SENAFTI
SEMINAR NASIONAL MAHASISWA
FAKULTAS TEKNOLOGI INFORMASI

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

PENERAPAN KRIPTOGRAFI DENGAN ALGORITMA AES-128 UNTUK PENGAMANAN DOKUMEN DIGITAL PADA BPJS KESEHATAN

Naufal Afif Fadhlurrohman

[1] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Kota Tangerang, Indonesia

Email: naufalopang89@gmail.com

Abstrak- Dalam era digitalisasi, keamanan dokumen digital menjadi isu yang sangat penting, terutama di sektor kesehatan yang menangani data sensitif. Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan adalah organisasi yang mengelola informasi kesehatan masyarakat Indonesia, termasuk data pribadi pasien, rekam medis, dan informasi keuangan. Untuk melindungi data ini dari ancaman siber seperti akses tidak sah dan pencurian data, diperlukan mekanisme keamanan yang andal. Algoritma Advanced Encryption Standard (AES) dengan kunci 128-bit merupakan salah satu metode kriptografi yang sangat efektif dalam mengamankan data. Kompleksitas matematisnya yang tinggi dan panjang kunci yang memadai menjadikannya pilihan yang tangguh untuk melindungi informasi sensitif dari akses yang tidak sah. Tujuan dari penelitian ini adalah menerapkan algoritma kriptografi Advanced Encryption Standard (AES-128) pada aplikasi pengamanan dokumen digital sehingga dapat menghasilkan aplikasi enkripsi dan dekripsi berbasis web. Hasil yang diperoleh setelah melakukan enkripsi dan dekripsi dokumen digital menggunakan AES-128, maka diperoleh hasil dokumen digital setelah di enkripsi tidak dapat dibuka, kemudian setelah didekripsi, maka dokumen digital akan Kembali seperti semula dan dapat dibuka. Kesimpulannya, algoritma AES-128 bit berhasil diterapkan pada pengamanan dokumen digital di BPJS Kesehatan. Pengamanan dokumen digital dilakukan melalui enkripsi sehingga hanya individu yang mengetahui kunci yang dapat mendekripsi dokumen digital dan mengembalikannya ke bentuk semula. Dengan demikian, dokumen digital tidak dapat diakses oleh pihak yang tidak berhak atau tidak memiliki kunci

Kata Kunci: AES-128, Dokumen Digital, Kriptografi, Enkripsi, Dekripsi

IMPLEMENTATION OF AES-128 CRYPTOGRAPHY FOR ENHANCED DIGITAL DOCUMENT SECURITY AT BPJS KESEHATAN

Abstract- *In the era of digitalization, the security of digital documents has become a crucial issue, especially in the healthcare sector, which handles sensitive data. The Social Security Administering Body (BPJS) Kesehatan is an organization that manages the health information of Indonesian citizens, including personal patient data, medical records, and financial information. To protect this data from cyber threats such as unauthorized access and data theft, a reliable security mechanism is required. The Advanced Encryption Standard (AES) algorithm with a 128-bit key is one of the most effective cryptographic methods for securing data. Its high mathematical complexity and sufficient key length make it a robust choice for protecting sensitive information from unauthorized access. The objective of this research is to implement the Advanced Encryption Standard (AES-128) cryptography algorithm in a digital document security application to create a web-based encryption and decryption application. The results obtained after encrypting and decrypting digital documents using AES-128 show that the encrypted digital documents cannot be opened, but after decryption, the digital documents are restored to their original state and can be opened. In conclusion, the AES-128-bit algorithm has been successfully implemented for digital document security at BPJS Kesehatan. Digital document security is achieved through encryption, so only individuals who know the key can decrypt the digital documents and restore them to their original form. Thus, digital documents cannot be understood by unauthorized parties or those who do not possess the key*.

Keywords*: AES-128, Digital Documents, Cryptography, Encryption, Decryption.*

1. PENDAHULUAN

Dalam era digitalisasi, keamanan dokumen digital menjadi isu yang sangat penting, terutama di sektor kesehatan yang menangani data sensitif. Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan adalah organisasi yang mengelola informasi kesehatan masyarakat Indonesia, termasuk data pribadi pasien, rekam medis, dan informasi keuangan. Untuk melindungi data ini dari ancaman siber seperti akses tidak sah dan pencurian data, diperlukan mekanisme keamanan yang andal. Salah satu metode yang paling efektif untuk menjaga keamanan data

adalah melalui kriptografi, khususnya dengan menggunakan algoritma Advanced Encryption Standard (AES) 128-bit [1].

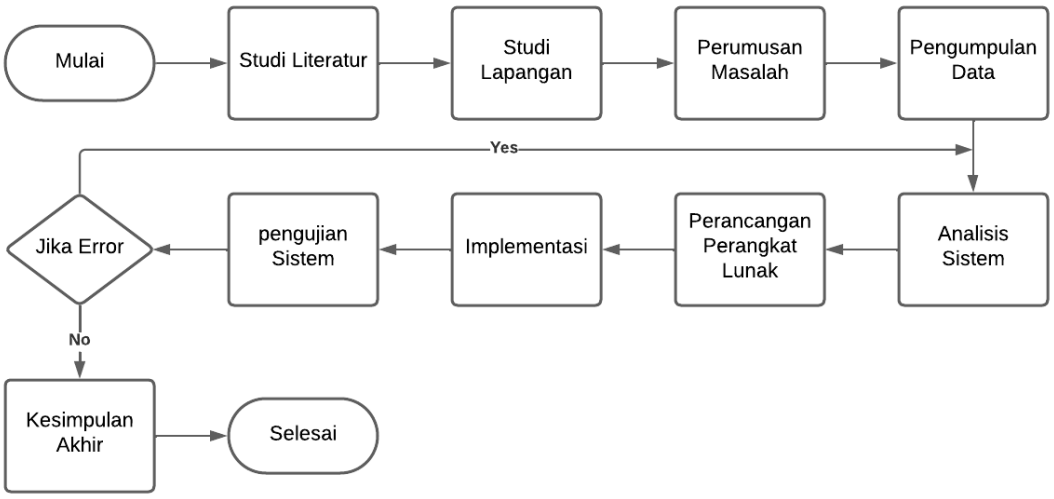
BPJS Kesehatan menghadapi tantangan signifikan dalam menjaga kerahasiaan, integritas, dan ketersediaan dokumen digitalnya. Ancaman terhadap keamanan data semakin meningkat seiring dengan berkembangnya teknologi dan metode serangan yang semakin canggih [2], [4]. Tanpa perlindungan yang memadai, data sensitif yang disimpan oleh BPJS Kesehatan dapat dengan mudah menjadi target bagi penjahat siber, yang dapat berdampak buruk pada kepercayaan masyarakat dan operasional organisasi.

Penelitian sebelumnya di Indonesia telah menunjukkan berbagai pendekatan untuk meningkatkan keamanan data digital. Sebagai contoh, penelitian oleh Fachrozi dan Fahmi dengan judul "Penerapan Metode AES-128 Untuk Pengamanan Data Absensi FingerPrint Di Balai Penelitian Sungei Putih" [3], menyoroti Implementasi algoritma enkripsi AES 128 pada sistem keamanan database menjamin integritas dan kerahasiaan data absensi, sehingga efektif mencegah akses atau modifikasi data oleh pihak yang tidak berwenang.

Penelitian ini mengusulkan untuk membuat system berbasis website dengan menerapkan algoritma kriptografi AES 128-bit dalam pengamanan dokumen digital di BPJS Kesehatan. Penelitian ini bertujuan untuk mengevaluasi efektivitas AES 128-bit dalam melindungi data sensitif, mengidentifikasi tantangan dalam implementasinya, dan memberikan rekomendasi untuk perbaikan lebih lanjut. Harapannya, penelitian ini dapat memberikan sumbangsih berarti dalam memperkuat keamanan data digital di BPJS Kesehatan, sekaligus menjadi acuan bagi penerapan teknologi serupa di institusi kesehatan lainnya di Indonesia.

2. METODE PENELITIAN

Penelitian ini menggunakan metode waterfall yang terstruktur dan sistematis untuk mencapai tujuannya. Tahapan-tahapan dalam metode ini dimulai dengan identifikasi masalah, dilanjutkan dengan studi literatur yang mendalam terhadap penelitian sebelumnya. Langkah-langkah detail dari metode ini diilustrasikan dalam Gambar 1.



Gambar 1. Penerapan Metode

2.1 Studi Literatur

Penelitian ini telah menggunakan berbagai alat dan konsep yang relevan, didukung oleh studi literatur yang komprehensif meliputi buku teks, jurnal, dan artikel ilmiah terkait kriptografi dan metode enkripsi Advanced Encryption Standard (AES). sehingga mempermudah dalam mencapai tujuan penyelesaian masalah.

2.2 Studi Lapangan

Pada fase ini, dilakukan studi kasus untuk mengamankan dokumen-dokumen digital penting di BPJS kesehatan. Langkah ini memungkinkan analisis terhadap permasalahan yang ada sehingga file tersebut dapat dirumuskan dan masalah dapat diselesaikan dengan lebih efektif.

2.3 Perumusan Masalah

Tahap ini mengidentifikasi permasalahan yang menjadi fokus penelitian dan yang akan dicari solusinya, yaitu pengamanan data pribadi pasien, rekam medis, serta data laporan keuangan di BPJS kesehatan. Masalah ini akan diatasi dengan menerapkan algoritma kriptografi Advanced Encryption Standard (AES).

2.4 Pengumpulan Data

Pada penelitian ini, metode pengumpulan data yang digunakan dilakukan dengan beberapa cara, yaitu:

a. Wawancara, Pada proses wawancara, dilakukan tanya jawab langsung dengan pihak-pihak yang terlibat dalam perancangan program untuk memperoleh informasi mendetail mengenai aplikasi dan sistem keamanannya.
b. Observasi, Pada observasi yang dilakukan di BPJS Kesehatan, bertujuan untuk mengamati dan memahami kondisi nyata objek penelitian. Observasi ini bertujuan untuk mendapatkan penjelasan mengenai data dan informasi yang dibutuhkan dalam penelitian.
c. Studi Kepustakaan, Aktivitas ini dilakukan dengan membaca jurnal, e-book, serta referensi yang berkaitan dengan teori kriptografi, teori keamanan dokumen digital, teori Advanced Encryption Standard (AES), dan teori-teori lainnya yang berhubungan dengan perancangan program kriptografi untuk pengamanan dokumen digital berbasis web.

2.5 Analisis Sistem

Penerapan keamanan sistem dilakukan dengan mengenkripsi dokumen digital sebelum disimpan dalam database. Enkripsi ini bertujuan untuk melindungi data sensitif dari akses yang tidak sah. Untuk mencapai hal ini, modul enkripsi terintegrasi ke dalam aplikasi dan diaktifkan saat pengguna ingin melihat data, sehingga memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses informasi asli.

2.6 Perancangan Perangkat Lunak

Tahap ini berfokus pada perancangan sistem berdasarkan hasil analisis sebelumnya, terutama pada pengembangan modul enkripsi dan dekripsi dokumen digital, serta modul pendukung lainnya yang akan diintegrasikan ke dalam aplikasi berbasis web. Selain itu, perancangan antarmuka pengguna (UI) juga menjadi bagian penting dalam tahap ini.

2.7 Implementasi

Tahap implementasi melibatkan pembuatan modul-modul yang telah dirancang sebelumnya dengan menggunakan bahasa pemrograman yang sesuai. Berikut adalah daftar aplikasi yang digunakan dalam proses implementasi ini:

1. Bahasa pemrograman yang digunakan untuk perancangan system pengamanan dokumen digital berbasis web yaitu python dan framework Django serta DBMS yan digunakan adalah SQLlite.
2. Perangkat keras yang digunakan diantaranya Prosessor Intel Core i5, RAM 8GB, 500GB SSD.

2.8 Pengujian Sistem

Tahap pengujian bertujuan untuk memverifikasi kesesuaian sistem yang dikembangkan dengan hasil analisis yang telah dilakukan sebelumnya, serta memastikan aplikasi berbasis web ini telah memenuhi harapan dan kebutuhan yang ditetapkan. Untuk itu, dibuatlah sebuah metode pengujian sebagai tolak ukur dalam pengujian ini. Metode pengujian yang digunakan adalah blackbox testing. Metode ini dipakai untuk menemukan kesalahan serta mendemonstrasikan fungsi dari aplikasi setelah dijalankan, guna memastikan apakah hasil input dan outputnya telah sesuai dengan kebutuhan.

2.9 Kesimpulan

Ini merupakan tahap terakhir dalam fase ini, di mana kesimpulan akhir ditarik mengenai penggunaan metode enkripsi-deskripsi Advanced Encryption Standard (AES) dalam melindungi dokumen digital pada BPJS Kesehatan. Hasilnya menunjukkan bahwa sistem tersebut berfungsi dengan baik dan benar. Pada tahapan ini juga disampaikan saran untuk perbaikan dan pengembangan sistem di masa mendatang.

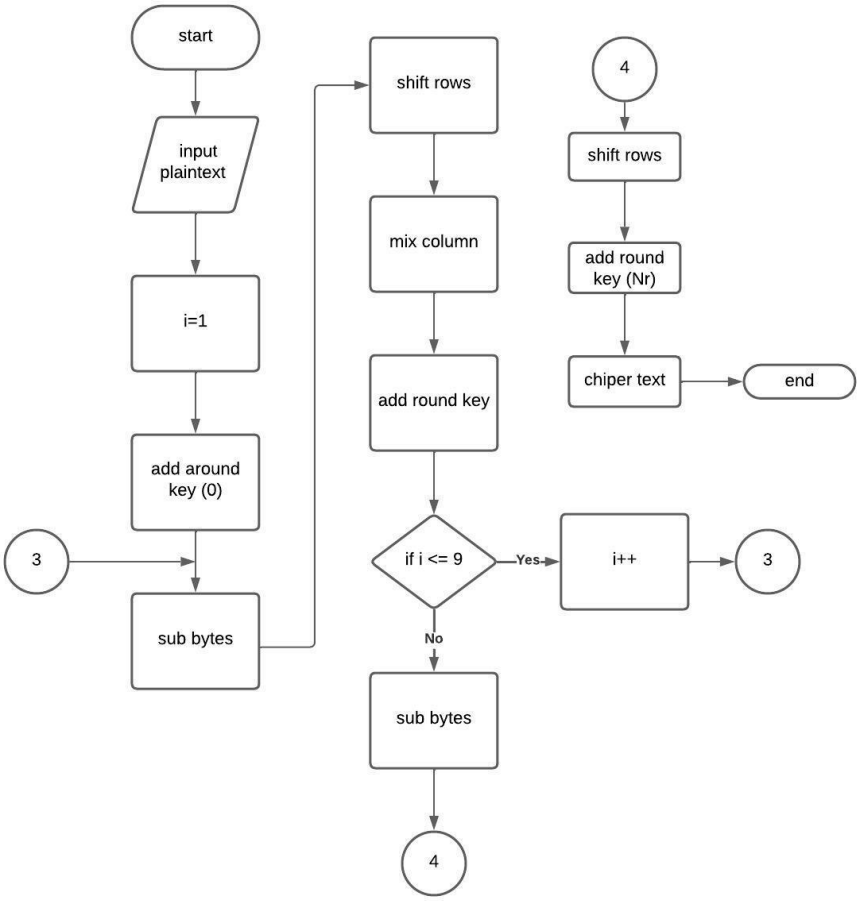
3. HASIL DAN PEMBAHASAN

3.1 Flowchart

Flowchart merupakan representasi grafis yang menggambarkan alur logika dan langkah-langkah yang terlibat dalam suatu program, dengan memanfaatkan simbol-simbol standar untuk memperjelas setiap tahapan dan pengambilan keputusan. Berikut adalah flowchart yang menggambarkan alur kerja pada aplikasi ini:

a. Flowchart Enkripsi AES-128

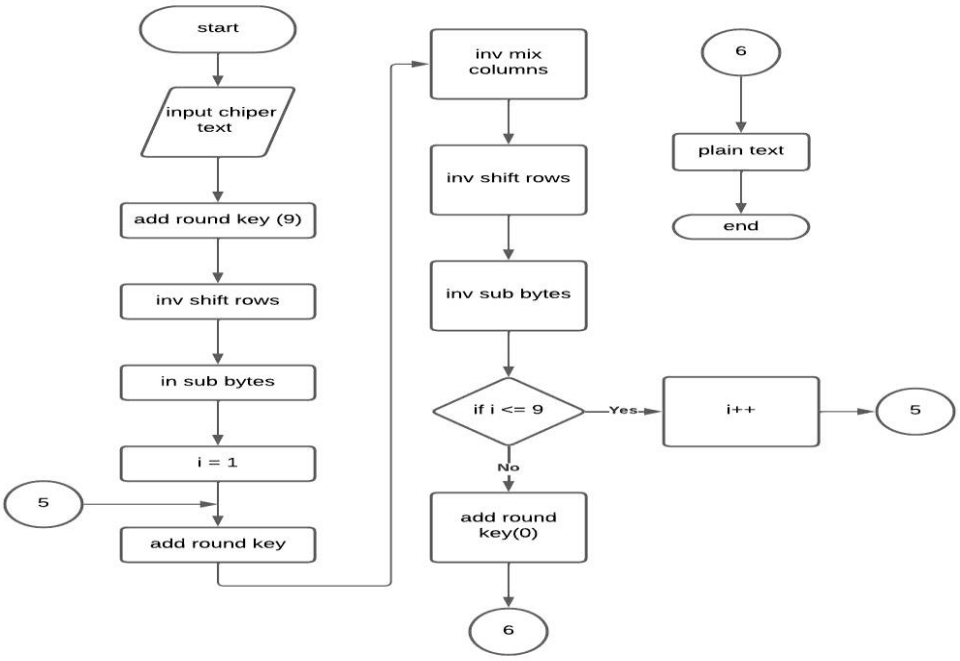
Berikut adalah flowchart dari proses enkripsi AES. Flowchart ini menjelaskan alur proses enkripsi menggunakan AES-128. Dapat dilihat pada gambar 2.



Gambar 2. Flowchart Enkripsi AES-128

b. Flowchart Dekripsi AES-128

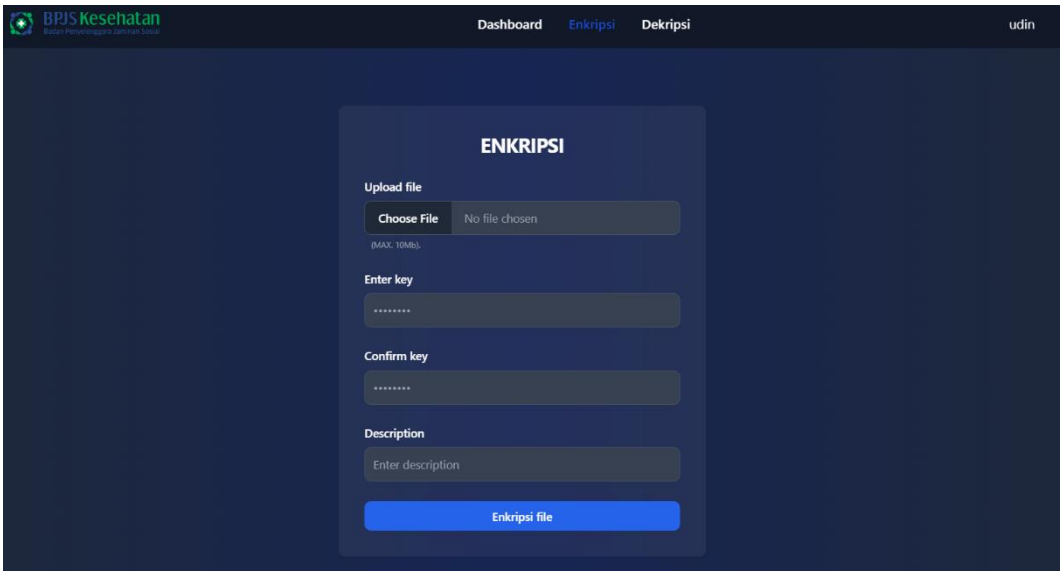
Berikut adalah flowchart dari proses dekripsi AES. Flowchart ini menjelaskan alur proses dekripsi menggunakan AES-128. Dapat dilihat pada gambar 3.



Gambar 3. Flowchart Dekripsi AES-128

3.2 Proses Enkripsi

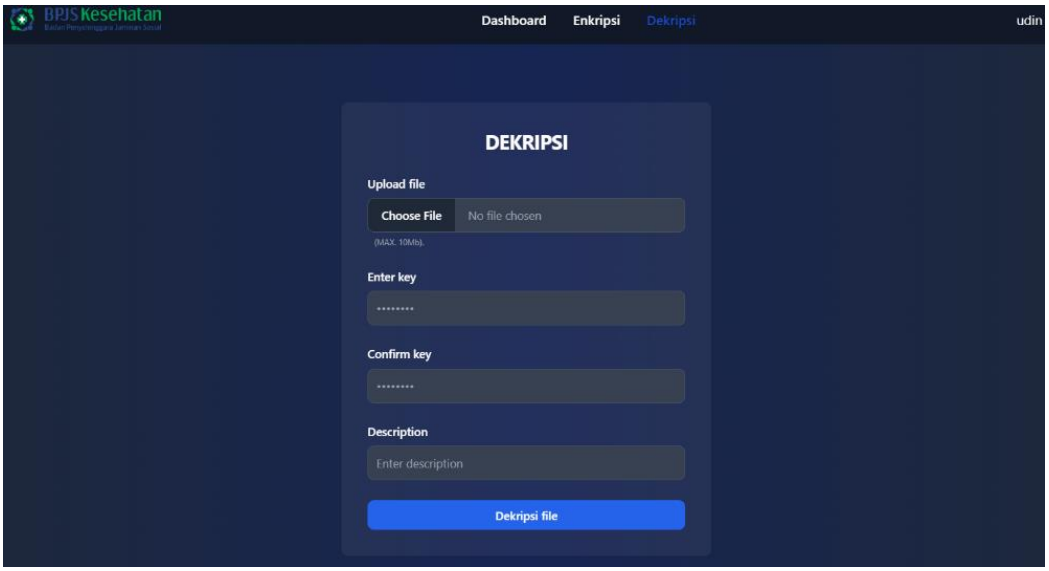
User harus melakukan login terlebih dahulu untuk melakukan proses enkripsi. Setelah berhasil login, user memilih halaman enkripsi. Pada halaman enkripsi, user ditampilkan form untuk mengenkripsi file. User harus memasukkan file yang akan di enkripsi, kunci dan deskripsi file tersebut. Dapat diamati pada gambar 4 ini:



Gambar 4. Tampilan Layar Halaman Enkripsi

3.3 Proses Dekripsi

User harus melakukan login terlebih dahulu untuk melakukan proses dekripsi. Setelah berhasil login, User yang mau mendekripsi file yang sudah di enkripsi sebelumnya, user akan ditampilkan form untuk mendekripsi. User harus memsukkan file yang didekripsi, kunci dan deskripsi file tersebut. Dapat diamati pada gambar 5 ini:



Gambar 5. Tampilan Layar Halaman Dekripsi

3.4 Pengujian

Pengujian akan melibatkan pemeriksaan apakah input data diolah dengan benar dan output yang dihasilkan sesuai dengan yang diharapkan. Secara khusus, pengujian akan dilakukan pada proses enkripsi dan dekripsi menggunakan algoritma *Advanced Encryption Standard* (AES-128) untuk mengevaluasi efektivitasnya dalam melindungi dokumen pada sistem aplikasi.

a. Pengujian Proses Enkripsi

Ukuran file memengaruhi waktu proses enkripsi, semakin besar ukuran file yang ingin di enkripsi maka proses enkripsi tersebut akan semakin lama. Nama file sebelum dan sesudah di enkripsi tidak mengalami perubahan, begitu juga dengan ukuran filenya. Dapat dilihat pada tabel 1 berikut:

Tabel 1. Pengujian Proses Enkripsi

No	Nama file	Ukuran file (KB)	Nama file setelah di enkripsi	Ukuran file setelah di enkripsi	Waktu enkripsi (detik)
1	Tabel Kriteria Skema Pembiayaan Kesehatan.docx	21.1 KB	Tabel Kriteria Skema Pembiayaan Kesehatan.docx	21.1 KB	0.18
2	surat Permohonan Rencana Implementasi dan Sertifikasi.docx	19.0 KB	surat Permohonan Rencana Implementasi dan Sertifikasi.docx	19.0 KB	0.2
3	Rencana Kerja Asdep Jaminan	48.9 KB	Rencana Kerja Asdep Jaminan	48.9 KB	0.47

	Kualitas Teknologi Informasi Tahun 2024.xlsx		Kualitas Teknologi Informasi Tahun 2024.xlsx		
4	Surat Pemberitahuan Kegiatan Audit Internal ISO 270012022.pdf	176.4 KB	Surat Pemberitahuan Kegiatan Audit Internal ISO 270012022.pdf	176.4 KB	1.52
5	AWARENESS SISTEM MANAJEMEN KEMANAN INFORMASI ISO 270012022.pptx	4.681.312 KB	AWARENESS SISTEM MANAJEMEN KEMANAN INFORMASI ISO 270012022.pptx	4.681.312 KB	40.56

b. Pengujian Proses Dekripsi

Sama seperti proses enkripsi, semakin besar ukuran file maka semakin lama proses untuk melakukan dekripsi. Namun pada proses dekripsi, nama file setelah di dekripsi mengalami perubahan tetapi unuk ukuran filenya tidak berubah. Dapat dilihat pada tabel 2 berikut:

Tabel 2. Pengujian Proses Dekripsi

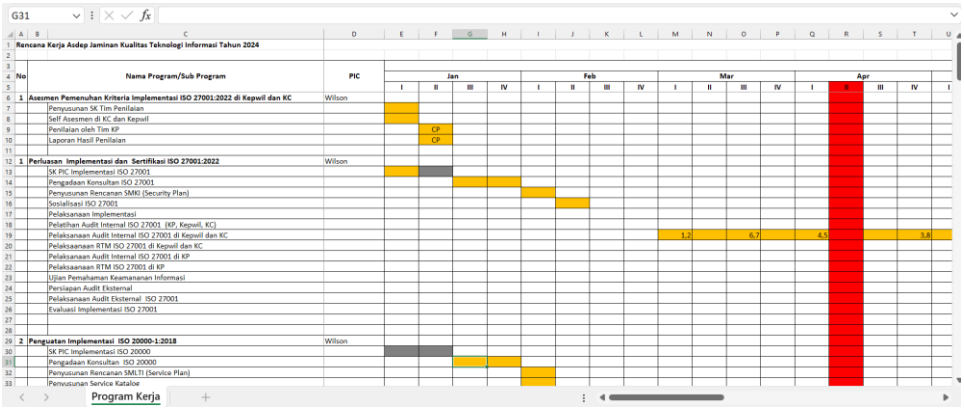
No	Nama file	Ukuran file (KB)	Nama file setelah di dekripsi	Ukuran file setelah di dekripsi	Waktu enkripsi (detik)
1	Tabel Kriteria Skema Pembiayaan Kesehatan.docx	21.1 KB	Tabel Kriteria Skema Pembiayaan Kesehatan_DuDsV2j.docx	21.1 KB	0.36
2	surat Permohonan Rencana Implementasi dan sertifikasi.docx	19.0 KB	surat Permohonan Rencana Implementasi dan Sertifikasi_LjcXIqk.docx	19.0 KB	0.34
3	Rencana Kerja Asdep Jaminan Kualitas Teknologi Informasi Tahun 2024.xlsx	48.9 KB	Rencana Kerja Asdep Jaminan Kualitas Teknologi Informasi Tahun 2024_PJvhlny.xlsx	48.9 KB	1.02
4	Surat Pemberitahuan Kegiatan Audit Internal ISO 270012022.pdf	176.4 KB	Surat Pemberitahuan Kegiatan Audit Internal ISO 270012022_pyrdwMM.pdf	176.5 KB	2.97
5	AWARENESS SISTEM MANAJEMEN KEMANAN	4.681.312 KB	AWARENESS SISTEM MANAJEMEN KEMANAN INFORMASI ISO 270012022_K08QsOz.pptx	4.681.312 KB	78.67

	INFORMASI ISO 270012022.pptx				

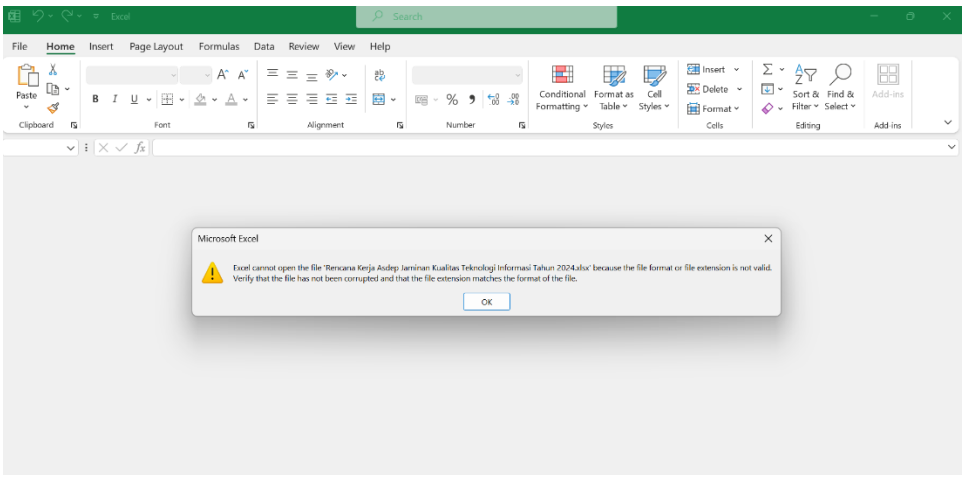
3.5 Rincian Pengujian

Berdasarkan pengujian yang telah dilakukan, sistem aplikasi Kriptografi dengan Implementasi Algoritma Advanced Encryption Standard (AES-128) terbukti efektif dalam mengamankan dokumen digital di BPJS Kesehatan.

Pada gambar di bawah ini, terdapat contoh sebelum dan setelah dokumen digital berhasil dienkripsi menggunakan Algoritma Advanced Encryption Standard (AES-128). Lihat pada Gambar 6 dan Gambar 7.



Gambar 6. Contoh Dokumen Sebelum Enkripsi



Gambar 6. Contoh Dokumen Setelah Enkripsi

4. KESIMPULAN

Berdasarkan pembahasan dan analisis terhadap masalah yang dihadapi, beberapa kesimpulan dapat diambil dan mungkin menjadi bahan pertimbangan untuk pengembangan sistem selanjutnya. penulis menyimpulkan: Sistem aplikasi kriptografi AES-128 untuk pengamanan dokumen digital di BPJS Kesehatan meningkatkan keamanan data dan mencegah dari serangan kejahatan siber, Ukuran dari dokumen digital memengaruhi kecepatan dalam proses enkripsi dan dekripsi, Data dari dokumen digital tidak mengalami perubahan setelah proses enkripsi dan dekripsi. Berdasarkan hasil dan kesimpulan penelitian, penulis mengajukan beberapa rekomendasi untuk

pengembangan lebih lanjut: Dapat dikembangkan dengan menambah fitur enkripsi dan dekripsi beberapa dokumen digital secara bersamaan, Membuat aplikasi memproses enkripsi dan dekripsi dokumen digital dengan ukuran yang besar secara cepat.

DAFTAR PUSTAKA

[1] M. Azhari, D. . I. Mulyana, F. 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, 2022.

[2] R. Ramadhan and . H. Soetanto, "Penerapan Kriptografi Menggunakan Advanced Encryption Standard 128 Untuk Pengamanan File Pada Smk Muhammadiyah 4," *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi,* vol. 1, no. 1, pp. 29-38, 2022.

[3] F. "Penggunaan Qr Code Berbasis Kriptografi Advanced Encryption Standard (Aes) Untuk Administrasi Rekam Medis," *Jurnal Syntax Admiration,* vol. 2, no. 10, 2021.

[4] M. F. Fachrozi and H. Fahmi, "Penerapan Metode AES-128 Untuk Pengamanan Data Absensi FingerPrint di Balai Penelitian Sungei Putih," *Jurnal Ilmu Komputer dan Sistem Informasi,* vol. 3, no. 3, pp. pp. 1-8, 2021.

[5] B. E. Nino, "Perbandingan Performa Algoritma AES dan Twofish Menggunakan Metode Strict Avalanche Criterion pada Nomor Induk Kependudukan Indonesia," *Jurnal Teknologi Informasi,* vol. 9, no. 1, 2023.

[6] Y. Fatma, A. Hafid and . H. O. Dani, "Peningkatan Keamanan Pengiriman Pesan Teks: Kombinasi Advanced Encryption Standard (AES) 128 dan Least Significant Bit (LSB)," *Jurnal Sistem Informasi,* vol. 6, no. 2, pp. 111-120, 2020.

[7] F. D. Hermawati, M. Tahir and M. Syaifurrohman, "Keamanan E-Voting di Indonesia Melalui Pemanfaatan Kriptografi pada Sistem AES (Advance Encryption Standard)," *Jurnal Teknik Mesin, Industri, Elektro dan Informatika,* vol. 2, no. 2, pp. 45-56, 2023.

[8] R. Tullah, M. I. Dzulhaq and Y. Setiawan, "Perancangan Aplikasi Kriptografi File dengan Metode Algoritma Advanced Encryption Standard (AES)," *Jurnal Sisfotek Global,* vol. 6, no. 2, 2016.

[9] M. . A. Hidayah, N. B. Nugoho and M. I. Perangin-Angin, "Penerapan Kriptografi Menggunakan Algoritma AES untuk Keamanan Data Penjualan pada PT. Mestika Sakti," *Jurnal CyberTech,* 2020.

[10] I. Priambudi and M. , "Implementasi Kriptografi dengan Metode AES-128 untuk Pengamanan File Berbasis Web pada SMP Yapipa," *JURNAL TEKNIK INFORMATIKA,* vol. 6, no. 1, pp. 22-31, 2023.