PENGAMANAN FILE UJIAN MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* 128 DI SMP NEGERI 22

Bonita Cerlia Ashari[1*], Sejati Waluyo[2]

[1,2]Fakultas Teknoloogi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta Selatan, Indonesia

Email: [1*]bonitacerliaashari@gmail.com, [2]sejati.waluyo@budiluhur.ac.id
(* : corresponding author)

Abstrak- Perkembangan teknologi sistem keamanan data semakin pesat. Hal ini memudahkan aktivitas individu untuk melakukan pertukaran informasi data. Sudah pasti data yang sangat penting ini dilihat bahkan dimanipulasi oleh orang – orang yang tidak berhak. SMPN 22 Kota Tangerang Selatan memanfaatkan aplikasi *Microsoft office* untuk mendukung sistem sekolah terkait soal-soal ujian sekolah yang ditempuh siswa. Namun SMPN 22 belum memiliki mekanisme keamanan data terhadap *file* soal ujian sekolah, sehingga data tersebut dapat dimanipulasi oleh pihak yang tidak berhak. Maka dari itu sangat penting untuk melakukan pengamanan data agar tetap terjaga keaslian dan kerahasiaan data tersebut. Penelitian ini bertujuan untuk mengamankan *file* soal ujian di SMP NEGERI 22 Kota Tangerang Selatan. Dimana data ujian tersebut dikemas dalam sebuah *file* dokumen, pengamanan data ini dilakukan dengan cara mengimplementasikan ilmu kriptografi dengan metode *Advanced Encryption Standard* (AES-128). Metode ini dapat mengenkripsi *file* dengan cara mengubah isi *file* asli kemudian diacak dengan perhitungan matematis sehingga isi *file* tidak dapat dibaca atau digunakan oleh pihak yang tidak berkepentingan. Data dapat dibaca setelah melalui proses dekripsi. Aplikasi pengamanan *file* ujian sekolah ini dirancang menggunakan bahasa pemrograman PHP berbasis *website* dengan menggunakan MySQL sebagai *Database Management System*. Dari hasil penelitian ini setelah dilakukan beberapa pengujian pada sistem dan didapatkan kesimpulan bahwa aplikasi ini dapat mengamankan *file* soal ujian sekolah dengan cara mengubah *file* asli yang semula berbentuk *plaintext* menjadi *ciphertext* sehingga isi *file* dokumen tidak dapat dipahami lagi maksudnya. Serta dilakukan juga pengujian kecepatan enkripsi data pada *file* soal ujian sekolah dengan ukuran yang berbeda-beda. Pada *file* yang berukuran 845 kb berhasil dienkripsi dengan waktu 19.0575 detik, pada percobaan berikutnya *file* dengan ukuran 705kb berhasil dienkripsi dengan waktu 15.7699 detik, selanjutnya pada *file* yang berukuran 56 kb berhasil dienkripsi dengan waktu 1.2990 Detik dan percobaan terakhir pada *file* yang berukuran 331kb berhasil dienkripsi dengan waktu 7.2303 detik.

Kata Kunci: Kriptografi, *File* soal ujian sekolah, Enkripsi, Dekripsi, Algoritma *Advanced Encryption Standard* (AES)

EXAM FILE SECURITY USING 128-BIT ADVANCED ENCRYPTION STANDARD ALGORITHM IN SMP NEGERI 22

Abstract- *The development of data security system technology is growing rapidly. This makes it easier for individual activities to exchange data information. It is certain that this very important data is seen and even manipulated by unauthorized people. SMPN 22 Tangerang Selatan City utilizes Microsoft office applications to support the school system related to school exam questions taken by students. However, SMPN 22 does not yet have a data security mechanism for school exam question files, so that data can be manipulated by unauthorized parties. Therefore, it is very important to protect the data in order to maintain the authenticity and confidentiality of the data. This study aims to secure the file for exam questions at SMP NEGERI 22, South Tangerang City. Where the test data is packaged in a document file, this data security is carried out by implementing the science of cryptography with the Advanced Encryption Standard (AES-128) method. This method can encrypt files by changing the contents of the original file and then scrambled with mathematical calculations so that the contents of the file cannot be read or used by unauthorized parties. The data can be read after going through the decryption process. This school exam file security application is designed using the website-based PHP programming language using MySQL as the Database Management System. From the results of this study, after several tests were carried out on the system, it was concluded that this application can secure the school exam question file by changing the original file which was originally in the form of plaintext into ciphertext so that the contents of the document file can no longer be understood. As well as testing the speed of data encryption on school exam question files with different sizes. The 845kb file was successfully encrypted with a time of 19.0575 seconds, on the next try the 705kb file was successfully encrypted in 15.7699 seconds, then the 56kb file was successfully encrypted with 1.2990 seconds and the last attempt on the 331kb file was successfully encrypted with the time 7.2303 seconds.*

Keywords*: Cryptography, School exam file, Encryption, Decryption, Advanced Encryption Standard Algorithm (AES)*

1. PENDAHULUAN

SMP Negeri 22 Tangerang Selatan merupakan salah satu sekolah yang memanfaatkan aplikasi *microsoft office* untuk mendukung sistem sekolah terkait soal – soal ujian sekolah yang ditempuh siswa. Guru akan menuliskan soal – soal ujian dalam bentuk teks dan angka, namun isi data pada soal ujian tersebut belum mengalami proses enkripsi (*plaintext*). Hal ini tentunya akan memudahkan pihak – pihak yang tidak berhak untuk membaca bahkan memanipulasi isi file tersebut. Oleh karena itu, SMP Negeri 22 membutuhkan suatu sistem keamanan untuk mengamankan soal – soal ujian untuk menghindari terjadinya kebocoran soal sebelum ujian dilaksanakan.

Untuk mengatasi masalah keamanan tersebut, maka dibutuhkan metode yang berguna untuk menjaga keamanan informasi. Kriptografi dapat digunakan sebagai salah satu metodenya. Kriptografi adalah ilmu yang mempelajari bagaimana suatu pesan atau dokumen tetap aman dan terjaga keasliannya sehingga tidak dapat dilihat atau dibaca oleh pihak – pihak yang tidak berwenang.

Ada beberapa istilah penting di dalam kriptografi seperti *plaintext*, *ciphertext*, enkripsi, dekripsi, *cryptanalysis*, dan *cryptology*. *Plaintext* merupakan data asli yang masih bisa dibaca, dan teknik untuk membuat suatu data tidak bisa dibaca disebut enkripsi. *Ciphertext* merupakan data hasil dari proses enkripsi, dan teknik untuk mengubah *ciphertext* kembali menjadi data asli atau *plaintext* disebut dekripsi.

Algoritma kriptografi dapat diterapkan sebagai salah satu cara untuk mengamankan data dengan melakukan enkripsi ke dalam data tersebut. Melalui proses enkripsi maka data tidak dapat dibaca karena teks asli atau *plaintext* telah diubah menjadi *ciphertext* atau data hasil enkripsi.

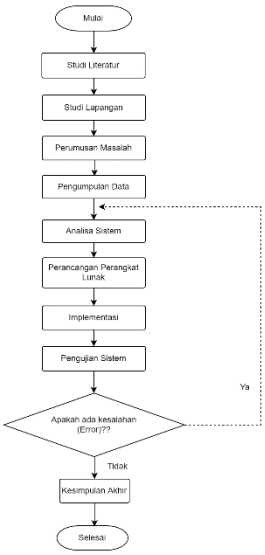
Berdasarkan dengan uraian diatas, penelitian ini bertujuan untuk membuat aplikasi pengamanan soal ujian menggunakan kriptografi dengan mengimplementasikan algoritma AES-128 sebagai metode untuk mengamankan isi dari *file* dokumen. Alasan utama memilih AES Rijndael ini bukan karena algoritmanya paling aman di antara MARS, RC6, Serpent, Twofish, dan lain sebagainya, tetapi AES Rijndael memiliki keseimbangan antara keamanan dan fleksibelitas di berbagai platform perangkat lunak dan perangkat keras [1].

Algoritma AES (*Advanced Encryption Standard*) adalah standar algoritma kriptografi terbaru yang diterbitkan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001 untuk menggantikan algoritma DES (*Data Encryption Standard*) yang diduga sudah usang. Algoritma AES adalah jenis algoritma *block cipher* dengan panjang kunci yang bervariasi, yaitu 128-bit, 192-bit, dan 256-bit.

2. METODE PENELITIAN

2.1 Penerapan Metode

Metode penelitian ini diterapkan untuk acuan pelaksanaan penelitian agar meraih hasil yang sesuai dengan tujuan yang telah dipakai sebelumnya. Gambar dibawah ini merupakan tahapan yang dilakukan dalam penerapan metode penelitian yang akan dilakukan dalam penelitian ini.



Gambar 1. Tahapan Penelitian

2.2 Metodologi Penelitian

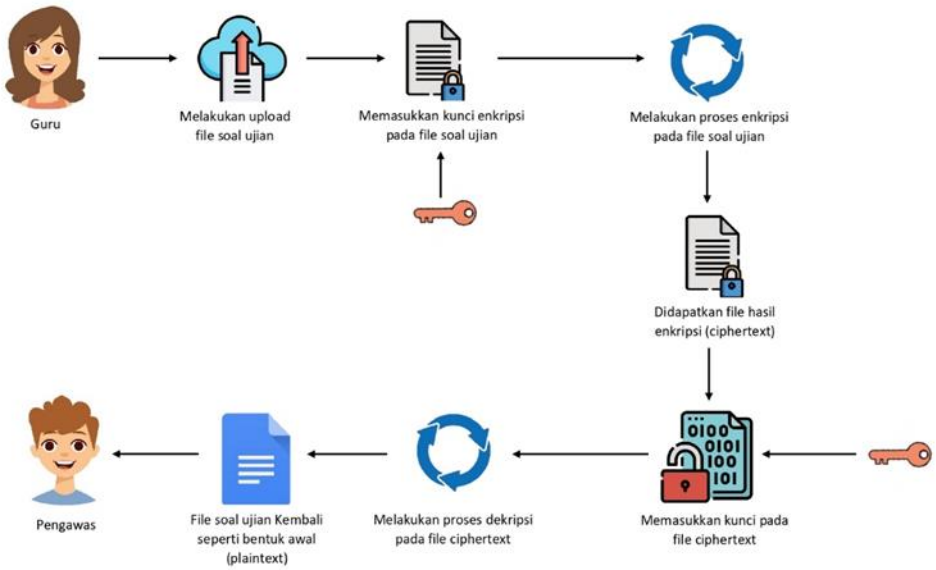
Dibawah ini merupakan 6 (enam) metode yang digunakan sebagai sumber informasi pada penelitian ini guna mengatasi masalah – masalah dalam penelitian:

a. Studi Literatur
   Studi dijalankan dengan mengkaji buku ilmiah, jurnal, makalah, internet dan berbagai sumber lainnya yang berkenaan dengan masalah yang sedang diteliti, yaitu kriptografi *Advanced Encryption Standard* (AES), dan memperoleh dasar referensi yang kuat bagi penulis untuk menetapkan metode yang tepat untuk menangani masalah yang diteliti.
b. Studi Lapangan
   Dilakukan studi kasus dalam melakukan pengamanan soal-soal ujian khususnya pada soal-soal ujian kenaikan atau kelulusan siswa dan siswi SMP Negeri 22 untuk dapat mengetahui permasalahan-permasalahan yang ada, kemudian akan dirumuskan saat melakukan perumusan masalah.
c. Pengumpulan Data
   Pada proses pengambilan data ini, didapat berdasarkan wawancara dan observasi.
d. Analisa Sistem
   Penerapan keamanan pada sistem yaitu proses enkripsi dan dekripsi *file* soal ujian yang akan disimpan ke dalam sebuah *database*.
e. Perancangan Perangkat Lunak
   Perancangan dibuat sesuai dengan hasil analisa sistem. Secara khusus, rancangan enkripsi, dekripsi dan dukungan lain yang terintegrasi pada sistem dan desain *interface*.
f. Pengujian Sistem
   Diadakan percobaan pada sistem untuk memastikan prosedur yang dijalankan sesuai dengan hasil analisa dan perancangan.

3. HASIL DAN PEMBAHASAN

3.1 Alur Proses Enkripsi dan Dekripsi

Alur proses enkripsi dan dekripsi menggambarkan situasi alur sistem secara keseluruhan berupa gambar – gambar yang akan memudahkan pembaca untuk memahami permasalahan yang ada pada situasi tersebut, seperti pada gambar dibawah ini.



Gambar 2. Alur Proses Enkripsi dan Dekripsi

3.2 Tampilan Layar

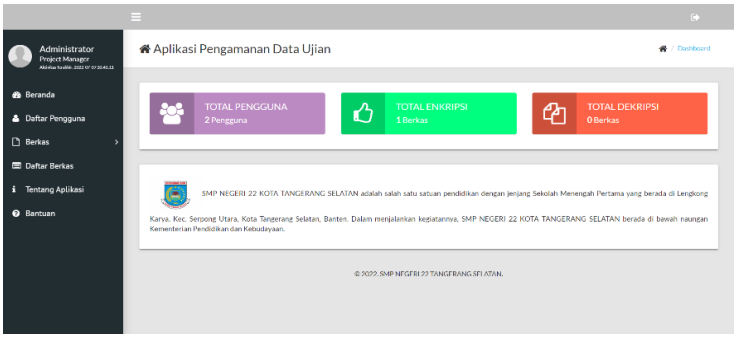
a. Tampilan Layar Login

Berikut ini merupakan tampilan layar Halaman *Login*. Pada Halaman *Login* ini pengguna harus memasukkan *username* dan *password* agar dapat masuk dan menggunakan aplikasi ini.

Gambar 3. Tampilan Halaman Utama

b. Tampilan Layar Halaman Utama

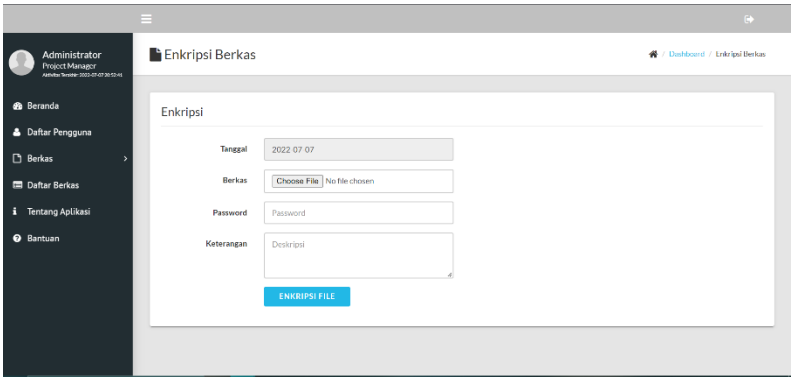
Setelah *login* berhasil maka akan masuk ke Halaman Utama, dimana pengguna dapat melihat keseluruhan data, menambah akun, melihat keseluruhan pengguna, mengubah dan menghapus akun.



Gambar 4. Tampilan Halaman Utama

c. Tampilan Layar Enkripsi

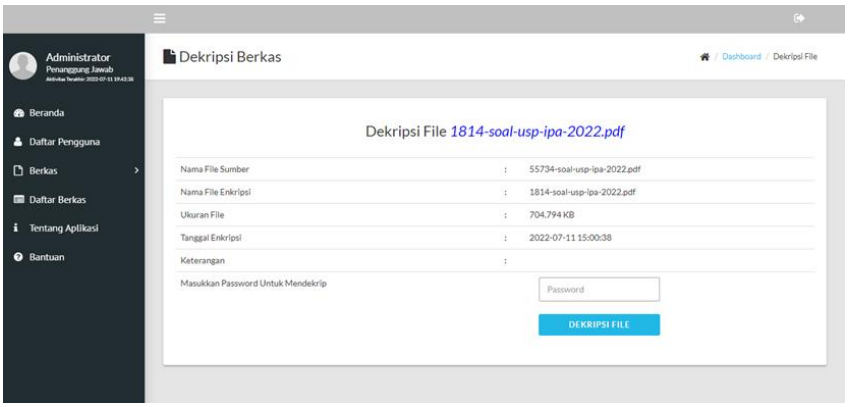
Berikut ini merupakan Tampilan Layar Halaman *Form* Enkripsi Berkas. pengguna dapat memilih memilih *file* yang ingin di enkripsi, *password* untuk keamanan enkripsi dan dekripsi *file* lalu tekan tombol enkripsi *file* untuk menyimpan data *inputan*.



Gambar 5. Tampilan Halaman Enkripsi

d. Tampilan Layar Dekripsi

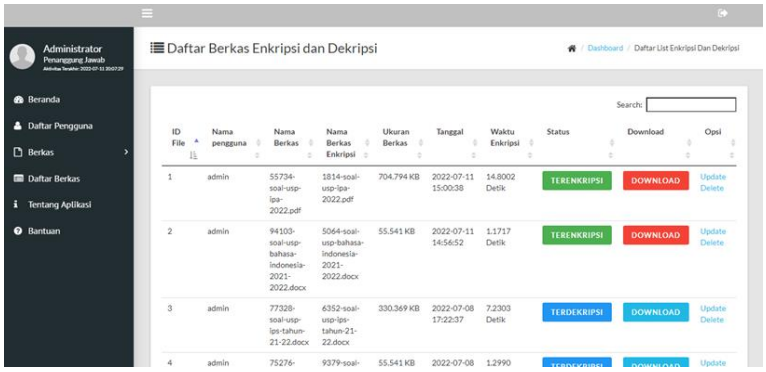
Pada *Form* Dekripsi Berkas ini pengguna dapat mendekripsi berkas dengan cara memasukkan *password* atau kunci yang sama saat enkripsi.



Gambar 6. Tampilan Halaman Dekripsi

e. Tampilan Layar Daftar Berkas

Pada Halaman Daftar Berkas ini, pengguna dapat mendekripsi, mendownload *file*, mengganti *password* bila terjadi lupa *password* dan menghapus *file* jika terjadi salah *input file*.

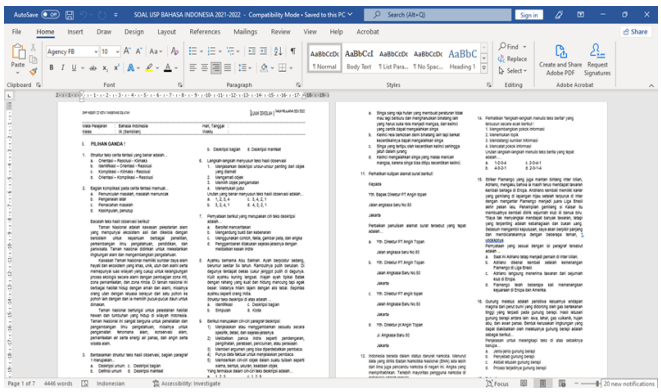


Gambar 7. Tampilan Halaman Daftar Berkas

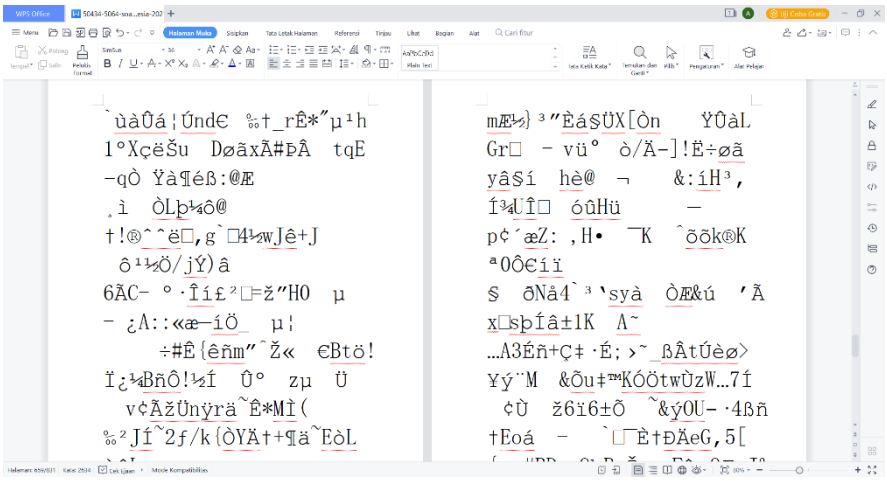
3.3 Analisa Hasil

Berikut ini merupakan hasil dari uji coba *file plaintext* dan *file* yang telah terenkripsi dengan menerapkan aplikasi yang telah memenuhi spesifikasi *hardware* dan *software*. *File* yang akan diuji adalah word dan pdf.

a. Tampilan *file* *docx yang asli (*plaintext*) dan yang telah dienkripsi dapat dilihat pada gambar –gambar berikut ini.

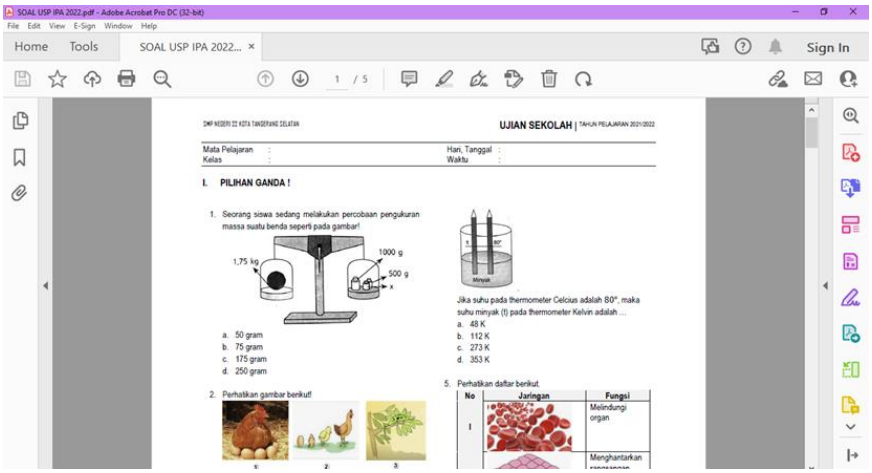


Gambar 8. *File Plaintext* Docx

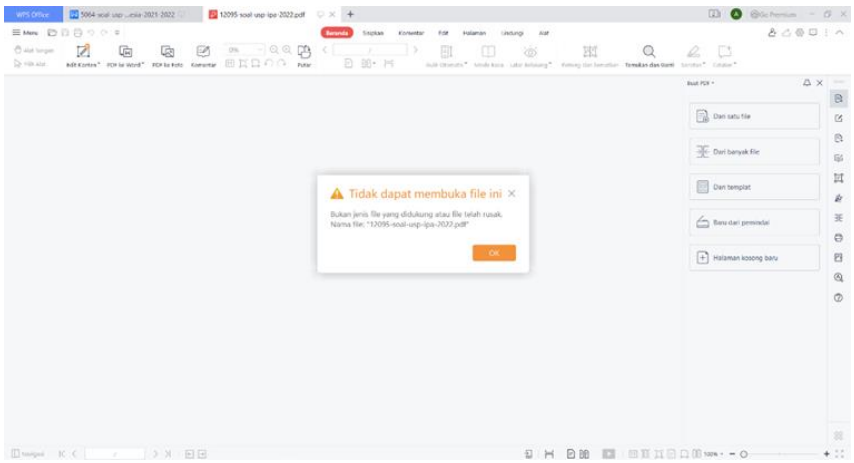


Gambar 9. *File Ciphertext* Docx

b. Tampilan *file* *pdf yang asli (*plaintext*) dan yang telah dienkripsi dapat dilihat pada gambar – gambar berikut ini.



Gambar 10. *File Plaintext* Pdf



Gambar 11. *File Ciphertext* Pdf

3.4 Tabel Pengujian

Pada percobaan kali ini memberikan perbandingan pada proses enkripsi dan dekripsi *file*. *File* yang diuji merupakan jenis *file* doc, docx dan pdf. Pengujiannya yaitu antara lain ukuran *file*, waktu proses enkripsi dan waktu proses dekripsi.

a. Tabel Enkripsi File DOCX dan PDF

Tabel 1 dibawah ini berisi proses pengujian enkripsi yang dikerjakan oleh sistem.

Tabel 1. Tabel Pengujian Proses Enkripsi

No	Nama *File*	Kunci	Waktu Enkripsi (Detik)	Nama *File* Enkripsi	Ukuran *File* Asli	Ukuran *File* Enkripsi
1	SOAL USP PPKN 2022	1234	19.0575 Detik	31251-soal-usp-ppkn-2022.docx	845 KB	844.515 KB
2	SOAL USP IPA 2022	1234	15.7699 Detik	75842-soal-usp-ipa-2022.pdf	705 KB	704.794 KB
3	SOAL USP BAHASA INDONESIA 2021-2022	1234	1.2990 Detik	9379-soal-usp-bahasa-indonesia-2021-2022.docx	56 KB	55.541 KB
4	SOAL USP IPS TAHUN 21-22	1234	7.2303 Detik	6352-soal-usp-ips-tahun-21-22.docx	331 KB	330.369 KB

Berdasarkan tabel pengujian berikut, maka dapat ditarik kesimpulan bahwa *file* berhasil dienkripsi, kecepatan waktu pada proses enkripsi dipengaruhi oleh besar kecilnya ukuran *file* dan ukuran *file* yang telah dienkripsi tidak mengalami perubahan.

b. Tabel Dekripsi *File* DOCX dan PDF

Tabel 2 dibawah ini berisi proses pengujian dekripsi yang dikerjakan oleh sistem.

Tabel 2. Tabel Pengujian Proses Dekripsi

No	Nama *File*	Kunci	Waktu Dekripsi (Detik)	Nama *File* Dekripsi	Ukuran *File* Asli	Ukuran *File* Dekripsi
1	31251-soal-usp-ppkn-2022.docx	1234	0.0360 Detik	40668-soal-usp-ppkn-2022.docx	845 KB	844.515 KB
2	75842-soal-usp-ipa-2022.pdf	1234	14.9276 Detik	22028-soal-usp-ipa-2022.pdf	705 KB	704.794 KB
3	9379-soal-usp-bahasa-indonesia-2021-2022.docx	1234	1.4029 Detik	75276-soal-usp-bahasa-indonesia-2021-2022.docx	56 KB	55.541 KB
4	6352-soal-usp-ips-tahun-21-22.docx	1234	7.3600 Detik	77328-soal-usp-ips-tahun-21-22.docx	331 KB	330.369 KB

Berdasarkan tabel pengujian berikut, maka dapat ditarik kesimpulan bahwa *file* berhasil didekripsi, kecepatan waktu pada proses dekripsi dipengaruhi oleh besar kecilnya ukuran *file*. Isi dari *file* yang telah didekripsi tidak mengalami perubahan sedikitpun dan ukuran *file* yang telah didekripsi tidak mengalami perubahan.

3.5 Kelebihan Aplikasi

Dari hasil pengujian yang dilakukan maka, diperoleh kesimpulan bahwa kelebihan dari aplikasi ini adalah sebagai berikut:

a. User dapat dengan mudah mengoperasikan program, karena aplikasi ini didesain dengan tampilan antarmuka yang cukup baik.
b. isi file dokumen doc, docx dan pdf yang sudah dienkripsi tidak bisa dibaca.
c. Isi dari dokumen doc, docx dan pdf hasil dekripsi tidak mengalami perubahan dan dapat dibaca.

3.6 Keterbatasan Aplikasi

Dari hasil pengujian yang dilakukan maka, diperoleh kesimpulan bahwa kekurangan dari aplikasi ini adalah sebagai berikut:

a. Aplikasi ini dibatasi untuk mengenkripsi *file* dokumen doc, docx dan pdf saja dan ukuran hanya 3 MB saja.
b. Semakin besar ukuran *file*-nya, semakin lambat proses enkripsi dan dekripsinya.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat ditarik kesimpulan yang sejalan dengan tujuan penelitian, yaitu:

a. Algoritma AES-128bit berhasil diimplementasikan dalam pengamanan *file* soal ujian sekolah pada SMP Negeri 22 Tangerang Selatan.
b. Aplikasi yang dibuat untuk mengamankan *file* yang bertipe word dan pdf.
c. Semakin besar ukuran *file* yang dienkripsi maka waktu yang dibutuhkan pada proses enkripsi semakin lama.

Berdasarkan kesimpulan diatas, maka diberikan saran yang dianggap dapat bermanfaat di kemudian hari, antara lain:

a. Aplikasi ini diharapkan dapat dikembangkan dengan menggabungkan dua atau tiga metode kriptogtafi lainnya dari penelitian sebelumnya.
b. Pada penelitian selanjutnya diharapkan dapat memperbesar kapasitas ukuran *file* untuk dienkripsi.
c. Waktu proses enkripsi dan dekripsi *file* dapat lebih cepat meskipun dengan ukuran *file* yang besar.

DAFTAR PUSTAKA

[1] A. Rukmana and I. Nurichsan, “Implementasi Algoritma AES Rijndael Untuk Enkripsi Dan Dekripsi Data SMS Pada Ponsel Berbasis Android” vol. 10, no. 2, pp. 129–144, 2019.
[2] 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.
[3] L. A. Indrayani and I. M. Suartana, “Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document,” *J. Informatics Comput. Sci.*, vol. 1, no. 01, pp. 42–47, 2019, doi: 10.26740/jinacs.v1n01.p42-47.
[4] D. Novianto and Y. Setiawan, “Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES),” *J. Ilm. Inform. Glob.*, vol. 9, no. 2, pp. 83–89, 2019, doi: 10.36982/jig.v9i2.561.
[5] R. Nuari and N. Ratama, “Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping,” *J. Artif. Intell. Innov. Appl.*, vol. 1, no. 2, pp. 2716–1501, 2020, [Online]. Available: http://openjournal.unpam.ac.id/index.php/JOAIIA
[6] 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.
[7] 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.
[8] A. . Putra, Herfina, S. Maryana, and A. Setiawan, “Implementasi Algoritma AES (Advance Encryption Standard) Rijndael Pada Aplikasi Keamanan Data,” *J. Ilm. Penelit. Teknol. Inf. Komput.*, vol. 1, no. 2, pp. 46–51, 2020.
[9] E. Setyaningsih, “Keamanan file dokumen menggunakan algoritme Advanced Encryption Standard pada aplikasi berbasis Android,” *Jnanaloka*, pp. 11–23, 2020, doi: 10.36802/jnanaloka.2020.v1-no1-13.
[10] R. Wijaya, K. Farandi, and S. Miharja, “Implementasi Algoritma Aes-128 Dan Sha-256 Dalam Perancangan Aplikasi Pengamanan File Dokumen,” vol. X, no. 2, pp. 2337–3601, 2021.