

# PENERAPAN APLIKASI KRIPTOGRAFI DENGAN ALGORITMA ADVANCED ENCRYPTION STANDARD PADA PERUSAHAAN PT CAHAYA TELEVISI INDONESIA

Hogan Prilandi<sup>1\*</sup>, Dewi Kusumaningsih<sup>2</sup>

<sup>1,2</sup>Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: <sup>1\*</sup>1811500212@student.budiluhur.ac.id, <sup>2</sup>dewi.kusumaningsih@budiluhur.ac.id

(\* : corresponding author)

**Abstrak-**Pada era ini, kemajuan teknologi sangat pesat dan sangat mempengaruhi gaya hidup masyarakat, manusia tidak pernah lepas dari kebutuhan sebuah informasi, terutama era sekarang dapat berkomunikasi dan bertukar informasi secara cepat. Dalam perusahaan PT Cahaya Televisi Indonesia pada bagian *Accounting* data atau *file* yang sering dikerjakan atau dibuat seperti *file* invoice, faktur pajak, pengajuan pembayaran, rekap kas kecil, dikarenakan data atau *file* yang ada belum terjaga keamanannya yang di mana masih disimpan didalam folder komputer, flash disk yang tentu bisa saja diketahui pihak yang tidak bertanggung jawab. Maka penulis membuat aplikasi enkripsi dan dekripsi *file* ini untuk kebutuhan menjaga keamanan data atau *file* pada perusahaan ini yang di mana dalam penelitian ini menggunakan metode kriptografi salah satunya yang digunakan adalah Algoritma AES-128. Kriptografi AES-128 dengan algoritma ini keamanan *file* akan aman dan terjaga dan juga tidak dapat diketahui oleh pihak yang tidak memiliki akses. Jika ada sebuah software yang dapat melihat *database*-nya dari aplikasi enkripsi dan dekripsi *file* akan tetap aman *file* tersebut, karena *password* atau *key* juga dienkripsi. Hasil dari penelitiannya ini diterapkan dalam bentuk aplikasi berbasis web yang bernama *EnDe File* dapat memudahkan pihak dari perusahaan PT Cahaya Televisi Indonesia, terutama pada bagian *Accounting* untuk mengamankan data atau *file* yang bersifat rahasia, di mana *file* tersebut di enkripsi dan *file* yang sudah di enkripsi hanya bisa di akses kembali oleh pemilik pada bagian *Accounting*. Pada tahap pengujian di mana ada *file* dengan format *xlsx* dengan *size* 2,96 KB waktu enkripsi 02:41 menit dan dekripsi 02:39 menit untuk *file* lain seperti *xlsx* 268 KB waktu enkripsi 15.67 detik untuk enkripsi 14.56 detik dari beberapa *file* menjelaskan bahwa waktu dekripsi lebih cepat daripada waktu enkripsi.

**Kata Kunci:** kriptografi, AES-128, enkripsi *file*, dekripsi *file*

## APPLICATION OF CRYPTOGRAPHIC APPLICATIONS WITH ADVANCED ENCRYPTION STANDARD ALGORITHM IN PT CAHAYA TELEVISI INDONESIA

**Abstract-**In this era, technological progress is very rapid and greatly affects people's lifestyles, humans have never been separated from the need for information, especially the current era can communicate and exchange information quickly. In the company PT Cahaya Televisi Indonesia in the Accounting section data or files that are often done or made such as invoice files, tax invoices, payment submissions, petty cash recaps, because the existing data or files have not been kept safe which are still stored in the computer folder, flash disks which of course can be known to irresponsible parties. So the author made this file encryption and decryption application for the needs of maintaining the security of data or files in this company which in this study used cryptographic methods, one of which was used was the AES-128 Algorithm. AES-128 cryptography with this algorithm the security of files will be safe and secure and also cannot be known by parties who do not have access. If there is a software that can view its database from an encryption and decryption application the file will remain safe, because the password or key is also encrypted. The results of his research are applied in the form of a web-based application called *EnDe File*, which can make it easier for parties from the company PT Cahaya Televisi Indonesia, especially in the Accounting section to name confidential data or files, where the file is encrypted and the file that has been encrypted can only be accessed again by the owner in the Accounting section. In the test stage where there is a file with *xlsx* format with a size of 2.96 KB encryption time 02:41 minutes and decryption 02:39 minutes for other files such as *xlsx* 268 KB encryption time 15.67 seconds for encryption 14.56 seconds of some files explains that the decryption time is faster than the encryption time.

**Keywords:** cryptography, AES-128, file encryption, file decryption

## 1. PENDAHULUAN

Sejarah yang Panjang dari kriptografi. Penulisan rahasia 3000 tahun SM pada saat itu digunakan oleh bangsa Mesir. Mereka menggunakan *hieroglyphs* untuk menyembunyikan tulisan dari mereka yang tidak diharapkan. *Hieroglyphs* diturunkan dari bahasi Yunani *Hieroglyphica* yang berarti ukiran rahasia. *Hieroglyphs* berevolusi

menjadi *hieratic*, yaitu *stylized script* yang lebih mudah digunakan. Sekitar 400 SM, kriptografi militer digunakan oleh bangsa Spartan dalam bentuk sepotong *papyrus* atau perkamen dibungkus dengan sebuah batang kayu. Sistem ini disebut juga dengan *Scytale* [1], [2].

Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi (*cryptologi*). Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Perancang algoritma kriptografi disebut kriptografer [3], [4], [5]. Kriptografi Simetris Kunci untuk enkripsi dan dekripsi yang sama merupakan konsep dasar dari kriptografi simetris. Istilah lainnya adalah *private-key cryptography*, *secretkey cryptography*, atau *conventional cryptography*. Dalam kriptografi kunci simetris, karena penerima dan pengirim pesan telah terlebih dahulu berbagi kunci sebelum pesan dikirim. Keamanan dari sistem ini terletak pada kerahasiaan kuncinya [6].

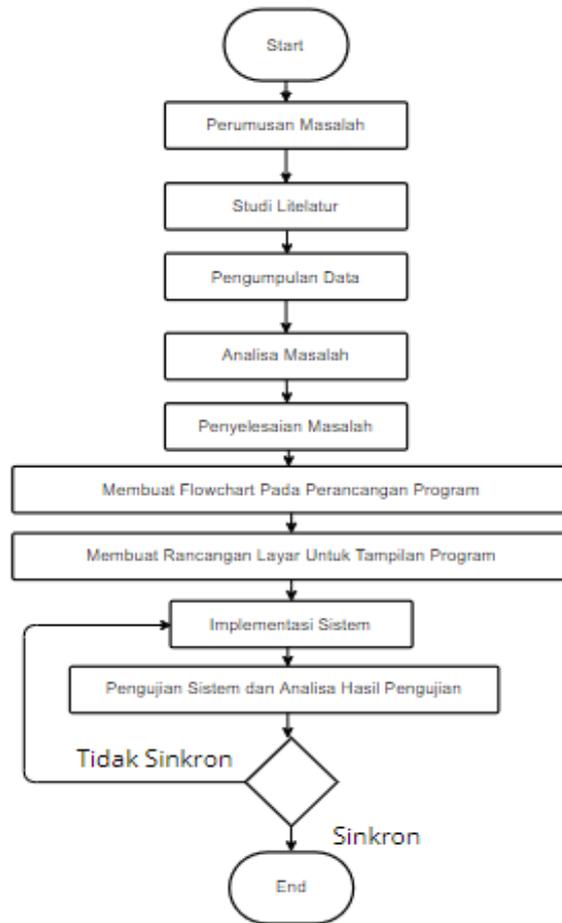
Kriptografi kunci asimetris atau kunci publik memiliki dua buah kunci yang berbeda pada proses enkripsi dan dekripsinya. Nama lainnya adalah kriptografi kunci publik (*public-key cryptography*). Kunci untuk enkripsi pada kriptografi asimetris ini tidak rahasia (diketahui oleh publik), sedangkan kunci untuk dekripsinya bersifat rahasia (kunci privat). Entitas pengirim akan mengenkripsi dengan menggunakan kunci publik, sedangkan entitas penerima mendekripsi pesan dengan menggunakan kunci privat [6]. Kriptografi memiliki tujuan selain menjaga keamanan data *Privacy / confidentiality* merupakan sebuah layanan yang bertujuan untuk menjaga pesan atau data tidak bisa dibaca oleh pihak yang tidak berhak. *Integrity* aspek ini menekankan bahwa setiap informasi tidak bisa diganti tanpa izin dari pemilik informasi. Informasi yang didapatkan harus sesuai dengan informasi yang dikirim, jika terdapat informasi atau data yang dikirim dengan diterima maka aspek *integrity* tersebut tidak dapat tercapai. *Authenticity* aspek ini berhubungan dengan suatu metode yang menyatakan bahwa informasi benar-benar asli dan orang yang dapat mengakses informasi adalah orang yang dimaksud. *Availability* aspek ini berhubungan adanya data dan informasi. Data dan informasi berbeda didalam sistem komputer yang dapat digunakan pihak yang berhak. *Access Control* aspek ini berhubungan dengan cara mengatur akses untuk informasi. Biasanya berhubungan dengan klasifikasi data, mekanisme autentikasi dan juga *privasi* [7], [10]

Pengertian *Advanced Encryption Standard AES* merupakan algoritma cryptographic yang digunakan untuk mengamankan sebuah data. AES merupakan simetri block cipher untuk menggantikan DES (*Data Encryption Standard*) [9], [11], [10]. Dalam perusahaan PT Cahaya Televisi Indonesia ini data atau *file* yang sering dikerjakan atau dibuat seperti *file invoice*, faktur pajak, pengajuan pembayaran, rekap kas kecil semua ini dilakukan oleh bagian *Accounting* untuk kebutuhan perusahaan sendiri atau rekapan stock digunakan untuk rekonsiliasi dengan vendor, dikarenakan data atau *file* yang ada belum terjaga keamanannya yang di mana masih disimpan didalam *folder* komputer, *flash disk* yang tentu bisa saja diketahui pihak yang tidak bertanggung jawab, maka penulis membuat aplikasi enkripsi dan dekripsi *file* ini untuk kebutuhan menjaga keamanan data atau *file* pada perusahaan ini yang di mana dalam penelitian ini menggunakan metode kriptografi salah satunya yang digunakan adalah Algoritma *Advanced Encryption Standard (AES-128)*.

Tujuan dari penelitian ini yaitu membuat website enkripsi dan dekripsi file dengan metode *Advanced Encryption Standard (AES-128)*, Mengimplementasikan algoritma kriptografi *AES-128* untuk enkripsi dan dekripsi file dengan berbasis website untuk perusahaan PT Cahaya Televisi Indonesia, Website ini dapat membuat file yang rahasia pada perusahaan bisa di simpan dengan aman. Manfaat dari penulisan penelitian ini adalah dapat mengamankan file dan isi yang penting agar tidak bisa di salahgunakan dan terjaga kerahasiaannya pada PT Cahaya Televisi Indonesia.

## 2. METODE PENELITIAN

Dalam metodologi penelitian digunakan sebagai panduan dalam pelaksanaan penelitian supaya penelitian ini tidak salah jalur dan tujuan yang telah dilakukan sebelumnya. Gambar 1 menyajikan metodologi penelitian.



Gambar 1. Metodologi Penelitian

## 2.1 Studi Literatur

Tahapan ini dilakukan terhadap beberapa bentuk yang digunakan dalam penelitian ini. Studi dilakukan berupa jurnal, karya tulis ilmiah, diktat kuliah dan teks, yang sesuai dengan masalah yang sedang dibahas yaitu tentang kriptografi *Advanced Encryption Standar* (AES) 128, sehingga penulis mendapatkan referensi untuk mengatasi masalah yang diteliti. Sedangkan mikrokontroler digunakan sebagai komponen utama yang sudah ditentukan dan dirancang sedemikian rupa.

## 2.2 Studi Lapangan

Tahapan ini dilakukan pada studi lapangan di PT Cahaya Televisi Indonesia untuk mengamankan *file* terutama pada bagian Accounting untuk mengetahui permasalahan yang terjadi.

## 2.3 Pengumpulan Data

Dalam penelitian ini, penulis menggunakan beberapa metode untuk mengumpulkan data, informasi, dan materi yang relevan dengan permasalahan yang dibahas pada PT. Cahaya Televisi Indonesia yaitu: Wawancara (*Interview*), Pengamatan (*Observation*), Analisa Dokumen, Studi Kepustakaan (*Library Reseach*).

## 2.4 Analisa Masalah

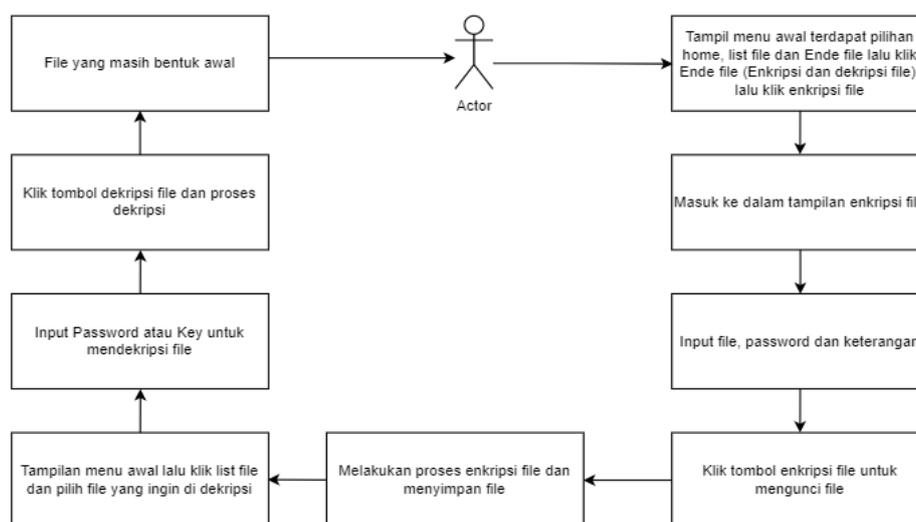
*File* memiliki fungsi yang sangat penting, ada yang berfungsi sebagai tempat untuk menyimpan berbagai hal dari perusahaan, Pendidikan, kepentingan sendiri dll. Oleh karena itu penulis akan mencoba membuat sebuah aplikasi berbasis *web*, untuk menjaga keamanan *file* di mana *file* tersebut seperti *file invoice*, faktur pajak, pengajuan pembayaran, rekap kas kecil semua ini dilakukan rekap stock digunakan untuk rekonsiliasi dengan vendor yang dilakukan oleh bagian Accounting PT Cahaya Televisi Indonesia.

## 2.5 Strategi Penyelesaian Masalah

Dari masalah yang di jelaskan di atas, dibuatlah sebuah aplikasi enkripsi dan dekripsi *file* berbasis *web* yang dapat di jalankan di *browser* dan tentu dapat mengamankan isi dari *file* tersebut menjadi *file* yang tidak bisa di lihat oleh pihak yang tidak memiliki tanggung jawab dan tidak bisa mengubah isinya. dengan begitu aplikasi enkripsi dan dekripsi *file* diharapkan dapat digunakan untuk sebuah solusi dari setiap permasalahan tersebut.

## 2.6 Perancangan Skema Aplikasi

Pada tahap ini berdasarkan analisa yang dilakukan maka untuk mengoptimalkan aplikasi yang akan dibuat, maka untuk melakukan sesuatu proses enkripsi *file*, yang dilakukan pengguna (*user*) hanya menginput *password* atau *key* dan setelah itu *file* sudah di enkripsi pada AES-128. Gambar 2 menyajikan skema proses dari enkripsi dan dekripsi *file*:



Gambar 2. Skema Proses Enkripsi Dan Dekripsi File

## 2.7 Implementasi

Tahapan ini dilakukan pembuatan dengan modul yang sudah dirancang. Dalam hal ini perangkat yang digunakan yaitu:

- Software* yang digunakan yaitu dalam mengamankan *file Accounting* dengan menggunakan bahasa pemrograman PHP dan untuk database MySQL.
- Hardware* yang digunakan Processor Intel(R) Celeron(R) CPU N2840 @ 2.16GHz, RAM 4 GB, Harddisk 500 GB.

## 2.8 Pengujian Sistem

Tahapan ini dilakukan bertujuan untuk menjamin dari sistem berjalan sesuai dengan proses analisa dan perancangan yang sebagaimana mestinya sistem ini sesuai yang diharapkan. Dalam proses pengujian ini didapatkan bahwa sistem sesuai tujuan awal dan dapat digunakan dengan baik sesuai dengan fungsi dari sistem yang diinginkan.

## 2.9 Kesimpulan

Tahapan terakhir ini di mana disimpulkan bahwa penerapan metode kriptografi *Advanced Encryption Standar (AES) 128*, berfungsi dengan baik dan dapat mengamankan *file* pada bagian *Accounting* pada PT Cahaya Televisi Indonesia dengan aman dan pada tahapan ini ada saran untuk perkembangan pada sistem ini.

## 2.10 Rancangan Layar Website Enkripsi dan Dekripsi File

Pada rancangan layar bagian yang penting dalam pembuatan program, maka dari itu tujuan dari rancangan layar ini yaitu yang dapat mudah di mengerti oleh *user*, di mana *user* bisa cepat paham dalam menggunakannya dan *user* tidak mengalami kesulitan. Gambar 3 menyajikan rancangan layar dari *Admin*.



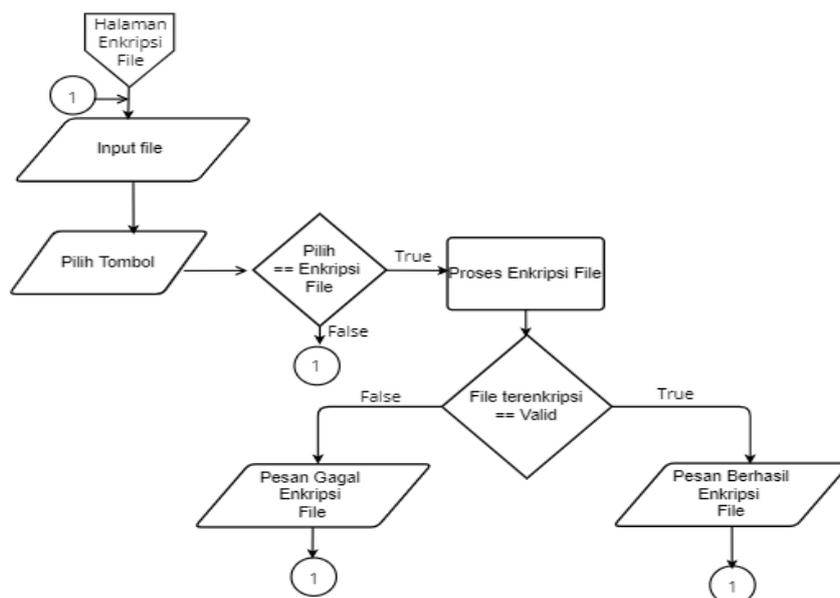
Gambar 3. Rancangan Layar Admin

### 3. HASIL DAN PEMBAHASAN

Berdasarkan dari metode pada bab sebelumnya, tentang algoritma kriptografi AES 128 bit untuk mengamankan *file*. Pada Implementasi metode ini akan dijelaskan *flowchart*, algoritma, proses dan hasil dari enkripsi dan dekripsi *file* pada aplikasi EnDe File.

#### 3.1 Flowchart Form Enkripsi File

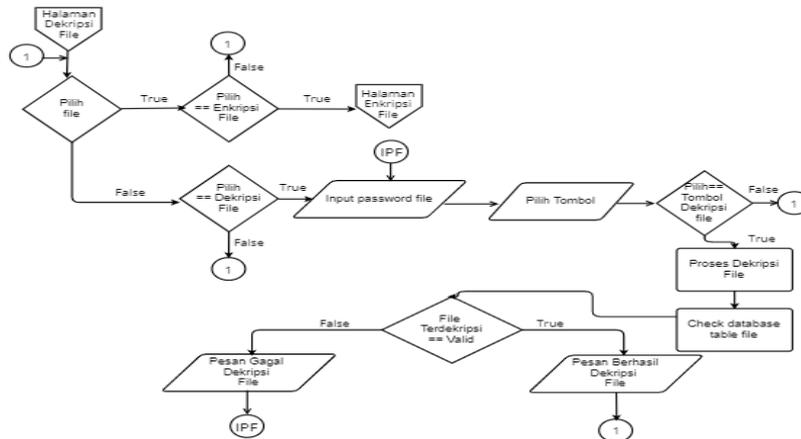
Alur proses ini dijelaskan bahwa untuk melakukan enkripsi *file*, masuk ke dalam halaman enkripsi *file*, input *file* yang akan di enkripsi, serta password dan keterangan, terdapat tombol untuk enkripsi *file* setelah tombol di pilih maka proses enkripsi *file* dengan aes 128 akan berjalan dari *subbytes*, *shiftrows*, *mixcolumns* dan *addroundkey*, setelah itu jika enkripsi *file* gagal akan tampil pesan gagal enkripsi lalu kembali ke halaman enkripsi *file*, lalu ketika berhasil enkripsi *file* akan kembali ke halaman enkripsi *file*. Gambar 4 menyajikan *Flowchart* Proses Form Enkripsi File.



Gambar 4. Flowchart Proses Enkripsi File

### 3.2 Flowchart Form Dekripsi File

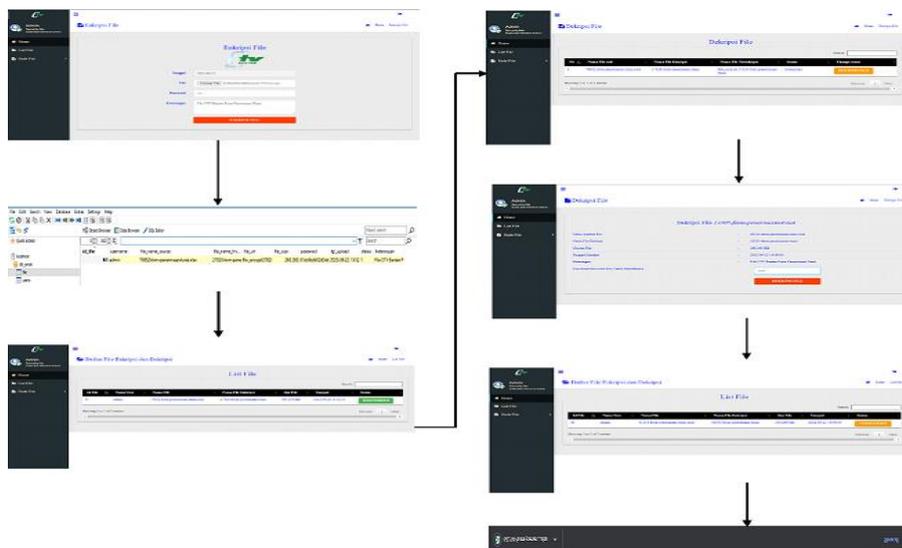
Alur proses ini dijelaskan bahwa untuk melakukan dekripsi *file* terdapat tabel yang di mana setiap *file* memiliki status yang berbeda yaitu enkripsi *file* dan dekripsi *file*, jika memilih enkripsi *file* maka akan tampil halaman enkripsi *file*, sedangkan pilih dekripsi *file* maka akan berada di tampilan untuk *input password*, lalu setelah input password terdapat tombol untuk dekripsi *file*, maka akan berjalan proses dekripsi *file* AES 128 proses yaitu *invshiftrows*, *invsubbytes*, *invmixcolumns* dan *AddRoundKey*, jika gagal dekripsi *file* maka akan tampil pesan gagal dekripsi *file* dan akan kembali ke tampilan untuk *input password*, sedangkan jika berhasil tampil pesan berhasil dekripsi *file* setelah itu kembali ke halaman dekripsi *file*. Gambar 5 menyajikan *Flowchart* Proses *Form Dekripsi File*.



Gambar 5. *Flowchart* Proses Enkripsi *File*

### 3.3 Proses Enkripsi Dan Dekripsi File

Pada proses ini Admin akan menginput *file* yang akan di enkripsi, lalu input password dan keterangan, setelah itu klik tombol “ENKRIPSI FILE”, di mana *file* yang berhasil di enkripsi akan tampil di database. Pada hasil enkripsi *file* juga dapat di lihat pada list *file* yang di mana terdapat status yang membutuhkan bahwa *file* telah terenkripsi. Proses ini Admin akan mendekripsi *file* yang telah terenkripsi, lalu tahapan yang dilakukan klik tombol “DEKRIPSI FILE”, pada tahapan proses dekripsi *file* dilakukan penginputan password lalu mengklik tombol “DEKRIPSI FILE”, *file* telah berhasil di dekripsi dan merubah status *file* menjadi terdekripsi pada list *file*. Pada proses terakhir ini di mana *file* yang sudah terdekripsi, ketika mengklik tombol “TERDEKRIPSI”, otomatis akan ter-download kecuali pada format *file* mp4, png dan jpg yang terbuka lalu bisa di download. Gambar 6 menyajikan proses dari pengujian mengenkripsi dan mendekripsi *file*.



Gambar 6. Proses Enkripsi *File* Dan Dekripsi *File*

### 3.4 Hasil Pengujian Enkripsi Dan Dekripsi File

Pada tahap pengujian di enkripsi *file* ini sesuai dengan teknik dari kriptografi menggunakan metode AES-128, tujuan dari pengujian enkripsi *file* ini yaitu untuk mengetahui apakah *file* yang di enkripsi berhasil terenkripsi atau tidak terenkripsi, jenis *file*-nya berbeda-beda dari ppt, word, pdf, mp4, excel, mp3, rar, jpg, png yang di mana *file* yang berasal dari perusahaan ctv banten hanya terdapat *file* excel, untuk tabel *file* terenkripsi terbagi menjadi dua karena kolom satu merupakan bentuk *file* yang sudah di enkripsi dan untuk kolom dua terdapat *file* yang sudah di enkripsi dan menambahkan nama *file* “file\_encrypt” dan satuan durasi enkripsi *file* menit dan detik. *Table 1* menyajikan dari pengujian enkripsi *file* di EnDe *File*.

**Tabel 1.** *File* yang sudah di enkripsi

Judul File Asli	Judul File Terenkripsi AES-128	File Size	Durasi Enkripsi File	Size Hasil Enkripsi	Status	
14184-40717-test-kriptografi.pptx	50576-40717-test-kriptografi	file_encrypt/50576-40717-test-kriptografi	32,5 KB	00:02.46	32,5 KB	Terenkripsi
60102-test-kriptografi-aplikasi-enkripsi-dan-dekripsi-file.docx	83562-test-kriptografi-aplikasi-enkripsi-dan-dekripsi-file	file_encrypt/83562-test-kriptografi-aplikasi-enkripsi-dan-dekripsi-file	11,6 KB	00:01.64	11,6 KB	Terenkripsi
39648-799-1501-1-pb.pdf	4244-799-1501-1-pb	file_encrypt/4244-799-1501-1-pb	4,77 MB	04:21.23	4,77 MB	Terenkripsi
54530-station-id-ctv-banten-(cahaya-televisi-banten).mp4	90607-station-id-ctv-banten-(cahaya-televisi-banten)-(2002)	file_encrypt/90607-station-id-ctv-banten-(cahaya-televisi-banten)-(2002)	2,14 MB	02:10.04	2,14 MB	Terenkripsi
91988-station-id-ctv-banten-(cahaya-televisi-banten).mp4	70081-station-id-ctv-banten-(cahaya-televisi-banten)	file_encrypt/70081-station-id-ctv-banten-(cahaya-televisi-banten)	991 KB	00:53.23	2,14 MB	Terenkripsi
99040-form-penerimaan-tunai.xlsx	89725-form-penerimaan-tunai	file_encrypt/89725-form-penerimaan-tunai	268 KB	00:15.67	268 KB	Terenkripsi
56736-pr-cp-2021.xls	45512-pr-cp-2021	file_encrypt/45512-pr-cp-2021	2,96 KB	02:41.58	2,96 KB	Terenkripsi
47506-040-cshop_1.jpg	69274-040-cshop_1	file_encrypt/69274-040-cshop_1	101 KB	00:05.87	101 KB	Terenkripsi
21130-8617-cshop-des21.pdf	80821-8617-cshop-des21	file_encrypt/80821-8617-cshop-des21	46,0 KB	00:02.96	46,0 KB	Terenkripsi
54410-woo_aha_text_message.mp3	3571-woo_aha_text_message	file_encrypt/3571-woo_aha_text_message	35,9 KB	00:02.50	35,9 KB	Terenkripsi
28922-file.rar	19058-file	file_encrypt/19058-file	24,6 KB	00:02.40	24,6 KB	Terenkripsi
24161-laptop-asus-x451ma.jpg	35234-laptop-asus-x451ma	file_encrypt/35234-laptop-asus-x451ma	6,93 KB	00:01.72	6,93 KB	Terenkripsi
89752-aes-addroundkey.png	10260-aes-addroundkey	file_encrypt/10260-aes-addroundkey	16,0 KB	00:02.96	16,0 KB	Terenkripsi

Pada proses pengujian dari enkripsi *file* berhasil dilakukan dan setelah pengujian ini masuk ke dalam pengujian dekripsi *file* yaitu di mana membuka *file* yang terkunci atau yang terdekripsi. *Table 2* menyajikan *file* yang sudah di dekripsi.

**Tabel 2.** File yang sudah di dekripsi

Judul Asli File	File Size	Durasi Dekripsi File	Size Hasil Dekripsi	Status
14184-40717-test-kriptografi.pptx	32,5 KB	00:02.25	32,5 KB	Terdekripsi
60102-test-kriptografi-aplikasi-enkripsi-dan-dekripsi-file.docx	11,6 KB	00.01.06	11,6 KB	Terdekripsi
39648-799-1501-1-pb.pdf	4,77 MB	00.02.15	4,77 MB	Terdekripsi
54530-station-id-ctv-banten-(cahaya-televisi-banten).mp4	2,14 MB	01:59.41	2,14 MB	Terdekripsi
91988-station-id-ctv-banten-(cahaya-televisi-banten).mp4	991 KB	00:53.05	991 KB	Terdekripsi
99040-form-penerimaan-tunai.xlsx	268 KB	00:14.56	268 KB	Terdekripsi
56736-pr-cp-2021.xls	2,96 KB	02:39.76	2,96 KB	Terdekripsi
47506-040-cshop_1.jpg	101 KB	00:05.87	101 KB	Terdekripsi
21130-8617-cshop-des21.pdf	46,0 KB	00:02.92	46,0 KB	Terdekripsi
54410-woo_aha_text_message.mp3	35,9 KB	00:02.32	35,9 KB	Terdekripsi
28922-file.rar	24,6 KB	00:00.61	24,6 KB	Terdekripsi
24161-laptop-asus-x451ma.jpg	6,93 KB	00:02.93	6,93 KB	Terdekripsi
89752-aes-addroundkey.png	16,0 KB	00:01.56	16,0 KB	Terdekripsi

#### 4. KESIMPULAN

Pada hasil perancangan, maka Sistem Keamanan data atau *file* menjadi solusi untuk mengamankan data atau *file* pada bagian Accounting seperti invoice, faktur pajak, pengajuan pembayaran, rekap kas kecil. Pada pada hasil implementasi, sistem yang dibangun dapat membantu perusahaan PT Cahaya Televisi Indonesia instansi dalam mengamankan data atau *file* menggunakan algoritma advanced encryption standard. Pada tahap pengujian di mana ada *file* dengan format xlsx dengan size 2,96 KB waktu enkripsi 02:41 menit dan dekripsi 02.39 menit untuk *file* lain seperti xlsx 268 KB waktu enkripsi 15.67 detik untuk dekripsi 14.56 detik dari beberapa *file* menjelaskan bahwa waktu dekripsi lebih cepat daripada waktu enkripsi. Diharapkan aplikasi ini dapat dikembangkan tidak hanya di platform website, tetapi dapat dikembangkan di platform Android atau IOS dan diharapkan agar penelitian selanjutnya dapat menyempurnakan dan mengembangkan aplikasi ini dari sisi tampilan agar terlihat menarik.

#### DAFTAR PUSTAKA

- [1] E. S. Han and A. goleman, daniel; boyatzis, Richard; Mckee, "Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah," *J. Chem. Inf. Model.*, vol. 53, no. 9, p. 2, 2019.
- [2] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Jurnal Pendidikan Sains dan Komputer Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard ( AES ) Jurnal Pendidikan Sains dan Komputer," vol. 2, no. 1, pp. 163–171, 2022.
- [3] 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, doi: 10.15408/aism.v3i2.14722.
- [4] 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," *J. Comput. Syst. Informatics*, vol. 1, no. 2, pp. 54–60, 2020.
- [5] S. Benyamin, E. Ahadi, D. P. S. Manrung, and I. Gunawan, "Pengamanan Pesan Teks Menggunakan Kriptografi Algoritma Vigenere Chiper Dari Serangan Eavesdropping," *J. Tek. Inform. Kaputama*, vol. 4, no. 1, pp. 35–40, 2020.
- [6] R. Firmansyah, "Implementasi Keamanan Pesan Teks Menggunakan Kriptografi Algoritma Rsa Dengan Metode Waterfall Berbasis Java," *Joutica*, vol. 4, no. 1, p. 174, 2019, doi: 10.30736/jti.v4i1.265.
- [7] I. Dian Widyawan, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite," vol. 4, no. 1, pp. 15–22, 2021.
- [8] D. Hulu, B. Nadeak, and S. Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSUD Imelda Medan," *KOMIK (Konferensi ...)*, vol. 4, pp. 78–86, 2020, doi:

- 10.30865/komik.v4i1.2590.
- [9] R. Andriyanto, K. Khairijal, and D. Satria, “Penerapan Kriptografi AES Class Untuk Pengamanan URL WEBSITE Dari Serangan SQL INJECTION,” *J. Unitek*, vol. 13, no. 1, pp. 34–48, 2020, doi: 10.52072/unitek.v13i1.153.
- [10] K. Zalukhu, Y. Syahra, and T. Syahputra, “Implementasi Sistem Keamanan Database Data Pelanggaran Hukum Disiplin Prajurit Menggunakan Algoritma Advanced Encryption Standard 128 Bit Pada Pengadilan Militer I-02 Medan,” *J-SISKO TECH (Jurnal Teknol. Sist. Inf. dan Sist. Komput. TGD)*, vol. 3, no. 2, p. 138, 2020, doi: 10.53513/jsk.v3i2.2419.