4th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
27 Maret 2024 – Jakarta, Indonesia
Volume 3, Nomor 1, April 2024 - ISSN 2962-8628 (*online*)

IMPLEMENTASI KRIPTOGRAFI DENGAN ALGORITME ADVANCE ENCRYPTION STANDARD (AES-128) UNTUK PENGAMANAN FILE PADA PT PRIMER GENERAL TRADING

Febi Ramadani[1*], Gunawan Pria Utama[2], Wahyu Pramusinto[3], Safrina Aimini[4]

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

Email: [1*]1911500658@student.budiluhur.ac.id, [2]gunawan.priautama@budiluhur.ac.id, [3]wahyu.pramusinto@budiluhur.ac.id, [4]safrina.amini@budiluhur.ac.id.
(*: corresponding author)

Abstrak- Keamanan data menjadi tantangan besar di era bisnis digital yang semakin kompleks. PT Primer General Trading berisiko terhadap pencurian dan akses tidak sah terhadap data sensitif, terutama saat bertukar dokumen dan PDF. Meskipun penelitian sebelumnya di Indonesia telah menyoroti pentingnya enkripsi, fokus penerapan AES-128 di perusahaan seperti PT Primer General Trading tampaknya masih belum komprehensif. Kesenjangan inilah yang mendorong dilakukannya penelitian ini, yang secara khusus berfokus pada penerapan enkripsi dengan algoritma AES-128 pada perusahaan-perusahaan tersebut untuk melindungi keamanan file berformat PDF atau dokumen. Permasalahan utama yang dibahas meliputi bagaimana menjaga keamanan file dokumen untuk meminimalkan risiko pencurian, efektivitas penerapan AES-128 sebagai solusi terhadap risiko keamanan yang teridentifikasi, dan perdagangan file PT Primer General, yang mencakup seberapa besar keamanan yang dapat dicapai. Ditingkatkan dengan menerapkan enkripsi AES-128. Penelitian ini memiliki keterbatasan yaitu memfokuskan pada aplikasi AES-128 yang diintegrasikan ke dalam database menggunakan PHP, dengan ukuran file tidak melebihi 5 MB. Penelitian ini menerapkan AES pada enkripsi web, menggunakan metode AES-128 untuk membuat aplikasi keamanan file terenkripsi berbasis situs web, dan berfokus pada penerapan enkripsi di perusahaan dengan persyaratan khusus untuk file mereka. Tujuannya adalah untuk memberikan kontribusi baru dalam penelitian keamanan data fokus pada bidang keamanan data keamanan. Penelitian ini mengarah pada aplikasi praktis untuk meningkatkan keamanan data PT Primer General Trading melalui teknik penelitian yang ditargetkan. Manfaatnya mencakup peningkatan keamanan data, penggunaan enkripsi yang efisien, dan peningkatan kesadaran organisasi akan risiko keamanan data. Kesimpulannya, penelitian ini memberikan pedoman praktis untuk meningkatkan keamanan data di lingkungan bisnis, khususnya melalui penerapan AES-128 dalam perlindungan file dokumen.

Kata Kunci: keamanan data, enkripsi, *advanced encryption standard* (AES-128), pengamanan file, pertukaran Informasi.

IMPLEMENTATION OF CRYPTOGRAPHY WITH ADVANCE ENCRYPTION STANDARD ALGORITHM (AES-128) TO SECURE FILES AT PT PRIMER GENERAL TRADING

Abstract- *Data security is a major challenge in the increasingly complex digital business era. PT Primer General Trading is at risk of theft and unauthorized access to sensitive data, especially when exchanging documents and PDFs. While previous research in Indonesia has highlighted the importance of encryption, the focus of AES-128 implementation in companies such as PT Primer General Trading still seems to be incomprehensive. It is this gap that prompted this research, which specifically focuses on the implementation of encryption with the AES-128 algorithm in such companies to protect the security of PDF files or documents. The main issues addressed include how to keep document files secure to minimize the risk of theft, the effectiveness of implementing AES-128 as a solution to the identified security risks, and the trade of PT Primer General files, which includes how much security can be achieved. Improved by applying AES-128 encryption. This research has limitations, namely focusing on the AES-128 application integrated into the database using PHP, with a file size not exceeding 5 MB. This research applies AES to web encryption, uses the AES-128 method to create a web-based encrypted file security application, and focuses on applying encryption in companies with specific requirements for their files. The goal is to make new contributions in data security research focusing on the field of data security security. This research leads to practical applications to improve the data security of PT Primer General Trading through targeted research techniques. The benefits include improved data security, efficient use of encryption, and increased organizational awareness of data security risks. In conclusion, this research provides practical guidelines for improving data security in a business environment, specifically through the application of AES-128 in the protection of document files.*

Keywords: data security, encryption, advanced encryption standard (AES-128), file security, information exchange.

1. PENDAHULUAN

Di era yang semakin digital saat ini, berbagi data sudah menjadi hal yang lumrah dalam dunia bisnis. Namun, kompleksitas dan urgensi keamanan data semakin meningkat. PT Primer General Trading, seperti banyak perusahaan lainnya, menghadapi risiko pencurian dan akses tidak sah terhadap data sensitif. Khususnya dalam konteks berbagi dokumen dan PDF, kebutuhan akan solusi keamanan yang canggih dan efektif untuk melindungi informasi dari akses yang tidak diinginkan sangatlah penting. Seiring kemajuan teknologi dan kebutuhan keamanan data yang meningkat, enkripsi muncul sebagai solusi penting untuk menjaga integritas dan kerahasiaan informasi. Salah satu algoritma yang mendapat perhatian khusus adalah Advanced Encryption Standard (AES-128), yang terbukti andal dan efisien dalam melindungi data digital [2].

Meskipun banyak penelitian di Indonesia yang menyoroti pentingnya enkripsi untuk melindungi data, fokus pada penerapan AES-128 oleh perusahaan seperti PT Primer General Trading masih dianggap kurang. Sebagian besar penelitian sebelumnya cenderung merinci aspek umum keamanan data tanpa mempertimbangkan tantangan dan kebutuhan spesifik yang dihadapi organisasi saat bertukar file dalam format dokumen. Oleh karena itu, untuk mengisi kesenjangan penelitian tersebut, penelitian ini mengusulkan untuk fokus pada implementasi enkripsi dengan algoritma AES-128 di PT Primer General Trading, khususnya dalam pengamanan file dalam format PDF atau dokumen.

Melalui penelitian ini, kami bertujuan untuk mengidentifikasi dan mengatasi potensi risiko keamanan yang timbul dari pertukaran informasi di lingkungan bisnis PT Primer General Trading. Meskipun penelitian sebelumnya telah memberikan landasan teoritis yang kuat, penelitian ini akan memberikan kontribusi yang signifikan dengan menyoroti penerapan keamanan file secara praktis dan konkrit dalam konteks bisnis. Temuan penelitian ini diharapkan tidak hanya memberikan informasi berharga mengenai strategi masa depan untuk meningkatkan keamanan data, namun juga memberikan rekomendasi khusus untuk pengelolaan keamanan data di PT Primer General Trading.

Menjaga kerahasiaan informasi, menjamin integritasnya, dan mengotentikasi pihak-pihak yang berkomunikasi adalah tujuan utamanya. Oleh karena itu, enkripsi membantu menjaga integritas data selama pertukaran informasi dan mencegah akses yang tidak sah [6].

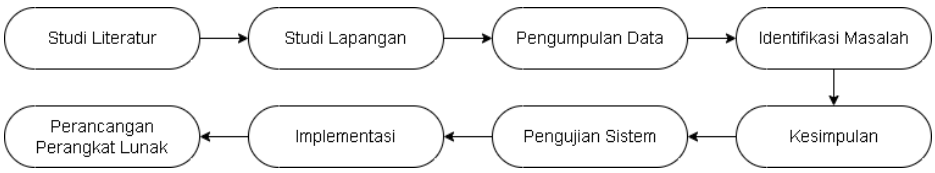
Enkripsi, juga dikenal sebagai "enkripsi", adalah seni dan ilmu yang mana untuk menjaga kerahasiaan pesan yang dikirimkan kepada penerimanya sehingga data atau pesan tersebut aman dan tidak diketahui pihak ketiga. Pihak ketiga akan menggunakan kode yang tidak dapat dipahami untuk mengirimkan informasi atau pesan [1]. Baik enkripsi maupun dekripsi dilakukan dengan menggunakan kunci kriptografi [3].

Untuk melindungi data, algoritme enkripsi simetris Advanced Encryption Standard (AES), juga dikenal sebagai enkripsi kunci simetris standar, digunakan. Tiga jenis algoritme AES-128, AES-192, dan AES-256 dapat digunakan untuk mengenkripsi serta mendekripsi data dalam blok 128-bit, yang merupakan ukuran tetap dari cipher yang digunakan [5].

Algoritma AES menggunakan empat jenis transformasi byte selama proses enkripsinya. Mereka adalah *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. *ShiftRows* adalah transformasi * yang menggunakan tabel substitusi (S-box) untuk memetakan setiap elemen dalam status. Perpindahan bit, atau rotasi bit, adalah proses di mana bit paling kiri digeser menjadi bit paling kanan. Setiap komponen kolom negara bagian dioperasikan oleh MixColumns. Ada kunci bulat yang ditambahkan ke status dengan menggunakan operasi XOR [4].

2. METODE PENELITIAN

Tema penelitian ini adalah metode air terjun atau waterfall. Metode ini digunakan sebagai pedoman untuk menyelesaikan tugas penelitian dan untuk memperoleh hasil penelitian yang lebih baik sehingga hasilnya tidak menyimpang dari tujuan penelitian. Gambar 1 menunjukkan flowchart penelitian.



Gambar 1. Flowchart Penelitian

2.1 Pengumpulan Data

Langkah pengumpulan data ini dilakukan untuk memperoleh informasi yang diperlukan untuk perancangan sistem. Di bawah ini adalah beberapa metode yang digunakan:

a. Wawancara
Dalam langkah ini, tujuan wawancara ditentukan dengan jelas, pihak-pihak yang relevan diidentifikasi, dan pertanyaan yang disusun dengan seksama diberikan kepada mereka. Untuk mengetahui info lebih lanjut tentang prosedural yang harus diikuti untuk menerapkan sistem pengamanan dokumen dan file di PT Primer General Trading.

b. Observasi
Mengumpulkan data dan mempelajari proses di PT Primer General Trading melalui pengamatan langsung.

c. Studi Pustaka
Caranya dengan membaca literatur terkait kriptografi, teori keamanan file, teori AES, dan lain-lain..

2.2 Advance Encryption standard (AES)

Algoritme enkripsi simetris Advanced Encryption Standard (AES) (juga dikenal sebagai standar enkripsi kunci simetris) digunakan untuk melindungi data. AES-128, AES-192, dan AES-256 merupakan tiga varian algoritma yang dapat digunakan untuk menyandikan dan mendekode data dalam blok 128-bit, ukuran tetap untuk enkripsi yang digunakan (Simarmata, J. 2019). Panjang kunci AES yang digunakan untuk enkripsi disebut nomor setelah AES. Tabel 1 menunjukkan bahwa setiap AES menggunakan jumlah putaran yang berbeda.

Tabel 1. Perbandingan Pada jumlah kunci AES

AES(bits)	Panjang kata Kunci (Nk Words)	Besaran Blok kata (Nb Words)	Banyak Putaran (NR)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

a. Proses Enkripsi

Algoritme AES memiliki empat jenis proses enkripsi: byte variabel SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Pada awal proses pengkodean, item yang disalin ke ruang status akan mengalami konversi byte AddRoundKey. Selanjutnya, status akan melalui transisi SubBytes berulang Nr, ShiftRows, MixColumns, dan AddRoundKey. Proses ini dikenal sebagai fungsi melingkar dalam algoritme AES. Babak final berbeda dari babak sebelumnya karena negara bagian tidak melakukan transisi MixColumns.

b. Proses Dekripsi

Untuk algoritme AES, *invers cipher* dapat dibalikkan dalam arah yang mudah dipahami dengan menggunakan transformasi *byte* seperti *InvShiftrows, InvSubBytes, InvMixColumns, dan AddRoundKey.* Tahapan dekripsi berbeda dari tahapan enkripsi, meskipun keduanya memiliki beberapa tahapan dan perhitungan yang sama.

2.3 Kriptografi

Tujuan utamanya adalah menjaga kerahasiaan informasi, menjamin integritasnya, dan mengotentikasi pihak-pihak yang berkomunikasi. Oleh karena itu, enkripsi bertindak sebagai pertahanan untuk mencegah akses tidak sah dan menjaga integritas data selama pertukaran informasi [6].

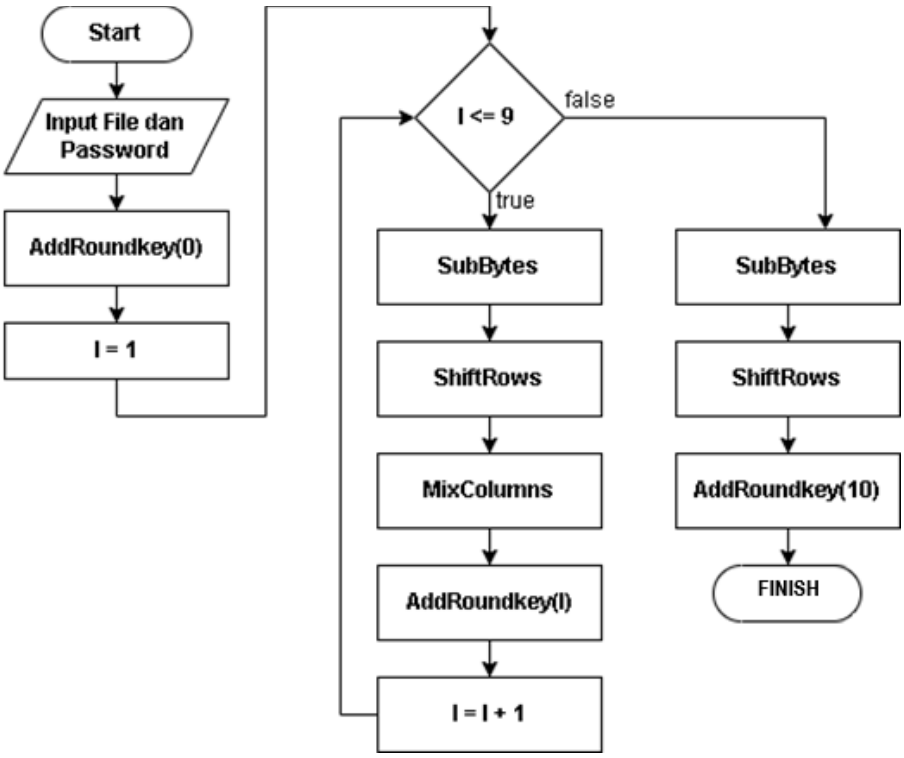
Penting juga untuk menyelidiki kunci enkripsi. Kunci ini merupakan faktor penting dalam menentukan seberapa baik keamanan informasi dapat dijaga. Manajemen kunci yang tepat dapat meningkatkan tingkat keamanan, namun manajemen kunci yang buruk dapat menyebabkan kerentanan terhadap serangan keamanan [6].

3. HASIL DAN PEMBAHASAN

Analisis, pembahasan topik penelitian, dan hasil implementasi atau pengujian dibahas dalam bagian ini. Ini juga memberikan penjelasan berupa deskripsi, foto, tabel, dll.

3.1 Flowchart Pada Enkripsi AES-128

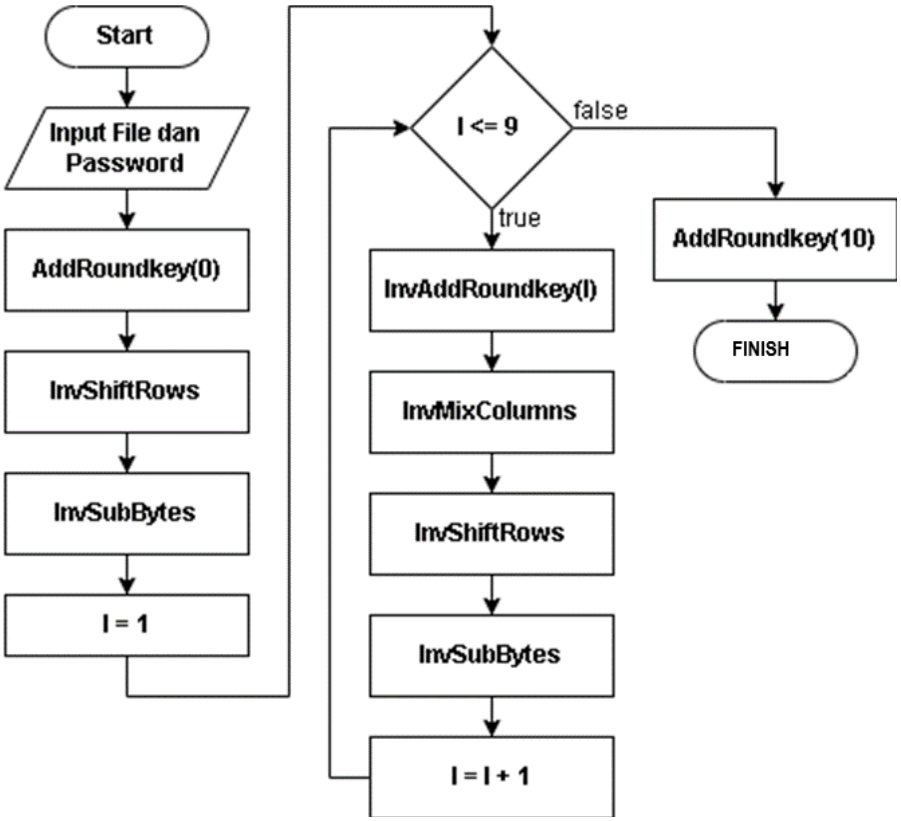
Gambar 3 menunjukkan diagram alur yang menjelaskan proses enkripsi AES-128 di aplikasi ini.



Gambar 3. Flowchart Enkrisi AES-128

3.2 Flowchart Pada Penjelasan AES - 128

Gambar 4 menunjukkan diagram alur yang menjelaskan proses dekripsi AES-128 yang digunakan oleh aplikasi ini.



Gambar 4. Flowchart Enkripsi AES-128

3.3 Algoritme Pada Enkripsi AES-128

Penjelasan algoritmik aliran proses yang terlibat dalam enkripsi AES-128 disajikan pada bagian penelitian ini pada algoritme 1.

Algoritme 1. Enkripsi AES-128

```
Start
Input berkas dan sandi
AddRoundkey(0)
I=1
        If I <= 9
        SubBytes
        ShiftRows
        MixColums
        AddRoundKey(I)
        I = I + 1
        Kembali ke baris 5
        Else
SubBytes
ShiftRows
AddRoundKey(10)
End
```

3.4 Algoritme Pada Penjelasan AES-128

Penjelasan algoritmik aliran proses yang terlibat dalam dekripsi AES-128 disajikan pada bagian penelitian ini pada algoritme 2.

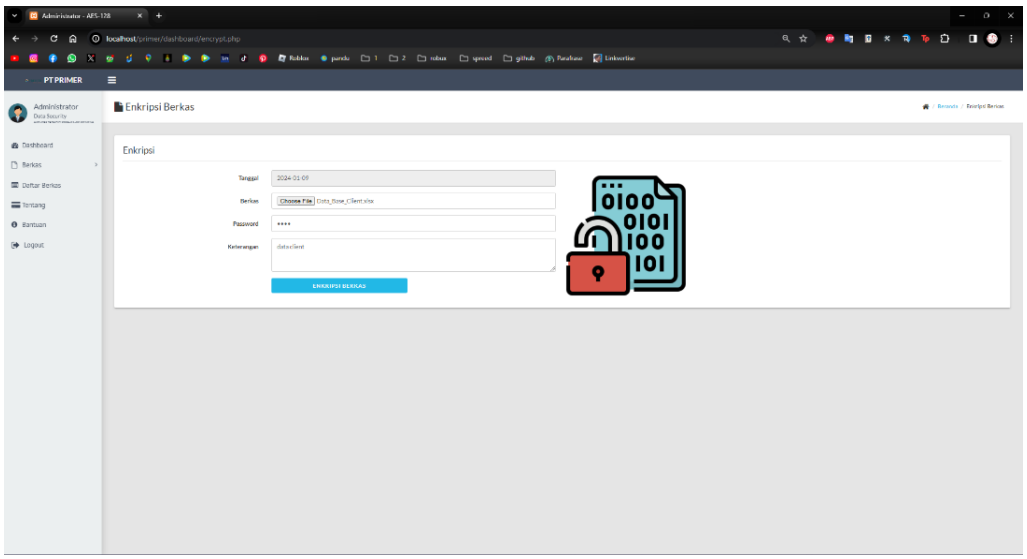
Algoritme 2. Dekripsi AES-128

```
Start
Input berkas dan sandi
AddRoundkey(0)
InvShiftRows
InvSubBytes
I=1
        If I<=9
        AddRoundKey(I)
        InvMixColums
        InvShiftRows
        InvSubBytes
        I=I+1
        Kembali ke baris 7
        Else
AddRoundKey(10)
End
```

3.5 Implementasi Metode

3.5.1 Proses Enkripsi

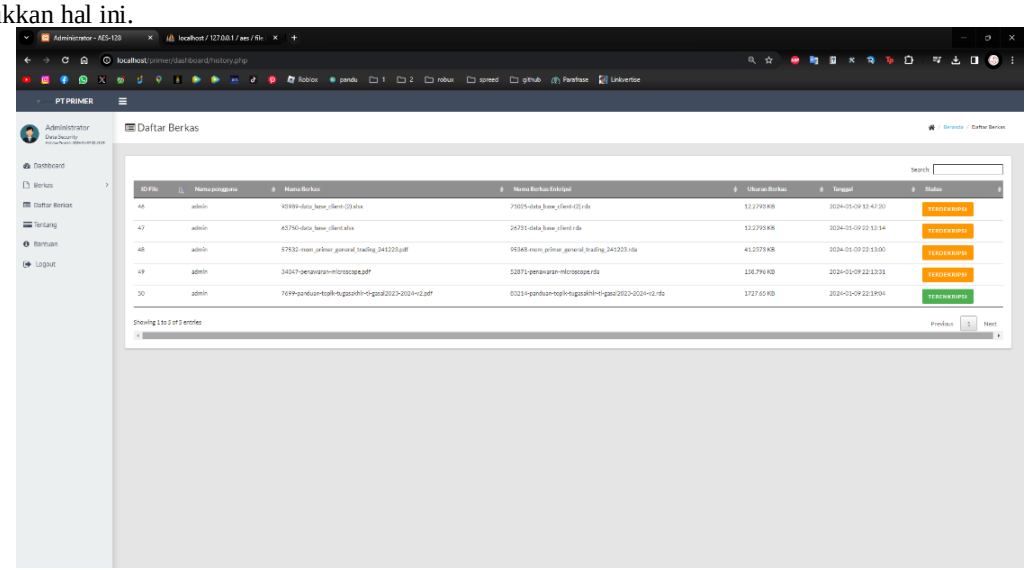
Penguna harus menggunakan login admin untuk memulai proses ini. Setelah Anda log in dan memilih opsi "Enkripsi Dokumen", tampilannya akan seperti gambar di bawah ini. Tanggal otomasi, kolom untuk memasukkan file yang ingin dienkripsi, kolom untuk memasukkan kata sandi sebagai "kunci", dan kolom untuk menjelaskan file apa yang dienkripsi ada di halaman form enkripsi. Gambar 5 menunjukkan tampilan ini.



Gambar 5. Halaman Form Enkripsi

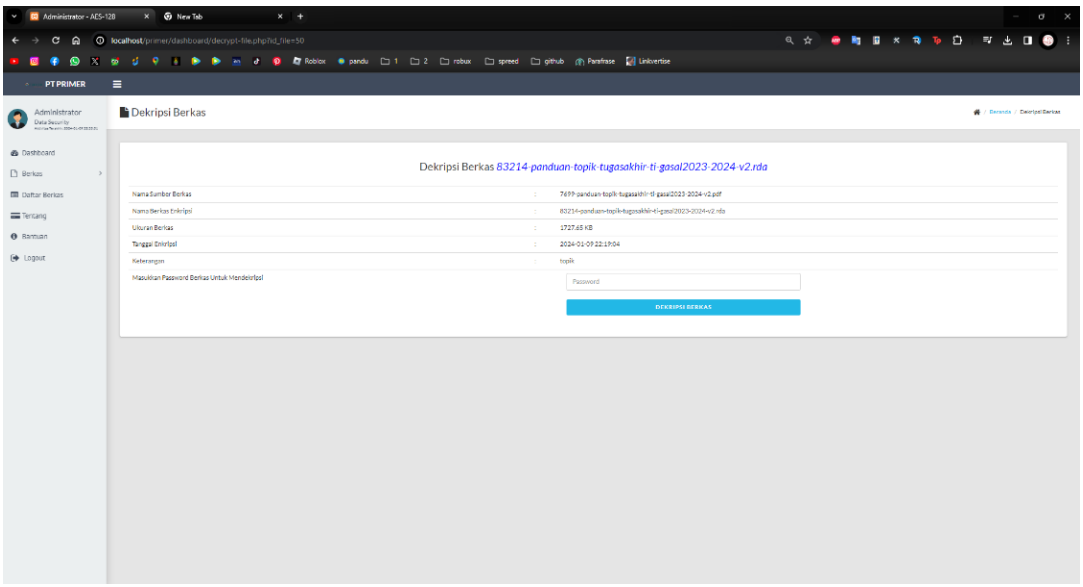
3.5.2 Proses Dekripsi

Penguna harus menggunakan login admin untuk memulai proses ini. Pastikan file telah dienkripsi sebelum memulai dekripsi. Ini dapat dilakukan dengan pergi ke menu "Berkas" dan memilih "Dekripsi Berkas", yang akan menampilkan tampilan seperti gambar. Pilih file yang akan didekripsi, lalu klik "DEKRIPSI BERKAS". Gambar 6 menunjukkan hal ini.



Gambar 6. Halaman Tabel Dekripsi

Setelah itu akan masuk ke halaman dekripsi file seperti gambar di bawah. Lalu masukan password yang telah diberikan pada saat file dienkripsi. Lalu klik tombol ‘DEKRIPSI BERKAS’. Berikut saya tampilkan pada gambar 7.



Gambar 7. Halaman Informasi Berkas Dekripsi

3.6 Pengujian Program

Setelah memenuhi persyaratan perangkat lunak dan perangkat keras, langkah berikutnya adalah menguji aplikasi yang Anda buat. Dalam bagian ini, pengujian untuk aplikasi enkripsi dan dekripsi dijelaskan. Pengujian ini digunakan untuk mengetahui hasil enkripsi file yang dienkripsi. Seberapa cepat file didekripsi dan seberapa lama file dienkripsi?

3.6.1 Tabel Pengujian Enkripsi

Tabel ini menunjukkan bagaimana sistem menguji enkripsi.

Tabel 4. Tabel Hasil Pengujian Enkripsi

No	Nama File Asli	Ukuran Asli (KB)	Waktu (detik)	Nama File Enkripsi	Ukuran File Enkripsi (KB)	Rasio
1	48331-data_base_client.xlsx	12,2	0,92	87957-data_base_client.rda	12,2	100%
2	75353-mom_primer_general_trading_241223.pdf	41,2	1,23	31637-mom_primer_general_trading_241223.rda	41,2	100%
3	98915-penawaran-microscope.pdf	158	2,41	23089-penawaran-microscope.rda	158	100%

3.6.2 Tabel Pengujian Dekripsi

Tabel ini menunjukkan bagaimana sistem menguji dekripsi.

Tabel 5. Tabel Hasil Pengujian Dekripsi

No	Nama File Asli	Ukuran Asli (KB)	Waktu (detik)	Nama File Enkripsi	Ukuran File Enkripsi (KB)	Rasio
1	87957-data_base_client.rda	12,2	0,82	48331-data_base_client.xlsx	12,2	100%
2	31637-mom_primer_general_trading_241223.rda	41,2	1,37	75353-mom_primer_general_trading_241223.pdf	41,2	100%
3	23089-penawaran-microscope.rda	158	2,37	98915-penawaran-microscope.pdf	158	100%

4. KESIMPULAN

Setelah serangkaian analisis menyeluruh, desain yang cermat, pembuatan aplikasi, dan pengujian intensif, hasil dari aplikasi kriptografi ini menjadi semakin jelas. Pertama, algoritma AES 128 terbukti menjadi solusi efektif untuk melindungi file terkait penyediaan barang ke konsumen di lingkungan PT Primer General Trading. Algoritme unggul ini memberikan lapisan keamanan penting, memastikan integritas dan kerahasiaan informasi penting selama proses penawaran. Selain itu, aplikasi ini dapat mengenkripsi dan mendekripsi file dengan ekstensi dokumen yang umum digunakan seperti .doc, .docx, .xls, .xlss, .ppt, .pptx, dll. Selain itu, file dalam format PDF juga dapat dimasukkan dalam target enkripsi sehingga meningkatkan keamanan pertukaran informasi di seluruh perusahaan. Prosedur ini memastikan perlindungan maksimal terhadap semua dokumen relevan yang sering digunakan di PT Primer General Trading, mengurangi risiko akses tidak sah dan melindungi kerahasiaan data perusahaan. Oleh karena itu, aplikasi kriptografi ini tidak hanya memenuhi standar keamanan, tetapi juga memberikan solusi konkrit dan terukur terhadap kebutuhan keamanan informasi di lingkungan perusahaan.

1. DAFTAR PUSTAKA

[1] Yuningrat Dwi Putri, Rosihan, Salkin Lutfi, "PENERAPAN KRIPTOGRAFI CAESAR CIPHER PADA FITUR CHATTING SISTEM INFORMASI FREELANCE", Jurnal Informatika dan Komputer,Vol. 2, 87-94, 2019.
[2] Wijaya, P. A., Damanik, M., Hartati, P., & Gunawan, I., "Implementasi Kriptografi AES-128 Untuk Mengamankan URL (Uniform Resource Locator) dari SQL Injection", Akademika Jurnal, Vol. 17, 8-13, 2020.
[3] Dedy Ronald Saragi, Janter Mamiel Gultom, Jose Andreas Tampubolon, Indra Gunawan, "Pengamanan Data File Teks (Word).
[4] Menggunakan Algoritme RC4", Jurnal Sistem Komputer dan Informatika, Vol. 1, 114-119, 2020.
[5] Simarmata, Sriadhi dan Robbin Rahim. (2019). KRIPTOGRAFI Teknik Keamanan Data dan Informasi. Yogyakarta: Penerbit Andi.
[6] Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography. CRC Press.
[7] Faturungi Muharram, Aziz, H., & Abdul Rachman Manga. (2018). Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES). Prosiding SAKTI (Seminar Ilmu Komputer Dan Teknologi Informasi), 3(2), 112–115. Retrieved from https://e-journals.unmul.ac.id/index.php/SAKTI/article/view/1844.
[8] A Azanuddin, Yakub, S., & Jaka Prayudha. (2022). Implementasi Keamanan Citra Menggunakan Algoritma AES-128 Dengan Aplikasi Client-Server. JURASIK : Jurnal Riset Sistem Informasi Dan Teknik Informatika, 7(1), 51–51. https://doi.org/10.30645/jurasik.v7i1.415.
[9] Anwar, N., Munawwar Munawwar, Muhammad Abduh, & Nugroho Budhi Santosa. (2018). Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA. Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 2(3), 783–791. https://doi.org/10.29207/resti.v2i3.606.

[10] Muhammad Azhari, Dadang Iskandar Mulyana, Faizal Joko Perwitosari, & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains Dan Komputer, 2(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390.
[11] Ariska Ariska, & Wahyuddin Wahyuddin. (2022). Penerapan Kriptografi Menggunakan Algoritma Des (Data Encryption Standard). Jurnal Sintaks Logika, 2(2), 9–19. https://doi.org/10.31850/jsilog.v2i2.1734.
[12] Irawan, C., & Mosess Setiadi, D. R. I. (2019). IMPLEMENTASI ALGORITMA AUTOKEY CIPHER DAN AES-128 PADA ENKRIPSI FILE. Retrieved January 31, 2024, from Unisbank.ac.id website: https://www.unisbank.ac.id/ojs/index.php/sendi_u/article/view/7385.