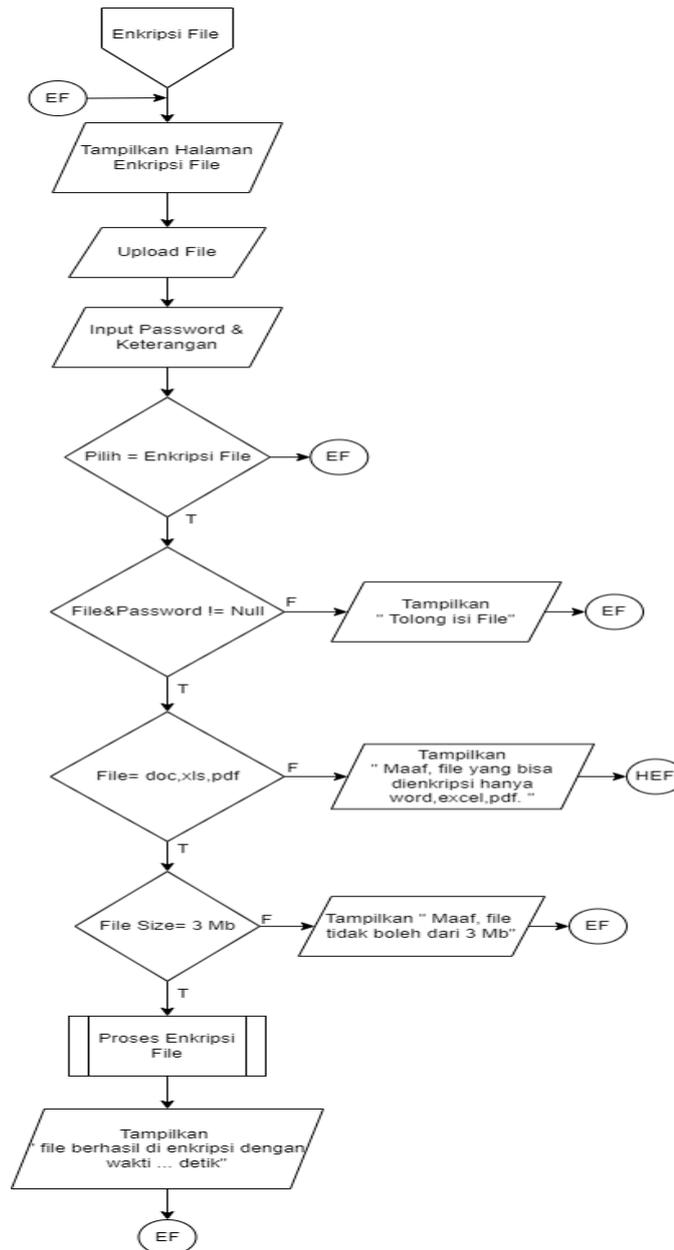
3. HASIL DAN PEMBAHASAN

3.1 Flowchart

Di bawah ini adalah *flowchart* yang digunakan untuk menelusuri proses program pada aplikasi pengamanan file.

a. Flowchart Enkripsi

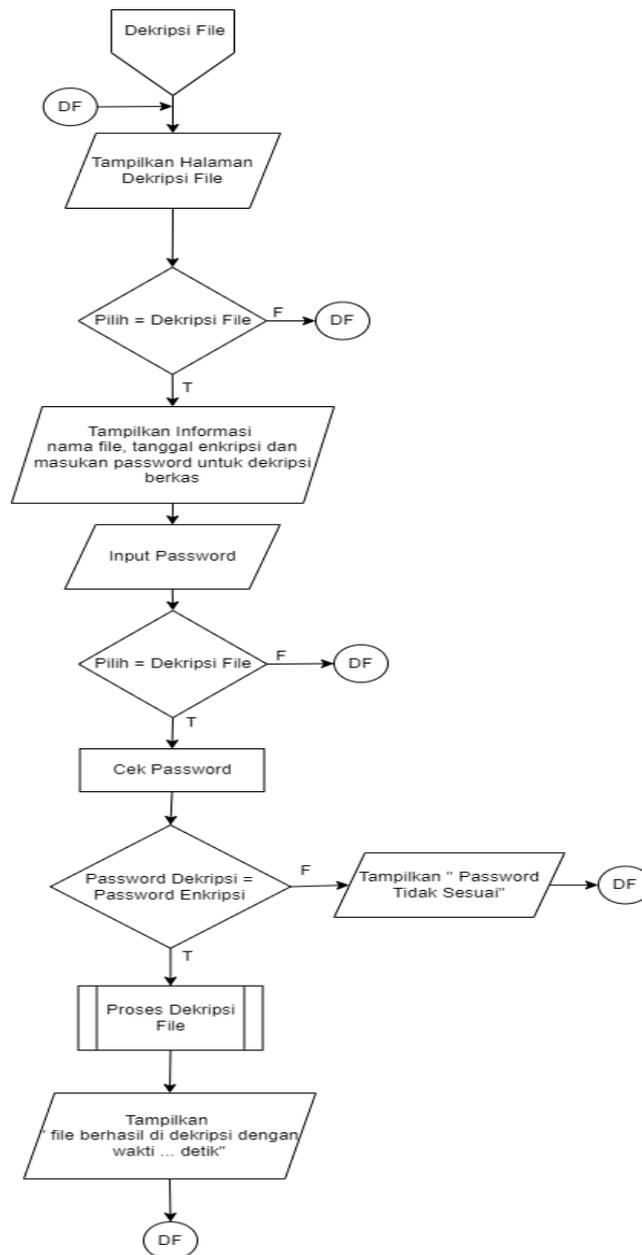
Flowchart ini menjelaskan tentang *enkripsi file*. Saat mengenkripsi file, pengguna admin harus memasukkan kata sandi, setelah itu program akan menangani *enkripsi*. Berikut adalah Gambar 2 Menunjukkan *Flowchart Enkripsi*.



Gambar 2. *Flowchart* Enkripsi.

b. Flowchart Dekripsi

Flowchart ini menjelaskan *dekripsi file*. *Dekripsi file* mengharuskan pengguna untuk memasukkan *password* atau *key* yang sama dengan *password enkripsi*. Setelah itu program akan memproses *dekripsi*, Gambar 3 menunjukkan *flowchart dekripsi*



Gambar 3. flowchart dekripsi

3.2 Algoritma

Bagian ini menampilkan dan menjelaskan algoritma dari *flowchart* sebelumnya. Hanya *source code* yang ditampilkan di bagian ini untuk membuat algoritme lebih mudah dibaca dan dimengerti.

a. Algoritma *enkripsi*

Algoritme 1 ini menjelaskan proses *form enkripsi*. Proses dimana *file* di *enkripsi*.

Algoritma 1 *Enkripsi*

1	Tampilkan Halaman Beranda
2	<i>Input</i> Pilih
3	<i>If</i> pilih = <i>Enkrip File</i>
4	Tampilkan <i>Form enkripsi</i>
5	<i>Input</i> File
6	<i>Input</i> Password
7	<i>Input</i> Deskripsi/Keterangan
8	<i>If</i> pilih = <i>enkripsi file</i>
9	<i>If</i> File & Password != null

10	<i>If file = doc,xls,pdf</i>
11	<i>If File Size <= 3mb</i>
12	<i>Proses Enkripsi</i>
13	Tampilkan Pesan file berhasil dienkrapsin
14	dengan waktu <i>.\$duration.detik</i>
15	<i>else</i>
16	Tampilkan Maaf file tidak boleh lebih dari
17	3mb
18	<i>End if</i>
19	<i>Else</i>
20	Tampilkan maaf file yang bisa dienkrapsi hanya
21	Word.excel,pdf
22	<i>End if</i>
23	<i>Else</i>
24	Tampilkan Tolong isi File
25	<i>End if</i>
26	<i>Else If pilih = Beranda</i>
27	Tampilkan Menu Halaman Utama
28	<i>End if</i>

b. Algoritma *dekripsi*

Algoritma 2 ini menjelaskan proses *form dekripsi*. Proses dimana *file* di yang telah dienkrapsi, dikembalikan seperti semula atau di *dekripsi*.

Algoritma 2 *Dekripsi*

1	Tampilkan Halaman Beranda
2	<i>Input Pilih</i>
3	<i>If pilih = Dekripsi</i>
4	Tampilkan Halaman <i>Form Dekripsi</i>
5	<i>If pilih = Dekripsi File</i>
6	Tampilkan Informasi yang akan di <i>dekripsi</i>
7	<i>Input file</i>
8	<i>If pilih = Dekripsi File</i>
9	Periksa Password
10	<i>If password dekripsi = password enkripsi</i>
11	Proses Enkripsi File
12	Tampilkan File Berhasil didekripsi dengan waktu
13 Detik
14	<i>Else</i> Tampilkan <i>Password Salah</i>
15	<i>Else If pilih = Beranda</i>
16	Menampilkan Halaman Beranda
17	<i>End if</i>
18	<i>End if</i>
19	<i>End if</i>
20	<i>End if</i>

3.3 Analisis Hasil

Tahapan ini merupakan hasil dari pengujian *file* asli dengan *file* terenkrapsi menggunakan *aplikasi* dengan kebutuhan yang telah terpenuhi.

a. Tampilan File Asli

Gambar 4 Menunjukkan tampilan file sebelum di *enkripsi*. dimana isi file masih bisa dibaca dan normal

No	Nama File Awal	Ukuran File	Nama File Hasil Enkripsi	Ukuran file Setelah Enkripsi	Keterangan & Durasi Enkripsi
3	DATA SISWA SISWI KELAS 12.pdf	168.885 bytes	11763-data-siswa-siswi-kelas-12.pdf	168.896 bytes	Berhasil 5.5629
4	DATA SISWA SMK PGRI 31 LEGOK.xlsx	51.516 bytes	57179-data-siswa-smk-pgri-31-legok.xlsx	51.520 bytes	Berhasil 1.7196
5	NILAI UAS DASAR DESAIN GRAFIS 10 TKJ.xlsx	18.215 bytes	63920-nilai-uas-dasar-desain-grafis-10-tkj.xlsx	18.224 bytes	Berhasil 0.6588
6	SMK31.jpg	73.123 bytes	-	-	File yang bisa di enkrip hanya word,excel dan pdf.
7	SURAT-SURAT.doc	7.522.112 bytes	-	-	File tidak boleh lebih dari 3 mb.

b. Tabel Hasil Pengujian Dekripsi

Tabel 2 Menunjukkan hasil pengujian *Dekripsi file*

Tabel 2. Hasil Pengujian *Dekripsi*

No	Nama File Enkripsi	Ukuran File Enkripsi	Nama File Hasil Dekripsi	Ukuran File Dekripsi	Keterangan dan Durasi Dekripsi
1	57179-data-siswa-smk-pgri-31-legok.xlsx	42.496 bytes	78978-nilai-uas-bahasa-indonesia-kelas-10.xlsx	42.491 bytes	Berhasil 1.3939
2	85470-nilai-uas-bahasa-inggris-kelas-10-otkp.doc	22.176 bytes	93700-nilai-uas-bahasa-inggris-10-otkp.doc	22.171 bytes	Berhasil 0.6971
3	11763-data-siswa-siswi-kelas-12.pdf	168.896 bytes	51812-data-siswa-siswi-kelas-12.pdf	168.885 bytes	Berhasil 5,3273
4	57179-data-siswa-smk-pgri-31-legok.xlsx	51.520 bytes	97520-data-siswa-smk-pgri-31-legok.xlsx	51.516 bytes	Berhasil 1.6519
5	63920-nilai-uas-dasar-desain-grafis-10-tkj.xlsx	18.224 bytes	76714-nilai-uas-dasar-desain-grafis-10-tkj.xlsx	18.215 bytes	Berhasil 0.5514
6	-	-	-	-	-
7	-	-	-	-	-

3.5 Tampilan Layar

a. Tampilan Layar Halaman Beranda

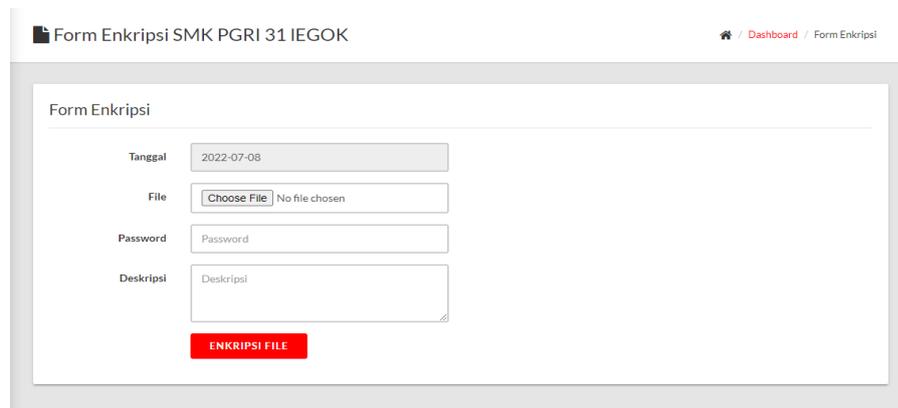
Gambar 8 Menunjukkan tampilan halaman beranda ini menampilkan jumlah file yang *dienkripsi* dan file yang *didekripsi*.



Gambar 8. Halaman Beranda

b. Tampilan Layar *Form Enkripsi*

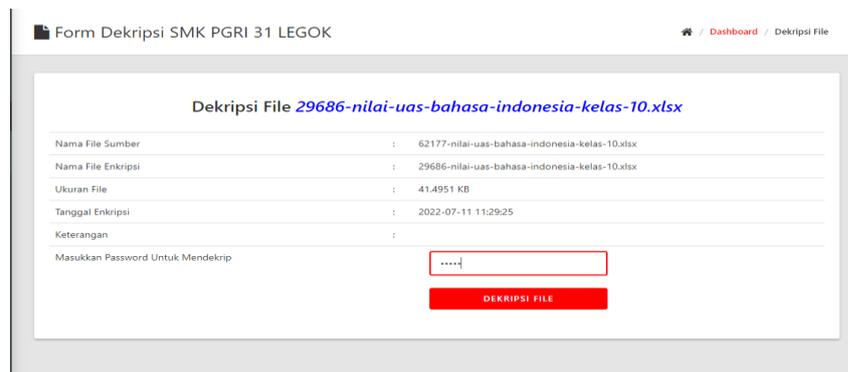
Gambar 9 Menunjukkan Halaman *Form Enkripsi* untuk memilih file mana yang akan di enkripsikan lalu mengisi kunci *enkripsi*, mengisi *deskripsi enkripsi* dan pilih *button enkripsi file*.



Gambar 9. Menunjukkan Halaman *Form Enkripsi*

c. Tampilan Layar Halaman *Form Dekripsi file*

Gambar 10 menunjukkan Halaman *form dekripsi file* untuk melakukan proses *dekripsi file* pengguna harus memasukan kunci/ *password* yang sama saat *enkripsi file*.



Gambar 10. Halaman *Form Dekripsi File*

4. KESIMPULAN

- Berdasarkan penjelasan serta uraian yang telah dibahas, maka dapat disimpulkan beberapa kesimpulan yaitu.
- Berhasil mengenkripsi file dengan format doc,excel,pdf.
 - Algoritma AES-128 dapat diterapkan pada aplikasi pengamanan file di SMK PGRI 31 Legok.
 - File yang berukuran kurang dari 3MB lebih cepat durasi *enkripsi* dan *dekripsinya*.

Berdasarkan kesimpulan yang ada untuk pengembangan lebih lanjut agar meningkatkan aplikasi ini, terdapat beberapa saran yaitu:

- Untuk perkembangan selanjutnya diharapkan dapat mengenkripsi dalam bentuk gambar, suara dan video.
- Untuk pengembangan selanjutnya diharapkan membuat aplikasi berbasis mobile dengan menggunakan algoritme yang sama atau berbeda.
- Untuk perkembangan selanjutnya di harapkan mengkombinasikan 2 metode dalam 1 aplikasi.
- Dalam perkembangan selanjutnya agar memakai *web hosting* agar aplikasi bisa digunakan saat di luar sekolah.

DAFTAR PUSTAKA

- [1] Hanadwiputra, S. "Implementasi Enkripsi Dalam Pengamanan File Data Karyawan Dengan Metode Algoritma DES (Data Encryption Standard) Pada CV. Sinergi Informasi Global," *Jurnal Gema Kampus*, vol. 13, no. 2, pp. 61-69, 2018.
- [2] D. Widyawan and I. Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *SKANIKA*, vol. 4, no. 1, pp. 15–22, 2021.
- [3] D. Hulu, B. Nadeak, and S. Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan," *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)* pp. 78–86, 2020.
- [4] B. Agung Nugroho, F. Sofian Efendi, T. Informatika, and P. Kediri, "Pengamanan Data Identitas Bus pada Kartu NFC Menggunakan Enkripsi AES-128 (Securing Bus Identity Data In a NFC Card Using AES-128 Encryption)," *J. Inform. Multimed.*, vol. 10, no. 02, pp. 56–62, 2018.
- [5] A. Eka Putri, A. Kartikadewi, and L. A. Abdul Rosyid, "Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang," *Appl. Inf. Syst. Manag.*, vol. 3, no. 2, pp. 69–78, 2021, [Online]. Available: <https://journal.uinjkt.ac.id/index.php/aism/article/view/14722>
- [6] R. V. H. Chandra, A. Kusyanti, and M. Data, "Analisis Performa Proses Enkripsi dan Dekripsi Menggunakan Algoritma AES-128 Pada Berbagai Format File," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 1, pp. 481–486, 2019.
- [7] I. Gunawan, S. Tunas, and B. Pematangsiantar, "Peningkatan Pengamanan Data File menggunakan Algoritma Kriptografi AES dari Serangan Brute Force 14 Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan *Brute Force*," *TECHSI*, vol. 13 no. 1 pp. 14–25, 2021.
- [8] B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy," *J. Tek. Inform.*, vol. 1, no. 2, pp. 69–77, 2020.
- [9] Mulyadi, Y,A. "Implementasi Algoritma AES-128 dan SHA-256 dalam Pengkodean Pada Sebagian *Frame Video CCTV MPEG-2*," *Jurnal Teori dan Aplikasi Ilmu Komputer*, vol. 1, pp. 30-26, Maret. 2018.
- [10] Suranta, I,A. and Sakti, Y,S,V,D, "Penerapan Algoritma AES (Advance Encryption Standard) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi," *SKANIKA*, vol. 5, no. 1, pp. 1-10, 2022.