

IMPLEMENTASI PENGAMANAN DOKUMEN MENGUNAKAN KRIPTOGRAFI DENGAN ADVANCED ENCRYPTION STANDARD 256 PADA CELEBES KONTRUKSINDO PT.

Hoerul Fiji Ardiansyah^{1*}, Noni Juliasari²

^{1,2}Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta,
Indonesia Email: ^{1*}1911500278@student.budiluhur.ac.id, ²noni.juliasari@budiluhur.ac.id

(* : corresponding author)

Abstrak- Perkembangan teknologi komputer yang semakin cepat membuat pertukaran informasi dan data sangat mudah dengan pesatnya teknologi memungkinkan manusia untuk berkomunikasi, bertukar informasi, atau bertukar data keamanan dan kerahasiaan data atau dokumen selalu menjadi masalah dalam suatu dunia bisnis maupun Lembaga lainnya. Dalam hal ini perusahaan Celebes Kontruksindo PT. Pada data file yang sering dikerjakan atau dibuat seperti data BOQ (Bill Of Quantity), data tower area Banten dan Jakarta,. Adapun Permasalahan yang dihadapi yaitu data atau file yang belum terjaga keamanannya yang dimana masih disimpan dalam folder komputer, flashdisk yang tentu bisa saja diketahui pihak yang tidak bertanggung jawab. Maka sebagai upaya dari pengamanan data diperlukan perlindungan data menggunakan teknik kriptografi dengan proses enkripsi dan dekripsi didalamnya. Enkripsi merupakan suatu proses yang dilakukan untuk mengubah suatu informasi menjadi serangkaian kode-kode yang rumit (chipertext) yang sulit di artikan. Dekripsi merupakan proses pengembalian informasi yang sudah dienkripsi menjadi kode-kode kemudian di ubah kembali menjadi sebuah informasi (plaintext). Salah satu algoritme kriptografi adalah Advanced Encryption Standard (AES-256), dimana algoritme ini memiliki 14 blok putaran yang cukup rumit sehingga dapat membantu proses pengamanan data di Celebes Kontruksindo PT. dari uraian di atas maka melakukan penelitian terhadap hal-hal tersebut yang akan di tuangkan dalam tulisan yang berjudul "Implementasi Pengamanan Dokumen Menggunakan Kriptografi Dengan Advanced Encryption Standard 256 pada Celebes Kontruksindo PT

Kata Kunci: Kriptografi, Advanced Encryption Standard 256, Enkripsi file, Dekripsi file

IMPLEMENTATION OF DOCUMENT SECURITY USING CRYPTOGRAPHY WITH ADVANCED ENCRYPTION STANDARD 256 AT CELEBES KONTRUKSINDO PT.

Abstract- The rapid development of computer technology makes the exchange of information and data very easy with the rapid pace of technology enabling humans to communicate, exchange information, or exchange data. Security and confidentiality of data or documents has always been a problem in a business world or other institutions. In this case, the company Celebes Kontruksindo PT. In data files that are often worked on or created, such as BOQ (Bill Of Quantity) data, Banten and Jakarta area tower data. The problems faced are data or files that have not been secured which are still stored in computer folders, flash drives which of course could be known to irresponsible parties. So as an effort to secure data, it is necessary to protect data using cryptographic techniques with encryption and decryption processes in it. Encryption is a process that is carried out to convert information into a series of complex codes (ciphertext) that are difficult to interpret. Decryption is the process of returning encrypted information into codes and then converting them back into information (plaintext). One of the cryptographic algorithms is the Advanced Encryption Standard (AES-256), where this algorithm has 14 round blocks that are quite complicated so that they can help process data security at Celebes Kontruksindo PT. from the description above, the writer conducted research on these matters which will be written in an article entitled "Implementation of Document Security Using Cryptography with Advanced Encryption Standard 256 at Celebes Kontruksindo PT

Keywords: Cryptography, Advanced Encryption Standard 256, File encryption, File decryption

1. PENDAHULUAN

Pesatnya perkembangan teknologi komputer pribadi memfasilitasi pertukaran informasi dan data. dalam hal ini juga berdampak pada meningkatnya kejahatan di dunia telekomunikasi. Teknologi informasi telah digunakan dalam kehidupan sehari-hari. Hampir semua informasi manajemen berbentuk data digital. Perkembangan teknologi tidak selalu memberikan dampak yang positif dan menguntungkan, salah satu hal yang dikhawatirkan

adalah penyalahgunaan data dan informasi. Oleh karena itu perlu dilakukan perlindungan terhadap informasi dengan berbagai cara. Keamanan dan kerahasiaan data selalu menjadi masalah dalam suatu bisnis atau lembaga lainnya. Namun ada saja oknum yang berusaha untuk mengetahui suatu data atau dokumen dengan cara yang tidak semestinya bahkan bermaksud merubah. Oleh karena itu pentingnya pengamanan data atau dokumen maka di butuhkan suatu cara agar data yang dimiliki tetap terjaga kerahasiaannya, salah satu dengan menjadikan isi informasi dari suatu data penting atau dokumen menjadi suatu kode yang tidak di mengerti siapapun.

Pada penelitian yang dilakukan oleh Yudi (2018) dijelaskan bahwa Enkripsi Data Menggunakan Advanced Encryption Standard 256 sangat mudah untuk dimengerti dan digunakan oleh pengguna serta dapat membantu mengamankan data atau informasi yang sebelumnya dapat dilihat oleh umum atau orang lain. Aplikasi enkripsi ini memiliki tingkat kesulitan enkripsi 32 bit. Sementara itu menurut Nizirwan (2018), pada Advanced Encryption Standard 256, Hasil proses perancangan dan pengujian data (eks maupun gambar) diperoleh tidak mengalami perubahan yang signifikan, Akan tetapi enkripsi/dekripsi pada metode algoritma RSA jauh lebih lambat dibandingkan kinerja time-processing metode algoritma AES. Selain itu Angga (2018) menyatakan bahwa AES, Rijndel memiliki keunggulan karena memiliki daya memori dan kecepatan komputasi dalam pengoprasian. Pengoprasian yang tidak memakan memori yang terlalu besar ini banyak di minati pasar karena kebutuhan efisiensi waktu yang relatif cepat identitas dan data lainnya tidak mudah di baca oleh orang lain yang tidak berwenang.

Pada penelitian yang dilakukan oleh Magdalena (2019), Sistem Merkle Hellman menggunakan 2 kunci asinkron, satu kunci melakukan enkripsi dan satu kunci melakukan dekripsi. Jadi cara kerja sistem ini adalah pesan diubah menjadi bilangan biner yang dikalikan dengan menggunakan kunci publik, kemudian karena bertambahnya kombinasi yang dikirim ke messenger, maka penerima pesan menggunakan kunci rahasia untuk menemukan kombinasi target menggunakan algoritma kombinasi, penerima menerima nilai pesan yang biasanya berupa bilangan biner [0,1]. Untuk mendapatkan informasi aslinya, tujuh angka ini diubah menjadi huruf aslinya. Kelebihan dari algoritma ini adalah sistem pembagian kunci pada media yang tidak aman seperti internet tidak memerlukan enkripsi, karena kunci yang dibagikan berarti kunci publik karena kunci ini hilang atau diketahui oleh orang lain yang tidak berhak menyimpan rahasia informasi yang dienkripsi tersebut. Pada titik ini, kunci privat masih disimpan atau didistribusikan. Keuntungan lainnya adalah efisiensi jumlah kunci publik: jika ada n pengguna, satu kunci publik sudah cukup. jadi untuk sejumlah besar pengguna ini efektif.

Celebes Kontruksindo PT. adalah perusahaan yang bergerak di bidang industri media konstruksi dan manajemen, berlokasi di Jati padang Rt.12/Rw05, Ps. Minggu, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12540. Dengan itu, Celebes Kontruksindo PT. Memiliki data yang dimana data tersebut masih di simpan secara manual rentan akan terjadinya pencurian data oleh karena itu keselamatan menjadi salah satu hal terpenting di dalamnya. Maka diperlukan perlindungan data dengan menggunakan teknik kriptografi. Kriptografi adalah suatu metode yang sering kali digunakan untuk melindungi berbagai macam data. Adapun proses di dalamnya adalah enkripsi dimana informasi yang ada dibuat sedemikian rupa agar tidak dapat dibaca atau di ketahui oleh orang lain yang tidak di inginkan. Menanggapi permasalahan yang ditemukan, maka disarankan untuk pembuatan sistem aplikasi berbasis web dengan kriptografi Advanced Encryption Standard 256 untuk melindungi data isi dokumen di Celebes Kontruksindo PT. seperti solusi basis data

Adapun rumusan masalah berdasarkan latar belakang yang telah dibahas yaitu bagaimana merancang sistem pengamanan dokumen file yang dapat dilakukan secara komputerisasi dan Bagaimana mekanisme sistem pengamanan yang akan di rancang menggunakan metode kriptografi Hindari AES-256? Sehingga tujuan dari penulisan ini yaitu untuk merancang suatu sistem untuk mengamankan data Tower yang dimiliki Celebes Kontruksindo PT, menyimpan data dalam proses enkripsi dan dekripsi file adalah database Xampp, serta mengimplementasikan algoritme kriptografi AES guna mengamankan data BOQ (Bill Of Quantity), data tower area Banten dan Jakarta dari ancaman pihak yang tidak berwenang.

2. METODE PENELITIAN

2.1 Definisi Kriptografi

Kriptografi artinya seni buat menjaga pesan agar terjaga pada hal keamanan serta kerahasiaannya. Para pakar kriptografi atau pengguna dikenal dengan kata cryptographers. algoritma kriptografi umumnya dianggap menggunakan chipper. Chipper ialah sebuah persamaan matematika yang digunakan buat proses melakukan enkripsi serta pelukisan. Biasa persamaan matematika tersebut mempunyai hubungan matematis yang erat. (Dwi Saputra & Syafrullah, 2022)

Secara umum teknik pengamanan isu yang dilakukan kriptografi dengan cara diolahnya berita awal (plaintext) dengan suatu kunci yaitu metode enkripsi sehingga membuat suatu informasi bari (chiphertext) yang

sama sekali tidak dapat dibaca secara pribadi. Chipertext tersebut bisa dikembali menjadi informasi awal (plaintext) menggunakan proses deskripsi (Widyawan and Imelda 2021)

2.2 Tujuan Kriptografi

Dari paparan awal dapat dirangkumkan bahwa kriptografi bertujuan untuk memberi layanan keamanan. Yang dinamakan aspek-aspek keamanan:(Pabokory et al. 2019)

- Kerahasiaan (confidentiality) adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
- Integritas data (data integrity) adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman.
- Otentikasi (authentication) adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (user authentication).
- Non-repudiation adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan

2.3 Teknik Dasar Kriptografi

Kriptografi memiliki teknik dasar yaitu sebagai berikut:

- Substitusi
Langkah pertama adalah membuat suatu table substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki table yang sama untuk keperluan deskripsi.
- Blocking
Sistem ini diberi sanksi teks dan jelas dalam anti-penutupan banyak karakter yang menafsirkan dirinya. Penggunaan nomor kolom memilih untuk menulis. Jumlah lajur atau kolom menjadu kunci bagi kriptografi menggunakan teknik ini. Plaintext dituliskan secara vertical kebawah beruntutan pada lajur, serta dilanjutkan di kolom berikutnya hingga seluruhnya tertulis. Ciphertext berarti hasil membaca teks biasa secara interaktif menggunakan blok.(Tullah, Dzulhaq, and Setiawan 2019)
- Permutasi
Salah satu batasan yang paling penting adalah bahwa yang diuji atau seroong dianggap sebagai proses. Tren ini dirangsang atau digunakan dalam hukum yang salah, pola yang bertentangan dengan proses mekanis. Dan sistem palem, karakter diatur tetapi tidak ada karakter. Dalam hal kegiatan, identitas karakter sudah diperbaiki, tetapi situasinya ada di Rambang. Sebelum replikasi dilakukan, teks terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama.(Simanjuntak, Pasaribu, and Rahmadilla 2019)
- Ekspansi
Suatu metode sederhana buat mengacak pesan artinya dengan memelerakan pesan itu dengan hukum eksklusif. salah satu contoh penggunaan teknik ini artinya menggunakan meleteakan huruf konsonan atau bilangan ganjil yang menjadi awal berasal suatu istilah di akhir istilah itu dan menambahkan akhiran "an".
- Pemampatan
Mengurangi Panjang pesan atau jumlah bloknnya adalah cara lain untuuk menyembunyikan isi pesan. Contoh sederhana ini menggunakan cara menghilangkan setiap karakter ke-tiga secara beruntutan. Karakter-karakter yang dihilangkan disatukan kembali dan diusulkan sebagai "lampiran" dan pesan utama, dengan diawali oleh suatu karakter khusus, dalam contoh ini digunakan "&".

2.4 Algoritma Advanced Encryption Standard (AES)

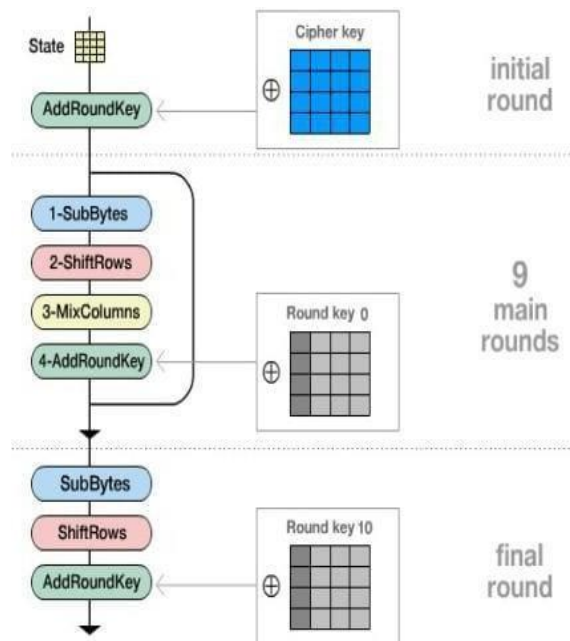
AES merupakan standar dekripsi yang merupakan singkatan dari DES, versi AES terbagi menjadi 3 yaitu AES-128, AES-192 dan AES 256. Angka di belakang kata AES merupakan panjang dari masing-masing AES yang digunakan. Input dan output dari algoritma AES terdiri dari 128 set data. Urutan data yang terdiri dari 128 bit disebut blok data atau teks biasa yang akan dienkrpsi dengan basis cipher. Kunci enkripsi AES memiliki panjang kunci 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah warna yang akan diimplementasikan pada algoritma AES ini. Di bawah ini adalah tabel yang menunjukkan jumlah belokan (Nr) yang ditetapkan untuk setiap tombol.

Tabel 1. Perbedaan Tiga jenis Algoritme AES (Munir,2019)

	Jumlah key (Nk)	Ukuran Blok (Nb)	Jumlah putaran (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

2.5 Proses Enkripsi *Advanced Encryption Standard (AES)*

Metode enkripsi algoritme AES terdiri dari 4 jenis variabel byte yaitu SubBytes, ShiftRows, MixColumns dan addRoundkey. Pada awal proses enkripsi, input yang disalin ke state akan membuat byte berubah menjadi AddRoundKey. Setelah itu, status akan menerima perubahan SubBytes, ShiftRows, MixColumns, dan AddRoundKey berulang kali untuk Nr. Proses ini disebut algoritma AES. Warna terakhir sedikit berbeda dengan warna sebelumnya dimana pada warna terakhir keadaan MixColumns tidak berubah, dibawah ini adalah gambar proses enkripsi AES. (Wijaya, Harahap, and Aisyah 2020)



Gambar 1. Proses Enkripsi AES (Wijaya et al. 2020)

2.6 Proses Dekripsi *Advanced Encryption Standard (AES)*

Transformasi cipher dapat dibalik dan di implementasikan dalam arah yang berlawanan untuk menghasilkan inverse, cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Algoritma dekripsi dapat dibuat pada skema berikut:

a. InvShiftRows

InvShiftRows adalah transformasi byte yang berlebihan dengan transformasi ShiftRows. Pada transformasi INvShiftRows, dilakukan penggeseran bit ke kanan sedangkan pada ShiftRowsn dilakukan penggeseran bit ke kiri,

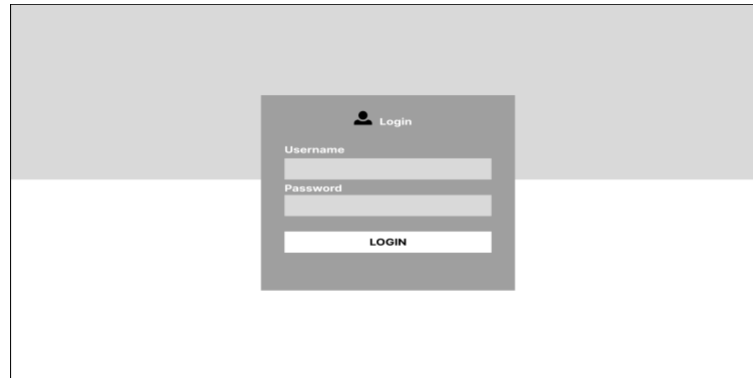
b. InvSubByte

InvSubByte juga merupakan transformasi byte yang berkebalikan dengan transformasi SubBytes. Pada InvSubBytes tiap elemen pada state diperlukan dengan menggunakan table inverse S-Box.

3. HASIL DAN PEMBAHASAN

3.1 Tampilan Halaman Login

Pada rancangan halaman login berfungsi memberikan akses kepada admin dan user. Halaman login ini terdiri dari logo Celebes Kontruksindo PT dan inputan yaitu name dan password. Berikut rancangan tampilan halaman login.



Gambar 2. Tampilan Halaman Login

3.2 Tampilan Halaman Utama

Pada rancangan layar halaman dashboard ini akan menampilkan menu utama yang terdapat logo Celebes Kontruksindo PT, ada juga beberapa pilihan menu yaitu beranda, berkas, daftar berkas yang berisi enkripsi dan dekripsi berkas. Terdapat 3 kotak berbentuk persegi panjang yang isinya terdapat total Enkripsi dan total Dekripsi dibagian bawah terdapat penjelasan tentang aplikasi. Ada fitur tampilan pada halaman home ini yaitu photo profile, nama, terakhir aktif, logo dan serta dilengkapi dengan pilihan menu sign out. Berikut tampilan rancangan halaman admin home.



Gambar 3. Tampilan Halaman Utama

3.3 Tampilan Halaman Daftar List

Pada rancangan layar halaman daftar list ini terdapat tampilan table dimana berisi No, user name, nama file, nama file enkripsi, ukuran file, tanggal dan status, dimana terdapat button status pada file tersebut sudah di enkripsi atau dekripsi, serta fitur- fitur lainnya. Berikut gambar halaman daftar list.

No	Username	Nama File	Nama File Enkripsi	Ukuran File	Tanggal	Status
34	admin	site-banten.xlsx	site-banten.rda	4.99512 KB	2023-07-08	Sudah Dekripsi
12	admin	site-jakarta.xlsx	site-jakarta.rda	4.99512 KB	2023-07-08	Terenkripsi

Gambar 4. Tampilan Halaman Daftar LList

3.4 Tampilan Halaman Enkripsi

Pada rancangan layar halaman ini enkripsi terdapat 4 kolom untuk menginput file yang akan di enkripsi yaitu tanggal dimana akan otomatis masuk sesuai tanggal pada saat di enkripsi, file yang dimana dapat memilih file yang ingin di enkripsi ,password untuk penguncian file dan keterangan ,lalu ada button enkripsi file untuk melakukan proses enkripsi file ,serta ada fitur lainnya .Berikut rancangan tampilan enkripsi file

Gambar 5. Tampilan Halaman Enkripsi

3.5 Tampilan Halaman Dekripsi

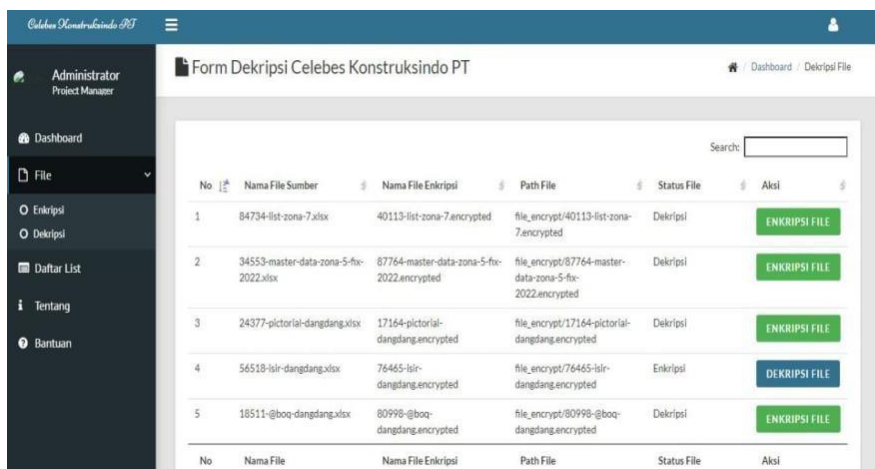
Pada rancangan layar halaman dekripsi ini terdapat tampilan table dimana table tersebut berisi berkas yang sudah di enkripsi maupun yang sudah di dekripsi, terdapat no,nama sumber file,nama file enkripsi,path file,status ,action dimana action in ada button untuk dekripsi ,serta fitur lainya berikut gambar tampilan dari rancangan dekripsi.



Gambar 6. Tampilan Halaman Dekripsi

3.6 Tampilan Halaman Mendekripsi User

Pada tampilan layar dekripsi file user ini terdapat tampilan berbentuk tabel yang berisi file yang telah di enkripsi dan dekripsi dengan isi pada tabel yaitu No, Username Nama file, Nama file enkripsi Tanggal, Status dimana aksi status ini bisa merubah file yang ingin di dekripsi, serta dilengkapi dengan pilihan menu dashboard, File, Enkripsi, Dekripsi, Daftar List, Tentang dan Bantuan. Berikut tampilan layar dekripsi file user.



Gambar 7. Tampilan Halaman Mendekripsi User

3.7 Tabel Pengujian

Tabel 2. Pengujian Enkripsi dan Dekripsi Berkas

No	Nama file sumber	Nama file enkripsi	Path file	Status file	aksi
1	18511-@boq-dangdang.xlsx	80998-@boq-dangdang.encrypted	File_encrypt/80998@boq-Dangdang.encrypted	Enkripsi	Dekripsi file
2	56518-isir-dangdang.xlsx	76465-isir-dangdang.encrypted	file_encrypt/76465-isir-dangdang.encrypted	Dekripsi	Enkripsi file

3	34553-master-data-zona-5-fix-2022.xlsx	87764-master-data-zona-5-fix-2022.encrypted	ile_encrypt/87764-master-data-zona-5-fix-2022.encrypted	Dekripsi	Enkripsi file
4	84734-list-zona-7.xlsx	40113-list-zona-7.encrypted	file_encrypt/40113-list-zona-7.encrypted	Dekripsi	Enkripsi file
5	24377-pictorial-dangdang.xlsx	17164-pictorial-dangdang.encrypted	file_encrypt/17164-pictorial-dangdang.encrypted	Enkripsi	Dekripsi file
N	Nama file sumber	Nama file enkripsi	Path file	Status file	aksi
1	18511-@boq dangdang.xlsx	80998-@boq dangdang.encrypted	File_encrypt/80998@boq Dangdang.encrypted	Enkripsi	Dekripsi file
2	56518-isir-dangdang.xlsx	76465-isir-dangdang.encrypted	file_encrypt/76465-isir-dangdang.encrypted	Dekripsi	Enkripsi file
3	34553-master-data-zona-5-fix-2022.xlsx	87764-master-data-zona-5-fix-2022.encrypted	ile_encrypt/87764-master-data-zona-5-fix-2022.encrypted	Dekripsi	Enkripsi file
4	84734-list-zona-7.xlsx	40113-list-zona-7.encrypted	file_encrypt/40113-list-zona-7.encrypted	Dekripsi	Enkripsi file
5	24377-pictorial-dangdang.xlsx	17164-pictorial-dangdang.encrypted	file_encrypt/17164-pictorial-dangdang.encrypted	Enkripsi	Dekripsi file

3.8 Kelebihan Aplikasi

1. Proses Enkripsi AES didesain untuk melakukan sebuah pembuatan password yang rahasia sehingga file dapat terjaga dengan aman
2. Pada hasil perancangan, maka Sistem keamanan data atau file menjadi solusi untuk mengamankan data BOQ(Bill Of Quantity) ,data Tower area Banten dan Jakarta
3. Dalam Pengguna kunci atau password adalah hal yang penting dalam sebuah proses enkripsi dan dekripsi file, sehingga membutuhkan kerahasiaan dalam penggunaan kunci atau password

3.9 Kekurangan Aplikasi

1. Semakin besar file maka semakin lama enkripsi filenya
2. Aplikasi hanya bisa enkripsi dan dekripsi file

4. KESIMPULAN

Berkembangnya teknologi pada zaman ini telah poly mempengaruhi rakyat pada melakukan aktivitas sehari-hari, terutama dalam bidang penyimpanan arsip yang dimana menggunakan software keamanan enkripsi serta dekripsi file ini bisa mempermudah pengguna dalam menyimpan file. Jadi bedasarkan penelitian di Celebes Kontruksindo PT, maka pada peroleh konklusi menjadi berikut:

1. Proses enkripsi AES didesain untuk melakukan sebuah proses pembuatan password yang rahasia sehingga file dapat terjaga dengan aman.

2. Pada hasil perancangan, maka Sistem Keamanan data atau file menjadi solusi untuk mengamankan data atau file pada bagian BOQ(Bill Of Quantity) ,data tower area Banten dan Jakarta .
3. Dalam pengguna kunci atau password adalah hal yang penting dalam sebuah proses enkripsi dan dekripsi file, sehingga membutuhkan kerahasiaan dalam pengguna kunci atau password

Penelitian ini mempunyai saran, yang dimana saran ini guna mengembangkan aplikasi dan sistem yang lebih baik ,berikut saran:

1. Diharapkan aplikasi ini dapat dikembangkan tidak hanya di platform website, tetapi dapat dikembangkan di platform Android maupun IOS.
2. Diharapkan agar penelitian ini selanjutnya dapat menyempurnakan dan mengembangkan aplikasi ini dari sisi tampilan agar menarik.
3. Diharapkan aplikasi ini kedepannya dapat mengenkripsi file dengan format video,gambar dan audio.

DAFTAR PUSTAKA

- [1] Arrijal, Irham Mu'alimin, Rusdi Efendi, and Boko Susilo. 2018. "Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks." *Pseudocode* 3(1):69–82. doi: 10.33369/pseudocode.3.1.69-82.
- [2] Bhaudhayana, Gede Wisnu, and I. Made Widiartha. 2018. "Implementasi Algoritma Kriptografi AES 256 Dan Metode Steganografi LSB Pada Gambar Bitmap." *Jurnal Ilmu Komputer* 8(2):9–25.
- [3] Han, Eunice S., and Annie goleman, daniel; boyatzis, Richard; Mckee. 2019. "Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah." *Journal of Chemical Information and Modeling* 53(9):2.
- [4] Kurniawan. 2018. "Teknik Dasar Kriptografi."
- [5] Munir, Rinaldi. 2019. "Slide Kuliah Pengantar Kriptografi." *Jurnal Ilmu Komputer Dan Informatika*.
- [6] Pabokory, Fresly Nandar, Indah Fitri Astuti, and Awang Harsa Kridalaksana. 2019. "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard." *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer* 10(1):20. doi: 10.30872/jim.v10i1.23.
- [7] Pramusinto, Wahyu, Nugrozho Wizaksono, and Ari Saputro. 2019. "Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman." *Jurnal BIT (Budi Luhur Information Technology)* 16(2):47–53.
- [8] Simanjuntak, Magdalena, Tioria Pasaribu, and Semiati Rahmadilla. 2019. "Implementasi Algoritma Merkle Hellman Untuk Keamanan Database." *MEANS (Media Informasi Analisa Dan Sistem)* 4(1):46–50. doi: 10.54367/means.v4i1.327.
- [9] Suhardi. 2019. "Aplikasi Kriptografi Data Sederhana Dengan Metode Exclusive-or (Xor)." *Jurnal Teknovasi* 03(2):23–31.
- [10] Tullah, Rahmat, Muhammad Iqbal Dzulhaq, and Yudi Setiawan. 2019. "108-427-1-Pb." 6(2).
- [11] Tulloh, Aditia Rahmat, Yurika Permanasari, Erwin Harahap, Prodi Matematika, Fakultas Matematika, Dan Ilmu, dan Pengetahuan Alam. 2019. "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen Cryptography Advanced Encryption Standard (AES) for File Document Encryption." *Jurnal Matematika UNISBA* Vol2(1):1–8.
- [12] Widyawan, Dian, and Imelda Imelda. 2021. "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi." *Skanika* 4(1):15–22. doi: 10.36080/skanika.v4i1.2216.
- [13] Wijaya, Bayu Angga, M. Harahap, and Siti Aisyah. 2020. "Perancangan Aplikasi Enkripsi Data Menggunakan Algoritma XXTEA." *Jurnal Sistem Informasi Dan Ilmu Komputer Prima(JUSIKOM PRIMA)* 3(2):7–12. doi: 10.34012/jusikom.v3i2.847.