5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
7 September 2024 – Jakarta, Indonesia
Volume 3, Nomor 2, September 2024 - ISSN 2962-8628 (*online*)

IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA AES 128 UNTUK MENGAMANKAN DOKUMEN PADA PT. AMEGA CAHAYA UTAMA

Danar Zulfian Wirakusumah[1], Painem[2]

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

Email: [1]2011501455@student.budiluhur.ac.id, [2*]painem@budiluhur.ac.id
(* : corresponding author)

Abstrak- Kerahasiaan data adalah aspek penting dalam pengelolaan dokumen proyek yang mengandung informasi finansial, seperti invoice. Banyak perusahaan, termasuk PT Amega Cahaya Utama, masih menyimpan dokumen tersebut secara offline tanpa sistem backup yang memadai, sehingga rentan terhadap risiko penyalahgunaan oleh pihak yang tidak berwenang. Kontribusi penelitian ini adalah mengembangkan aplikasi keamanan dokumen yang mengenkripsi dan mendekripsi data dalam format PDF, DOCX, XLS, dan TXT menggunakan algoritma AES 128-bit. Aplikasi ini dirancang untuk beroperasi di lingkungan offline, memberikan solusi keamanan yang dapat diadaptasi oleh perusahaan lain dengan kebutuhan serupa. Proses pengujian menggunakan metode blackbox testing menunjukkan hasil yang memuaskan. Sebagai contoh, file "Invoice Ring 17 Term 2 ACU-BHMA.pdf" berukuran 2,412 KB membutuhkan waktu enkripsi 98,54 detik, sedangkan file "Logo_pt.png" berukuran 38 KB hanya memerlukan 1,75 detik. Hasil pengujian memperlihatkan bahwa waktu enkripsi meningkat seiring dengan ukuran file, dan seluruh proses enkripsi berhasil tanpa kegagalan. Selain itu, aplikasi ini memiliki fitur peran superadmin, yang dapat mengenkripsi dan mendekripsi file, serta peran admin, yang hanya dapat melihat file. Implementasi algoritma AES 128-bit dalam sistem ini terbukti efektif dalam meningkatkan keamanan data sensitif di PT Amega Cahaya Utama, melindungi dokumen dari akses tidak sah, dan menawarkan perlindungan yang kuat bagi perusahaan yang beroperasi secara offline tanpa sistem backup berbasis cloud.

Kata Kunci: aes-128, kriptografi, keamanan data

IMPLEMENTATION OF CRYPTOGRAPHY USING THE AES 128 ALGORITHM FOR SECURING DOCUMENTS AT PT. AMEGA CAHAYA UTAMA

Abstract- *Data confidentiality is a crucial aspect of managing project documents that contain financial information, such as invoices. Many companies, including PT Amega Cahaya Utama, still store these documents offline without adequate backup systems, making them vulnerable to unauthorized misuse. This research contributes by developing a document security application that encrypts and decrypts data in PDF, DOCX, XLS, and TXT formats using AES 128-bit encryption. The application is designed to operate in an offline environment, providing a security solution that can be adapted by other companies with similar needs. Blackbox testing methods have shown satisfactory results. For instance, the file "Invoice Ring 17 Term 2 ACU-BHMA.pdf," sized 2,412 KB, required 98.54 seconds for encryption, while the file "Logo_pt.png," sized 38 KB, only took 1.75 seconds. Testing results indicate that encryption time increases with file size, and the entire encryption process was completed without failure. Additionally, the application features a superadmin role, capable of encrypting and decrypting files, and an admin role, which only has file viewing privileges. The implementation of AES 128-bit encryption in this system proves effective in enhancing the security of sensitive data at PT Amega Cahaya Utama, protecting documents from unauthorized access, and providing robust protection for companies operating offline without cloud-based backup systems.*

Keywords*: aes-128, cryptography, data security*

1. PENDAHULUAN

Kerahasiaan sebuah data atau informasi merupakan aset yang sangat berharga dan harus dijaga agar tidak diketahui oleh pihak yang tidak memiliki kepentingan. Data atau informasi merupakan salah satu aset yang penting untuk dilindungi keamanannya. Selain daripada itu, kerahasiaan sebuah data sudah tercetus sejak jaman dahulu, tepatnya pada jaman Romawi kuno dengan metode pergeseran huruf atau karakter dengan dasar nilai tertentu yang bertujuan untuk menyembunyikan pesan atau informasi agar tidak diketahui oleh pihak yang tidak berkepentingan.

Perlindungan data sangat penting untuk mencegah potensi kebocoran, terutama data yang bersifat sensitif dan berhubungan dengan individu atau organisasi. Data mencakup segala hal yang dapat digunakan untuk mengidentifikasi perusahaan baik secara langsung maupun tidak langsung, baik melalui sistem elektronik maupun

non-elektronik. Perlindungan yang memadai diperlukan untuk memastikan bahwa data ini tidak jatuh ke tangan yang salah atau disalahgunakan, sehingga menjaga privasi dan keamanan tetap terjamin. Dalam konteks pengelolaan data berkas proyek yang melibatkan informasi finansial seperti invoice, perlindungan data menjadi sangat penting untuk menghindari potensi penyalahgunaan yang dapat merugikan perusahaan atau klien. PT Amega Cahaya Utama, yang bergerak di bidang pembangunan jaringan serat optik, menyimpan dokumen proyek yang mencakup informasi teknis, laporan kemajuan, serta data finansial dalam format file seperti PDF, DOC, XLS, dan TXT, pada komputer secara offline tanpa adanya sistem backup yang memadai. Hal ini membuat data tersebut rentan terhadap akses yang tidak sah dan kemungkinan kehilangan data. Selain itu, belum ada aplikasi yang menggunakan metode tertentu dalam mengamankan penyimpanan data untuk melindungi informasi tersebut dari ancaman keamanan.

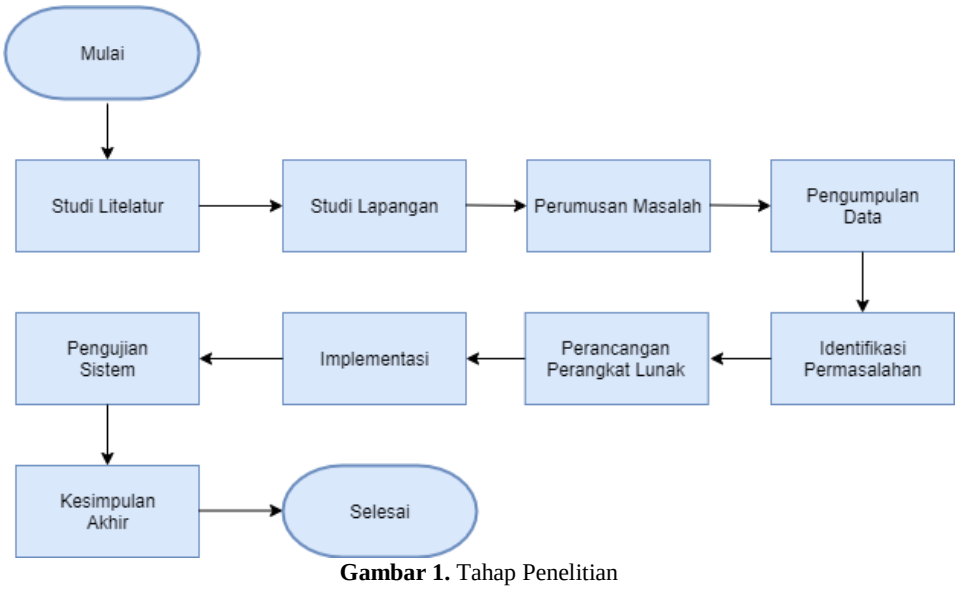
Berdasarkan latar belakang dan masalah di atas, maka perlu dibuatkan aplikasi untuk mengamankan penyimpanan data tersebut dengan menggunakan sebuah metode tertentu. Salah satu metode yang digunakan adalah AES 128. Metode ini mampu mengamankan data.

Penelitian ini melakukan pengembangan aplikasi yang tidak hanya mengamankan data finansial seperti invoice pada PT Amega Cahaya Utama, tetapi juga menawarkan solusi keamanan yang dapat diadaptasi oleh perusahaan lain dengan kebutuhan serupa. Selain itu, aplikasi ini dirancang untuk beroperasi dalam lingkungan offline, yang merupakan tantangan tersendiri karena memerlukan metode enkripsi yang kuat tanpa ketergantungan pada sistem backup berbasis cloud.

Penelitian terkait kriptografi yang sudah dilakukan oleh [1] yaitu dengan mengimplementasikan metode enkripsi Rivest Shamir Adleman (RSA) dan algoritma Huffman untuk mengenkripsi file dokumen dengan format file hasil enkripsi yaitu .doc dan .txt yang sudah dikompresi. Penelitian juga dilakukan oleh [2] dengan menerapkan algoritma AES untuk pengamanan data berjenis dokumen dengan tipe pdf, doc, txt pada SMK Harapan Bangsa. Penelitian yang dilakukan oleh [3], sistem yang dirancang berfungsi untuk mengamankan data data penting perusahaan menggunakan algoritma asimetris yaitu RSA. Dalam penelitian ini mengusulkan penggunaan AES 128-bit sebagai metode enkripsi utama, yang memiliki keunggulan dalam hal efisiensi dan tingkat keamanan yang lebih tinggi dibandingkan dengan metode asimetris seperti RSA yang telah digunakan dalam penelitian sebelumnya.

2. METODE PENELITIAN

2.1 Tahap Penelitian



Gambar 1. Tahap Penelitian

Gambar 1 diatas bertujuan untuk mencapai hasil-hasil yang diinginkan didalam penelitian dan juga berfungsi sebagai panduan dalam melaksanakan penelitian agar mencapai tujuan yang telah ditatapkan sebelumnya. Langkah-langkah ini diperlukan untuk menjaga agar penelitian tetap fokus pada tujuan dan membuatnya lebih terstruktur serta sistematis. Metode yang digunakan dalam penelitian ini adalah metode waterfall.

2.2 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan dengan tujuan menjaga kerahasiaan informasi yang terkandung dalam data, sehingga hanya dapat diakses oleh pihak yang 5 berkepentingan dan tidak diketahui oleh pihak yang tidak berwenang.. Untuk memastikan keamanan dan integritas suatu data, diperlukan proses penyandian di mana data asli diubah menjadi data terenkripsi yang tidak dapat dibaca. Proses ini bertujuan untuk melindungi informasi saat data tersebut dikirim atau disimpan. Proses dekripsi dilakukan oleh penerima untuk mengembalikan data ke bentuk aslinya setelah data terenkripsi tersebut diterima. Dengan cara penyandian tersebut, maka data yang asli tidak mungkin terbaca oleh pihak yang tidak berkepentinagan [4].

Dalam bidang kriptografi, dua konsep inti yang perlu dipahami adalah enkripsi dan dekripsi. Enkripsi melibatkan transformasi data ke dalam bentuk yang tidak dapat dipahami atau dikenali, menggunakan berbagai teknik dan algoritma khusus. Di sisi lain, dekripsi adalah proses mengembalikan data terenkripsi ke bentuk aslinya, membuatnya dapat dibaca dan dimengerti kembali [5].

2.2.1 Algoritma Simetris

Algoritma simetris, sering disebut sebagai algoritma kriptografi konvensional, mengandalkan kunci yang sama untuk enkripsi dan dekripsi. Beberapa contoh algoritma simetris adalah DES, AES, RC4, RC6, dan 3DES. Kriptografi simetris memiliki keunggulan dalam kecepatan operasi yang lebih tinggi dibandingkan dengan algoritma asimetris, memungkinkannya untuk efektif digunakan dalam sistem real-time.

Kelemahannya terletak pada kebutuhan untuk memiliki kunci yang berbeda untuk setiap pengiriman pesan kepada pengguna yang berbeda, yang mengakibatkan tantangan dalam manajemen kunci. Permasalahan ini dikenal sebagai "key distribution problem" [6].

2.2.2 Algoritma Asimetris

Kriptografi kunci publik atau kriptografi asimetris melibatkan sepasang kunci di mana salah satunya digunakan untuk enkripsi dan yang lainnya untuk dekripsi. Kunci publik dapat digunakan oleh siapa saja untuk mengenkripsi pesan, tetapi hanya penerima yang memiliki kunci privat yang dapat mendekripsi pesan yang dikirimkan kepada mereka.

2.3 Algoritma Advanced Encryption Standard (*AES*)

Advanced Encryption Standard (AES) adalah algoritma block cipher simetris yang menggunakan kunci simetris dalam proses enkripsi dan dekripsi. AES dikenal karena keamanannya yang tinggi dan kecepatan pemrosesannya yang efisien.

Algoritma AES tidak hanya dirancang untuk keamanan, tetapi juga untuk kecepatan tinggi. Algoritma ini direkomendasikan oleh NIST (National Institute of Standards and Technology) sebagai pengganti DES. Proses enkripsi AES melibatkan pengolahan blok data 128 bit melalui 10, 12, atau 14 putaran, tergantung pada ukuran kunci yang digunakan. AES dapat diterapkan di berbagai platform, termasuk perangkat kecil, dan telah diuji secara luas untuk berbagai aplikasi keamanan [7].

2.4 Ekspansi Kunci

Pembangkitan atau ekspansi kunci dilakukan dengan tujuan mendapatkan kunci ronde atau round key yang akan digunakan untuk proses enkripsi dan dekripsi, tepatnya pada tahap transformasi AddRoundKey. Tanpa proses pembangkitan kunci maka proses enkripsi dan dekripsi tidak akan berjalan sebagaimana mestinya [8]. Kunci round ini kemudian digunakan dalam setiap 9 putaran enkripsi untuk memperkuat keamanan data. Berikut adalah langkah-langkah dalam proses ekspansi kunci:

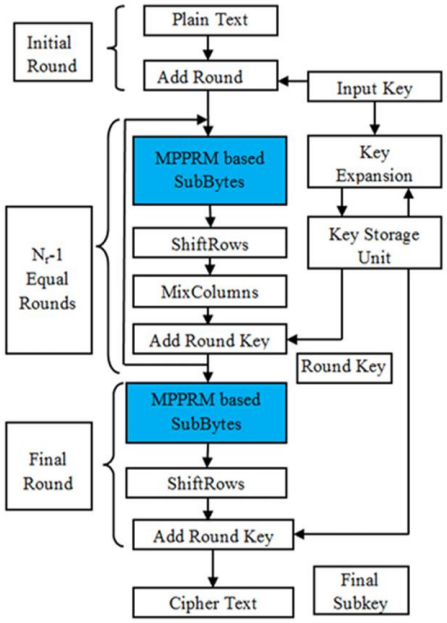
Langkah pertama dalam ekspansi kunci adalah RotWord, di mana byte terakhir dari kunci digeser ke kiri dan byte pertama dipindahkan ke akhir. Selanjutnya, SubWord menggantikan setiap byte dalam kata yang telah dirotasi dengan byte yang sesuai dari S-Box. Kemudian, Rcon meng-XOR kata yang telah diubah dengan nilai konstan (round constant) yang berbeda untuk setiap putaran. Hasil XOR ini kemudian di-XOR dengan kata pertama dari kunci ronde sebelumnya untuk menghasilkan kata pertama dari kunci ronde baru.

Kata-kata berikutnya dihasilkan dengan meng-XOR kata sebelumnya dengan kata dari kunci ronde sebelumnya yang berada pada posisi yang sama. Proses ini diulang sampai semua kunci ronde yang diperlukan dihasilkan sesuai dengan jumlah putaran dalam algoritma AES. Ekspansi kunci memastikan bahwa setiap putaran enkripsi menggunakan kunci yang berbeda, memperkuat keamanan dan mempersulit analisis kriptografi. Dengan memahami ekspansi kunci, kita dapat melihat bagaimana kunci asli diubah menjadi serangkaian kunci yang meningkatkan keamanan proses enkripsi dan dekripsi dalam AES.

2.5 Proses Enkripsi AES

Dalam enkripsi menggunakan Advanced Encryption Standard (AES), terdapat empat jenis transformasi byte yang penting, yaitu Addroundkey, Subbytes, Shiftrows, dan Mixcolumns. Transformasitransformasi ini memainkan peran krusial dalam setiap tahap enkripsi AES. Mereka digunakan untuk meningkatkan kompleksitas data yang akan dienkripsi, sehingga membuatnya lebih sulit untuk diretas. 10 Masing-masing transformasi memiliki tujuan dan fungsi khusus, dan mereka diterapkan dalam beberapa putaran enkripsi untuk menghasilkan kunci yang aman dan efektif dalam melindungi data [9].

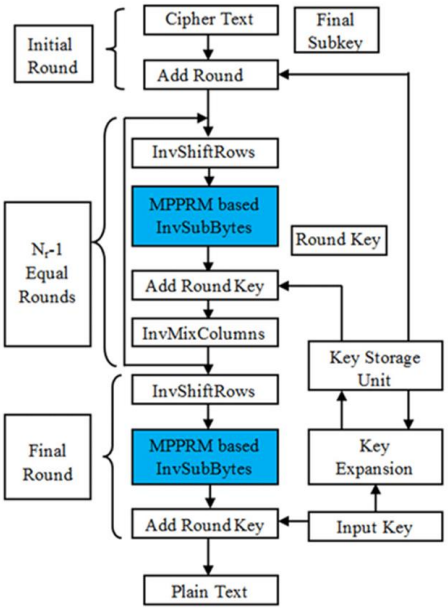
Enkripsi menggunakan AES mencakup empat transformasi utama: AddRoundKey, SubBytes, ShiftRows, dan MixColumns, yang diterapkan dalam sejumlah putaran sebanyak Nr. Pada putaran terakhir, transformasi MixColumns tidak diterapkan. Hasil dari proses enkripsi ini disimpan sebagai output byte dan dapat dilihat lebih rinci pada Gambar 2 dibawah ini:



Gambar 2. Proses Enkripsi

2.6 Proses Dekripsi AES

Dekripsi AES terdiri dari langkah-langkah yang merupakan kebalikan dari enkripsi, yaitu invShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Urutan proses dekripsi AES tidak merupakan kebalikan dari enkripsi, namun urutannya yang ditukarkan, walaupun penggunaan kuncinya sama [10]. Ilustrasi proses dekripsi AES dapat dilihat lebih detail pada Gambar 3 di bawah ini:



Gambar 3. Proses Dekripsi

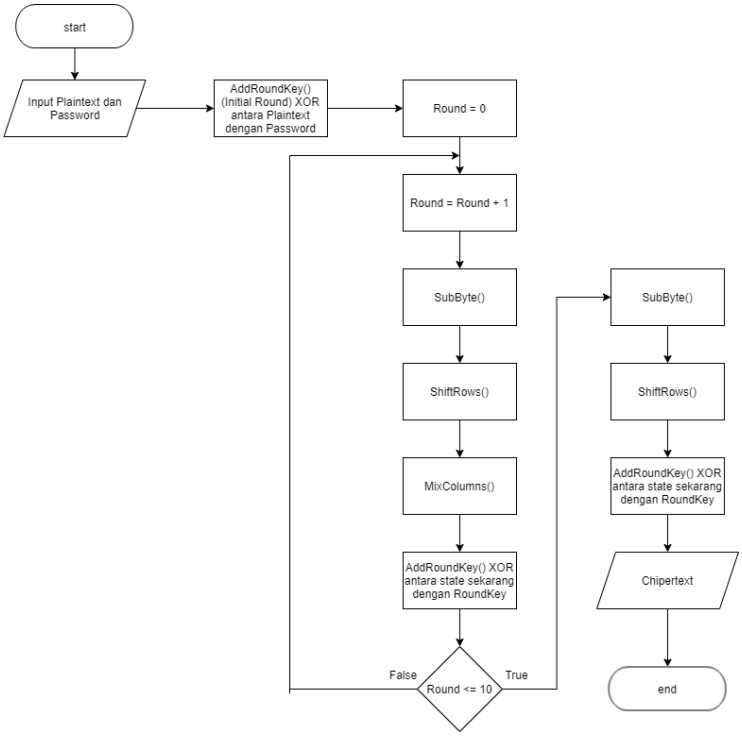
3. HASIL DAN PEMBAHASAN

3.1 Flowchart

Flowchart adalah sebuah diagram yang memvisualisasikan langkahlangkah dan keputusan dalam sebuah proses atau sistem. Setiap langkah dalam proses tersebut direpresentasikan oleh simbol atau bentuk diagram tertentu, dan langkah-langkah ini dihubungkan oleh garis atau panah untuk menunjukkan urutan atau aliran proses secara visual. Tujuan dari flowchart adalah untuk memberikan visualisasi yang jelas tentang alur program sehingga lebih mudah dipahami.

3.1.1 Flowchart Proses Enkripsi AES

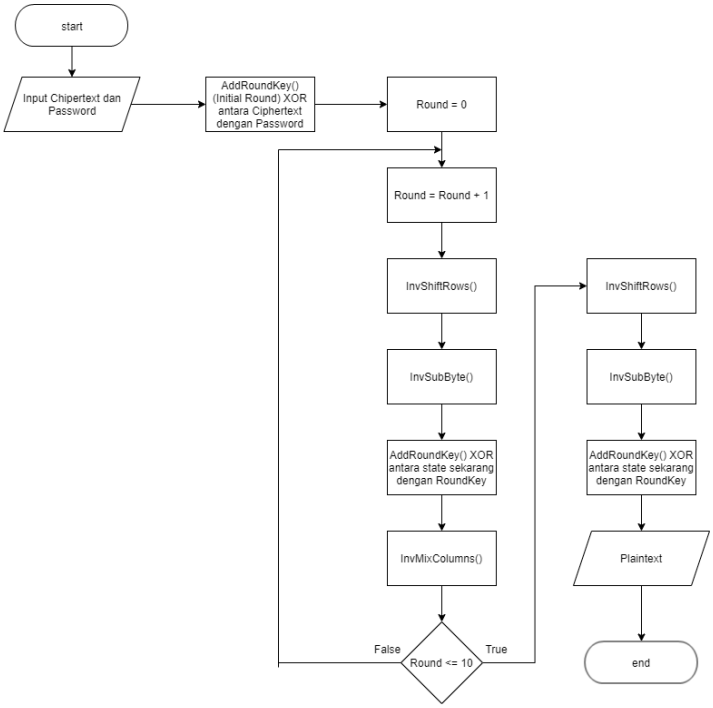
Pada flowchart ini dijelaskan proses pengenkripsian file. Flowchart ini memaparkan langkah-langkah proses AES. Flowchart proses enkripsi AES dapat dilihat pada Gambar 4:



Gambar 4. Flowchart Proses Enkripsi

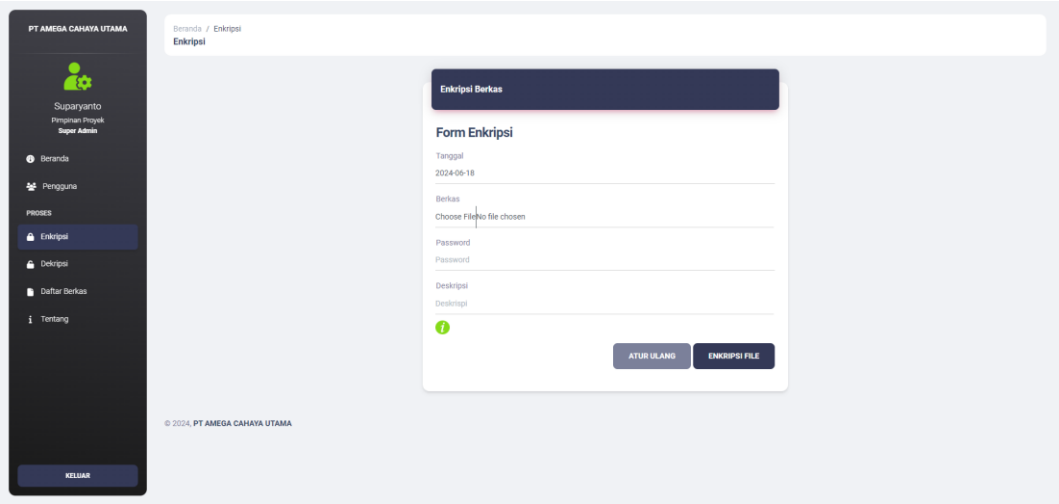
3.1.2 Flowchart Proses Dekripsi AES

Pada flowchart ini dijelaskan proses pendekripsian file. Flowchart ini memaparkan langkah-langkah proses AES, dalam pengembalian file dari ciphertext menjadi plaintext. Flowchart proses dekripsi AES dapat dilihat pada Gambar 5:

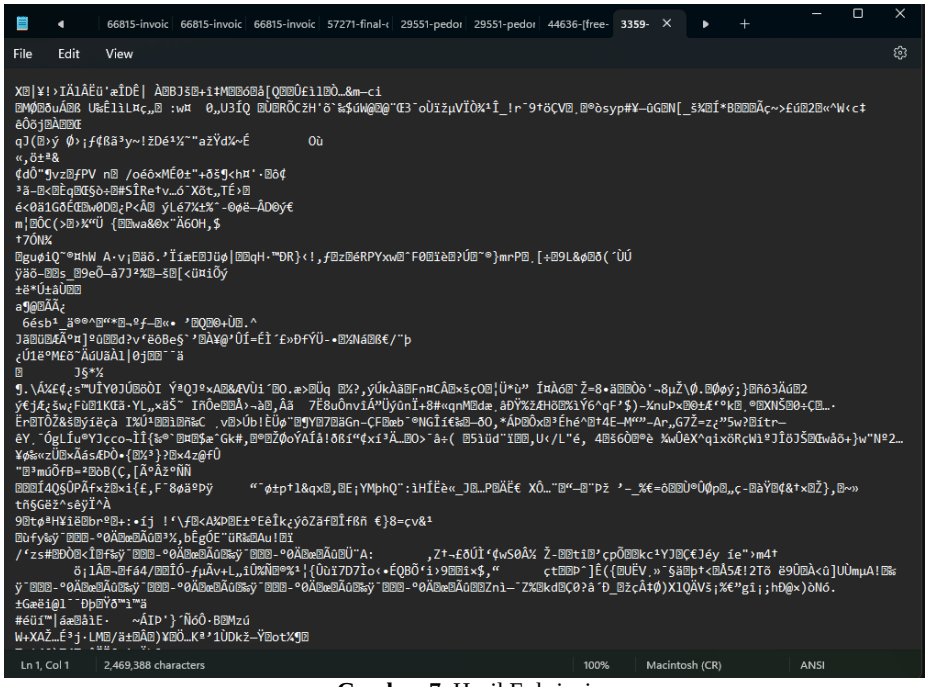


Gambar 5. Flowchart Proses Dekripsi

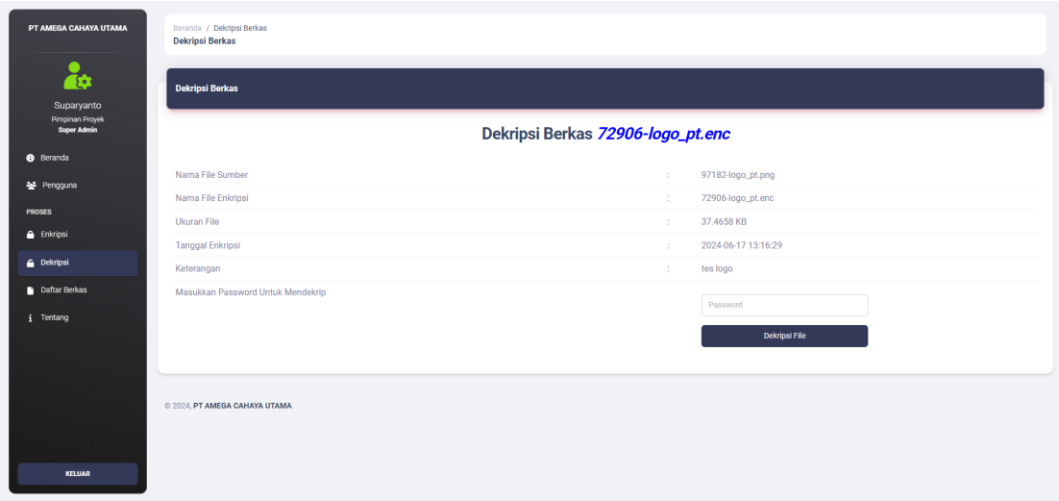
3.2 Hasil Pembahasan



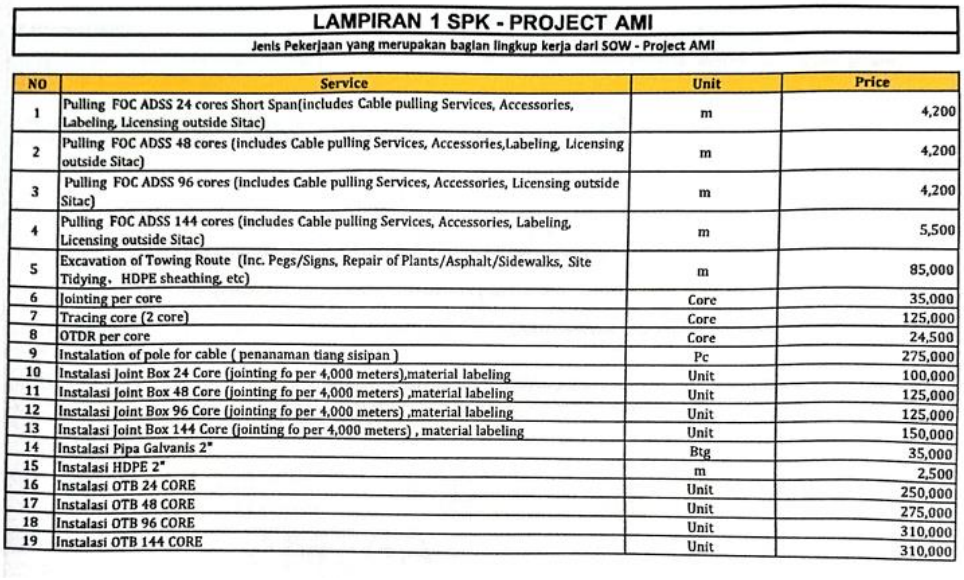
Gambar 6. Proses Enkripsi



Gambar 7. Hasil Enkripsi



Gambar 8. Proses Dekripsi



LAMPIRAN 1 SPK - PROJECT AMI

Jenis Pekerjaan yang merupakan bagian lingkup kerja dari SOW - Project AMI

NO	Service	Unit	Price
1	Pulling FOC ADSS 24 cores Short Span(includes Cable pulling Services, Accessories, Labeling, Licensing outside Sitac)	m	4,200
2	Pulling FOC ADSS 48 cores (includes Cable pulling Services, Accessories,Labeling, Licensing outside Sitac)	m	4,200
3	Pulling FOC ADSS 96 cores (includes Cable pulling Services, Accessories, Licensing outside Sitac)	m	4,200
4	Pulling FOC ADSS 144 cores (includes Cable pulling Services, Accessories, Labeling, Licensing outside Sitac)	m	5,500
5	Excavation of Towing Route (Inc. Pegs/Signs, Repair of Plants/Asphalt/Sidewalks, Site Tidying, HDPE sheathing, etc)	m	85,000
6	Jointing per core	Core	35,000
7	Tracing core (2 core)	Core	125,000
8	OTDR per core	Core	24,500
9	Instalation of pole for cable (penanaman tiang sisipan)	Pc	275,000
10	Instalasi Joint Box 24 Core (jointing fo per 4,000 meters),material labeling	Unit	100,000
11	Instalasi Joint Box 48 Core (jointing fo per 4,000 meters) ,material labeling	Unit	125,000
12	Instalasi Joint Box 96 Core (jointing fo per 4,000 meters) ,material labeling	Unit	125,000
13	Instalasi Joint Box 144 Core (jointing fo per 4,000 meters) , material labeling	Unit	150,000
14	Instalasi Pipa Galvanis 2"	Btg	35,000
15	Instalasi HDPE 2"	m	2,500
16	Instalasi OTB 24 CORE	Unit	250,000
17	Instalasi OTB 48 CORE	Unit	275,000
18	Instalasi OTB 96 CORE	Unit	310,000
19	Instalasi OTB 144 CORE	Unit	310,000

Gambar 9. Hasil Dekripsi

3.3 Tabel Hasil Pengujian

Pada bagian ini, disajikan tabel yang merangkum hasil dari pengujian proses enkripsi dan dekripsi file yang dilakukan oleh sistem melalui aplikasi. Tabel ini menunjukkan hasil pengujian terhadap file-file yang diuji.

a. Hasil Uji Enkripsi

Tabel 1. Hasil Uji Enkripsi

No.	Nama File Awal	Ukuran File Awal	Nama File Enkripsi	Ukuran File Setelah Dienkripsi	Durasi Enkripi	Keterangan
1.	invoice ring 17 term 2 ACU-BHMA.pdf	2,412 KB	33741-invoice-ring-17-term-2-acu-bhma.enc	2,412 KB	98.54 detik	BERHASIL
2.	Logo_pt.png	38 KB	29303-logo_pt.enc	38 KB	1.75 detik	BERHASIL

3.	PedomanTeknisPenulisanKKP-TA-FTI-20212-OK.PDF	1,000 KB	29551-pedomanteknispenulisankkp-ta-fti-20212-ok.enc	1,000 KB	43.18 detik	BERHASIL
4.	Tes-format-docx.docx	722 KB	6918-tes-format-docx.enc	722 KB	30.1 detik	BERHASIL
5.	Tes-format-xlsx.xlsx	8 KB	46019-tes-format-xlsx.enc	8 KB	0.45 detik	BERHASIL
6.	Profile.jpg	111 KB	61303-profile.enc	111 KB	1.25 detik	BERHASIL
7.	Book1.xlsx	57 KB	2513-book1.enc	57 KB	2.21 detik	BERHASIL
8.	document.pdf	742 KB	8362-document.enc	742 KB	32.21 detik	BERHASIL
9.	simpson.gif	212 KB	4321-simpson.enc	212	3.87 detik	BERHASIL
10.	Jurnal Population.pdf	742 KB	521-jurnal-population.enc	742 KB	32.9 detik	BERHASIL

Proses enkripsi yang dilakukan pada berbagai jenis file menunjukkan bahwa ukuran file tetap sama setelah dienkripsi. Selain itu, durasi waktu enkripsi bervariasi tergantung pada ukuran file, dengan file yang lebih besar membutuhkan waktu enkripsi yang lebih lama.

b. Hasil Uji Dekripsi

Tabel 2. Hasil Uji Dekripsi

No.	Nama File Awal	Ukuran File Awal	Nama File Dekripsi	Ukuran File Dekripsi	Durasi Dekripsi	Keterangan
1.	invoice ring 17 term 2 ACU-BHMA.pdf	2,412 KB	33741-invoice-ring-17-term-2-acu-bhma.enc	2,412 KB	102.31 detik	BERHASIL
2.	Logo_pt.png	38 KB	29303-logo_pt.enc	38 KB	1.81 detik	BERHASIL
3.	PedomanTeknisPenulisanKKP-TA-FTI-20212-OK.PDF	1,000 KB	29551-pedomanteknispenulisankkp-ta-fti-20212-ok.enc	1,000 KB	48.37 detik	BERHASIL
4.	Tes-format-docx.docx	722 KB	6918-tes-format-docx.enc	722 KB	28.2 detik	BERHASIL
5.	Tes-format-xlsx.xlsx	8 KB	46019-tes-format-xlsx.enc	8 KB	0.93 detik	BERHASIL
6.	Profile.jpg	111 KB	61303-profile.enc	111 KB	1.15 detik	BERHASIL
7.	Book1.xlsx	57 KB	2513-book1.enc	57 KB	2.81 detik	BERHASIL
8.	document.pdf	742 KB	8362-document.enc	742 KB	31.21 detik	BERHASIL

9.	simpson.gif	212 KB	4321-simpson.enc	212	3.17 detik	BERHASIL
10.	Jurnal Population.pdf	742 KB	521-jurnal-population.enc	742 KB	31.9 detik	BERHASIL

Hasil pengujian dekripsi menunjukkan bahwa setiap file yang didekripsi berhasil dikembalikan ke ukuran dan format aslinya, dengan durasi dekripsi yang berbeda-beda tergantung pada ukuran file.

4. KESIMPULAN

Dari analisis, perancangan, pembuatan, dan pengujian program aplikasi kriptografi ini, dapat disimpulkan bahwa semakin besar ukuran file yang dienkripsi, semakin lama waktu yang dibutuhkan untuk proses enkripsi. Penerapan Kriptografi AES 128 dalam aplikasi ini berhasil mengamankan dokumen-dokumen penting milik PT. Amega Cahaya Utama. Selain itu, aplikasi ini telah berfungsi sesuai dengan yang diharapkan berdasarkan hasil pengujian dengan metode blackbox testing.

Sebagai saran untuk penelitian selanjutnya, disarankan untuk mengembangkan sistem yang menggabungkan lebih dari satu algoritma kriptografi guna meningkatkan tingkat keamanan. Tujuan dari pengembangan ini adalah untuk mempersulit pihak yang tidak bertanggung jawab dalam mencuri data.

DAFTAR PUSTAKA

[1] A. I. Auliyah, "Implementasi Kombinasi Algoritma Enkripsi Rivest Shamir Adleman (Rsa) dan Algoritma Kompresi Huffman Pada File Document," *Indones. J. Data Sci.*, vol. 1, no. 1, pp. 23–28, 2020, doi: 10.33096/ijodas.v1i1.6.

[2] N. Cristy and F. Riandari, "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," *J. Ilmu Komput. dan Sist. Inf.*, vol. 4, no. 2, pp. 75–85, 2021.

[3] M. Rizki and P. Farida Ariyani, "Penerapan Kriptografi Dengan Menggunakan Algoritma Rsa Untuk Pengamanan Data Berbasis Desktop Pada Pt Trias Mitra Jaya Manunggal," *Skanika*, vol. 4, no. 2, pp. 1–6, 2021, doi: 10.36080/skanika.v4i2.1991.

[4] H. A. Sagala, "Perancangan Aplikasi Audit Internal Dengan Menerapkan Algoritma AES 128 Bit Untuk Pengamanan Data," *J. Glob. Technol. Comput.*, vol. 2, no. 2, pp. 75–86, 2023, doi: 10.47065/jogtc.v2i2.3348.

[5] A. Putra Ramadani Tarigan, P. S. Ramadhan, and K. Ibnutama, "Penerapan Kriptografi Untuk Pengamanan Data Penjualan Sepatu Dengan Metode AES (Advanced Encryption Standard)," *J. Cyber Tech*, vol. 5, no. 1, pp. 26–35, 2023, doi: 10.53513/jct.v5i1.7851.

[6] R. Febrianto and S. Waluyo, "Implementasi Algoritme Kriptografi Advanced Encryption Standard (AES-256) Untuk Mengamankan Database Penilaian Karyawan Pada KJPP NDR," *Bit (Fakultas Teknol. Inf. Univ. Budi Luhur)*, vol. 20, no. 1, p. 44, 2023, doi: 10.36080/bit.v20i1.2223.

[7] M. R. Alfani, M. Furqan, and Y. R. Nasution, "Pengamanan Data Teks Menggunakan Metode Digital Signature Algorithm (Dsa) Dan Advanced Encryption Standard (Aes)," *J. Sci. Soc. Res.*, vol. 4307, no. 1, pp. 301–306, 2024, [Online]. Available: http://jurnal.goretanpena.com/index.php/JSSR.

[8] R. D. Putranto, "Analisa dan Perancangan Sistem Keamanan File Dengan Advanced Encryption Standard (AES) Berbasis Website," *J. Inform. MULTI*, vol. 1, no. 6, pp. 601–611, 2023.

[9] B. Arianto, H. Kurniadi, and I. Kurniasari, "Implementasi Pengarsipan Elektronik Menggunakan Enkripsi Dan Dekripsi Dengan Metode Aes Di Uniska," *J. Fasilkom*, vol. 13, no. 02, pp. 259–268, 2023, doi: 10.37859/jf.v13i02.5060.

[10] S. Oktaviani, F. Rizky, and I. Gunawan, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," *J. Media Inform.*, vol. 4, no. 2, pp. 97–101, 2023, doi: 10.55338/jumin.v4i2.435.