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 ALGORITME ADVANCED ENCRYPTION STANDARD (AES-128) UNTUK PENGAMANAN DOKUMEN BERBASIS WEB PADA PT. XYZ

Yoga Rizky Setiawan[1], Sri Mulyati[2]

[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia
Email: [1]1911510384@student.budiluhur.ac.id, [2*]sri.mulyati@budiluhur.ac.id
(* : corresponding author)

Abstrak- Dalam era di mana informasi menjadi aset berharga bagi perusahaan, keamanan informasi menjadi sangat penting terutama dalam industri telekomunikasi. PT. XYZ, sebuah perusahaan di industri telekomunikasi, menghadapi tantangan besar terkait keamanan dan keandalan penyimpanan informasi. Saat ini, proses dan penyimpanan dokumen masih menggunakan metode konvensional dengan menggunakan dokumen fisik, meninggalkan celah terhadap risiko keamanan. Ancaman kebocoran data, manipulasi informasi, dan kerugian akibat kehilangan dokumen merupakan ancaman nyata yang dapat merusak reputasi dan kredibilitas perusahaan di industri telekomunikasi. Berdasarkan masalah yang dihadapi oleh PT XYZ, sebuah sistem aplikasi dikembangkan untuk mengamankan informasi dengan menerapkan algoritme kriptografi Advanced Encryption Standard (AES-128). Hasil penelitian ini diimplementasikan dalam bentuk aplikasi berbasis web yang bertujuan untuk mengamankan dokumen melalui proses enkripsi sebelum disimpan ke dalam database. Proses dekripsi hanya dapat diakses oleh pihak yang memiliki kunci dekripsi yang benar. Dari hasil dan uji coba implementasi aplikasi pengamanan dokumen menggunakan algoritme Advanced Encryption Standard (AES-128), terbukti mampu mengamankan dokumen melalui proses enkripsi dan mengembalikan data pada dokumen seperti semula melalui proses dekripsi.

Kata Kunci: Pengamanan, Kriptografi, Enkripsi, Dekripsi, AES.

1. PENDAHULUAN

Di era di mana informasi menjadi aset berharga bagi perusahaan, keamanan informasi menjadi sangat penting terutama dalam industri telekomunikasi. PT. XYZ, sebagai salah satu pelaku bisnis di industri telekomunikasi, menghadapi tantangan besar terkait keamanan dan keandalan penyimpanan informasi.[3][5]

Saat ini, proses dan penyimpanan dokumen masih mengandalkan metode konvensional dengan menggunakan dokumen fisik. Hal ini meninggalkan celah terbuka terhadap risiko keamanan. Ancaman kebocoran data, manipulasi informasi, dan kerugian akibat kehilangan dokumen menjadi ancaman nyata yang dapat merusak reputasi dan kredibilitas perusahaan di industri telekomunikasi.[1]

Berdasarkan masalah yang dihadapi oleh PT. XYZ, sebuah sistem aplikasi dikembangkan untuk mengamankan informasi dengan menerapkan kriptografi algoritme Advanced Encryption Standard (AES-128). Algoritme Advanced Encryption Standard (AES-128) dipilih sebagai metode utama dalam pengembangan sistem aplikasi keamanan informasi untuk PT. XYZ karena merupakan salah satu standar kriptografi yang paling diakui dan dipercaya secara luas di dunia. AES-128 menawarkan tingkat keamanan yang tinggi dengan kunci yang cukup panjang, sehingga membuatnya sulit untuk diretas atau dipecahkan oleh pihak yang tidak sah. Hasil penelitian ini diimplementasikan dalam bentuk aplikasi berbasis web yang bertujuan untuk mengamankan dokumen melalui proses enkripsi sebelum disimpan ke dalam database, sedangkan untuk melihat data melalui proses dekripsi hanya dapat diakses oleh pihak yang memiliki kunci dekripsi yang benar.[6][7][8]

Penelitian ini bertujuan untuk memberikan solusi bagi PT. XYZ dengan mengimplementasikan algoritme AES-128 berbasis web. Diharapkan melalui pendekatan teknologi berbasis web, proses enkripsi-dekripsi dokumen dapat dijalankan dengan efisien, meningkatkan tingkat keamanan penyimpanan dokumen[9], serta mengurangi risiko kebocoran informasi yang dapat merugikan perusahaan[10].

2. METODE PENELITIAN

2.1 Implementasi Metode

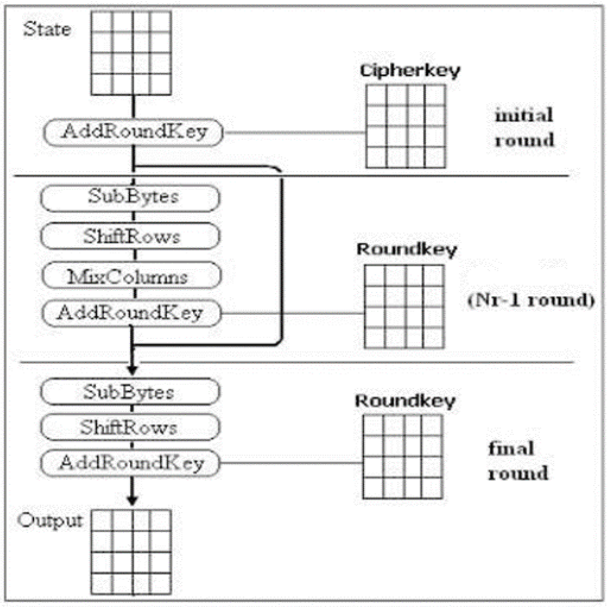
Dalam upaya menerapkan pembangunan aplikasi pengamanan dokumen berbasis web, pada bagian ini akan digunakan langkah-langkah keamanan yang telah ditetapkan. Keamanan penyimpanan file akan diimplementasikan dengan memanfaatkan algoritme Advanced Encryption Standard (AES-128).

2.2 Algoritme Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES), juga dikenal sebagai Standar Enkripsi Lanjutan, merupakan teknik enkripsi modern yang telah diadopsi sebagai standar oleh Federal Information Processing Standards (FIPS) dari National Institute of Standards and Technology (NIST) pada tahun 2001. AES menggantikan Data Encryption Standard (DES) sebagai standar enkripsi di Amerika Serikat untuk abad ke-21. Pada bulan November 2001, AES mengonfirmasi algoritme baru yang berdasarkan teknik enkripsi Rijndael, yang dipilih melalui proses seleksi AES dari beberapa algoritme, dengan Rijndael menjadi salah satu dari mereka. Teknik enkripsi AES, yang merupakan jenis block cipher seperti DES, memiliki perbedaan utama dengan DES. AES menggunakan substitusi (S-box) langsung pada teks, sementara DES hanya menggunakan substitusi S-box dalam fungsi cipher f, yang hasilnya kemudian dioperasikan pada teks menggunakan Exclusive OR (XOR). Perbedaan lainnya terletak pada ukuran kunci enkripsi; AES dapat menggunakan kunci 128 bit, 192 bit, atau 256 bit.[2]

2.3 Proses Enkripsi

Enkripsi dalam algoritme kriptografi AES dilakukan melalui empat tahap utama, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Sebelum memulai proses enkripsi, langkah awal yang penting adalah ExpansionKey, yang bertujuan untuk menghasilkan kunci ronde atau round key yang akan digunakan dalam tahap transformasi AddRoundKey. Informasi terperinci mengenai urutan proses enkripsi AES dapat ditemukan dalam gambar 1.[4]



Gambar 1. Proses Enkripsi[4]

Secara garis besar, proses enkripsi AES-128 dengan kunci 128 bit adalah sebagai berikut :

a. AddRoundKey : melakukan XOR antara state awal (plainteks) dengan cipher key. Pada tahap ini disebut juga initial round.

b. Round : Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
   - SubBytes : substitusi byte dengan menggunakan tabel substitusi (S-box).
   - ShiftRows : pergeseran baris-baris array state secara wrapping.

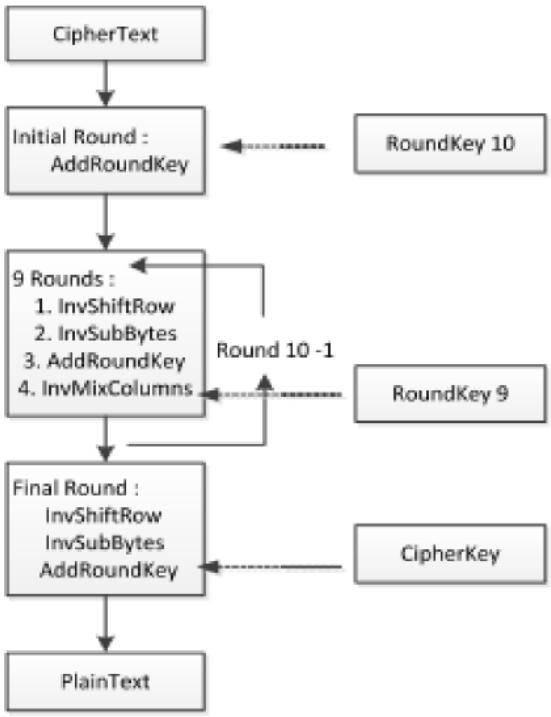
c. MixColumns : mengacak data pada masing-masing kolom array state dengan persamaan sebagai berikut : A(x) = {03}x2 + {01}x2 + {01}x2 + {02} (1)

d. AddRoundKey : melakukan XOR antara state sekarang round key.
e. Final Round : proses untuk putaran terakhir antara lain:
   - SubBytes
   - ShiftRows
   - AddRoundKey

f. Pada proses terakhir akan menghasilkan karakter atau teks yang berbentuk chipertext.

2.4 Proses Dekripsi

Dalam proses Dekripsi AES-128, diperlukan transformasi cipher yang dijalankan secara terbalik untuk menghasilkan cipher invers dengan langkah-langkah berikut: InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey[4]. Proses dekripsi AES ini dapat ditemukan dalam Gambar 2



Gambar 2. Proses Dekripsi[4]

Secara keseluruhan, proses dekripsi AES-128 menggunakan kunci 128 bit dengan langkah-langkah sebagai berikut:

a. InvShiftRows : Melakukan pergeseran bit ke kanan pada setiap baris blok,
b. InSubBytes : Setiap elemen dalam keadaan dipetakan menggunakan tabel Inverse S-Box.
c. InvMixColumns : Setiap kolom dalam keadaan dikalikan dengan matriks AES..
d. AddRoundKey : Menggabungkan array keadaan dan round key dengan operasi XOR..
e. Pada tahap akhir, akan menghasilkan teks atau karakter asli (plaintext).

2.5 Pengujian Blackbox

Pengujian blackbox adalah pendekatan yang akan digunakan untuk menguji aplikasi karena hanya memerlukan informasi mengenai batas bawah dan batas atas dari data yang diharapkan, jumlah kolom entri data yang akan diuji, aturan yang harus dipatuhi oleh entri tersebut, dan batas atas dan bawah yang harus terpenuhi. Dengan metode ini, dapat dipastikan apakah fungsionalitas aplikasi masih mampu menerima masukan data yang

tidak diinginkan, yang berpotensi menghasilkan data yang kurang diperlukan untuk disimpan. Peningkatan dalam pengembangan sistem aplikasi sangat penting untuk dapat segera memperbaiki kelemahan-kelemahan yang ada.

3. HASIL DAN PEMBAHASAN

Pada bagian ini, terdapat penjelasan tentang lingkungan percobaan, spesifikasi perangkat keras dan perangkat lunak, implementasi metode, uji coba, dan antarmuka.

3.1 Lingkungan Percobaan

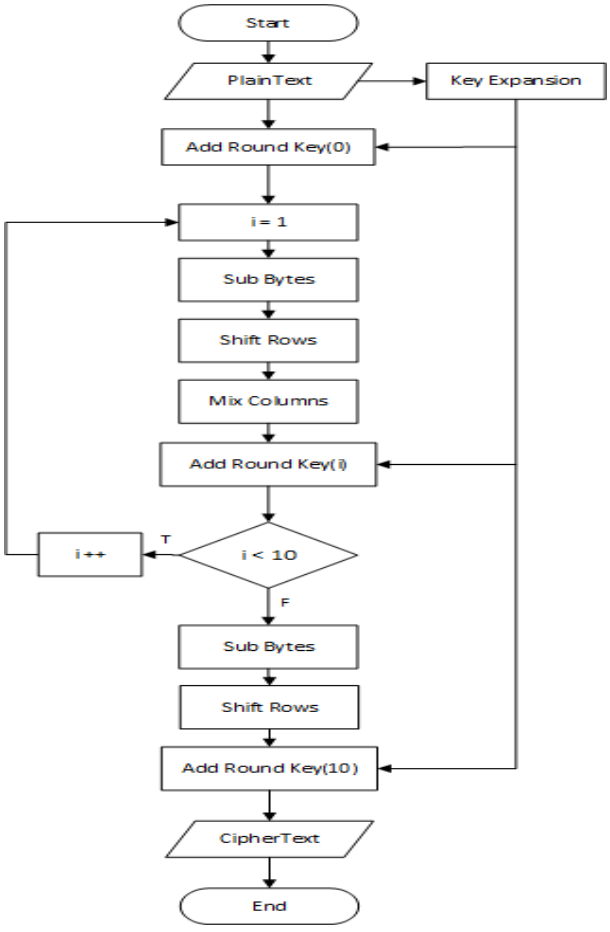
Sebelum mengimplementasikan dan menjalankan aplikasi enkripsi dan dekripsi, dibutuhkan spesifikasi perangkat keras (hardware) dan perangkat lunak (software) tertentu guna aplikasi bisa berjalan dengan baik. Pada penelitian ini, penulis memilih menggunakan bahasa pemrograman HTML dan PHP, serta dengan menggunakan framework boostrap untuk desain website guna meningkatkan estetika tampilan dari pemrograman sehingga dapat terlihat lebih menarik

3.2 Flowchart

Flowchart adalah representasi grafis dengan simbol-simbol khusus yang menunjukkan urutan instruksi yang terkait dalam suatu program. Berikut adalah flowchart dari proses kriptografi yang menggunakan metode Advanced Encryption Standard (AES-128) yang diterapkan.

a. Flowchart Enkripsi Algoritme AES-128

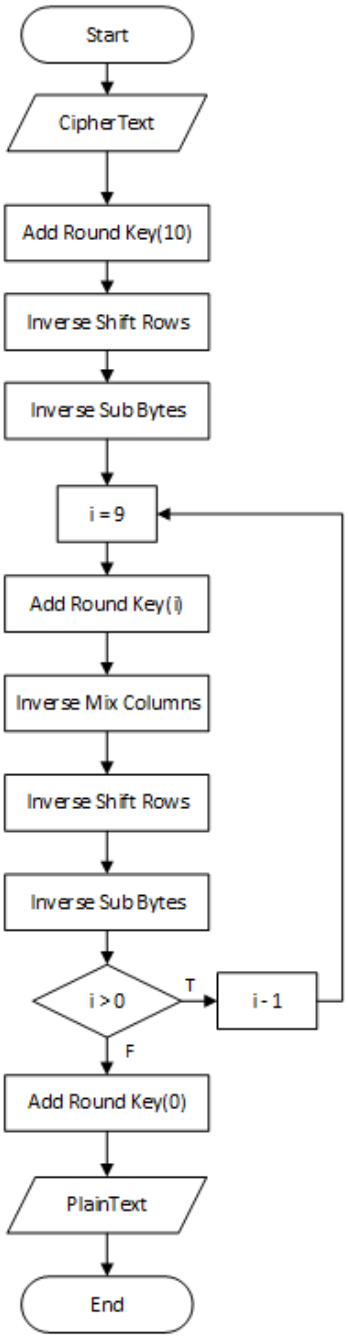
Flowchart ini menggambarkan proses langkah demi langkah untuk mengubah teks biasa (plaintext) menjadi teks terenkripsi (ciphertext) menggunakan Algoritme Advanced Encryption Standard (AES-128), sebagaimana terlihat pada Gambar 3:



Gambar 3. Flowchart Enkripsi Algoritme AES-128

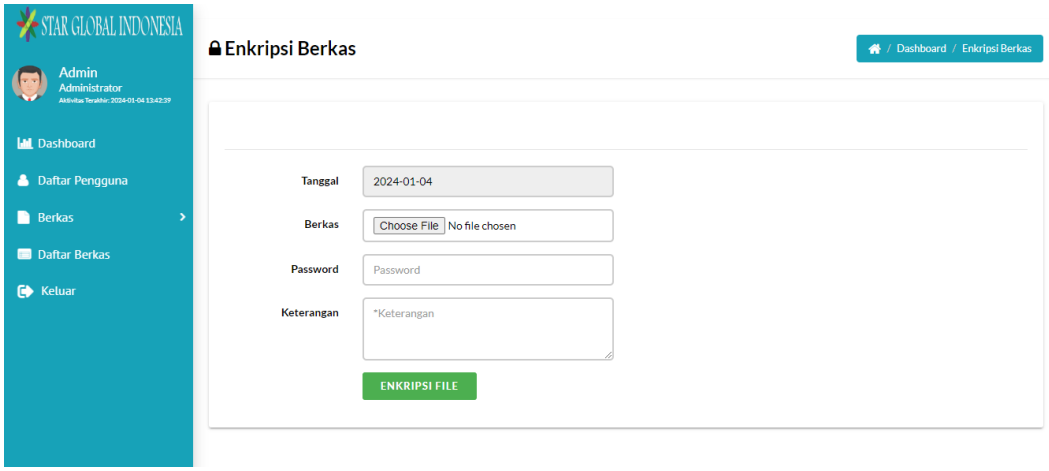
b. Flowchart Dekripsi Algoritme AES-128

Flowchart ini memberikan gambaran mengenai langkah-langkah proses mengubah teks terenkripsi (ciphertext) menjadi teks biasa (plaintext) menggunakan Algoritme Advanced Encryption Standard (AES-128), seperti yang ditunjukkan pada Gambar 4:



Gambar 4. Flowchart Dekripsi Algoritme AES-128

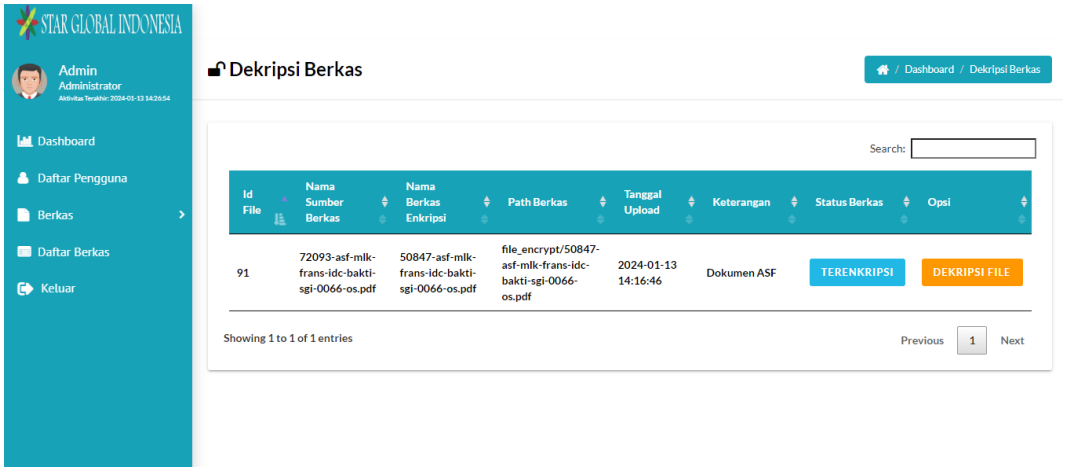
3.3 Antarmuka Layar Halaman Enkripsi Berkas



Gambar 5. Antarmuka Layar Halaman Enrkipsi Berkas

Pada antarmuka layar halaman enkripsi berkas menampilkan form tanggal untuk menandakan kapan berkas diproses untuk enkripsi, form berkas untuk menginput file berkas ke database, form password untuk membuat password enkripsi, dan keterangan untuk memberikan keterangan pada berkas yang diinputkan.

3.4 Antarmuka Layar Halaman Dekripsi Berkas



Gambar 6. Antarmuka Layar Halaman Dekripsi Berkas

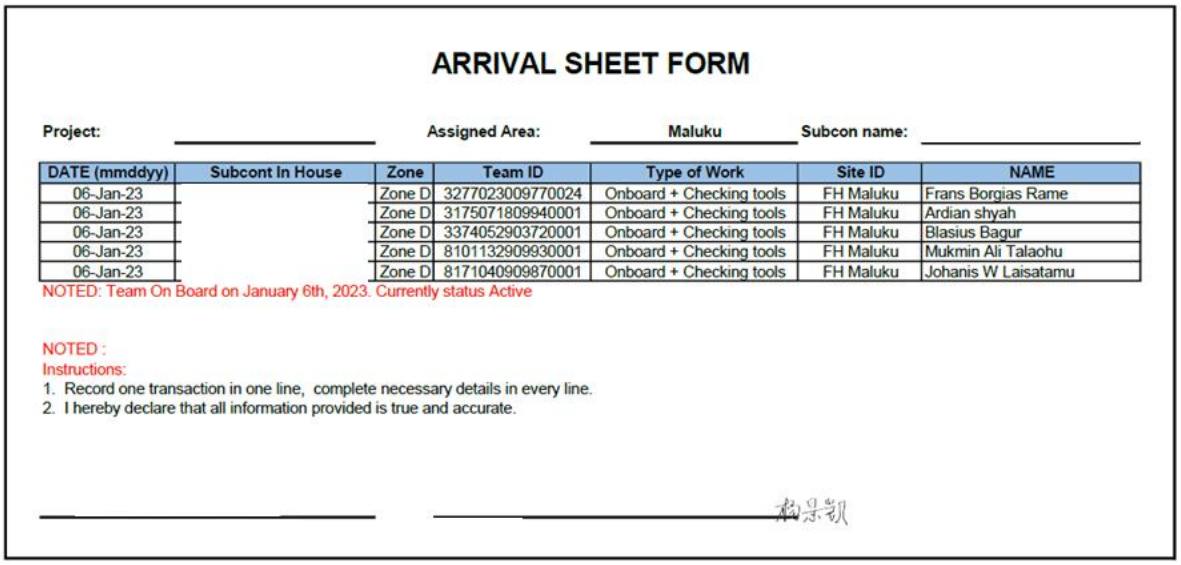
Setelah dokumen berhasil dienkripsi maka data akan masuk ke database dan ditampilkan pada halaman dekripsi berkas yang bisa dilihat pada gambar 6. Untuk mendekripsi berkas maka perlu memilih berkas dan menekan tombol dekripsi file pada halaman dekripsi berkas.

3.5 Antarmuka DokumenTerenkripsi

Gambar 7. Antarmuka Dokumen Terenkripsi

Di gambar 7, menampilkan file yang telah mengalami proses enkripsi, penampilan file yang telah terenkripsi akan dipengaruhi oleh jenis Algoritme enkripsi yang dipakai. Proses enkripsi merubah data asli menjadi format yang tak terbaca, dan hanya bisa dikembalikan ke bentuk semula dengan menggunakan kunci dekripsi yang sama.

3.6 Antarmuka Dokumen Terdekripsi



ARRIVAL SHEET FORM

Project: _____ Assigned Area: Maluku Subcon name: _____

DATE (mmddyy)	Subcont In House	Zone	Team ID	Type of Work	Site ID	NAME
06-Jan-23		Zone D	3277023009770024	Onboard + Checking tools	FH Maluku	Frans Borgias Rame
06-Jan-23		Zone D	3175071809940001	Onboard + Checking tools	FH Maluku	Ardian shyah
06-Jan-23		Zone D	3374052903720001	Onboard + Checking tools	FH Maluku	Blasius Bagur
06-Jan-23		Zone D	8101132909930001	Onboard + Checking tools	FH Maluku	Mukmin Ali Talaohu
06-Jan-23		Zone D	8171040909870001	Onboard + Checking tools	FH Maluku	Johanis W Laisatamu

NOTED: Team On Board on January 6th, 2023. Currently status Active

NOTED :
Instructions:
1. Record one transaction in one line, complete necessary details in every line.
2. I hereby declare that all information provided is true and accurate.

Gambar 8. Antarmuka Dokumen Terdekripsi

Di gambar 8, file akan kembali ke antarmuka aslinya sebelum proses enkripsi setelah didekripsi. Tujuan dari proses dekripsi adalah mengembalikan data yang telah dienkripsi ke bentuk semula menggunakan kunci dekripsi yang sesuai.

3.7 Pengujian

Penulis melakukan dua tahap pengujian pada aplikasi keamanan berkas pada PT. XYZ, yang mencakup penelitian terhadap hasil proses enkripsi file dan dekripsi file menggunakan algoritme AES. Proses pengujian ini dirancang untuk mengumpulkan informasi yang berkaitan dengan kinerja sistem keamanan. Tabel pengujian berikut memberikan contoh hasil dari pengujian enkripsi dan dekripsi yang menggunakan program atau algoritme AES-128.

a. Hasil Pengujian Enkripsi

Tabel 1. Tabel Hasil Pengujian Enkripsi

No	Nama *File* Asli	Ukuran *File* Asli per(KB)	Nama *File* Setelah Dienkripsi	Ukuran *File* Setelah dienkripi(kb)	Waktu Enkripsi (Detik)
1	rekening-koran-sgi.pdf	25.0879 KB	8612-rekening-koran-sgi.pdf	25.0879 KB	0.5831 Detik
2	invoice-kn-0036.pdf	1214.31 KB	13696-invoice-kn-0036.pdf	1214.31 KB	21.6439 Detik
3	asf-mlk-frans-idc-bakti-sgi-0066-os.pdf	260.998 KB	6329-asf-mlk-frans-idc-bakti-sgi-0066-os.pdf	260.998 KB	4.5173 Detik
4	minutes-of-meeting-sp-1.docx	79.7842 KB	64843-minutes-of-meeting-sp-1.docx	79.7842 KB	1.5425 Detik
5	rekapan-petty-cash-2023_sgi.xlsx	51.1064 KB	92553-rekapan-petty-cash-2023_sgi.xlsx	51.1064 KB	1.0440 Detik

Terdapat lima file yang telah dienkripsi. Ukuran file setelah dienkripsi tetap sama dengan ukuran file asli dalam semua kasus. Proses enkripsi berlangsung dengan cepat, dengan waktu enkripsi berkisar antara 0.5831 detik hingga 21.6439 detik. File-file yang dienkripsi memiliki beragam ukuran, mulai dari 25.0879 KB hingga 1214.31 KB. Nama file setelah dienkripsi berbeda dari nama file asli, dengan penambahan nomor atau kode tertentu untuk menunjukkan bahwa file tersebut telah dienkripsi. Dengan demikian, kesimpulan utama adalah bahwa proses enkripsi dilakukan dengan sukses tanpa mengubah ukuran file, dan waktu yang diperlukan untuk proses tersebut relatif cepat.

b. Hasil Pengujian Dekripsi

Tabel 2. Tabel Hasil Pengujian Dekripsi

No	Nama *File* Enkripsi	Ukuran *File* Asli per(KB)	Nama *File* Setelah Didekripsi	Ukuran *File* Setelah didekripsi(kb)	Waktu Dekripsi (Detik)
1	8612-rekening-koran-sgi.pdf	25.0879 KB	8612-rekening-koran-sgi.pdf	25.0879 KB	0.4586 Detik
2	13696-invoice-kn-0036.pdf	1214.31 KB	13696-invoice-kn-0036.pdf	1214.31 KB	19.5293 Detik
3	6329-asf-mlk-frans-idc-	260.998 KB	6329-asf-mlk-frans-idc-	260.998 KB	4.3051 Detik

	bakti-sgi-0066-os.pdf		bakti-sgi-0066-os.pdf		
4	64843-minutes-of-meeting-sp-1.docx	79.7842 KB	64843-minutes-of-meeting-sp-1.docx	79.7842 KB	1.4855 Detik
5	92553-rekapan-petty-cash-2023_sgi.xlsx	51.1064 KB	92553-rekapan-petty-cash-2023_sgi.xlsx	51.1064 KB	1.0049 Detik

Ada lima file yang telah dienkripsi dan kemudian didekripsi. Ukuran file setelah didekripsi sama dengan ukuran file asli dalam semua kasus, menunjukkan bahwa proses dekripsi berhasil mengembalikan file ke kondisi semula. Waktu yang dibutuhkan untuk proses dekripsi bervariasi antara 0.4586 detik hingga 19.5293 detik. Nama file setelah didekripsi sama dengan nama file enkripsi, menunjukkan bahwa proses dekripsi mengembalikan nama file ke kondisi semula. Ukuran file yang didekripsi bervariasi, mulai dari 25.0879 KB hingga 1214.31 KB. Dengan demikian, hasil dari proses dekripsi adalah pengembalian file ke kondisi semula tanpa mengubah ukuran, serta proses dekripsi berlangsung dengan waktu yang bervariasi tergantung pada ukuran dan kompleksitas file.

4. KESIMPULAN

Berdasarkan hasil dan analisis yang dilakukan, penulis menyimpulkan bahwa implementasi sistem aplikasi kriptografi AES-128 pada PT. XYZ telah membuktikan keberhasilannya dalam mengamankan dokumen. Proses enkripsi dilakukan dengan cepat, dengan rentang waktu antara 0.5831 hingga 21.6439 detik, sementara proses dekripsi membutuhkan waktu antara 0.4586 hingga 19.5293 detik. Ukuran file setelah enkripsi dan dekripsi tetap sama dengan ukuran file asli dalam semua kasus, menunjukkan bahwa integritas data berhasil dipertahankan. Nama file setelah proses enkripsi dan dekripsi tetap konsisten, mengindikasikan keberhasilan dalam menjaga kerahasiaan dan keutuhan data. Langkah-langkah ini membantu menghindari potensi kebocoran data dan memastikan keamanan dokumen. Dokumen yang dienkripsi langsung menuju ke database, sehingga kerahasiaan informasi tetap terjaga. Dengan demikian, sistem aplikasi ini telah memenuhi komponen utama kriptografi, yakni kerahasiaan, keutuhan, dan keaslian data.

c. DAFTAR PUSTAKA

[1] Andika, R. R. D., & Mulyati, S. (2022). PENERAPAN ALGORITME AES-128 UNTUK APLIKASI PENGARSIPAN DOKUMEN BERBASIS WEB PADA PT STUDIO INOVASI TEKNOLOGI APPLICATION OF AES-128 ALGORITHM FOR WEB-BASED DOCUMENT ARCHIVING APPLICATION AT PT STUDIO INOVASI TEKNOLOGI. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia*, 411–420.

[2] Andriyanto, M. R., & Sukmasetya, P. (2022). Penerapan Algoritme *Advanced Encryption Standard* (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace. *Journal of Computer System and Informatics (JoSYC)*, *4*(1), 179–187. https://doi.org/10.47065/josyc.v4i1.2451

[3] Azhari, M., Perwitosari, J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritme Kriptografi *Advanced Encryption Standard* (AES). *Jurnal Pendidikan Sains Dan Komputer*, *2*(1), 2809–476. https://doi.org/10.47709/jpsk.v2i1.1390

[4] Cristy, N., & Riandari, F. (2021). Niolinda Cristy 1 , Fristi Riandari 2 [Implementasi Metode *Advanced Encryption Standard* (AES 128 Bit) Untuk Mengamankan Data Keuangan. *JIKOMSI [Jurnal Ilmu Komputer Dan Sistem Informasi]*, *4*(2), 75.

[5] Randi, A., Lazuardy, K., Chandra, S., & Dharma, A. (2020). Implementasi Algoritme *Advanced Encryption Standard* pada Aplikasi Chatting berbasis Android. *JIKOMSI Jurnal Ilmu Komputer Dan Sistem Informasi*, *3*(2), 1–10.

[6] Sidiq, R. F., Erwin, R., Rahayu, G., & Supriatna, A. D. (2023). Implementasi Kriptografi *Advanced Encryption Standard* dan Least Significant Bit untuk Keamanan Pesan Email dalam Gambar. *Jurnal Algoritme*, *20*(2), 305–315. https://jurnal.itg.ac.id/

[7] Wahyudi. (2022). Penerapan Metode *Advanced Encryption Standard* (AES) Pada Keamanan Password Server Cloud Universitas Budi Darma. *Nasional Teknologi Informasi Dan Komputer)*, *6*(1). https://doi.org/10.30865/komik.v6i1.5769

[8] Widodo, B. E., & Purnomo, A. S. (2020). IMPLEMENTASI *ADVANCED ENCRYPTION STANDARD* PADA ENKRIPSI DAN DEKRIPSI DOKUMEN RAHASIA DITINTELKAM POLDA DIY. *Jurnal Teknik Informatika (Jutif)*, *1*(2), 69–77. https://doi.org/10.20884/1.jutif.2020.1.2.21

[9] L. Mustika, "Implementasi Algoritma AES untuk Pengamanan Login dan Data Customer pada E-Commerce Berbasis Web," JURIKOM (Jurnal Riset Komputer), vol. 7, no. 1, pp. 148–155, Feb. 2020, doi: 10.30865/jurikom.v7i1.1943

[10] F. A. Sitorus, N. B. Nugroho, and U. F. S. S. Pane, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data Transaksi Penjualan Pada PT. Mitsubishi Electric Indonesia," Jurnal CyberTech, pp. 1–15, 2020, [Online]. Available: https://ojs.trigunadharma.ac.id/