PENERAPAN ALGORITMA KRIPTOGRAFI AES 256 UNTUK MENGAMANKAN DOKUMEN BERBASIS *WEB* PADA KELURAHAN BELENDUNG

Irfan Kurnia Nurhareza[1*], Siswanto Siswanto[2]

[1,2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia
[1*]1811502275@student.budiluhur.ac.id, [2]siswanto@budiluhur.ac.id
(* : corresponding author)

Abstrak-Dalam menjalankan tugasnya, Lurah Kelurahan Belendung yang dibantu oleh para kepala bagian dan beberapa *staff* memiliki sebuah hambatan, yaitu kekhawatiran tentang kerahasian dokumen- dokumen penting ataupun laporan hasil kerja, agar tidak disalahgunakan oleh pihak- pihak yang tidak bertanggung jawab. Karena kurang pengetahuan tentang cara pengamanan dokumen atau laporan hasil kerja. Tujuan dari penelitian ini adalah untuk membuat aplikasi berbasis *web* penerapan algoritme kriptografi AES 256 bit untuk mengamankan dokumen penting, dokumen kerja, data masyarakat, surat-surat dan hasil perkerjaan yang ada di Kelurahan Belendung. Sehingga tidak terjadi pengambilan atau pencurian dokumen penting dan laporan haisil kerja oleh pihak-pihak yang ingin penyalahgunaan dokumen penting, dokumen kerja, data masyarakat, surat- surat dan hasil perkerjaan. Adapun metode yang dipergunakan adalah algoritme kriptografi AES 256 bit dengan menggunakan kunci dengan panjang kuncinya yang sama atau kunci simetri saat proses enkripsi dan dekripsi 32 *byte*/ karakter. Aplikasi pengamanan dokumen ini dibuat dengan bahasa pemrograman PHP berbasis *web* dan hanya bisa menggunakan dokumen dengan format .pdf, serta .txt. Hasil akhir pengujian aplikasi pengamanan dokumen berbasis *web* ini diperoleh hasil dari proses enkripsi rata- rata ukuran dokumen 2496069,1 *byte*, dengan lama waktu proses 1181000 milli detik dan hasil proses dari dekripsi rata- rata ukuran dokumen 2496128 *byte*, dengan lama waktu proses 1167000 milli detik**.**

Kata Kunci: kriptogarfi, AES 256 bit,, dokumen, Kelurahan

APPLICATION OF THE AES 256 CRYPTOGRAPHY ALGORITHM TO SECURE WEB-BASED DOCUMENTS IN KELURAHAN BELENDUNG

Abstract- *In carrying out his duties, the Belendung Village Head, who is assisted by the section heads and several staff, has an obstacle, namely concerns about the confidentiality of important documents or work reports, so as not to be misused by irresponsible parties. Due to lack of knowledge about how to secure documents or work reports. The purpose of this research is to create a web-based application applying the AES 256-bit cryptographic algorithm to secure important documents, work documents, community data, letters and work results in Belendung Village. So that there is no taking or theft of important documents and work results reports by parties who want to misuse important documents, work documents, community data, letters and work results. The method used is the AES 256 bit cryptographic algorithm using a key with the same key length or a symmetric key during the encryption and decryption process of 32 bytes/character. This document security application is made using the web-based PHP programming language and can only use documents in .pdf and .txt formats. The final result of testing this web-based document security application is obtained from the encryption process, the average document size is 2496069.1 bytes, with a processing time of 1181000 milli seconds and the results of the decryption process are the average document size is 2496128 bytes, with a long processing time of 1167000 milli. second.*

Keywords*: Cryptography, AES 256, Document*

1. PENDAHULUAN

Semakin berkembangnya teknologi membuat setiap orang dapat denganmudah melakukan pertukaran data dan informasi..Keamanan data merupakan masalah yang sangat penting, apalagi terkait data bagi kelurahan yang memang cukup krusial akan keamanannya.Kelurahan Belendung berada di wilayah Kecamatan Benda, Kota Tangerang, Provinsi Banten, Indonesia dipimpin oleh seorang Lurah dan para kepala bagian. Dalam menjalankan tugasnya, Lurah Kelurahan Belendung yang dibantu oleh para kepala bagian memiliki sebuah hambatan, yaitu kekhawatiran tentang kerahasian dokumen-dokumen penting ataupun laporan kerja, agar tidak digunakan oleh pihak yang tidak berwewenang. Itulah yang menjadi salah satu permasalahan di Kelurahan Belendung. Karena kurang pengetahuan tentang pengamanan dokumen atau laporan kerja.

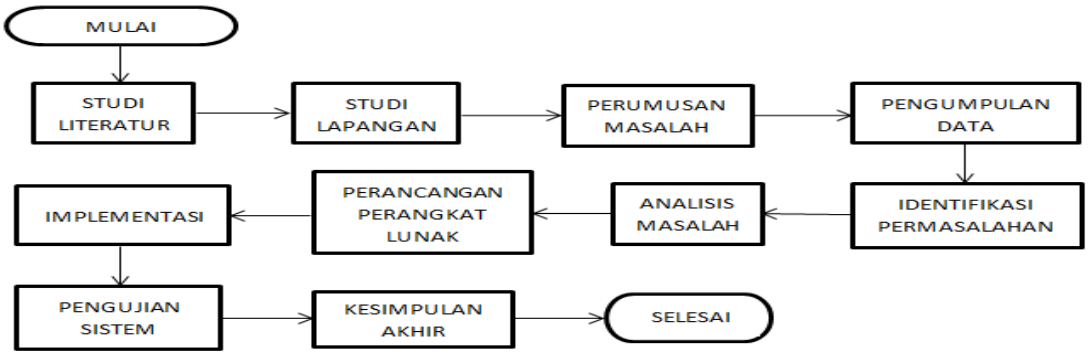
Rumusan permasalahan dalam penelitian ini bagaimana cara mengamankan dokumen Kelurahan Belendung menggunakan Kriptografi AES 256 bit? Adapun tujuan dari penelitian ini adalah membuat aplikasi penerapan algoritme kriptografi AES 256 bit untuk mengamankan data, dokumen penting, dokumen kerja, data masyarakat, surat-surat dan hasil perkerjaan yang ada di Kelurahan Belendung. Adapun manfaat penelitian ini adalah membantu kelurahan untuk pengamanan *file* dokumen penting, dokumen kerja, data masyarakat, surat-surat dan hasil perkerjaan yang ada di Kelurahan Belendung dalam format .pdf, dan .txt.

Proses transformasi pesan *asli* menjadi pesan yang diacak dan sebaliknya merupakan pengamanan data [1]. Aplikasi *Secret Fichier* dengan algoritma AES-256 bit dan SHA-256 dapat mengenkripsi berkas dengan berbagai ekstensi seperti *berkas* dokumen, suara, video serta gambar dengan baik [2]. Penerapan enkripsi data menggunakan kombinasi AES dan RSA dapat diterapkan untuk mengenkripsi dan mendekripsi data dengan aman [3]. Pengamanan *file* hasil radiologi dengan menggunakan algoritma kriptografi AES 128 bit berbasis *web* dengan metode pengembangan SDLC mampu mengamankan berkas hasil radiologi [4].

Penerapan metode AES 128 dapat menjadi rekomendasi bagi perlindungan data dokumen rekam medis [5]. Hasil aplikasi kriptografi AES ini memiliki fungsi untuk mengamankan pesan atau *file* dengan cara teknik mengubah pesan asli (*plaintext*) menjadi pesan atau *file* rahasia (*ciphertext*) yang tidak dapat dipahami atau dibaca oleh orang yang tidak berwenang [6]. Penerapan algoritma kriptografi AES 128 bit dapat mengamankan dokumen ekspedisi *shipping* [7]. Penerapan AES 128 Rijndael digunakan untuk pengujian waktu dan perubahan *size* proses enkripsi dan dekripsi [8]. Penerapan algoritma AES-128 dan *Affine Cipher* dapat mengamankan layanan surat keterangan pada BAAK Universitas Budi Luhur [9]. Penerapan algoritma kriptografi AES 256 bit dapat mengamankan soal-soal ujian [10]. Kriptografi merupakan sebuah metode yang dapat mrngacak teks asli menjadi teks tidak dapat dibaca seperti aslinya [11].

2. METODE PENELITIAN

Tahapan-tahapan dari metode penelitian dapat di lihat pada gambar 1.



Gambar 1. Tahapan-tahapan Penelitian

2.1 Studi Literatur

Studi literatur dilakukan dengan mempelajari konsep-konsep *Encryption Standard 256* (AES 256).

2.2 Studi Lapangan

Pada tahap ini dilakukan pengamatan langsung dokumen Kelurahan Belendung.

2.3 Perumusan Masalah

Bagaimana cara mengamankan dokumen Kelurahan Belendung menggunakan Kriptografi AES 256 bit?

2.4 Pengumpulan Data

Pengumpulan data pada Kelurahan Belendung untuk mrmperoleh dokumen yang perlu diamankan.

2.5 Identifikasi Permasalahan

Megidentifikasi permasalahan yang akan dibuat sesuaidengan batasan yang ada.

2.6 Analisis Masalah

Analisis masalah perlu dilakukan untuk persiapan apa saja kebutuhan aplikasi pengamanan dokumen dengan metode AES 256 bit

2.7 Perancangan Perangkat Lunak

Pada tahap ini dilakukan perancangan sesuai dengan hasil analisis sistem khusunya perancangan proses enkripsi dan dekripsi serta perancangan antarmuka. Dalam pengembangan perangkat lunak akan digunakan metode konvensional dengan menggunakan metode Waterfall.Model ini mensyaratkan penyelesaian suatu tahap secara tuntas sebelum beranjak pada tahap selanjutnya dan hasil masing-masing tahap harus didokumentasikan dengan baik.

2.8 Implementasi

Pada langkah awal dalam melakukan proses enkripsi AES 256 bit sebuah data harus melakukan proses *AddROUNDKey*. Proses *AddROUNDKey* ini dilakukan operasi XOR antara *plainteks* dengan kunci. Proses enkripsi ini terdiri dari 4 jenis transformasi *bytes*, yaitu *SubBytes, ShiftRows, MixColumns*, dan *AddROUNDKey*. Pada awal proses enkripsi atau *ROUND* = 0, *input* akan mengalami transformasi *byte AddROUNDKey*. Setelah itu, *state* akan mengalami transformasi *SubBytes, ShiftRows, MixColumns,* dan *AddROUNDKey* secara berulang-ulang sebanyak *ROUND* = 13, Jika *ROUND* = 14 maka akan melakukan tiga proses transformasi *SubBytes, ShiftRows*, dan *AddROUNDKey* dan akan menghasilkan cipherteks. Proses enkripsi selesai. Dan akan muncul tampilan hasil enkripsi.

Dalam proses dekripsi AES 256 bit *user* memilih *file* dokumen terenkripsi yang terdapat pada media penyimpanan, kemudian memasukkan *key* yang sama untuk dekripsi dan terakhir menekan tombol dekripsi, jika dekripsi berhasil maka dari hasil cipherteks dan dari proses kunci random akan dilakukan penggabungan kunci dalam satu blok yaitu dengan melakukan proses *AddROUNDKey* yaitu cipherteks ditambahkan pada *state* dengan operasi XOR dengan kunci. Proses dekripsi ini terdiri dari 4 jenis transformasi *bytes*, yaitu *InverseSubByte, InverseShiftRows, InverseMixColumn,* dan *AddROUNDKey*. Pada awal proses dekripsi atau *ROUND* = 0, input yang telah *state* akan mengalami transformasi *byte AddROUNDKey*. Setelah itu, *state* akan mengalami transformasi *InverseSubBytes, InverseShiftRows, InverseMixColumns*, dan *AddROUNDKey* secara berulang-ulang sebanyak *ROUND* = 13, Jika *ROUND* = 14 maka akan melakukan tiga proses transformasi *InverseSubBytes, InverseShiftRows, dan AddROUNDKey* dan akan menghasilkan plainteks atau data asli. Proses dekripsi selesai. Dan akan muncul tampilan dekripsi berhasil. Pada tahap ini dilakukan proses implementasi dengan pembuatan modul-modul yang telah dirancang dalam tahap perancangan kriptografi dengan metode *Advanced Encryption Standard* (AES 256) ke dalam bahasa pemrograman PHP.

2.9 Pengujian Sistem

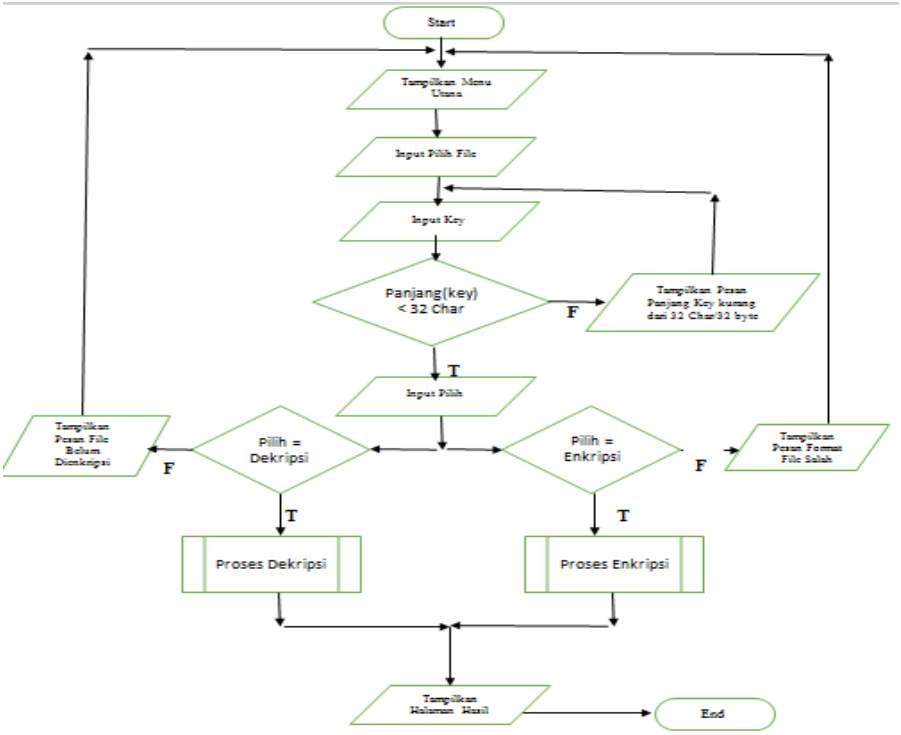
Pada tahap pengujian ini dilakukan dengan tujuan untuk menjamin sistem yang telah dibuat sesuai dengan hasil analisis dan perancangan serta menghasilkan satu kesimpulan apakah sistem tersebut sesuai denganyang diharapkan berdasarkan permasalahan dan atasan masalah. Untuk itudibutuhkan sebuah metode pengujian yang menjadi ukuran atau parametersehingga dapat ditarik kesimpulan bahwa sistem memang telah berjalan sesuai dengan tujuan. 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.

2.10 Kesimpulan Akhir

Pada tahap ini diambil kesimpulan akhir dalam penerapan metode kriptografi A*dvanced Encryption Standard* (AES 256) untuk mengamankan *file* dokumen pada Kelurahan Belendung,berdasarkan hasil pengujian yang telah dilakukan sehingga mengetahui apakah implementasi metode *Advanced Encryption Standard 256* (AES 256) yang telah dilakukan dapat melakukan pengamanan terhadap *file* dokumen Kelurahan Belendung dengan baik.Pada tahap ini juga diberikan saran untuk perbaikan pengembangan sistem.

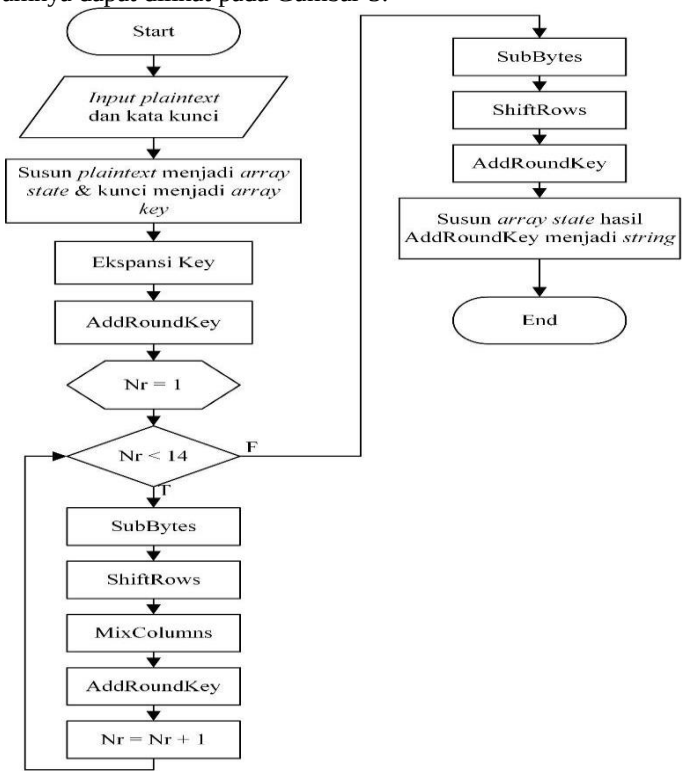
3. HASIL DAN PEMBAHASAN

Program *flowchart* menu utama untuk menjelaskan proses aplikasi pengamanan dokumen berbasis *web* ini dari memilih dokumen, mengisi kata kunci dengan panjang 32 karakter dan memilih tombol enkripsi atau dekripsi untuk melakukan proses kriptografi AES 256 bit maka alur programnya dapat dilihat pada Gambar 2.



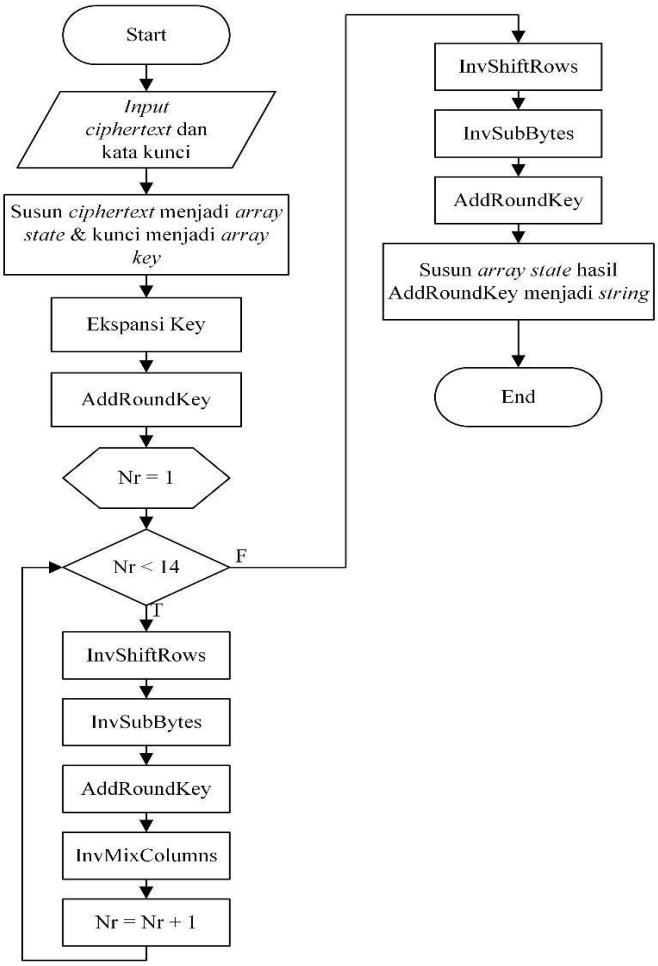
Gambar 2. *Flowchart* Halaman Utama

Program *flowchart* untuk menjalankan proses enkripsi dari aplikasi bila telah memilih dan mengklik *button* enkripsi maka alur programnya dapat dilihat pada Gambar 3.



Gambar 3. *Flowchart* Proses Enkripsi

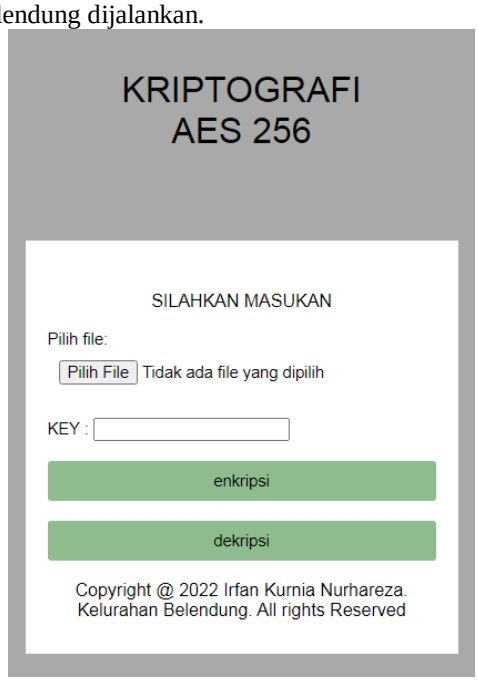
Program *flowchart* untuk menjalankan proses dekripsi dari aplikasi bila telah memilih dan mengklik *button* dekripsi maka alur programnya dapat dilihat pada Gambar 4.



Gambar 4. *Flowchart* Proses Dekripsi

3.1 Tampilan Layar Halaman Utama

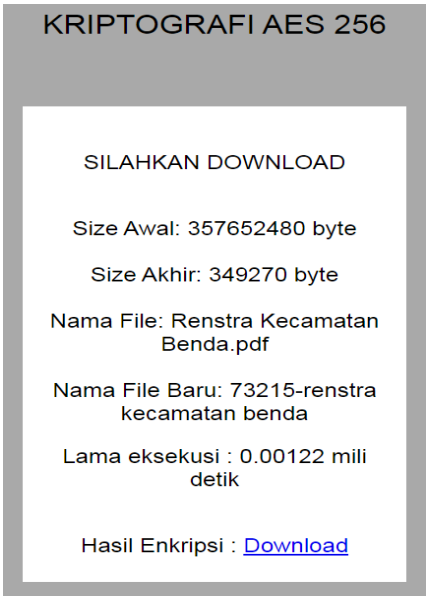
Tampilan layar halaman utama seperti gambar 5 akan tampil pada saat pertama kali aplikasi *web* enkripsi dan dekripsi *file* dokumen Kelurahan Belendung dijalankan.



Gambar 5 Tampilan Layar Halaman Utama

3.2 Tampilan Layar Hasil Enkripsi

Pada gambar 5 setelah memilih file dokumen Rentra Kecamatan Benda dengan extension .pdf yang akan dienkripsi, lalu memasukkan kunci, kemudian klik menu enkripsi, maka proses enkripsi dengan metode AES 256 akan dijalankan dan akan muncul tampilan layar hasil enkripsi, berisikan informasi beserta hasil dari enkripsi seperti gambar 6.



Gambar 6. Tampilan Layar Hasil Enkripsi

3.3 Tampilan Layar Hasil Dekripsi

Pada gambar 5 setelah memilih file dokumen dengan 73215-renstra-kecamatan-benda yang berextension .rda yang akan didekripsi, lalu memasukkan kunci yang sama waktu proses enkripsi, kemudian klik menu dekripsi, maka proses dekripsi dengan metode AES 256 akan dijalankan dan akan muncul tampilan layar hasil dekripsi, menu ini berisikan informasi beserta hasil dari dekripsi seperti gambar 7.

Gambar 7. Tampilan Layar Hasil Dekripsi

3.4 Hasil Percobaan

Tabel 1 merupakan hasil percobaan dari pengujian enkripsi dan dekripsi *file* dokumen dengan menggunakan algoritma AES 256. Pengujian ini dilakukan terhadap kesesuaian proses, untuk membuktikan apakah saat proses enkripsi *file* dokumen dapat dienkripsidan sebaliknya pada saat proses dekripsi, apakah *file* dokumen yang telah dienkripsi berhasil dan kembali ke bentuk semula. Hasil akhir pengujian aplikasi ini diperoleh hasil proses enkripsi rata-rata ukuran dokumen 2496069,1 *byte*, lama waktu proses 1181000 milli detik dan hasil proses dekripsi rata-rata ukuran dokumen 2496128 *byte*, lama waktu proses 1167000 milli detik**.**

Tabel 1. Tabel Hasil Pengujian

NO	NAMA *FILE* DOKUMEN ASLI	SIZE ASLI (*BYTE*)	SIZE HASIL ENKRIPSI (*BYTE*)	WAKTU ENKRIPSI (Milli Second)	SIZE DEKRIPSI (*BYTE*)	WAKTU DEKRIPSI (Milli Second)
1.	827 KK di Kecamatan Benda Kota Tangerang Terdampak Banjir	147446	143991	116000	144000	113000
2.	Banjir di wilayah Benda Tangerang ganggu aktifitas ekonomi warga	269185	262876	121000	262880	117000
3.	Rencana Anggaran Biaya	353155	344878	112000	344880	123000
4	Diduga Langgar Perda, Ketua LSM Portas Minta Tindak Tegas RSIA Makiyah	415214	405483	116000	405488	113000
5	Hibah Bantuan Dana Pembangunan	247783	241976	115000	241984	115000
6	pengajuan dana hibah	436417	426189	113000	426192	114000
7	Perwal_No_50_Tahun_2021	190158	185702	126000	185712	123000
8	Renstra Kecamatan Benda	357652	349270	123000	349280	115000
9	Segera Hadir Kampung Mancing	184018	179706	115000	179712	114000
10	Transportasi Umum ke Kantor Kelurahan Belendung di Kota Tangerang	876441	85590	124000	85600	120000
	Rata-rata	347746,9	2496069,1	1181000	2496128	1167000

4. KESIMPULAN

Kesimpulan yang diperoleh dari penelitian ini adalah: implementasi dengan menggunakan metode algoritma kriptografi AES 256 berhasil mengubah dan mengembalikan isi dokumen Kelurahan Belendung, aplikasi *web* yang dibuat mampu untuk mengamankan isi dokumen dengan baik dan hasil dari proses enkripsi menjadikan isi dokumen tidak dapat terbaca, aplikasi *web* berhasil mengembalikan isi dokumen yang telah di enkripsi ke dalam bentuk awalnya dan dibaca dengan baik, dan hasil akhir pengujian aplikasi ini diperoleh hasil proses enkripsi rata-rata ukuran dokumen 2496069,1 *byte*, lama waktu proses 1181000 milli detik dan hasil proses dekripsi rata-rata ukuran dokumen 2496128 *byte*, lama waktu proses 1167000 milli detik**.**

Beberapa saran yang mungkin bisa dijadikan pertimbangan untuk ke depannya dalam pengembangan sistem ke tahap yang lanjut, antara lain sebagai berikut: penambahan fitur pada aplikasi *web* seperti, tombol kembali untuk kembali kehalaman utama, dan tombol *SEND* untuk mengirimkan *file* melalui *internet* sehingga bisa lebih mempermudah *user*, serta qplikasi *web* tidak hanya dapat mengakses dokumen berformat PDF dan txt saja, akan tetapi seluruh format lainnya.

DAFTAR PUSTAKA

[1] N. Anwar, Munawwar, M. Abduh, And N. B. Santosa, "Komparatif *Performance* Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA," *Jurnal RESTI*, vol. 2, no. 3, pp. 783 – 791, 2018.

[2] A. Fathurrozi, And Selviyani,"Penerapan Algoritma *Advanced Encryption Standard* (AES-256) Dengan Mode CBC DanSecure Hash Algorithm (SHA-256) Untuk Pengamanan Data *File*," *JIFORTY*, vol. 2, no. 2, pp. 227-238, 2021.

[3] A. Hermawan, And E. Iman, "Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA," *Infotekjar: Jurnal Nasional Informatika Dan Teknologi Jaringan, vol. 5, no. 2*, pp. 326-330, 2021.

[4] 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), vol. 4, no. 1*, pp. 78-86, 2020.

[5] O. G. Khoirunnisa, And Djuniadi, "Implementasi Algoritma AES untuk Keamanan Data Rekam Medis," *PETIR: Jurnal Pengk ajian dan Penerapan Teknik Informatika, vol. 15, no. 1*, pp. 21-27, 2022.

[6] K. Muttaqin, And J. Rahmadoni," Analysis And Design of File Security System AES (Advanced Encryption Standard) Cryptography Based," *Journal of Applied Engineering and Technological Science, vol. 1, no. 2*, pp. 113-123, 2020.

[7] R. Nuari, And N. Ratama, "Implementasi Algoritma Kriptografi AES (*Advanced Encryption Standard*) 128 Bit Untuk Pengamanan Dokumen Shipping," *Journal Of Artificial Intelligence And Innovative Applications*, vol. 1, no. 2, pp. 37-44, 2020.

[8] A. P. Putra, Herfina,, S. Maryana, And A. Setiawan, "Implementasi Algoritma AES (*Advance Encryption Standard*) Rijndael Pada Aplikasi Keamanan Data," *JIPETIK*, vol. 1, no. 2, pp. 46-51, 2020.

[9] A. P. Lia, and A. Solichin, "Pengamanan Aplikasi Mobile BluCampus dengan Algoritma AES-128 dan Affine Cipher : Studi Kasus Universitas Budi Luhur," *SKANIKA*, vol. 1, no. 1, pp. 68-75, 2018.

[10] Y. Wiharto, And A. Irawan, "Enkripsi Data Menggunakan *Advanced Encryption Standard* 256", *JurnaL KILAT*, vol. 7, no. 2, pp. 91-99, 2018.

[11] S. Y. Irawan, dkk. "Pengamanan *File* Video dengan algoritma *Advanced Encryption Standard* (AES)," *SYSTEMATICS*, vol. 2, no. 1, pp. 28-32, 2020.