5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
7 September 2024 – Jakarta, Indonesia
Volume 3, Nomor 2, September 2024 – ISSN 296-8628 (*online*)

KRIPTOGRAFI MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES-128) UNTUK MENGAMANAN FILE KEPENDUDUKAN PADA KELURAHAN SUDIMARA BARAT

Andika Pratama[1*], Painem[2]

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

Email: [1*]2011501513@student.budiluhur.ac.id, [2]painem@budiluhur.ac.id
(* : corresponding author)

Abstrak- Kerahasiaan data adalah salah satu aspek terpenting dalam keamanan informasi pribadi. Data pribadi seperti Nomor Induk Kependudukan (NIK), Kartu Keluarga, dan informasi kependudukan lainnya memerlukan perlindungan yang sangat ketat untuk mencegah akses oleh pihak-pihak yang tidak berwenang. Pengamanan data ini sangat penting karena jika data tersebut jatuh ke tangan yang salah dan disalahgunakan, hal tersebut dapat mengakibatkan kerugian yang signifikan bagi individu yang bersangkutan. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan sistem yang efektif dalam mengamankan data dengan menggunakan teknik enkripsi dan dekripsi yang canggih.Penelitian ini fokus pada perlindungan data kependudukan yang disimpan dalam berbagai format file, seperti PDF, DOC, XLS, dan TXT. Untuk mencapai tujuan tersebut, metode enkripsi dan dekripsi yang digunakan adalah AES 128 Bit, yang dikenal karena kemampuannya dalam menyediakan tingkat keamanan yang tinggi. Proses enkripsi ini mengubah data asli menjadi bentuk *ciphertext*, yang sulit untuk diakses tanpa kunci dekripsi yang tepat. Dengan cara ini, bahkan jika file yang terenkripsi dicuri atau diakses secara tidak sah, data tersebut tetap tidak dapat dibaca tanpa proses dekripsi yang sesuai. Sistem ini dirancang untuk menangani berbagai format file dan memastikan bahwa data kependudukan yang terenkripsi dapat didekripsi kembali dengan akurasi tinggi. Dalam uji coba sistem, ditemukan bahwa persentase kemiripan antara file asli dan file yang telah didekripsi mencapai 90%. Hal ini menunjukkan bahwa sistem enkripsi dan dekripsi yang dikembangkan tidak hanya melindungi data dari akses tidak sah, tetapi juga memastikan bahwa integritas data tetap terjaga setelah proses dekripsi. Dengan demikian, sistem ini diharapkan dapat memberikan solusi yang efektif untuk menjaga kerahasiaan dan keamanan data kependudukan.

Kata Kunci: Kependudukan, Enkripsi, Dekripsi.

CRYPTOGRAPHY USING ADVANCED ENCRYPTION STANDARD (AES-128) ALGORITHM TO SECURE POPULATION FILES IN SUDIMARA BARAT VILLAGE

Abstract- *Data confidentiality is one of the most important aspects of personal information security. Personal data such as Population Identification Number (NIK), Family Card, and other population information require very strict protection to prevent access by unauthorized parties. Securing this data is very important because if the data falls into the wrong hands and is misused, it can result in significant losses for the individual concerned. Therefore, this study aims to develop an effective system for securing data using sophisticated encryption and decryption techniques. This study focuses on protecting population data stored in various file formats, such as PDF, DOC, XLS, and TXT. To achieve this goal, the encryption and decryption method used is AES 128 Bit, which is known for its ability to provide a high level of security. This encryption process converts the original data into ciphertext, which is difficult to access without the right decryption key. In this way, even if the encrypted file is stolen or accessed unauthorizedly, the data remains unreadable without the appropriate decryption process. This system is designed to handle various file formats and ensure that encrypted population data can be decrypted again with high accuracy. In the system trial, it was found that the percentage of similarity between the original file and the decrypted file reached 90%. This shows that the encryption and decryption system developed not only protects data from unauthorized access, but also ensures that data integrity is maintained after the decryption process. Thus, this system is expected to provide an effective solution to maintain the confidentiality and security of population data.*

Keywords*: Population, Encryption, Decryption*

1. PENDAHULUAN

Data atau informasi adalah data yang penting dan harus dilindungi agar tidak diketahui oleh orang lain. 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.

Kerahasian data terkait dengan kebocoran data, terutama data pribadi. Menurut UU Perlindungan Data Pribadi Pasal 1 Ayat 1, Data pribadi adalah setiap data individu yang dapat diidentifikasi atau dapat digabungkan

dengan informasi lainnya melalui sistem elektronik dan/atau nonelektronik. Data kependudukan juga merupakan bagian dari data pribadi yang harus dijaga kerahasiannya. Contohnya Kelurahan Sudimara Barat menyimpan data kependudukan area Sudimara Barat. Penyimpanan data pada kelurahan tersebut di simpan pada komputer secara offline dan tidak mempunyai backup penyimpanan data, sehingga rentan untuk dibobol oleh pihak lain. Dan belum ada aplikasi dengan menggunakan metode tertentu dalam mengamankan penyimpanan data.

Berdasarkan latar belakang dan masalah diatas 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 terkait Kriptografi beberapa penelitian yang sudah dilakukan [1] . Sistem ini mempunyai fungsi untuk mengenkripsi atau mengamankan data Adminstrasi Kependudukan dengan memanfaatkan metode enkripsi SHA-1. Hasil enkripsi dari metode ini menghasilkan file dengan format .txt. Penelitian serupa lainnya yang dilakukan [2] yaitu dengan mengimplementasikan metode Algoritma Huffman dan Enkripsi Rivest Shamir Adleman (RSA) untuk mengenkripsi file dokumen dengan format file hasil enkripsi yaitu .doc dan .txt yang sudah dikompresi. Penelitian juga dilakukan oleh [3] dengan mengkombinasikan metode AES dan DES untuk enkripsi file dokumen proposal yang menghasilkan file txt dengan isi *ciphertext*.sistem yang dirancang berfungsi untuk mengamankan data dokumen word menggunakan Algoritma Enkripsi Triple DES dengan hasil enkripsi menggunakan format *.usb.

2. METODE PENELITIAN

2.1 Kajian Teori

Dalam penelitian ini, peneliti mengacu pada beberapa penelitian yang telah dilakukan sebelumnya, antara lain oleh [1] Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1. Penelitian ini mengamankan Data Administrasi Kependudukan dengan menggunakan Algoritma SHA-1 dengan mengenkripsi *plaintext* data kependudukan menjadi *ciphertext*. Data yang dienkripsi berbentuk text atau data string yang berkaitan dengan data kependudukan seperti NIK, Nama, dan sejenisnya. Hasil enkipsi dari sistem ini menggunakan format file *.txt. Implementasi dari sistem ini menggunaan perangkat lunak Visual Basic atau berbasis dekstop.

Penelitian lainnya yang menjadi acuan adalah penelitian yang dilakukan oleh [2] mengenai Implementasi Algoritma Enkripsi Rivest Shamir Adleman (Rsa) dan Algoritma Kompresi Huffman bersama-sama dalam File Dokumen. Impelementasi sistem ini menerapkan kombinasi 2 metode yaitu Rivest Shamir Adleman (RSA) untuk proses enkripsi dan dekripsinya dan Kompresi Huffman untuk proses kompresi agar mengurangi ukuran dari file dokumen. Format file atau dokumen yang dienkripsi dapat berupa file pdf, doc, dan txt, dan file hasil enkripsinya menggunakan format *.doc dan *.txt.

Studi tambahan yang relevan adalah penelitian yang dilakukan oleh [3] tentang kombinasi algoritma kriptografi AES dan DES untuk enkripsi file dokumen proposal. Ada perbedaan utama antara metode enkripsi AES dan DES, yaitu bahwa plaintext dalam blok DES dibagi menjadi dua bagian sebelum algoritma utama dimulai, sedangkan dalam blok AES seluruh blok diproses untuk Selama implementasi, sistem ini mengirimkan hasil enkripsi dalam format file yang sesuai dengan input.

Penelitian tentang data penduduk [4], yang mencakup informasi tentang keberadaan seseorang di negara tersebut, merupakan penelitian tambahan yang menjadi acuan. Keamanan dan kerahasiaan data ini sangat penting karena mereka berkaitan dengan identitas seseorang. Sistem keamanan data harus diterapkan untuk melindungi data dari pencurian dan manipulasi. Kriptografi adalah bidang ilmu yang mempelajari metode matematika yang berkaitan dengan aspek keamanan data dan informasi seperti keabsahan, integritas, dan autentikasi data. Salah satu metode untuk mengamankan data dan informasi adalah Advanced Encryption Standard (AES). Algoritma AES dapat menghasilkan pesan yang tidak dapat dibaca atau dipahami oleh manusia (enkripsi) dan menghasilkan pesan yang sama seperti plaintext awal yang diimput (dekripsi). AES juga dapat digunakan untuk mengamankan data penduduk Dinas Kependudukan dan Pencatatan Sipil.

Penelitian lainnya yang menjadi acuan adalah penelitian yang dilakuan oleh [5] Keamanan data kerahasiaan data sangatlah penting. Keamanan data dan keamanan data yang tidak dapat di pisahkan. Keamanan data dalam ilmu Komputer hadir dalam bentuk *Advanced Encryption Standard* (AES). AES merupakan salah satu bentuk keamanan data yang dapat digunakan untuk melindungi data dari intrusi atau serangan pihak lain. AES sendiri merupakan salah satu bentuk enkripsi dan terdiri dari beberapa proses untuk mengenkripsi data.

Penelitian lainnya yang menjadi acuan adalah penelitian yang dilakuan oleh [6] Meskipun keamanan sangat penting untuk sistem informasi, pemilik dan pengelola sistem informasi sering kali mengabaikan masalah keamanan. Salah satu hasil dari 444 kejadian adalah pembobolan data 2,3 juta pemilih Indonesia. Data dalam

bentuk file PDF berukuran 2,36 GB. Untuk mengatasi masalah ini, gunakan konsep enkripsi untuk melindungi data. Deskripsi dan enkripsi adalah dua konsep yang sangat penting dalam kriptografi.

Tujuan dari penelitian ini adalah untuk melindungi dokumen menggunakan algoritma AES, yang membuat file yang lulus uji enkripsi menjadi tidak dapat dibaca. Algoritma ini diperlukan untuk mencegah penyadapan dan pembajakan file yang berisi informasi penting bagi pengguna dan menjaga integritas file tersebut.

Penelitian lainnya yang menjadi acuan adalah penelitian yang dilakuan oleh [7] Kebutuhan akan bantuan yang sangat besar untuk menyelesaikan banyak tugas dengan cepat, akurat, dan tepat telah meningkat sebagai akibat dari kemajuan dalam teknologi komputer dan telekomunikasi. Namun, karena pihak yang tidak berwenang dapat menyadap data sensitif, keamanan data dianggap penting. Kriptografi adalah bidang keilmuan yang berkaitan dengan teknik enkripsi data, dan merupakan salah satu metode terbaik untuk keamanan data yang dapat meningkatkan keamanan data dan informasi kita. Dua kategori enkripsi berbeda:modern dan klasik, masing-masing menggunakan kunci asimetris dan simetris. *Advanced Encryption Standard* (AES), atau Rijndael, adalah kunci simetris. AES adalah algoritma enkripsi aman yang dapat melindungi data dan informasi sensitif dengan menggunakan berbagai teknik enkripsi dan dekripsi dengan panjang kunci 128 bit, 192 bit, dan 256 bit. Dalam versi 2001, algoritma AES menggunakan empat transformasi dasar: *subbyte*, *shift-row*, *mix-column*, dan urutan transformasi *AddRoundKey*. Untuk dekripsi, algoritma AES menggunakan seluruh transformasi dasar algoritma kecuali *AddRoundKey* dengan rangkaian transformasi *invShiftRows*, yang memungkinkan data dan informasi sensitif.

Studi tentang keamanan data dan informasi komputer yang sangat penting [8] juga menarik perhatian. Salah satu masalah keamanan data adalah biaya kuliah. Data keuangan SPP adalah kumpulan data sensitif sekolah yang tersedia untuk pengelola sekolah dalam bentuk catatan pembayaran atau ringkasan. Pencuri data dan informasi dapat memanipulasi data. Jadi, enkripsi adalah cara untuk melindungi data. Advanced Encryption Standard (AES) adalah salah satu algoritma atau metode enkripsi yang digunakan. AES memiliki loop kunci untuk proses enkripsi dan dekripsi, dan dipilih karena memberikan tingkat keamanan yang tinggi yang dihasilkan oleh kunci privat yang kompleks, yang memastikan bahwa data yang dilindungi tetap rahasia.

Studi lain yang relevan adalah studi yang dilakukan oleh [9] Keamanan data dan data elektronik sangat penting. Salah satu masalah keamanan data adalah biaya kuliah. Data keuangan SPP adalah kumpulan data sensitif sekolah yang tersedia untuk pengelola sekolah dalam bentuk catatan pembayaran atau ringkasan. Pencuri data dan informasi dapat memanipulasi data. Jadi, enkripsi adalah cara untuk melindungi data. Advanced Encryption Standard (AES) adalah salah satu algoritma atau metode enkripsi yang digunakan. AES memiliki loop kunci untuk proses enkripsi dan dekripsi, yang memberikan tingkat keamanan yang tinggi berdasarkan kunci privat yang kompleks yang memastikan bahwa data yang dilindungi tetap rahasia.

Penelitian lainnya yang menjadi acuan adalah penelitian yang dilakuan oleh [10] Setiap bisnis memiliki data yang harus disimpan secara digital. Karena perusahaan semakin berkembang, kapasitas penyimpanan yang diperlukan pun meningkat. Faktor-faktor yang berkaitan dengan keamanan data juga harus diperhatikan. Enkripsi adalah cara untuk melindungi data. Penelitian ini menganalisis algoritma enkripsi, dan hasilnya menunjukkan bahwa algoritma AES disarankan untuk mengamankan penggunaan file. Dalam penelitian ini, kami menyarankan untuk menganalisis skema enkripsi AES dengan beberapa parameter. Pengujian berbagai format file terenkripsi dan terdekripsi, terutama dengan mempertimbangkan biaya enkripsi, waktu komputasi, dan ukuran file untuk format dokumen dan gambar, serta durasi penggunaan file audio dan video yang terkait. lalu dua ekstensi file digunakan untuk menguji masing-masing format file yang dipilih. Hasil pengujian menunjukkan bahwa algoritma enkripsi AES bekerja dengan baik untuk sejumlah format file. AES-128 dapat mengenkripsi file dengan baik, tetapi memerlukan waktu komputasi untuk beberapa ekstensi file yang diuji. Ukuran file memengaruhi jumlah waktu yang diperlukan untuk proses enkripsi dan dekripsi algoritma AES. Jumlah waktu yang dibutuhkan untuk mengolah file berkorelasi positif dengan ukuran file yang digunakan.

2.2 *Plaintext* Dan *Chipertext*

Pada gambar 1 menjelaskan Sesuai dengan pengertian Kriptografi diatas, teknik dari kriptografi adalah mengubah pesan biasa menjadi pesan yang tidak dapat dimengerti maknanya. Kriptografi mempunyai dua istilah dalam proses penyandiannya. Pesan biasa yang akan diubah disebut sebagai *plaintext*, sedangkan hasil dari perubahan *plaintext* disebut sebagai *ciphertext*.

Plaintext dapat berupa teks, file, atau format data lainnya. Ini adalah data asli yang berisi pesan biasa yang akan diubah maknanya menjadi *ciphertext*. Sedangkan, *Ciphertext* adalah pesan yang telah disandikan sehingga tidak bermakna lagi.

Plaintext:

Program Studi Teknik Informatika

Chipertext:

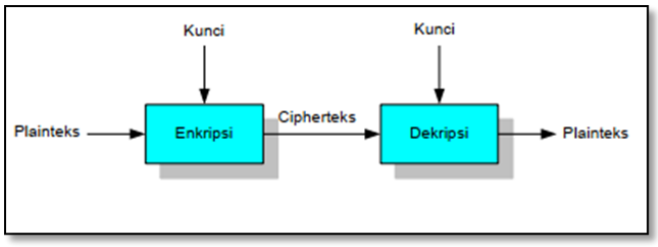
SURJUDP VWXGL WHNQLQ LQIRUPDWLND

Gambar 1. *Plaintext* dan *Chipertext*

2.3 *Enkripsi dan Dekripsi*

Pada gambar 2 menjelaskan Proses Enkripsi & Dekripsi bisa dikatakan sebagai proses utama dalam hal mengamankan sebuah data. Dimana, data berbentuk teks maupun file yang awalnya berupa pesan atau *plaintext* dirubah menjadi *ciphertext* agar tidak dapat dibaca dan dipahami maknanya oleh pihak yang tidak berhak dan menjaga kerahasaiaan data tersebut.

Enkripsi adalah proses menyandikan *plaintext* (pesan biasa) menjadi *ciphertext* (pesan tersembunyi) yang tidak dapat dipahami. Dekripsi adalah proses sebaliknya, mengubah *ciphertext* menjadi *plaintext* atau pesan yang dapat dibaca dan dipahami.



Gambar 2. Enkripsi dan Dekripsi

2.4 Kunci Simetri

Setiap proses Enkripsi dan Dekripsi dalam ilmu Kriptografi mempunyai sebuah kunci simetri yang berfungsi sebagai kunci utama dalam membuka pesan yang akan dienkripsi maupun pesan yang akan didekripsi. Menurut (Rosianto, H. dkk (2012) Kunci simetri adalah jenis kunci kriptografi yang paling umum digunakan untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan tersebut.

Ada beberapa keuntungan menggunakan kunci simetri yang sudah diketahui, termasuk kecepatan operasi yang lebih tinggi, meskipun peningkatan ukuran file berkorelasi langsung dengan kecepatan proses enkripsi dan dekripsi; waktu yang dibutuhkan untuk enkripsi dan dekripsi bergantung pada ukuran file, dan karena kecepatan yang cukup tinggi, dapat digunakan pada sistem real-time. Namun, kelemahannya adalah bahwa setiap pengiriman pesan memerlukan kunci yang berbeda untuk setiap pengguna, sehingga sulit untuk mengelola kunci tersebut.

Jadi, pembuat pesan dan penerimanya harus memiliki kunci yang sama persis. Sebagai contoh, jika ingin masuk ke dalam sebuah rumah maka kita memerlukan kunci yang sesuai dengan pintunya. Begitupun juga Kriptografi dalam proses Enkripsi dan Dekripsinya memerlukan sebuah kunci agar data yang bersifat rahasia dapat dibuka oleh pihak yang mempunyai kunci dan wewenang.

2.4.1 Algoritma AES 128 Bit

Pada gambar 3 menjelaskan Salah satu algoritma block chiper yang memiliki sifat simetri, *Advanced Encryption Standard* (AES) digunakan sebagai standar kriptografi terbaru oleh NIST pada tahun 2001. AES menggunakan kunci simetri selama proses enkripsi dan dekripsi.

	Panjang Kunci	Panjang Blok	Jumlah Putaran
AES-128	4	4	10
AES-129	6	4	12
AES-256	8	4	14

Gambar 3. Jenis Algoritma AES

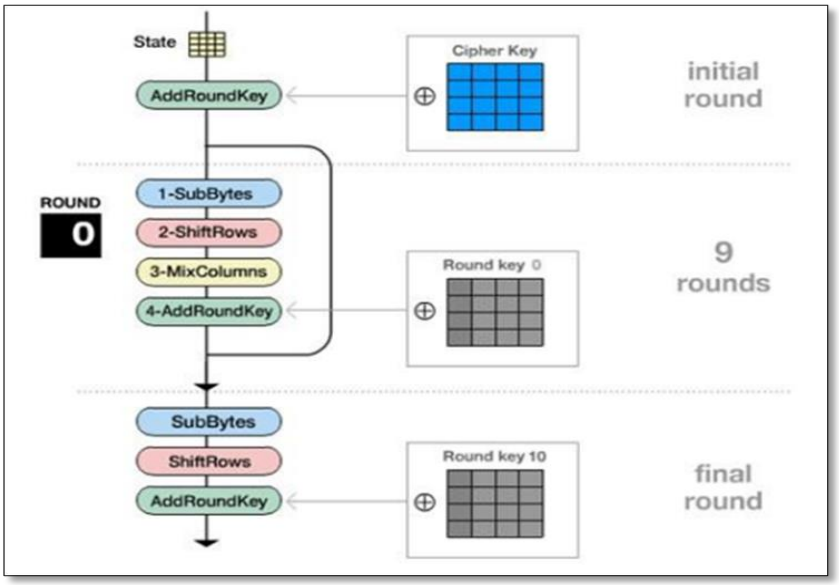
Dalam penelitian ini, Algoritma AES 128 Bit digunakan, yang memiliki 10 putaran enkripsi dan 4 tranformasi putaran untuk dekripsi.

1. *SubBytes* menggunakan tabel substitusi (S-BOX) untuk menukar isi dari byte.
2. *ShiftRows* adalah proses pergeseran blok per baris pada state array
3. *MixColumn* adalah proses mengalikan blok data (pengacakan) di masing-masing state array.
4. kunci bulat dan array dengan hubungan XOR

Dalam proses dekripsi menggunakan tahap berikut

1. Setiap blok baris memiliki *InvShiftRows* yang mengubah bit ke kanan.
2. Tabel *Inverse* S-Box memetakan semua elemen pada state.
3. *InvMixColumn* Matriks AES dikalikan untuk setiap kolom state.
4. Tambahkan *Key Round* untuk menggabungkan *state array* dan *key round* dengan hubungan XOR.

Selama proses enkripsi awal, seperti yang ditunjukkan pada gambar nomor 4, input file atau data yang telah disalin ke dalam state akan melalui tahap transformasi *AddRoundKey*. Setelah tahap transformasi ini selesai, state akan melalui proses *SubBytes, ShiftRows, MixColumns,* dan *AddRoundKey* selama sepuluh putaran atau putaran. Proses AES 128 Bit dikenal sebagai "fungsi putaran". Dalam AES 128 Bit, state tidak melewati proses tranformasi *MixColumns* pada putaran atau putaran terakhir; sebaliknya, putaran atau putaran terakhir adalah hasil dari enkripsi AES 128 Bit. Proses ini digambarkan dalam Gambar 4.



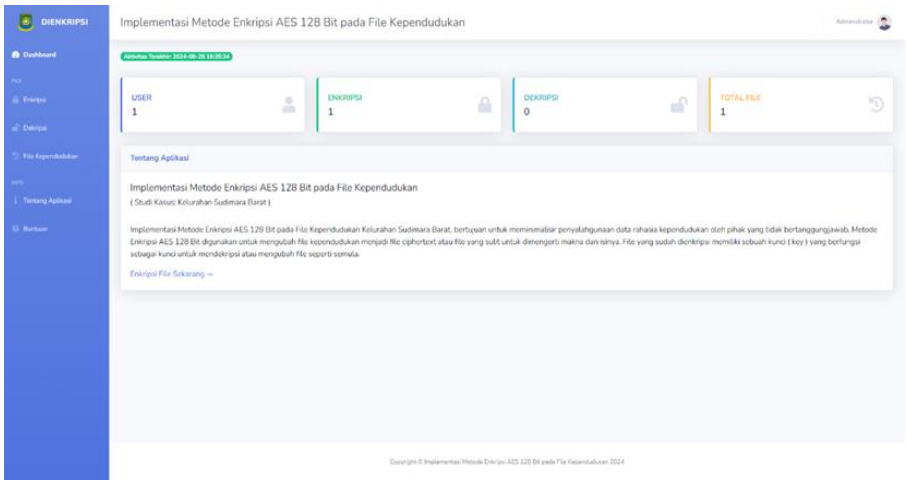
Gambar 4. Proses Enkripsi AES 128

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Metode

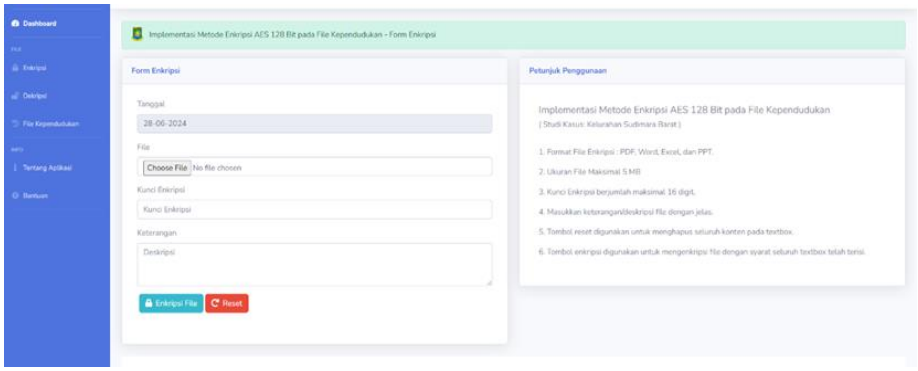
Tahap implementasi adalah penerapan cara kerja sistem dari analisis dan perancangan sebelumnya ke dalam bentuk pemrograman yang mana sistem telah siap untuk digunakan. Pada langkah implementasi ini, script program akan dijelaskan tentang proses enkripsi menggunakan metode AES 128 Bit pada file kependudukan kelurahan Sudimara Barat. Program ini dijalankan dengan bahasa pemrograman PHP dan database manajemen sistem

MySQL. Script yang digunakan untuk menerapkan teknik enkripsi AES 128 Bit pada File Kependudukan Kelurahan Sudimara Barat.



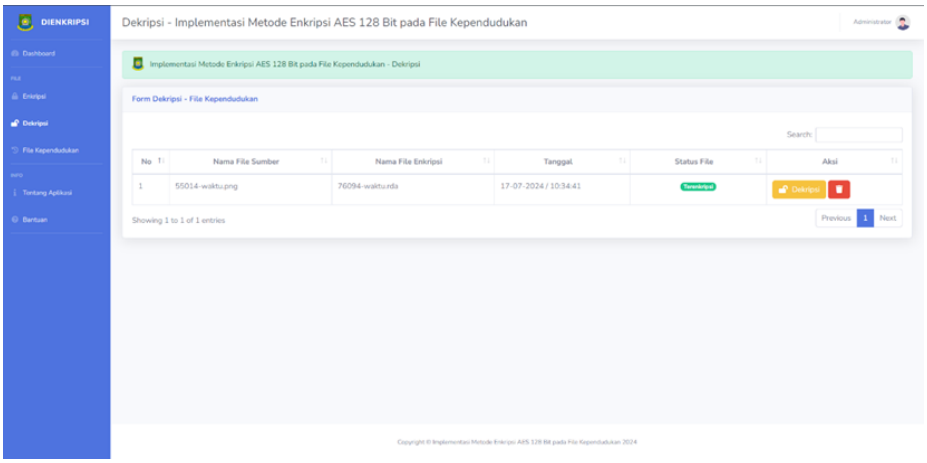
Gambar 5. Halaman Dashboard

Gambar 5 menjelaskan Pada Halaman dashboard adalah halaman utama sistem yang telah dibuat. Ini akan muncul pertama kali saat user masuk ke sistem dan berisi informasi tentang sistem, seperti yang ditunjukkan pada gambar.



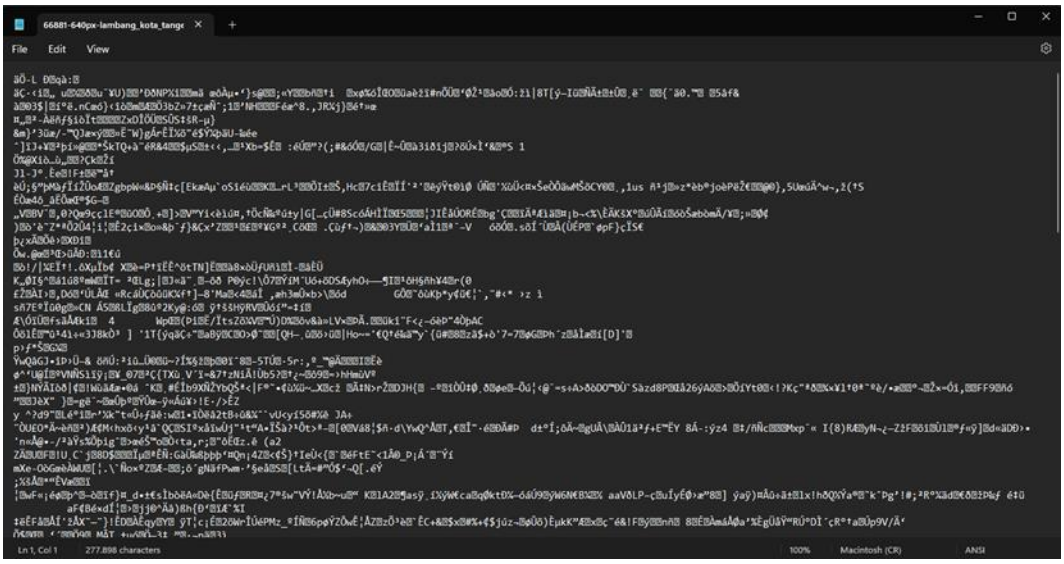
Gambar 6. Halaman Enkripsi

Gambar 6 menjelaskan Halaman Dekripsi digunakan untuk mendekripsi file kependudukan yang telah dienkripsi. Ini mendaftar semua file yang telah dienkripsi, dan jika Anda menekan tombol "Dekripsi", Anda akan dibawa ke halaman berikutnya, "Dekripsi", di mana Anda juga dapat menghapus file.



Gambar 7. Halaman Dekripsi

Gambar 7 menjelaskan Halaman Dekripsi digunakan untuk mendekripsi file kependudukan yang telah dienkripsi. Ini mendaftar semua file yang telah dienkripsi, dan jika Anda menekan tombol "Dekripsi", Anda akan dibawa ke halaman berikutnya, "Dekripsi", di mana Anda juga dapat menghapus file. Halaman ini dapat dilihat pada gambar di bawah ini.



Gambar 8. Hasil Enkripsi

Gambar 8 menjelaskan Setelah file dienkripsi menggunakan metode AES 128 bit, hasilnya berupa file dengan ekstensi *.rda, yang dapat dibuka menggunakan notepad. Metode AES juga menggunakan fitur randomize karakter untuk meningkatkan keamanan file yang telah dienkripsi. Hasil enkripsi dari file kependudukan, yang mencakup data Kelurahan Sudimara barat dalam format file Excel, dapat dilihat di sini. Hasil enkripsi tampak pada gambar.

3.2 Hasil Pengujian

Pada tahap ini terdapat tabel yang berisi dari hasil pengujian proses enkripsi dan dekripsi file.

Tabel 1 Tabel hasil pengujian Enkripsi

No.	Nama File	Nama File Enkripsi	Ukuran File Setelah Enkripsi	Durasi Enkripsi (Detik)	Keterangan
1	test-plagiat.pdf	86728-test-plagiat.rda	2118.99 KB	40.22 Detik	Berhasil
2	123.txt	29309-123.rda	1.21387 KB	0.02 Detik	Berhasil
3	laporan-penduduk.xlsx	30932laporan penduduk.rda	9.96191 KB	0.22 Detik	Berhasil
4	laporan-kkp.docx	42869-laporan-kkp.rda	469.667 KB	9.26 Detik	Berhasil

Tabel 2 Tabel hasil pengujian Dekripsi

No.	Nama File	Nama File Enkripsi	Ukuran File Setelah Enkripsi	Durasi Dekripsi(Detik)	Keterangan
1	test-plagiat.pdf	86728-test-plagiat.rda	2118.99 KB	32.53 Detik	Berhasil
2	123.txt	29309-123.rda	1.21387 KB	0.03 Detik	Berhasil
3	laporan-penduduk.xlsx	30932laporan penduduk.rda	9.96191 KB	0.15 Detik	Berhasil
4	laporan-kkp.docx	42869-laporan-kkp.rda	469.667 KB	7.17 Detik	Berhasil

Untuk tabel 1 dan tabel 2 menjelaskan tentang pengujian dari proses enkripsi dan dekripsi dan yang berbeda antara tabel 1 dan tabel 2 adalah waktu pelaksaanya

4. KESIMPULAN

Hasil penelitian tentang penerapan Metode Enkripsi AES 128 Bit pada File Kependudukan Kelurahan Sudimara Barat menunjukkan bahwa penerapan metode ini pada file kependudukan dapat mengurangi kebocoran dan penyalahgunaan data, serta menjaga keamanan file kependudukan, yang dianggap penting untuk dijaga kerahasiaannya.

DAFTAR PUSTAKA

[1] L. Silalahi, A. Sindar, and S. Pelita Nusantara, "Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1," *Jurnal Nasional Komputasi dan Teknologi Informasi*, vol. 3, no. 2, pp. 182–186, 2020.

[2] A. I. Auliyah, "Indonesian Journal of Data and Science Implementasi Kombinasi Algoritma Enkripsi Rivest Shamir Adleman (Rsa) dan Algoritma Kompresi Huffman Pada File Document," *Indonesian Journal of Data and Science*, vol. 1, no. 1, pp. 23–28, 2020.

[3] C. Irawan and A. Winarno, "Kombinasi Algoritma Kriptografi AES dan DES Untuk Enkripsi File Dokumen Proposal," *SENDIU 2020*, pp. 28–35, 2020.

[4] I. Asih, 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," *Journal of Computer System and Informatics (JoSYC)*, vol. 1, no. 2, pp. 54–60, 2020.

[5] N. Wachid Hidayatulloh, M. Tahir, H. Amalia, N. Afdlolul Basyar, A. F. Prianggara, and M. Yasin, "Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data," *Digital Transformation Technology (Digitech)* | *e*, vol. 3, no. 1, pp. 1–10, 2023, doi: 10.47709/digitech.v3i1.2293.

[6] J. Handoyo and Y. M. Subakti, "Keamanan Dokumen Menggunakan Algoritma Advanced Encrytion Standard (AES)," 2020. [Online]. Available: http://www.jurnal.umk.ac.id/sitech

[7] M. Azhari, J. Perwitosari, and F. Ali, "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, doi: 10.47709/jpsk.v2i1.1390.

[8] N. Cristy and F. Riandari, "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]*, vol. 4, no. 2, pp. 75–85, 2021.

[9] R. Nuari and N. Ratama, "Implementasi Algoritma Kriptografi AES (*Advanced Encryption Standard*) 128 Bit Untuk Pengamanan Dokumen Shipping," 2020. [Online]. Available: http://openjournal.unpam.ac.id/index.php/JOAIIA

[10] R. Visdya, H. Chandra, A. Kusyanti, and M. Data, "Analisis Performa Proses Enkripsi dan Dekripsi Menggunakan Algoritme AES-128 Pada Berbagai Format File," 2019. [Online]. Available: http://j-ptiik.ub.ac.id