3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
30 Agustus 2023 – Jakarta, Indonesia
Volume 2, Nomor 2, September 2023 - ISSN 2962-8628 (*online*)

IMPLEMENTASI KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD (AES-128)* UNTUK PENGAMANAN DOKUMEN PADA KLINIK *PET LOVE CENTER*

Bagus Eka Prayoga[1*], Reva Ragam Santika[2]

[1,2] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: [1*]1711502219@student.budiluhur.ac.id, [2]reva.ragam@budiluhur.ac.id
(* : corresponding author)

Abstrak- Pengamanan pada sebuah data yang dimiliki oleh sebuah organisasi baik itu instansi pemerintah, industri, rumah sakit, sekolah dan lainnya adalah langkah yang penting. Kemajuan dan perkembangan teknologi informasi saat ini berpengaruh pada beberapa aspek kehidupan dan mengalami kemajuan setiap informasi di bidang kesehatan. Klinik *Pet Love Center* merupakan klinik hewan yang berdiri sejak 2016 dan terletak di kota jakarta. Klinik *Pet Love Center* terdapat banyak data sensitif yang harus dijaga kerahasiaannya. Selain kemajuan teknologi yang kian meningkat, kejahatan di dunia digital juga kian meningkat, sehingga mulai dari penyimpanan data hingga pengelolaan data, penggunaan teknologi keamanan data menjadi sangat penting diperlukan. Data yang disimpan haruslah aman dari ancaman pihak yang mencoba meretas atau merusak data tersebut. Untuk mengatasi masalah tersebut pada Klinik *Pet Love Center*, diperlukan suatu aplikasi proteksi data yang dapat memproteksi dan mengamankan dokumen yang dimiliki. Aplikasi pelindung data disini menggunakan algoritma enkripsi AES-128 (*Advanced Encryption Standard*-128). Aplikasi ini dibangun dengan menggunakan bahasa pemrograman PHP berbasis web, dan dapat melakukan enkripsi dan dekripsi data menggunakan jenis *file* *.xls, *.xlsx, *.txt, *.pdf, *.doc, *.docx, *.ppt, dan *.pptx. Aplikasi ini dibuat agar dapat memberikan keamanan serta menjaga kerahasiaan data dan informasi Klinik *Pet Love Center*, serta mencegah pencurian dan manipulasi data oleh pihak yang tidak berkepentingan.

Kata Kunci: Kriptografi, AES-128, *File*

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES-128) CRYPTOGRAPHY FOR SECURING FILES AT PET LOVE CENTER CLINIC

Abstract- *Securing data owned by an organization, be it government agencies, industry, hospitals, schools and others, is an important step. Advances and developments in information technology currently affect several aspects of life and experience progress in every information in the health sector. Pet Love Center Clinic is a veterinary clinic that was founded in 2016 and is located in the city of Jakarta. The Pet Love Center Clinic has a lot of sensitive data that must be kept confidential. In addition to increasing technological advances, crime in the digital world is also increasing, so that from data storage to data management, the use of data security technology is very important. The data stored must be safe from the threat of parties trying to hack or damage the data. To overcome this problem at the Pet Love Center Clinic, we need a data protection application that can protect and secure the documents that are owned. The data protection application here uses the AES-128 encryption algorithm (Advanced Encryption Standard-128). This application was built using the web-based PHP programming language, and can encrypt and decrypt data using file types *.xls, *.xlsx, *.txt, *.pdf, *.doc, *.docx, *.ppt, and *. pptx. This application was created in order to provide security and maintain the confidentiality of data and information at the Pet Love Center Clinic, as well as prevent data theft and manipulation by unauthorized parties.*

***Keywords**: Cryptography, AES-128, File*

1. PENDAHULUAN

Teknologi komputer dan telekomunikasi saat ini telah mengalami kemajuan dan sudah menjadi suatu kebutuhan yang penting bagi setiap orang, karena banyaknya pekerjaan yang dapat diselesaikan dengan cepat [1]. Karena kemudahan teknologi, setiap orang menggunakan suatu alat teknologi internet untuk bertukar data seperti dokumen, dan lain - lain. Seiring dengan perkembangan tersebut, kejahatan di dunia digital kian meningkat pesat dari adanya perbuatan seperti pengambilan informasi yang dapat disalahgunakan oleh oknum yang tidak bertanggung jawab. Keamanan dan kerahasiaan data adalah salah satu aspek yang sangat penting dalam dunia teknologi pada saat ini. Disebabkan munculnya ilmu pengetahuan yang memungkinkan Teknik-teknik untuk melakukan kejahatan pada informasi, sehingga dapat merugikan pemilik informasi [2].

Klinik *Pet Love Center* merupakan suatu instansi kesehatan yang berlokasi di Kecamatan Kebayoran Baru, Jakarta Selatan. Dalam instansi tersebut memiliki cukup data yang penting seperti data karyawan, data pasien maupun berkas pembayaran pasien yang berbentuk digital. Data dari dokumen tersebut tidak dapat diakses maupun dibuka oleh setiap orang dan hanya orang yang mempunyai akses yang dapat membuka dokumen tersebut. Data tersebut mencakup .pdf, .docx, .pptx, .xlsx, .pdf.

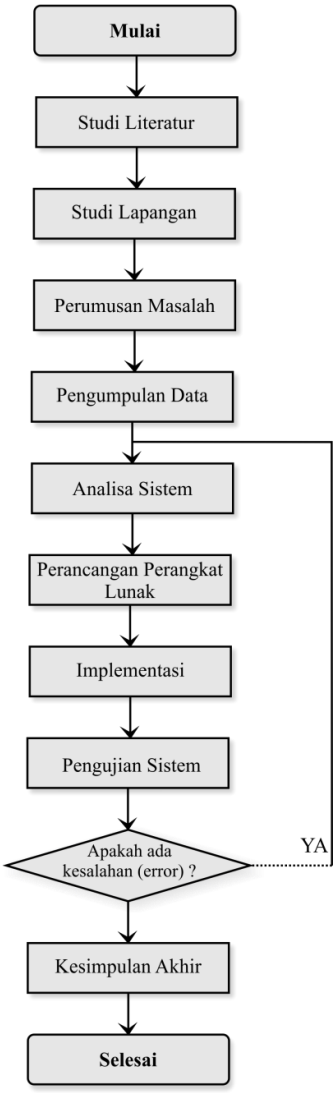
Permasalahannya adalah instansi ini masih menyimpan data yang berbentuk digital tersebut di dalam suatu *folder* pada komputer tanpa adanya sistem pengaman data. Instansi ini juga tidak mempunyai sistem penyimpanan dan pengamanan *database* yang berguna untuk media penyimpanan file sehingga para karyawan apabila membutuhkan suatu *file*, mereka harus meminta kepada kepala operasional yang memiliki *file* bersangkutan. Apabila hal ini dibiarkan maka akan mendapatkan masalah besar karena bocornya data perusahaan ke pihak yang tidak bertanggung jawab [3]. Oleh karena itu dibutuhkan suatu metode atau cara yang dapat menjaga kerahasiaan informasi ini, yang salah satunya dikenal dengan sebutan kriptografi. Dalam kriptografi terdapat banyak algoritma, diantaranya algoritma DES, AES, IDEA dan Blowfish [4]. Pengamanan *file* dengan menggunakan Teknik kriptografi telah banyak dilakukan dalam berbagai penelitian [5].

Kriptografi adalah ilmu dan seni menjaga keamanan pesan, yaitu kriptografi adalah ilmu yang mempelajari metode matematika yang berkaitan dengan keamanan informasi (seperti kerahasiaan, integritas data, dan verifikasi identitas). Kata "seni" dalam definisi diatas berarti ada cara unik untuk menjaga kerahasiaan informasi. Kata *"graphy"* didalam *"cryptography"* itu sendiri sudah menyiratkan sebuah seni [6]. Dalam kriptografi terdapat banyak algoritma, salah satunya adalah algoritma AES *(Advanced Encryption Standard)* [7]. Penelitian ini menggunakan algoritma enkripsi kunci simetris AES *(Advance Encryption Standard)* 128 karena memiliki tingkat keamanan yang tinggi yaitu, dokumen menjadi lebih aman setelah diubah menjadi data terenkripsi karena dokumen hanya dapat dibuka oleh pihak yang berwenang.

AES adalah algoritma kriptografi untuk mengamankan data dimana algoritmanya adalah *blokchipertext* simetrik yang dapat mengenkripsi dan mendekripsi informasi [8]. Pada 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang di publikasikan oleh NIST *(National Institute of Standard and Technology)* sebagai pengganti algoritma DES (Data *Encryption Standard*) yang sudah berakhir masa penggunaannya [9]. Keuntungan menggunakan algoritma ini dapat melakukan enkripsi untuk jumlah data yang besar dan mengkonsumsi sedikit dalam pelaksanaannya [10]. Berdasarkan penelitian sebelumnya yang dilakukan oleh [4] yang berjudul "Perbandingan Algoritma DES,AES,IDEA, dan Blowfish dalam Enkripsi dan Dekripsi Data" Algoritma AES memiliki kecepatan paling tinggi dibandingkan dengan ketiga algoritma tersebut. Oleh karena itu tujuan penelitian ini yaitu membuat sebuah alat bantu berupa *website* yang dapat mengamankan *file* dokumen menggunakan metode *Advanced Encryption Standard* (AES-128) agar dokumen atau file Klinik Pet Love Center menjadi aman dari pencurian data dan orang yang tidak bertanggung jawab.

2. METODE PENELITIAN

Melakukan penelitian dengan berpedoman pada metode penelitian, agar hasil penelitian tidak menyimpang dari sasaran, sehingga mencapai hasil yang lebih baik. Dengan demikian seperti terlihat pada Gambar 1 dibawah menggambarkan metodologi penelitian yang dilakukan yaitu analisis kebutuhan, desain sistem, pengujian, implementasi dan hasil.



Gambar 1 Metode Penelitian

2.1 Pengumpulan Data

Pada tahap ini pengumpulan data dilakukan melalui studi literatur, wawancara dan observasi.

a. Studi Literatur
   Dilakukan dengan membaca, mempelajari buku dan artikel terkait keamanan, kriptografi, aplikasi AES-128 yang mendukung topik yang sedang dibahas.
b. Wawancara
   Melakukan wawancara dengan pihak-pihak terkait untuk mengetahui permasalahan yang ada, sehingga dapat dirumuskan suatu sistem yang dapat mengatasi permasalahan tersebut.
c. Observasi
   Observasi adalah salah satu metode pengumpulan data yang efektif untuk mempelajari sebuah sistem. Hal ini dilakukan dengan pengamatan secara langsung terhadap prosedur sistem yang sedang berjalan.

2.2 Rancangan Penguji

Rancangan pengujian yang diterapkan yaitu apakah sistem aplikasi dapat berjalan sesuai dengan tujuannya yaitu mengamankan data menggunakan algoritme *AES-128.*

2.3 Rancangan Basis Data

Berikut adalah struktur *database* yang akan digunakan untuk merancang aplikasi enkripsi AES-128. Struktur tabel lihat Tabel 1 dibawah ini menunjukan spesifikasi *database users* dan Tabel 2 menunjukan spesifikasi *database file*.

Tabel 1 Spesifikasi *Database Users*

Nama Field	***Type***	***Ukuran***	***Keterangan***
UserName	*Varchar*	*15*	*Nama user*
Password	*Varchar*	*100*	*Password*
FullName	*Varchar*	*50*	*Nama Lengkap*
Job_Title	*Varchar*	*50*	*Jabatan*
Join_Date	*Timestamp*	*-*	*Tanggal Gabung*
Last_Activity	*Timestamp*	*-*	*Terakhir aktivitas*
status	*Enum*	*2*	*Status*

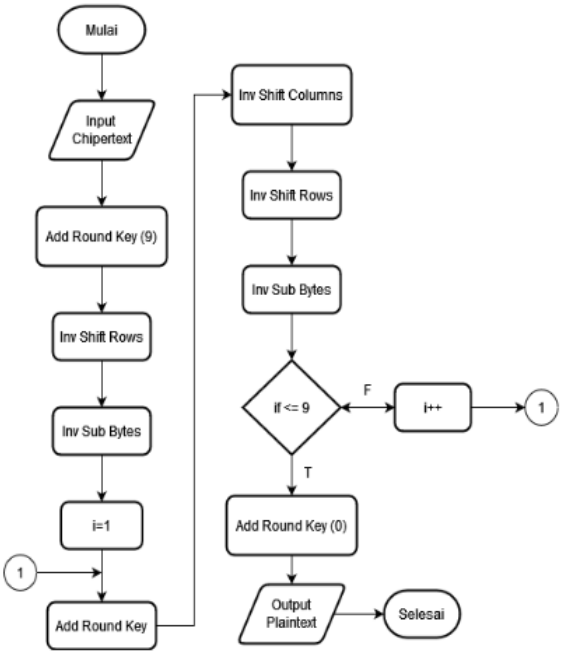
Tabel 2 Spesifikasi *Database File*

Nama_Field	***Type***	***Ukuran***	***Keterangan***
Id_file	*Int*	*11*	*Id_file*
UserName	*Varchar*	*15*	*Nama User*
File_Name_Source	*Varchar*	*255*	*Nama File Awal*
File_Name_Finish	*Varchar*	*255*	*Nama File Akhir*
File_Url	*Float*	*255*	*Url*
File_Size	*Varchar*	*-*	*Ukuran*
Password	*Varchar*	*16*	*Password*
Keyaes	*Timestamp*	*16*	*Kunci Aes*
Tgl_Upload	*Timestamp*	*-*	*Tanggal Upload*
Status	*Enum*	*2*	*Status*
Keterangan	*Varchar*	*255*	*Keterangan*

3. HASIL DAN PEMBAHASAN

Pada bagian ini adalah penjelasan dari implementasi algoritma AES 128 yang digunakan untuk mengenkripsi dan mendekripsikan *file* atau dokumen. Pada bagian ini juga menjelaskan tentang alur proses enkripsi dan dekripsi, hasil pengujian, dan *flowchart* enkripsi dan dekripsi.

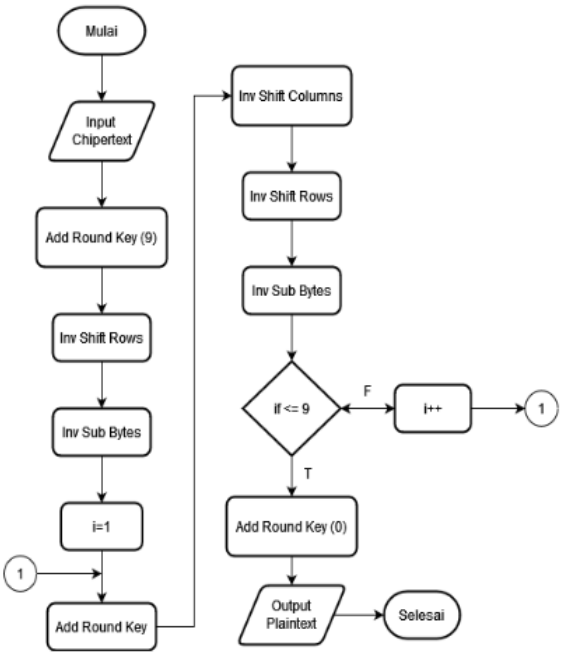
3.1 *Flowchart* Proses Enkripsi



Gambar 2 *Flowchart* Proses Enkripsi

Pada Gambar 2 diatas adalah *flowchart* dari proses enkripsi *Advanced Encryption Standard* (AES). Menjelaskan alur proses yang terjadi pada algoritma AES-128 untuk mengenkripsi *Plaintex* menjadi *Chipertext*.

3.2 *Flowchart* Proses Dekripsi



Gambar 3 *Flowchart* Proses Dekripsi

Pada Gambar 3 diatas adalah *flowchart* dari proses dekripsi *Advanced Encryption Standard* (AES). Menjelaskan alur proses yang terjadi pada algoritma AES-128 untuk mendekripsi *Chipertext* menjadi *Plaintext*.

3.3 Pengujian

Pada bagian ini merupakan tahap pengujian enkripsi dan dekripsi *file*, pengujian tersebut nantinya akan menghasilkan perbandingan *file* yang belum terenkripsi dengan *file* yang sudah terenkripsi.

a) Pengujian Enkripsi
Pada tahap ini, terlihat hasil pengujian enkripsi pada beberapa *file* yang dapat dilihat pada Tabel 3 dibawah ini.

Tabel 3 Hasil Enkripsi

No	Nama *File* Asli	Ukuran Awal (kb)	Waktu (detik)	Nama *File* Enkripsi	Ukuran Akhir (kb)	% Kenaikan Ukuran *File*
1	ABSTRAK.pdf	109	0,14	abstrak.rda	110	0,01
2	BAB 1.docx	25,1	0,07	bab-1.rda	26	0,9
3	BUKU TAMU.docx	20,4	0,05	buku-tamu.rda	21	0,6
4	Data Pasien 020423.doc	98,0	0,06	data-pasien-020423.rda	98,0	0
5	File-1.txt	0,039	0,02	file-1.rda	0,048	0,009
6	Keuangan-2023.xlsx	9,08	0,09	Keuangan-2023.rda	10	0,92
7	Laporan Kas.xls	137	1,56	Laporan-kas.rda	137	0
8	PANDUAN-TOPIK-TUGASAKHIR-TI-GASAL20222023-20Oktober2022-v3.pdf	1,257	3,68	panduan-topik-tugasakhir-ti-gasal20222023-20oktober2022-v3.rda	1,757	0,50
9	PPT-2022	242	2,10	Ppt-2022.rda	243	0,01
10	Presentasi23.pptx	404	2,56	Presentasi-23.rda	405	0, 0

b) Pengujian Dekripsi
Pada tahap ini, dilakukan pengujian dekripsi kepada *file* yang sebelumnya sudah di enkripsi. Hasil dekripsi dapat dilihat pada Tabel 4 dibawah ini.

Tabel 4 Hasil Dekripsi

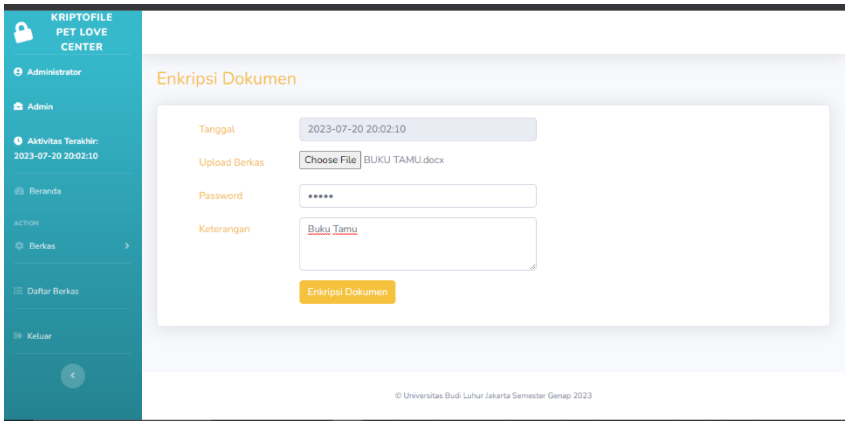
No	Nama *File* Enkripsi	Ukuran Awal (kb)	Waktu (detik)	Nama *File* Dekripsi	Ukuran Akhir (kb)
1	abstrak.rda	110		-abstrak.pdf	110
2	bab-1.rda	26		-bab-1.docx	26
3	buku-tamu.rda	21		-buku-tamu.docx	21
4	data-pasien-020423.rda	98		-data-pasien-020423.doc	98
5	file-1.rda	0,0048		-file-1.txt	1
6	keuangan-2023.rda	10		-keuangan-2023.xlsx	10
7	laporan-kas.rda	137		-laporan-kas.xls	137
8	panduan-topik-tugasakhir-ti-gasal-20222023-	1,757		-panduan-topik-tugasakhir-ti-gasal20222023-	1,257

	20oktober2022-v3.rda		20oktober2022-v3.pdf	
9	ppt-2022.rda	243	-ppt-2022.ppt	243
10	presentasi23.rda	405	-presentasi23.pptx	405

3.4 Tampilan Layar

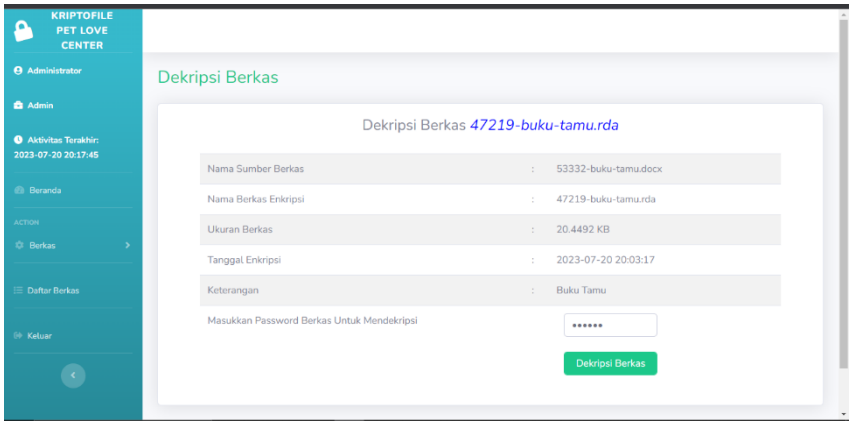
Pada bagian ini akan dijelaskan tampilan layar untuk mengenkripsi *file*, tampilan layar untuk mendekripsi *file*, tampilan layar daftar berkas, dan tampilan hasil dari enkripsi dan dekripsi *file.*

a. Pada tampilan menu enkripsi adalah tampilan menu yang berguna untuk memasukkan *file* yang ingin diamankan kemudian memasukan *password.* Tampilan menu enkripsi dapat dilihat pada Gambar 4 dibawah ini.



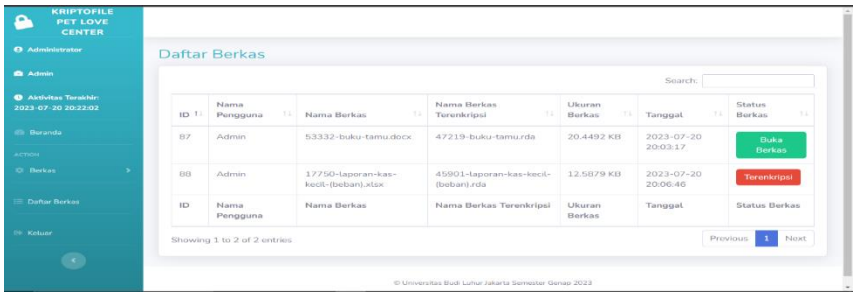
Gambar 4 Tampilan Enkripsi

b. Pada tampilan menu dekripsi adalah tampilan halaman menu yang digunakan untuk memasukkan *file* yang sudah di enkripsi untuk dilakukan proses dekripsi. Tampilan halaman dapat dilihat pada Gambar 5 dibawah ini.



Gambar 5 Tampilan Dekripsi

c. Tampilan Daftar Berkas merupakan halaman yang akan menampilkan hasil *file* yang sudah di enkripsi maupuin di dekripsi. Tampilan halaman dapat dilihat pada Gambar 6 dibawah ini.

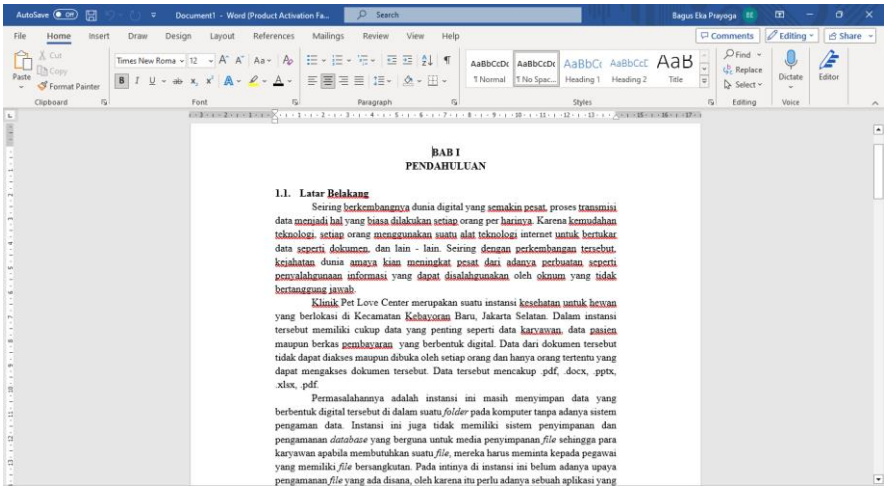


Gambar 6 Tampilan *Daftar Berkas*

d. Tampilan hasil enkripsi pada gambar 7 dibawah ini adalah hasil dari *file* yang telah berhasil terenkripsi sehingga isi *file* akan menjadi *chipertext.*

Gambar 7 Tampilan Hasil *File* Enkripsi

e. Tampilan hasil dekripsi pada gambar 8 dibawah ini adalah hasil dari *file* yang telah berhasil di dekrpisi sehingga *file* akan kembali seperti semula.



Gambar 8 Tampilan Hasil *File* Dekripsi

4. KESIMPULAN

Kesimpulan yang di dapat dari analisis terhadap masalah dan uji coba yang telah dilakukan, dapat ditarik kesimpulan bahwa aplikasi yang telah dibuat untuk mengamankan *file* dokumen berbasis *website* dengan menggunakan metode algoritma AES 128 dapat berfungsi dengan baik dan mampu mengamankan *file* dokumen

pada Klinik Pet Love Center dari pihak-pihak yang tidak berwenang dan bertanggung jawab. Dan untuk kecepatan waktu proses enkripsi dan dekripsi bergantung dari ukuran *file* yang akan di proses.

DAFTAR PUSTAKA

[1] N. Cristy and F. Riandari, "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," *JIKOMSI (Jurnal Ilmu Komputer dan Sistem Informasi,* vol. 4, no. 2, pp. 75-85, 2021.

[2] D. Widyawan and Imelda, "PENGAMANAN FILE MENGGUNAKAN KRIPTOGRAFI DENGAN," *SKANIKA,* vol. 4, no. 1, pp. 15-22, 2021.

[3] Y. Putra, Y. Yunus and Sumijan, "Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Serangan Cross Site Scripting," *Jurnal Sistim Informasi dan Teknologi,* vol. 3, no. 2, pp. 56-63, 2021.

[4] D. A. Meko, "Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data," *Jurnal Teknologi Terpadu,* vol. 4, no. 1, pp. 8-15, 2018.

[5] M. Azhari, D. I. Mulyana, F. J. Perwitosari and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan," *Jurnal Pendidikan Sains dan Komputer,* vol. 2, no. 1, pp. 163-171, 2022.

[6] A. A. Permana and D. Nurnaningsih, "RANCANGAN APLIKASI PENGAMANAN DATA DENGAN ALGORITMA ADVANCED ENCYPTION STANDARD (AES)," *Jurnal Teknik Informatika,* vol. 11, no. 2, pp. 177-186, 2018.

[7] L. Mustika, "Implementasi Algoritma AES untuk pengamanan Login dan Data Customer pada E-Commerce Berbasis Web," *JURIKOM (Jurnal Riset Komputer),* vol. 7, no. 1, pp. 148-155, 2020.

[8] I. A. R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi and S. Solikhun, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," *Journal of Computer System and Informatics (JoSYC),* vol. 1, no. 2, pp. 54-60, 2020.

[9] A. Prameshwari and N. P. Sastra, "Implementasi Algortima Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika,* vol. 8, no. 2, pp. 52-58, 2018.

[10] T. Hidayat, "Encryption Security Sharing Data Cloud Computing By Using AES Algorithm: A Systematic Review," *TEKNOKOM,* vol. 2, no. 2, pp. 11-16, 2019.