2nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
21 Maret 2023 – Jakarta, Indonesia
Volume 2, Nomor 1, April 2023 - ISSN 2962-8628 (*online*)

PENERAPAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* 128 UNTUK PENGAMANAN DOKUMEN PADA PT. INDOTRADE JASAMA

Cesario Novanada Limenta[1*], Utomo Budiyanto[2], Windarto[3], Dewi Kusumaningsih[4]

[1,2,3,4] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]cesarionovanada@gmail.com, [2]utomo.budiyanto@budiluhur.ac.id, [3]windarto@budiluhur.ac.id, [4]dewi.kusumaningsih@budiluhur.ac.id
(* : corresponding author)

Abstrak- *File* merupakan dokumen yang berisikan hasil pekerjaan maupun informasi-informasi penting yang tersimpan di dalam komputer. *File* yang dianggap penting harus dijaga kerahasiaannya dengan membutuhkan pengamanan sehingga dapat terhindar dari hal yang tidak diinginkan. PT. Indotrade Jasama merupakan perusahaan yang bergerak di bidang *chemical trading* atau penjualan bahan baku kimia. Perusahaan ini memiliki data penting seperti dokumen transaksi, dokumen data *client*, dokumen keuangan, dan masih banyak dokumen lainnya yang dimana dokumen tersebut tidak boleh diketahui sembarang orang yang disimpan pada komputer. Perusahaan ini belum memiliki *database* yang berfungsi sebagai media penyimpanan dokumen sehingga apabila karyawan membutuhkan suatu dokumen, mereka harus meminta kepada karyawan yang mempunyai dokumen yang dibutuhkan, kegiatan ini dapat menimbulkan kebocoran data. Oleh karena itu, penelitian ini bertujuan untuk membuat aplikasi pengamanan data agar tidak dapat dicuri oleh pihak yang tidak berhak. Aplikasi ini menggunakan metode *Advanced Encryption Standard* (AES)-128 untuk enkripsi dan dekripsi data. AES-128 adalah suatu algoritme *simetris block* yang cukup aman karena memiliki 10 putaran dalam proses enkripsi serta dekripsinya. Aplikasi ini di buat menggunakan bahasa pemrograman PHP. Data yang di enkripsi adalah *file* dokumen. Berdasarkan implementasi dan pengujian program, dapat disimpulkan bahwa aplikasi ini mampu untuk mengamankan dan menjaga isi *file* dokumen penting perusahaan. Kontribusi penelitian ini adalah untuk mengatasi kebocoran atau pencurian data berupa *file* dokumen pada PT. Indotrade Jasama. Hasil dari penelitian ini adalah *file* berhasil di enkripsi sehingga *file* terjaga keamanannya.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, Pengamanan Dokumen, AES-128.

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD 128 ALGORITHM FOR DOCUMENT SECURITY AT PT. INDOTRADE JASAMA

Abstract- *A file is a document that contains work results and important information stored on a computer. Files that are considered important must be kept confidential by requiring security so that unwanted things can be avoided. PT. Indotrade Jasama is a company engaged in chemical trading or the sale of chemical raw materials. This company has important data such as transaction documents, client data documents, financial documents, and many other documents where these documents cannot be known by just anyone stored on a computer. This company does not yet have a database that functions as a document storage medium so that if employees need a document, they must ask the employee who has the required document, this activity can cause data leakage. Therefore, this study aims to create data security applications so that they cannot be stolen by unauthorized parties. This application uses the Advanced Encryption Standard (AES)-128 method for data encryption and decryption. AES-128 is a symmetric block algorithm that is quite secure because it has 10 rounds in the encryption and decryption process. This application is made using the PHP programming language. The encrypted data is a document file. Based on the implementation and testing of the program, it can be concluded that this application is able to secure and maintain the contents of important company document files. The contribution of this research is to overcome data leakage or theft in the form of document files at PT. Indotrade Jasasama. The result of this research is that the file is successfully encrypted so that the file is kept safe*

Keywords*: Cryptography, Encryption, Decryption, Document Security, AES-128.*

1. PENDAHULUAN

File merupakan dokumen yang berisikan hasil pekerjaan maupun informasi-informasi penting yang tersimpan didalam komputer. *File* yang dianggap penting harus dijaga kerahasiaannya dengan membutuhkan pengamanan sehingga terhindar dari hal yang tidak diinginkan [1]. PT. Indotrade Jasama merupakan perusahaan yang bergerak di bidang *chemical trading* atau penjualan bahan baku kimia. Perusahaan ini memiliki data penting seperti dokumen transaksi, dokumen data *client*, dokumen keuangan, dan masih banyak dokumen lainnya yang dimana dokumen tersebut tidak boleh diketahui sembarang orang yang disimpan di dalam komputer tanpa adanya

sistem pengamanan.Perusahaan ini juga belum memiliki *database* yang berfungsi sebagai media penyimpanan *file* dokumen sehingga apabila karyawan membutuhkan suatu *file,* mereka harus meminta kepada karyawan yang mempunyai *file* yang dibutuhkan, kegiatan ini dapat menimbulkan kebocoran data.

Berdasarkan pada latar belakang di atas, salah satu cara untuk mengamankan dokumen pada perusahaan, yakni dibutuhkan alat bantu berupa aplikasi keamanan dokumen berbasis Web menggunakan teknik kriptografi. Kriptografi sangat berhubungan dengan pengamanan data digital. Ilmu ini berdasar dari beberapa mekanisme perancangan yang berdasarkan algoritme dalam matematik dengan tawaran sejumlah keamanan informasi yang bersifat fundamental [2]. Kriptografi berasal dari bahasa Yunani, *"cryptos"* yang artinya "*secret*" (rahasia) dan *"grapheirl"* yang berarti "*writing*" (tulisan) [3]. Kriptografi bisa diartikan sebagai ilmu untuk menjaga kerahasiaan informasi dengan metode dan teknik yang mencakup *Confidentiality, Integritas, Authentication* [4].Tujuan kriptografi adalah memberikan keamanan yaitu *Confidentially*/(Kerahasiaan), *Data Integrity*/(Integritas data), *Authentication*/(Autentifikasi), *Non-repudiation*/(Penyangkalan) [5].

Berdasarkan penelitian sebelumnya yang dilakukan oleh [6] membahas, *Advanced Encryption Standard* (AES) dikenal sebagai algoritme yang memiliki keamanan yang cukup tinggi. Karena AES mempunyai panjang *key* yang paling sedikit adalah 128bit, maka dari itu AES dapat bertahan terhadap serangan *exhaustive key search* [6]. Sehingga dalam penelitian ini dibuat sistem Aplikasi berbasis Web menggunakan metode *Advanced Encryption Standard* (AES 128). AES merupakan algortima kriptografi yang dapat mengenkripsi dan mendekripsi data atau informasi dengan panjang *key* yang beragam, yakni 128, 192 dan 256 bit [7]. AES-128 menggunakan 10 putaran, AES-192 dengan 12 putaran, dan AES-256 dengan 14 putaran. Setiap round atau putaran mengandung pergantian byte [8]. Enkripsi merupakan proses pengubahan data *plaintext* menjadi *chipertext* [9]. Dekripsi merupakan proses pengembalian *chipertext* menjadi *plaintext* [10].

Maka dari itu tujuan dari penelitian ini yakni membuat sebuah alat bantu berupa perangkat lunak yang menggunakan metode *Advanced Encryption Standard* (AES)-128 agar dokumen PT. Indotrade Jasama menjadi aman dari pihak yang tidak berkepentingan.

2. METODE PENELITIAN

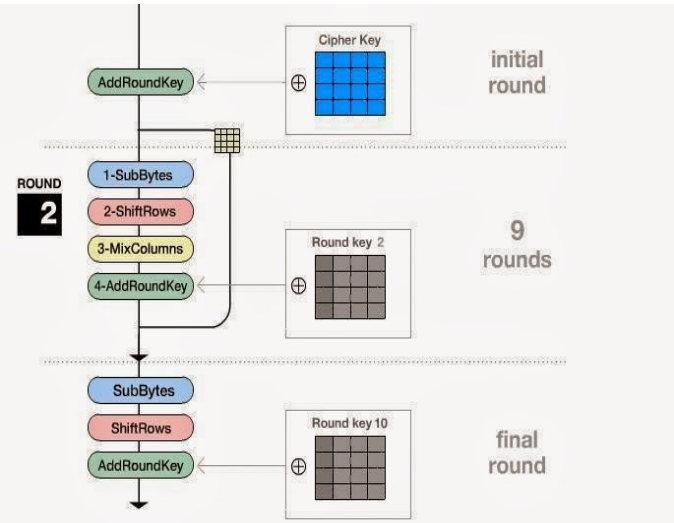
2.1 Pengumpulan Data

Dalam fase ini dilakukan pengumpulan data dan informasi yang relevan dengan permasalahan yang ada. Proses mengumpulkan data dan informasi didapat dari wawancara serta observasi. Wawancara dilakukan dengan mengajukan pertanyaan kepada pihak perusahaan yang ada hubungannya dengan pengamanan dokumen yang dilakukan pada direktur perusahaan, agar mendapatkan informasi tentang sistem pengamanan dokumen yang digunakan, lalu observasi dengan melakukan pengamatan secara langsung terhadap prosedur sistem keamanan dokumen yang sedang digunakan di perusahaan tersebut.

2.2 Penerapan Metode

Dalam fase ini menjelaskan bagaimana proses enkripsi dan dekripsi algoritma AES-128. Berikut adalah tahapan enkripsi pada Algoritma AES-128 [11]:

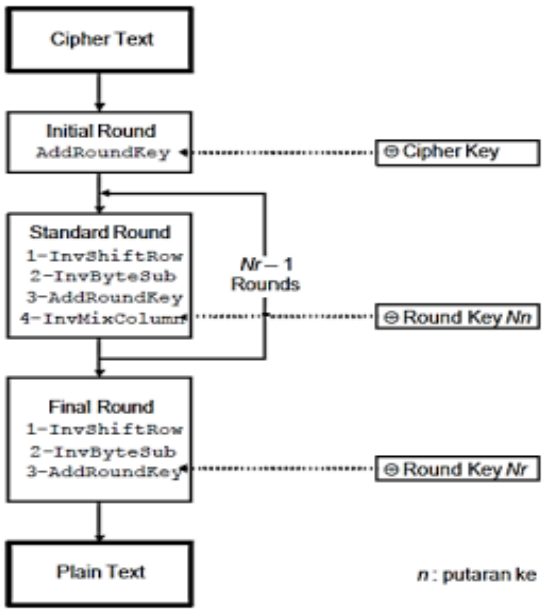
a. *AddRoundKey :* yaitu proses melakukan X-OR (*Exclusive Or*) antara *state* awal (*plaintext*) dan *chiperkey.* Tahap ini disebut juga dengan *initial round.*
b. *Round :* yaitu, putaran sebanyak NR – 1 kali. Pada setiap putaran atau ronde memiliki beberapa proses, diantaranya adalah :
    1. *SubBytes :* yaitu, mensubstitusikan *byte* dengan menggunakan table S-box (tabel substitusi).
    2. *ShiftRows :* yaitu, melakukan pergeseran tiap baris array *state* secara *wrapping.*
    3. *Mixcolumn :* yaitu, mengacak data pada tiap kolom array *state.*
    4. *AddRoundKey :* yaitu, melakukan X-OR antara hasil state sekarang dengan kunci hasil proses *expand key.*
c. *Final Round :* yaitu proses untuk putaran atau ronde terakhir:
    1. *SubBytes*
    2. *ShiftRows*
    3. *AddRoundKey*



Gambar 1. Proses Enkripsi AES-128

Berikut adalah tahapan dekripsi pada Algoritma AES-128 [12]:

a. *AddRoundKey* : melakukan XOR antara state awal(*chipertex*) dengan *chiperkey*. Tahap ini disebut juga *initial round*.
b. Putaran sebanyak Nr-1 kali. Proses yang dilakukan pada setiap putaran adalah :
   1. *InverseShiftRows* : pergeseran baris-baris array *state* secara wrapping kebalikan dari ShiftRows.
   2. *InverseSubBytes* : substitusi *byte* dengan menggunakan tabel invers substitusi (invers S-box).
   3. *AddRoundkey* : melakukan XOR antara state sekarang dengan *round key*.
   4. *InverseMixColumns*: membalikkan operasi MixColumns
c. *Final round* : proses untuk putaran terakhir :
   1. *InverserShiftRows*
   2. *InverseSubBytes*
   3. *AddRoundKey*



Gambar 2. Proses Dekripsi AES-128

2.3 Perancangan Perangkat Lunak

Dalam fase ini akan dilakukan perancangan yang sebanding dengan hasil dari analisa sistem terutama perancangan untuk enkripsi serta dekripsi. Selain itu pendukung lain yang akan digabungkan dengan aplikasi dan perancangan interface. Dalam pengembangan perangkat lunak yang akan dipakai menggunakan metode *waterfall.* Model ini harus membutuhkan penyelesaian secara berututan sebelum lanjut ke tahap berikutnya.

2.4 Implementasi

Dalam fase ini akan dilakukan pengembangan dengan modul yang sudah dirancang. Perangkat lunak yang digunakan dalam pengamanan dokumen yaitu Visual Studio Code serta bahasa pemrograman PHP, *Database* yang digunakan MySQL dan perangkat keras yang dipakai adalah Intel Core I3-10110U, RAM 4GB, SSD 256GB.

2.5 Pengujian Sistem

Dalam fase ini akan dilaksanakan pengujian pada sistem yang sudah dibuat dengan tujuan untuk memastikan bahwa sudah sesuai dengan hasil analisa dan perancangan serta sistem-sistem yang dibuat sesuai yang diharapkan. Metode pengujian yang dipakai adalah *blackbox* yakni sebuah metode pengujian perangkat lunak dengan cara test fungsionalitas dari aplikasi.

2.6 Kesimpulan

Dalam fase ini dapat diambil kesimpulan dari penerapan *Advanced Encryption Standard* (AES 128) untuk pengamanan dokumen pada PT. Indotrade Jasama. Untuk membuktikan apakah penerapan *Advanced Encryption Standard* (AES 128) yang sudah dibuat bisa melakukan pengamanan dokumen dengan baik. Dan juga akan diberi masukan serta saran untuk melakukan perbaikan dan pengembangan pada aplikasi.

2.7 Spesifikasi *Database*

Berikut adalalah struktur-struktur dari spesifikasi *database* yang digunakan untuk membuat aplikasi ini. Tabel 1 merupakan spesifikasi dari *database file* dan Tabel 2 merupakan spesifikasi dari *database users*.

a. Tabel *file*
Nama tabel : *file*
Isi : File hasil enkripsi dan dekripsi
Primary key : id_file

Tabel 1. Spesifikasi Tabel *file*

Nama	Type data	Ukuran	Keterangan
id_file	int	11	Id *file*
username	varchar	15	*Username*
file_name_source	varchar	255	Nama *file* asli
file_name_finish	varchar	255	Nama hasil *file*
file_url	varchar	255	Url *file*
file_size	float	-	Ukuran *file*
password	varchar	16	*Password*
tgl_upload	timestamp	-	Tanggal upload
status	enum	(‘1’.’2’)	Enkripsi dan Dekripsi
keterangan	varchar	255	Keterangan
durasi_enkripsi	varchar	255	Waktu enkripsi

b. Tabel *users*
Nama tabel : *users*
Isi : Data *user*
Primary key : *username*

Tabel 2. Spesifikasi Tabel *users*

Nama	Type data	Ukuran	Keterangan
username	varchar	15	*Username*
password	varchar	100	*Password*
full_name	varchar	50	Nama *user*
job_title	varchar	50	Jabatan
join_date	timestamp	-	Tanggal gabung
last_activity	Timestamp	-	Aktivitas terakhir
status	enum	(‘1’.’2’)	Admin dan *user*

3. HASIL DAN PEMBAHASAN

3.1 Lingkungan Percobaan

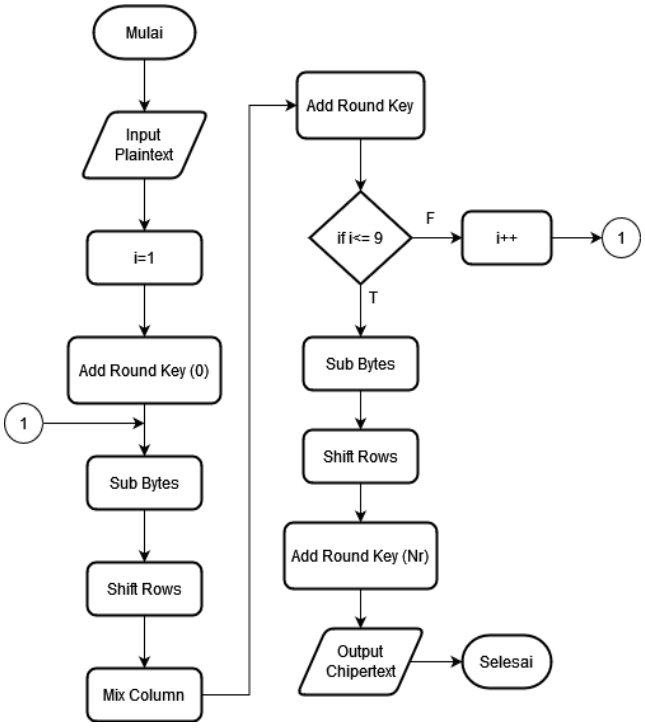
Dalam lingkungan percobaan akan diberikan spesifikasi yang diperlukan untuk membuat aplikasi pengamanan dokumen dengan Algoritme *Advanced Encryption Standard* (AES 128) pada PT. Indotrade Jasama agar dapat digunakan dengan lancar dan spesifikasi yang akan dipakai untuk mengembangkan aplikasi ini juga harus mendukung. Spesifikasi perangkat keras yang dipakai dalam pembuatan alat bantu aplikasi pengamanan dokumen adalah *processor* Core i3-10110U 2.59 Ghz, RAM 4GB, SSD 256GB. Spesifikasi perangkat lunak yang dipakai dalam pembuatan alat bantu aplikasi pengamanan dokumen adalah *Microsoft Windows* 11, MySQL, Visual Studio Code, XAMPP, Microsoft Edge.

3.2 *Flowchart*

Flowchart dipakai untuk menggambarkan alur dari sebuah program yang dibuat. Setiap alur tersebut digambarkan dalam bentuk diagram serta dihubungkan dengan garis. Berikut adalah *flowchart* dari aplikasi pengamanan dokumen.

3.2.1 *Flowchart* Proses Enkripsi

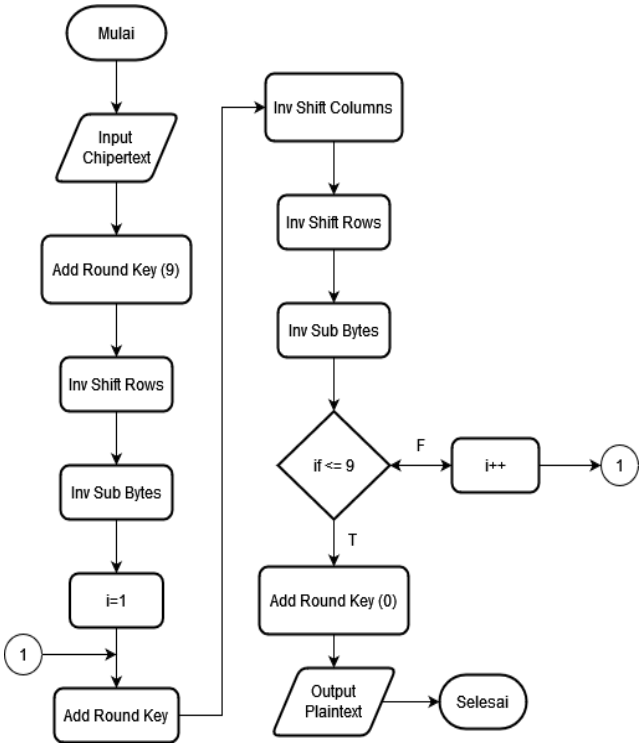
Gambar 4 adalah *flowchart* dari proses enkripsi *Advanced Encryption Standard* (AES). Menjelaskan alur proses yang terjadi pada algoritme AES-128 untuk mengenkripsi *Plaintext*.



Gambar 3. *Flowchart* Proses Enkripsi

3.2.2 *Flowchart* Proses Dekripsi

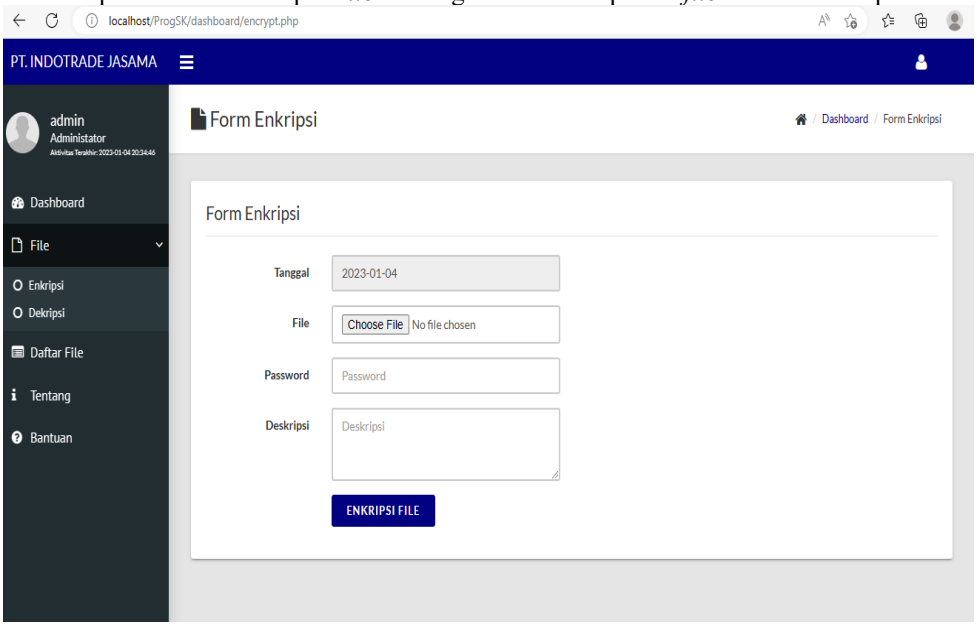
Gambar 5 adalah *flowchart* dari proses dekripsi *Advanced Encryption Standard* (AES). Menjelaskan alur proses yang terjadi pada algoritme AES-128 untuk mendekripsi *ciphertext*.



Gambar 4. *Flowchart* Proses Dekripsi

3.3 Tampilan Layar Halaman Enkripsi

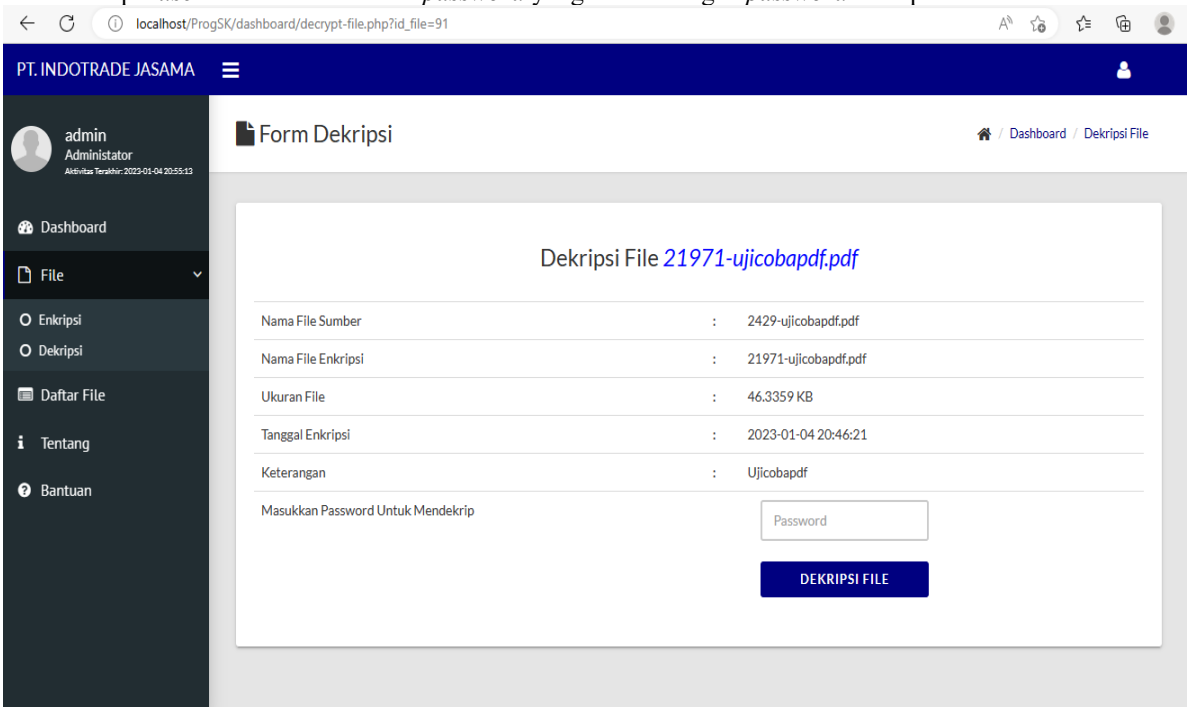
Gambar 5 menampilkan halaman enkripsi tempat untuk melakukan enkripsi *file*. Dalam halaman enkripsi terdapat *form* untuk memilih *file* yang ingin di enkripsi dan *form* untuk memberikan *password* dan deskripsi kepada *file* yang ingin di enkripsi. Tombol Enkripsi *File* berfungsi untuk memproses *file* untuk di enkripsi.



Gambar 5. Tampilan Layar Halaman Enkripsi

3.4 Tampilan Layar Halaman Dekripsi

Gambar 6 menampilkan halaman dekripsi tempat untuk mendekripsi file, ketika *user* mengklik tombol Dekripsi *File*, maka akan ditampilkan halaman *form* dekripsi. Pada halaman *form* dekripsi, untuk melakukan proses dekripsi *user* harus memasukkan *password* yang sesuai dengan *password* enkripsi.



Gambar 6. Tampilan Layar Halaman Dekripsi

3.5 Pengujian

Dalam fase ini dilakukan pengujian pada aplikasi yang sudah dibuat untuk mengetahui ukuran *file* hasil proses enkripsi serta dekripsi dari metode *Advanced Encryption Standard* (AES 128) apakah berbeda atau sama, lalu untuk mengetahui juga berapa lama waktu proses enkripsi serta dekripsi *file*. Berikut adalah hasil dari proses enkripsi serta dekripsi.

3.5.1 Hasil Pengujian

Berikut adalah hasil dari pengujian *file* yang telah dilakukan terhadap *file* yang berekstensi docx, xlsx, pptx, pdf, dan txt. Tabel 3 dan Tabel 4 adalah hasil dari pengujian enkripsi dan dekripsi.

Tabel 3. Tabel Hasil Pengujian Enkripsi

Nama *File*	*Password*	Ukuran File	Waktu Enkripsi (Detik)	Output File
1190-datatransaksiword.docx	qwerty	114 KB	2,918 Detik	10117-datatransaksiword.docx
46728-datatransaksiexcel.xlsx	qwerty	112 KB	2,927 Detik	99358-datatransaksiexcel.xlsx
34660-datatransaksipdf.pdf	12345678	130 KB	3,410 Detik	56552-datatransaksipdf.pdf
99814-datatransaksippt.pptx	12345678	138 KB	3.620 Detik	35769-datatransaksippt.pptx
20713-datatxt.txt	qwerty	0.213877 KB	0,011 Detik	10861-datatxt.txt

Tabel 4. Tabel Hasil Pengujian Dekripsi

Nama *File*	*Password*	Ukuran File	Waktu Dekripsi (Detik)	*Output File*
10117-datatransaksiword.docx	qwerty	114 KB	2,974 Detik	1190-datatransaksiword.docx
99358-datatransaksiexcel.xlsx	qwerty	112 KB	2,972 Detik	46728-datatransaksiexcel.xlsx
56552-datatransaksipdf.pdf	12345678	130 KB	3,382 Detik	34660-datatransaksipdf.pdf
35769-datatransaksippt.pptx	12345678	138 KB	3,575 Detik	99814-datatransaksippt.pptx
10861-datatxt.txt	qwerty	0,213867 KB	0,013 Detik	20713-datatxt.txt

4. KESIMPULAN

Berdasarkan analisis yang sudah dilaksanakan terhadap permasalahan dan pengujian dari berbagai analisa yang sudah dilakukan terhadap permasalahan dari aplikasi yang telah dikembangkan, bahwa aplikasi pengamanan dokumen menggunakan algoritma kriptografi dengan metode *Advanced Encryption Standard* (AES 128) dapat mengamankan dokumen PT. Indotrade Jasama sehingga dapat terhindar dari kebocoran data. Dan kecepatan waktu ketika proses enkripsi serta dekripsi tergantung besar/kecilnya ukuran *file* dokumen yang akan diproses.

DAFTAR PUSTAKA

[1] F. A. Nurbi and U. Budiyanto, "Penerapan Algoritme Rivest Code 4 Untuk Pengamanan Dokumen Di CV. Bintang Pratama Mandiri," *Semin. Nas. Mhs. ...*, no. September, pp. 182–191, 2022.
[2] R. Priambudi, J. Jayanta, and C. Nugrahaeni, "Penerapan Algoritma Kriptografi AES (Advanced Encryption Standard) dan Algoritma Kompresi RLE (Run Length Encoding) Untuk Pengamanan File Dokumen," *Format J. Ilm. Tek. Inform.*, vol. 11, no. 1, p. 11, 2022.
[3] F. Akbar and S. Waluyo, "Sistem Keamanan Database Menggunakan Algoritma Advanced Encryption Standard(AES-128) Studi Kasus : Red Avenue Indonesia," *Skanika*, vol. 1, no. 2, pp. 821–828, 2018.
[4] D. Pratomo, N. B. Nugroho, and R. I. Ginting, "Implementasi Kriptografi Untuk Mengamankan Data Penjualanan Di PT. Papparich Medan Menggunakan Metode AES 128," *J. Cyber Tech*, no. x, 2021.
[5] L. Sodikin and T. Hidayat, "Analisa Keamanan E-Commerce Menggunakan Metode Aes Algoritma," *Teknokom*, vol. 3, no. 2, pp. 8–13, 2020.
[6] Asriyanik, "Studi Terhadap Advanced Encryption Standard (Aes) Dan Algoritma Knapsack Dalam Pengamanan Data," 2017.
[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] G. Grehasen and S. Mulyati, "Pengamanan Database Pada Aplikasi Test Masuk Karyawan Baru Berbasis Web Menggunakan Algoritma Kriptografi AES-128 Dan RC4," *Budi Luhur Inf. Technol.*, vol. 14, no. 1, pp. 52–60, 2017.
[9] J. Prayudha, _ S., and _ I., "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 2, p. 119, 2019.
[10] M. Ziaurrahman, E. Utami, and F. W. Wibowo, "Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut," *J. Inform. dan Teknol. Inf.*, vol. 4, no. 1, p. (halaman 2), 2019.
[11] T. Erlangga and D. Kusumaningsi, "Implementasi Algoritma Advanced Encryption Standard-128 (AES-128) Untuk Pengamanan Database Berbasis Desktop Pada Icaltoys," *Skanika*, vol. 1, no. 2, pp. 565–569, 2018.
[12] S. Waluyo, Ferdiansyah, and firman, "Sistem Keamanan Management File Menggunakan Algoritma Advanced Encryption Standard (AES-128) Studi Kasus : Tabitha Indonesia," *Semin. Nas. Teknol. Inf. Univ. Ibn Khaldun Bogor*, p. 639, 2018.