Pengenkripsian File Data Pasien untuk Menjamin Kerahasian Informasi Medis

Gary Melvin Lie[a1], Luh Gede Astuti[a2]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Udayana, Bali
Jln. Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, 08261, Bali, Indonesia
[1]garymelvinlie@gmail.com
[2]lg.astuti@unud.ac.id (Corresponding Author)

Abstract

In the era of digitalization of medical information, safeguarding patient data confidentiality has become paramount. This research aims to address the issue of data leakage by implementing file encryption using the AES-128 algorithm. The research methodology encompasses problem identification, system design, testing, and evaluation. The encryption steps of AES-128, namely SubBytes, ShiftRows, MixColumns, and AddRoundKey, are applied to enhance the security of patient data. Testing is conducted using various types of medical data, and an analysis is performed to assess the level of security and algorithm performance. The results indicate that file encryption with AES-128 can provide a high level of security for patient medical information. The AES-128 algorithm generates secure ciphertext that cannot be easily decrypted without the corresponding key. This research contributes to the field of medical information security by implementing AES-128 file encryption in patient data management systems. By enhancing data privacy and security, the utilization of this algorithm has the potential to provide strong protection against data breaches. Further studies can explore the wider application of AES-128 in the context of medical data security and improve algorithm performance.

Keywords: *AES, Encryption, Medical*

1. Pendahuluan

Dalam era digital yang semakin maju, pertukaran dan penyimpanan data medis menjadi semakin penting dalam sektor perawatan kesehatan. Data medis sensitif seperti riwayat penyakit, hasil laboratorium, dan informasi identitas pasien harus dijaga kerahasiaannya agar tidak jatuh ke tangan yang tidak berwenang. Keamanan informasi medis menjadi hal yang sangat penting untuk memastikan privasi pasien terjaga dan mencegah penyalahgunaan data.

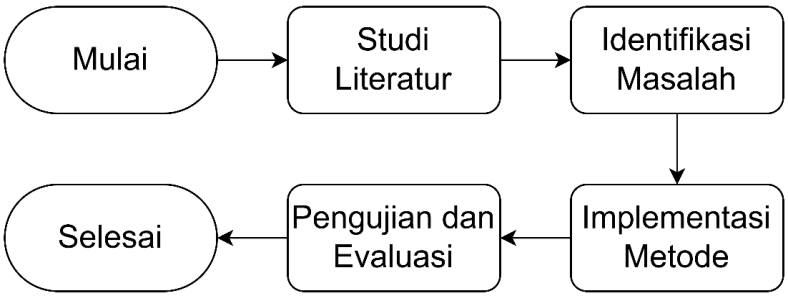
Sebelum kita menggunakan metode untuk keamanan sistem atau informasi, kita harus mengetahui apa itu kriptografi, ilmu yang dapat mempelajari metode matematis yang berkaitan dengan tujuan informasi dan keamanan informasi, seperti keakuratan, kualitas dan keamanan informasi [1]. Salah satu pendekatan yang efektif untuk menjaga kerahasiaan informasi medis adalah melalui pengenkripsian file. Pengenkripsian file melibatkan pengubahan isi file menjadi bentuk yang tidak dapat dibaca (ciphertext) menggunakan algoritma enkripsi. Hanya pihak yang memiliki kunci enkripsi yang benar dapat mendekripsi dan mengakses kembali informasi dalam file tersebut. Dalam konteks ini, *Advanced Encryption Standard* (AES) telah menjadi salah satu algoritma yang paling banyak digunakan dan diakui secara luas karena keamanannya yang tinggi dan efisiensinya.

Penelitian ini bertujuan untuk menginvestigasi penggunaan pengenkripsian file dengan menggunakan AES pada data pasien untuk menjaga kerahasiaan informasi medis. Melalui penerapan pengenkripsian file yang tepat, diharapkan data medis dapat diamankan secara efektif dari akses yang tidak sah dan penggunaan yang tidak diinginkan. Selain itu, penelitian ini juga akan mengevaluasi kinerja algoritma AES dalam konteks pengenkripsian file data medis, termasuk waktu enkripsi dan dekripsi, serta ukuran file hasil enkripsi.

Hasil dari penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan sistem keamanan informasi medis yang handal dan dapat dipercaya. Selain itu, temuan penelitian ini dapat menjadi pedoman praktis bagi organisasi kesehatan dan penyedia layanan kesehatan dalam melindungi privasi pasien dan memenuhi standar kepatuhan privasi data yang berlaku. Pada bagian selanjutnya, penelitian ini akan membahas metodologi yang digunakan, termasuk studi literatur, identifikasi masalah, implementasi metode, serta pengujian dan evaluasi.

2. Metode Penelitian

Pada metodelogi penelitian ini menjelaskan gambaran dari langkah-langkah yang akan dilakukan dalam penelitian ini.



Gambar 1. Flowchart Penelitian

2.1 Studi Literatur

Pada tahap ini akan dilakukan pengumpulan referensi mengenai kriptografi dan Algoritma AES dengan studi pustaka. Dilakukan dengan cara mengumpulkan, membaca, dan memahami jurnal, makalah, serta referensi lainnya guna mendapatkan informasi yang dibutuhkan untuk penelitian ini.

2.2 Identifikasi Masalah

Pada tahap ini, identifikasi masalah dilakukan untuk memahami permasalahan utama yang ingin diselesaikan. Permasalahan dalam penelitian ini adalah rentannya informasi data pasien terhadap kebocoran data medis yang dapat mengakibatkan penyalahgunaan informasi penting dan menimbulkan kerugian bagi pasien. Maka dari itu, pengenkrepsian file pada data pasien menjadi salah satu solusi yang efektif dalam menjaa kerahasiaan informasi medis.

2.3 Implementasi Metode

Tahap selanjutnya adalah Implementasi Algoritma yang dipilih ke dalam sistem. Dalam hal ini Algoritma AES akan diimplementasikan untuk pengenkripsian file data pasien dengan bahasa pemrograman PHP. Pemilihan panjang kunci AES dan mode operasi yang sesuai harus dipertimbangkan. Proses enkripsi dan dekripsi akan dilakukan Menggunakan kunci yang sama untuk memastikan kompabilitas antara pengirim dan penerima data terenkripsi.

2.4 Pengujian dan Evaluasi

Pada tahap pengujian dan evaluasi, dilakukan uji coba apakah Algoritma AES ini sudah berjalan dengan baik di bahasa pemrograman PHP, serta mengevaluasi apabila masih terdapat kesalahan dan kekurangan.

2.5 Kriptografi

Kriptografi adalah ilmu yang berkaitan dengan teknik dan metode untuk mengamankan dan melindungi informasi dari akses yang tidak sah atau penyalahgunaan [2]. Tujuan utama

kriptografi adalah menjaga kerahasiaan, integritas, dan otentikasi pesan atau data. Kriptografi juga merupakan salah satu persyaratan keamanan terpenting untuk teknologi informasi saat mengirimkan pesan penting dan rahasia [3].

2.6 *Advanced Encryption Standard (AES)*

AES adalah algoritma enkripsi yang dapat digunakan untuk melindungi data. Algoritma AES adalah blok ciphertext simetris yang dapat mengenkripsi dan mendekripsi data [4]. AES memiliki blok ukuran tetap sebesar 128-bit dan mendukung tiga varian kunci yaitu 128-bit, 192 bit, dan 256 bit. Algoritma AES menggunakan operasi substitusi dan permutasi yang kompleks untuk menciptakan lapisan keamanan yang kuat. Proses enkripsi AES melibatkan beberapa putaran transformasi pada blok data yang dienkripsi, di mana setiap putaran terdiri dari operasi substitusi *byte*, pergeseran baris, campuran kolom, dan operasi XOR dengan kunci ronda. Proses dekripsi AES dilakukan dengan langkah-langkah yang berlawanan.

a. Proses Enkripsi AES-128
   Proses enkripsi dalam algoritma AES mencakup 4 jenis *byte* variabel: *SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey* [5].

   1. *SubBytes*: Setiap *byte* dalam blok plaintext diubah menggunakan substitusi non-linear dengan menggunakan tabel substitusi (S-box) AES.

   2. *ShiftRows*: *Byte* dalam setiap baris blok plaintext digeser ke kiri. Pada putaran pertama, baris kedua bergeser satu langkah ke kiri, baris ketiga bergeser dua langkah ke kiri, dan baris keempat bergeser tiga langkah ke kiri.

   3. *MixColumns*: Setiap kolom blok plaintext diubah melalui operasi perkalian matriks dalam Galois Field. Ini menghasilkan percampuran nilai *byte* dalam kolom-kolom tersebut.

   4. *AddRoundKey*: Blok plaintext hasil dari langkah sebelumnya di-XOR-kan dengan kunci putaran (round key). Kunci putaran dihasilkan dari ekspansi kunci yang berasal dari kunci utama.

   Langkah-langkah di atas diulangi secara berurutan sebanyak 10 putaran (putaran terakhir tidak termasuk langkah MixColumns).

b. Proses Dekripsi AES-128
   Transformasi cipher dapat dilakukan secara terbalik dan berlawanan arah untuk menghasilkan cipher terbalik yang mudah dipahami untuk algoritma AES. Konversi *byte* yang digunakan dalam enkripsi terbalik adalah *InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey*.

   1. *AddRoundKey*: Blok ciphertext di-XOR-kan dengan kunci putaran terakhir dari ekspansi kunci

   2. *Invers MixColumns*: Setiap kolom blok ciphertext diubah melalui operasi invers perkalian matriks dalam Galois Field.

   3. *Invers ShiftRows*: Byte dalam setiap baris blok ciphertext digeser ke kanan. Pada putaran pertama, baris kedua bergeser satu langkah ke kanan, baris ketiga bergeser dua langkah ke kanan, dan baris keempat bergeser tiga langkah ke kanan.

   4. *Invers SubBytes*: Setiap byte dalam blok ciphertext diubah menggunakan substitusi non-linear dengan menggunakan tabel substitusi invers (inverse S-box) AES.

   Langkah-langkah di atas diulangi secara berurutan sebanyak 10 putaran (putaran terakhir tidak termasuk langkah MixColumns).

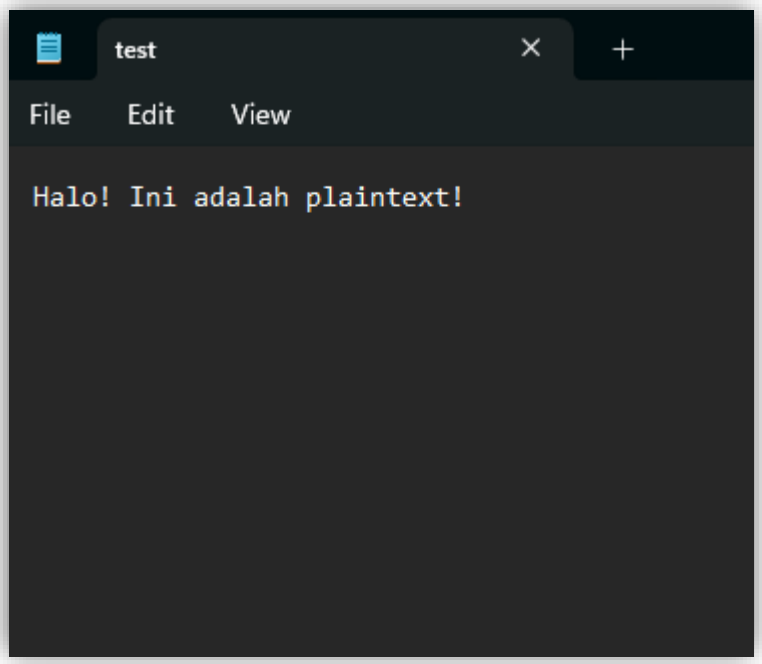
3. Hasil dan Pembahasan

3.1. Rancangan Pengujian

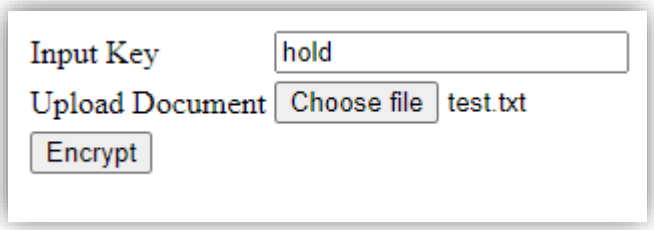
Adapun rancangan pengujian yang diimplementasikan menggunakan algoritma *Advanced Encryption Standard* untuk setiap format yang termasuk dalam aplikasi berbasis web yang akan dirancang. Pengujian ini bermaksud untuk mengetahui apabila data yang sudah diuji, akan terenkripsi dengan baik di dalam database. Untuk mengetahuinya, bisa dengan membuka file yang dienkripsi, apabila file yang sudah dienkripsi muncul di folder dan berubah menjadi *ciphertext* maka enkripsi telah berhasil, begitupun sebaliknya.

3.2. Implementasi *Advanced Encryption Standard* (AES-128)

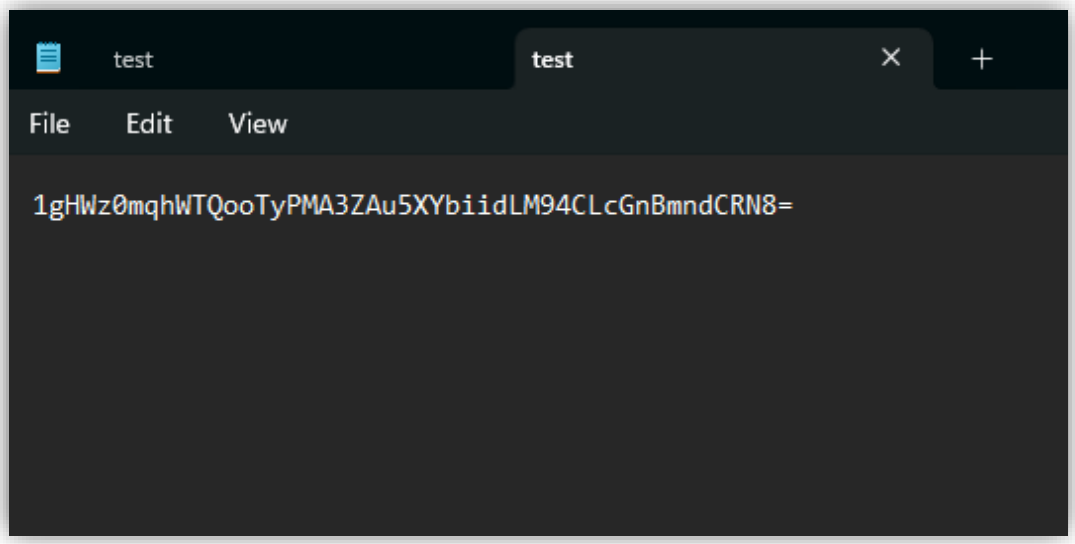
a. Implementasi Enkripsi
Pada proses ini pertama-tama kita harus memiliki sebuah file yang akan dienkripsikan, Kemudian user memasukkan kunci dan mengupload file yang ingin dienkripsikan.



Gambar 2. *Plaintext*

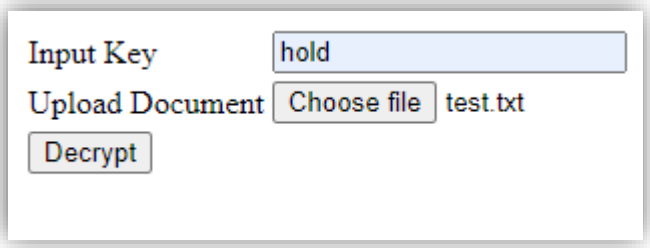


Gambar 3. Proses Enkripsi

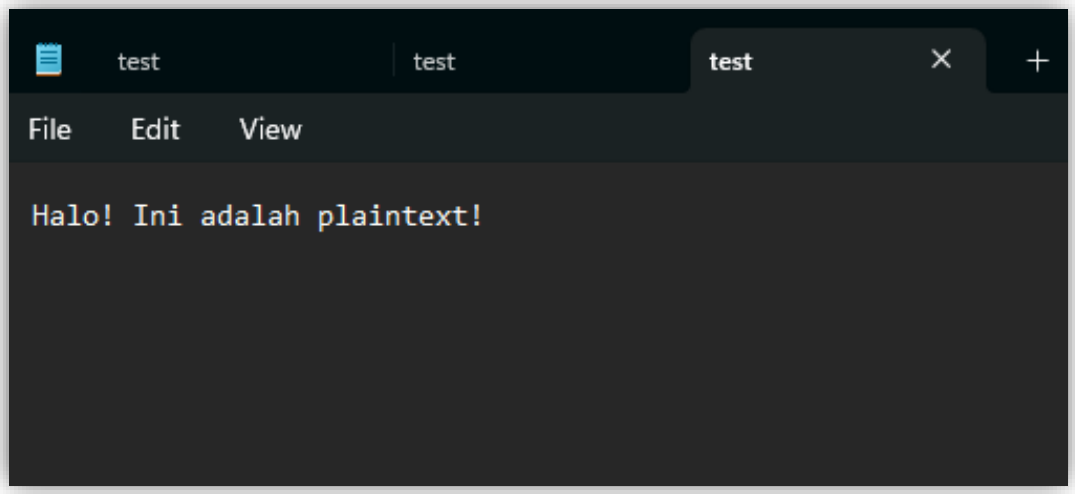


Gambar 4. *Ciphertext*

b. Implementasi Dekripsi
Pada tahap dekripsi, kita dapat melakukan pendekripsian file dengan cara memasukkan kunci dan mengupload file *ciphertext* tadi.



Gambar 5. *Proses Dekripsi*



Gambar 6. *Plaintext*

4. Kesimpulan

Berdasarkan hasil percobaan terhadap proses enkripsi dan dekripsi, dapat disimpulkan bahwa file yang melalui percobaan enkripsi berubah bentuk menjadi file yang tidak dapat dibaca. File dapat kembali ke bentuk aslinya saat melalui proses dekripsi menggunakan kunci yang sama saat enkripsi. Waktu pemrosesan data hasil enkripsi dan dekripsi juga dapat dipengaruhi oleh besar ukuran data yang diuji. Pengenkripsian file data pasien menggunakan AES-128 dapat menjadi solusi yang efektif untuk menjaga kerahasiaan informasi medis. Penggunaan algoritma AES-128 memberikan tingkat keamanan yang tinggi dan dapat melindungi data medis sensitif dari akses yang tidak sah. Penelitian ini memberikan kontribusi dalam bidang keamanan informasi medis dan dapat digunakan sebagai dasar untuk pengembangan sistem keamanan yang lebih lanjut dalam pengelolaan data pasien.

Daftar Pustaka

[1] D. Hulu, B. Nadeak, dan S. Aripin, “Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan,” vol. 4, no. 1, 2020, doi: 10.30865/komik. v4i1.2590.

[2] A. R. Tulloh, Y. Permanasari, dan E. Harahap, “Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen,” *Jurnal Matematika UNISBA*, vol. 15, no. 1, 2016, [Daring]. Tersedia pada: http://ejournal.unisba.ac.id

[3] D. R. Saragi, J. M. Gultom, J. A. Tampubolon, dan I. Gunawan, “Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4,” *Jurnal Sistem Komputer dan Informatika (JSON)*, vol. 1, no. 2, hlm. 114, Jan 2020, doi: 10.30865/json. v1i2.1745.

[4] D. A. Meko, “Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data,” *Jurnal Teknologi Terpadu*, vol. 4, no. 1, 2018.

[5] F. Muharram, “Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard,” *Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi*, vol. 3, no. 2, 2018.