JURNAL ILMIAH SISTEM INFORMASI DAN ILMU KOMPUTER
Halaman Jurnal: http://journal.sinov.id/index.php/juisik/index
Halaman UTAMA Jurnal : https://journal.sinov.id/index.php

Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)

Melenia Bayu Aryanto [1], Muhlis Tahir [2], Silvia Irma Devita [3], Zuda Nuril Mustofa [4], Qurrotun Ainiyah [5], Shelviatus Sundoro [6]
[1, 2, 3, 4, 5] *Program Studi Pendidikan Informatika, Universitas Trunojoyo Madura, Madura, Indonesia*

Email: [1]190631100084@student.trunojoyo.ac.id ,[2] muhlis.tahir@trunojoyo.ac.id , [3]190631100090@student.trunojoyo.ac.id , [4]190631100074@student.trunojoyo.ac.id , [5]190631100081@student.trunojoyo.ac.id , [6]190631100069@student.trunojoyo.ac.id

Abstract

Data security refers to the confidentiality of information exchanged, especially when the data is on a computer network that is connected to other networks. Of course, this is risky when irresponsible individuals gain access to confidential or valuable information. To avoid the undesired possibility of damage or loss leading to significant material loss. To solve this problem, you need a security system that helps encrypt and decrypt data files. Cryptography is the study of cryptography in which plaintext is encrypted with an encryption key and transformed into a script that is difficult for others to read without the decryption key. Cipher sare class ified intot wotypes. classic and modern. Classical encryption works in character mode using the alphabet (A-Z) and the algorithms used are simple enough to easily break the ciphertext, while modern algorithms use ASCII (American Standard Code for Information It is formed using binary bits (0's and 1's) derived from the Interchange. Creating a key is so complicated that knowing the key makes it difficult to guess the ciphertext. In this study, we create a cryptographic application that uses the 128-bit Advanced Encryption Standard (AES) encryption algorithm. The programming language is PHP and uses MySQL as the web application print and database. Files uploaded for encryption are stored in the database. It is expected that students will be able to maintain the security of their file data with the help of this application.

Keywords: *implementation, file security using AES*

Abstrak

Keamanan data mengacu pada kerahasiaan informasi yang dipertukarkan, terutama ketika data berada di jaringan komputer yang terhubung ke jaringan lain. Tentu saja, ini berisiko ketika individu yang tidak bertanggung jawab mendapatkan akses ke informasi rahasia atau berharga. Untuk menghindari kemungkinan kerusakan atau kerugian yang tidak diinginkan yang menyebabkan kerugian material yang signifikan. Untuk mengatasi masalah ini, Anda memerlukan sistem keamanan yang membantu mengenkripsi dan mendekripsi file data. Kriptografi adalah ilmu yang mempelajari kriptografi dimana plainteks dienkripsi dengan kunci enkripsi dan diubah menjadi skrip yang sulit dibaca orang lain tanpa kunci dekripsi. Cipher diklasifikasikan menjadi dua tipe. klasik dan modern. Enkripsi klasik bekerja dalam mode karakter menggunakan alfabet (A-Z) dan algoritma yang digunakan

Received Januari 30, 2023; Revised Februari 28, 2023; Accepted Maret 30, 2023

cukup sederhana untuk memecahkan ciphertext dengan mudah, sedangkan algoritma modern menggunakan ASCII (American Standard Code for Information) yang dibentuk menggunakan bit biner (0 dan 1) yang berasal dari Interchange Membuat kunci sangat rumit sehingga mengetahui kunci membuat sulit untuk menebak ciphertext Pada penelitian ini, kami membuat aplikasi kriptografi yang menggunakan algoritma enkripsi Advanced Encryption Standard (AES) 128-bit Bahasa pemrogramannya adalah PHP dan menggunakan MySQL sebagai aplikasi web cetak dan database. File yang diunggah untuk dienkripsi disimpan di database. Diharapkan mahasiswa dapat menjaga keamanan data filenya dengan bantuan aplikasi ini.

Kata Kunci: implementasi, keamanan file dengan menggunakan AES

PENDAHULUAN

Keamanan sebuah data sangat diperlukan seiring dengan kemajuan teknologi informasi. Keamanan data yang dimaksudkan yakni sebuah keamanan terhadap kerahasiaan informasi yang saling dipertukarkan, utamanya data dalam sebuah jaringan computer yang terkoneksi dengan jaringan lainnya. Bila informasi sensitive dan berharga di dalam nya di nakses oleh orang yang tidak bertanggung jawab tentu menimbulkan resiko. Kemungkinan besar akan merugikan dan membahayakan orang yang akan mengirimkan pesan ataupun organisasinya jika hal tersebut terjadi. Penerima pesan sangat mungkin salah menafsirkan dan menyebabkan kesalahpahaman atas informasi yang terkandung di dalamnya. Pembajakan data sangat memungkinkan terjadinya beberapa hal diluar kendali kita, missal data tersebut bisa jadi rusak atau hilang yang akhirnya dapat menimbulkan kerugian material yang besar. Perlu adanya sebuah system keamanan yang bisa membantu meng enkripsi dan mendeskripsi file untuk menangani masalah tersebut.

Beberapa permasalahn menarik menjadi focus utama dalam penelitian ini, salah satunya yakni mengenai keamanan file atau data. Banyak sekali jenis data yang perlu di amankan missal data kuliah, data tugas akhir mahasiswa, tugas-tugas kuliah dan berkas-berkas mahasiswa yang telah di ubah dalam file missal file biodata diri atau cv ataupun ijazah dan lain sebagai nya. Data-data tersebut merupakan data penting yang harus di amankan agar tidak ada pihak-pihak yang tidak bertanggung jawab yang bisa merusak, menghilanhkan atau memodifikasi data tersebut. Maka sebab itu perlu adanya sebuah system yang mampu membantu mengamankan data tersebut. System tersebut harapannya mampu membantu meng-enskripsi dan men-deskripsi data tersebut.

Ada sebuah ilmu yang mempelajari Teknik kriptografi yakni ilmu kriptografi. Teknik kriptografi yakni sebuah Teknik yang mampu mengubah plaintext (naskah asli) menjadi ciptext (naskah teracak). Sehingga naskah asli tersebut tidak akan terbaca tanpa kunci enkripsi. Macam-macam cipher dibagi menjadi dua jenis yakni klasik dan modern. Adapun cipher klasik bekerja menggunakan mode karakter, abjad (A-Z) dan algoritma, biasanya digunakan untuk memecahkan ciphertext yang mudah sedangkan algoritma modern bekerja menggunakan bit biner yakni angka 0 dan 1 yang terbentuk dari American Standart Code for Information Interchange yang biasa di singkat menjadi ASCII, hal ini membuat kunci menjadi kompleks sehingga menjadi sulit untuk mengetahui ciphertext tanpa mengetahui kuncinya.

Kunci kriptografi sendiri dibagi menjadi dua jenis yakni kunci simetris dan asimetris. Yang menggunakan kunci yang sama untuk melakukan fungsi enkripsi dan deskripsi disebut dengan Algoritma enkripsi simetris sedangkan Algoritma enkripsi asimetris, di sisi lain, menggunakan satu kunci untuk mengenkripsi data dan kunci lain untuk mendekripsi data. Salah satu skema kunci simetris adalah Advanced Encryption Standard (AES), atau disebut Rijndael. AES merupakan algoritma enkripsi yang aman untuk melindungi data atau file dengan berbagai teknik enkripsi dan dekripsi. panjang kunci AES yaitu 128bit, 192bit, dan 256bit.

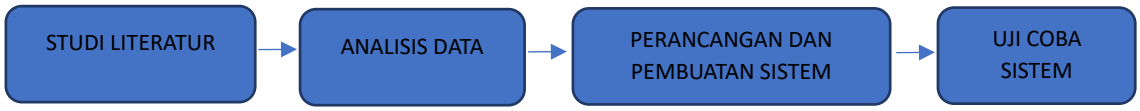
Penulis membuat sebuah aplikasi sesuai dengan paparan di atas, yakni sebuah aplikasi enkripsi dengan menggunakan algoritma enkripsi Advanced Encryption Standard (AES) 128-bit. Bahasa pemrogramannya adalah PHP dengan pencetakan aplikasi web dan MySQL sebagai databasenya. File yang diunggah untuk enkripsi disimpan dalam database. Dengan bantuan aplikasi ini diharapkan dapat membantu mahasiswa untuk menjaga keamanan data file.

Acuan penelitian sebelumnya oleh Aji Teguh Utomo1*, Rizky Pradana2*, yang berjudul "Implementasi Algoritma Advanced Encryption Standard (Aes-128) Untuk Enkripsi Dan Dekripsi File" dengan menggunakan algoritma AES-128 untuk mengamankan sebuah data pelanggan biznet, sehingga dibuatlah aplikasi kriptografi AES-128 berbasis web.

METODE PENELITIAN

A. Metode Penelitian

Langkah-langkah penelitian dimulai dengan tinjauan literatur yang berhubungan dengan kriptografi dan khususnya algoritma AES. Langkah selanjutnya adalah menganalisis data dan mempelajari apa yang perlu dilakukan untuk meningkatkan keamanan. Kemudian membuat desain aplikasi berdasarkan literature review dan analisis data untuk membuat aplikasi keamanan informasi berbasis web. Setelah aplikasi dibangun, sistem diuji. Fase-fase ini ditunjukkan pada Gambar 1.



Gambar 1. Metode Penelitian

B. Data Penelitian

Data yang digunakan dalam Implementasi Kriptografi merupakan data-data yang didapat dari tempat penelitian yaitu, data tugas-tugas kuliah mahasiswa prodi Pendidikan Infromatika. Data ini merupakan data yang digunakan untuk menguji implementasi enkripsi AES-128. Data yang akan diuji adalah data dalam ekstensi file yang berbeda: Portable Document Format (.pdf), Teks (.txt), Dokumen (.docx), Gambar (.jpg), Powerpoint (.ppt) dan Excel (.xls). Enkripsi AES-128 untuk pengujian.

C. Algoritma AES (Advanced Encryption Standard)

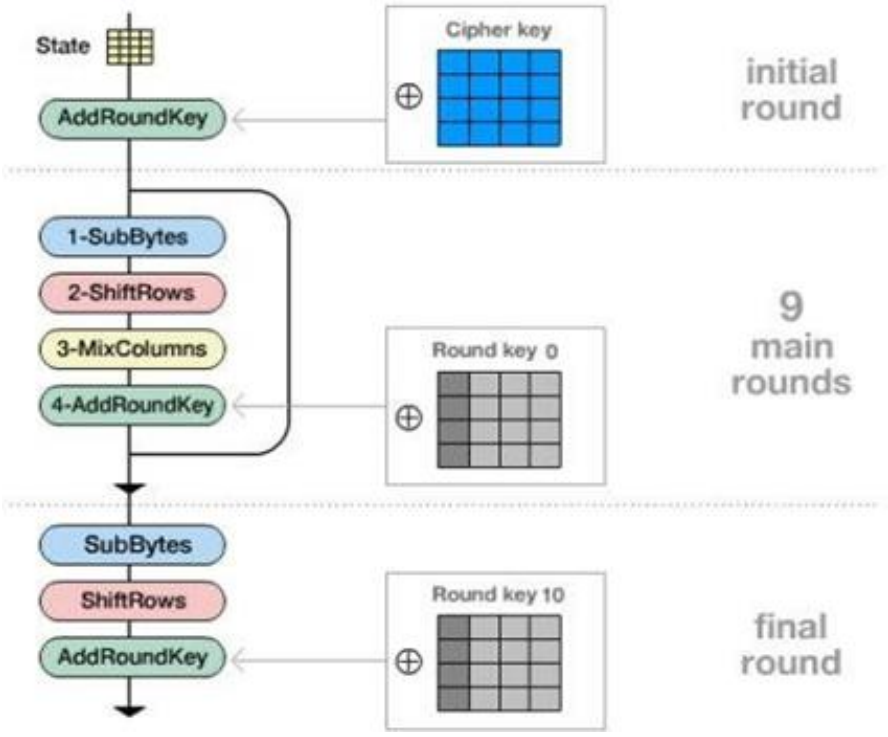
a. Advanced Encryption Standard (AES) merupakan block chiper simetris. AES diterbitkan oleh Institut Standar dan Teknologi Nasional AS pada tahun 2001. AES diperkenalkan untuk menggantikan DES karena DES menggunakan kunci enkripsi yang sangat kecil dan algoritmanya lambat. Algoritma AES menggunakan plaintext 128bit dan kunci privat 128bit, yang bersama-sama membentuk blok 128bit yang digambarkan sebagai matriks persegi 4x4. Matriks persegi 4x4 ini adalah konversi pertama yang diterima. Langkah ini diikuti oleh 10 putaran. Diantaranya, 9 putaran meliputi tahapan sebagai berikut:
b. Subbytes : Gunakan S-Box untuk melakukan permutasi byte untuk seluruh blok matriks.
c. Shift Rows : Menggeser baris matriks.
d. Mix Collumn : Kolom matriks diacak dari kanan ke kiri.
e. Add Round Key : Di sini blok saat ini di-XOR dengan kunci yang diperluas.

10 putaran terakhir hanya berisi subbyte, menggeser baris dan menambahkan tahap kunci untuk menghasilkan 16 byte (128bit) ciphertext.

1. Proses Enkripsi AES-128

Berikut adalah ringkasan dari algoritma AES yang bekerja di blok 128bit menggunakan kunci 128bit (selain proses pembuatan round kunci).

1. AddRoundKey : XOR state awal (plainteks) dengan cipherkey. Langkah ini disebut initial round.
2. Putaran sebanyak Nr – 1 kali. Langkah yang dilakukan dalam setiap putaran adalah :
    a. SubBytes : Substitusi byte dengan S- box (tabel substitusi).
    b. ShiftRows : Memindahkan baris array state dengan wrapping.
    c. MixColumns : Acak data pada setiap kolom state array.
    d. AddRoundKey : Melakukan XOR antara state saat ini dengan round key.
3. Final round : langkah putaran terakhir:
    a. SubBytes
    b. ShiftRows
    c. AddRoundKey



Gambar 2. Proses Enkripsi AES-128

2. Proses Dekripsi AES-128

Langkah dekripsi AES, juga dikenal sebagai Invers Cipher dari algoritma Rijndael, yang beroperasi blok 128bit dengan kunci 128bit, adalah :

a. InitialRound : Tahap AddRoundKey yang melakukan XOR antara state awal (ciphertext) dan kunci enkripsi. Langkah ini juga disebut InitialRound.

b. Putaran sebanyak Nr – 1 kali. Proses yang terjadi pada setiap putaran yaitu :

1) InvShiftRow : Memindahkan baris state array dengan wrapping.

2) InvByteSub : Substitusi byte dengan tabel substitusi kebalikan (inverse S-box).

3) AddRoundKey : Yaitu XOR antara state saat ini dengan round key.

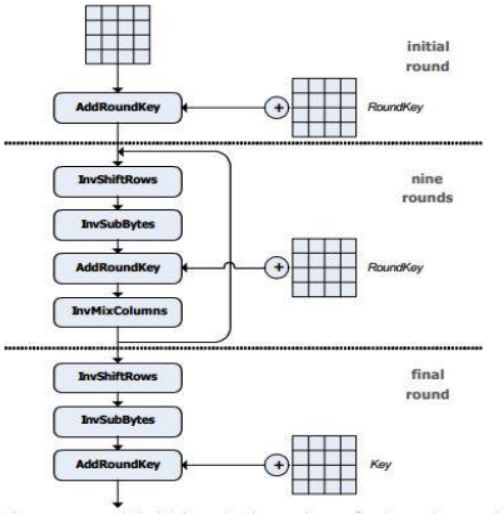
4) InvMixColumn: Acak data di setiap kolom state array.

c. Final Round : Langkah untuk putaran terakhir :

1) InvShiftRow,

2) InvByteSub,

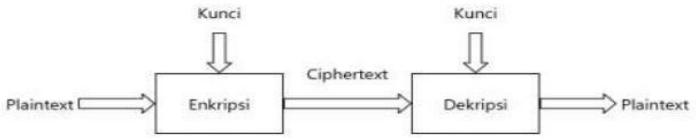
3) AddRoundKey



Gambar 3. Proses Dekripsi AES-128

D. Skema Enkripsi dan Dekripsi

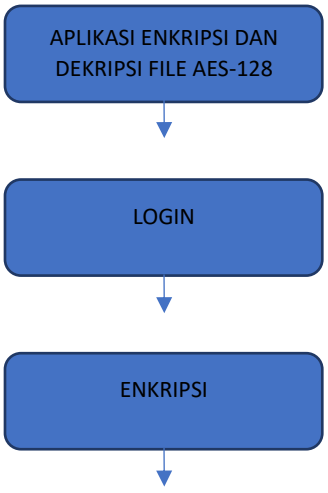
Gambar 4 berikut adalah gambaran dari proses enkripsi dan dekripsi.

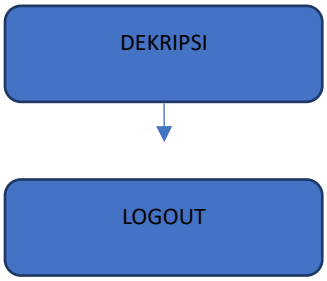


Gambar 4. Skema Enkripsi dan Dekripsi AES-128

E. Rancangan Menu

Perancangan menu aplikasi Enkripsi dan Dekripsi File digunakan untuk memberikan gambaran spesifik tentang proses yang dilalui pengguna saat mengenkripsi, melihat riwayat, dan mendekripsi file. Perancangan menu aplikasi dapat dilihat pada gambar 5 di bawah ini.

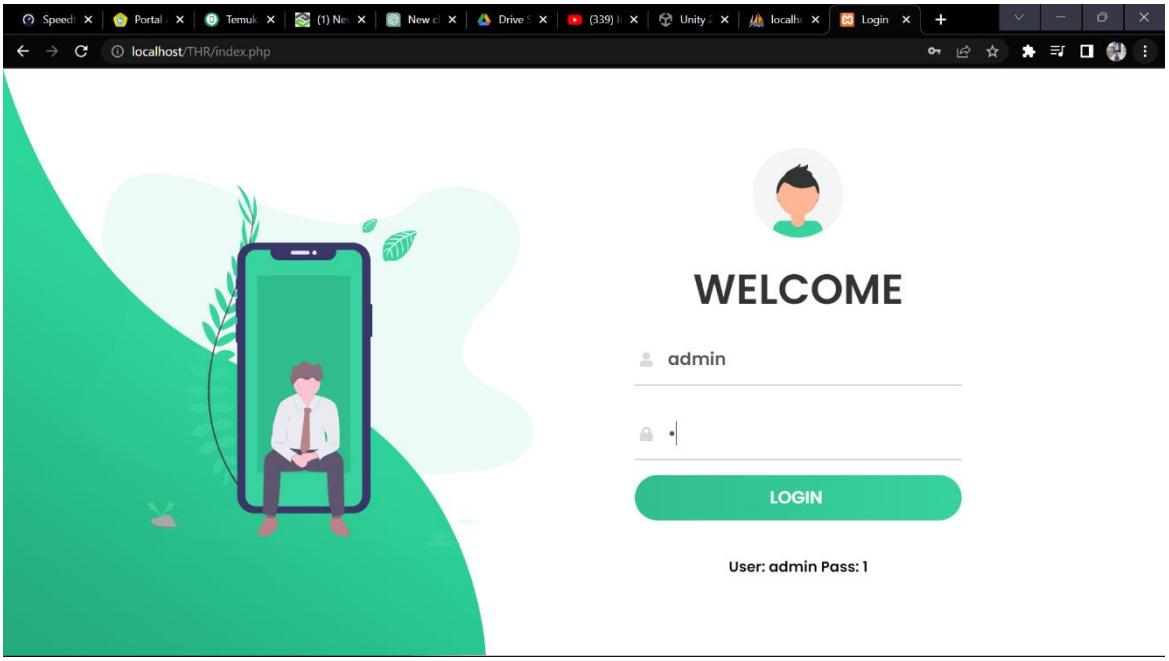




Gambar 5. Rancangan Menu

HASIL DAN PEMBAHASAN

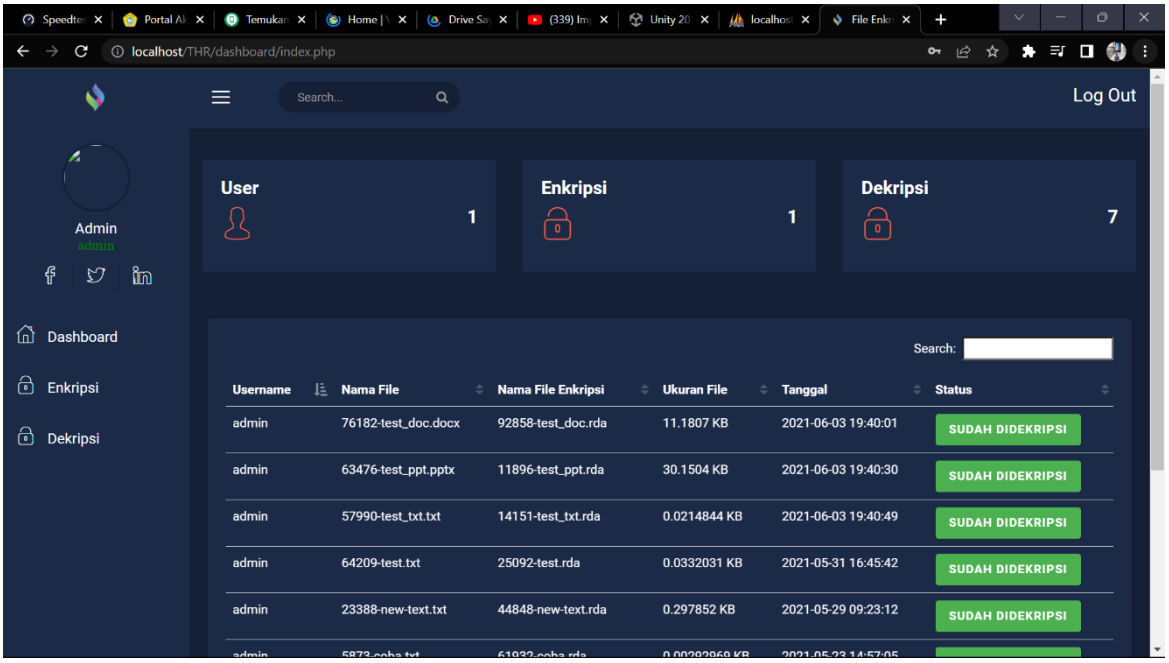
Hasil dan pembahasan meliputi analisa, hasil pengimplementasian, pengujian, dan bahasan dari topik penelitian. Selain itu, terdapat juga uraian gambar, tabel, dan lain-lain. **Tampilan Layar** Tampilan Layar Login Ketika user membuka laman login, ada 2 kolom nama pengguna (username) serta kata sandi (password). Berikut tampilan laman loginnya:



Gambar 6. Tampilan Layar Login

a. Tampilan Layar Dashboard

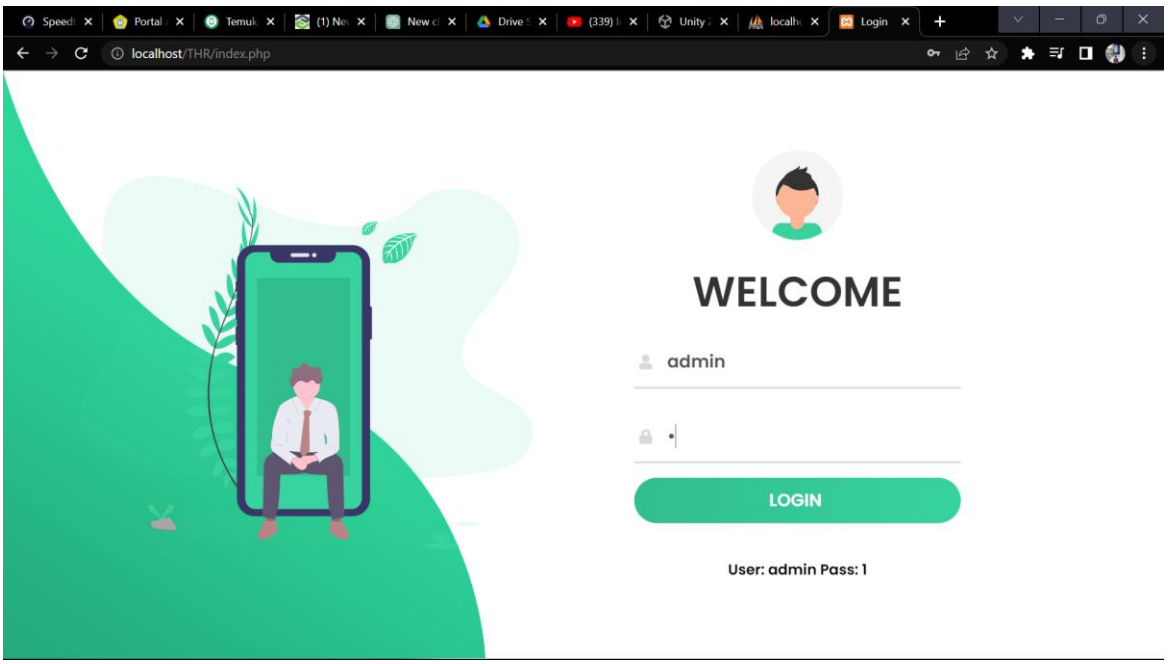
Kemudian ketika diklik laman dashboard, akan muncul menu-menu pada sebelah kiri layar. Menu tersebut adalah enkripsi serta dekripsi. Berikut tampilan laman dashboard:



Gambar 7. Tampilan Layar Dashboard

b. Tampilan Layar Enkripsi File

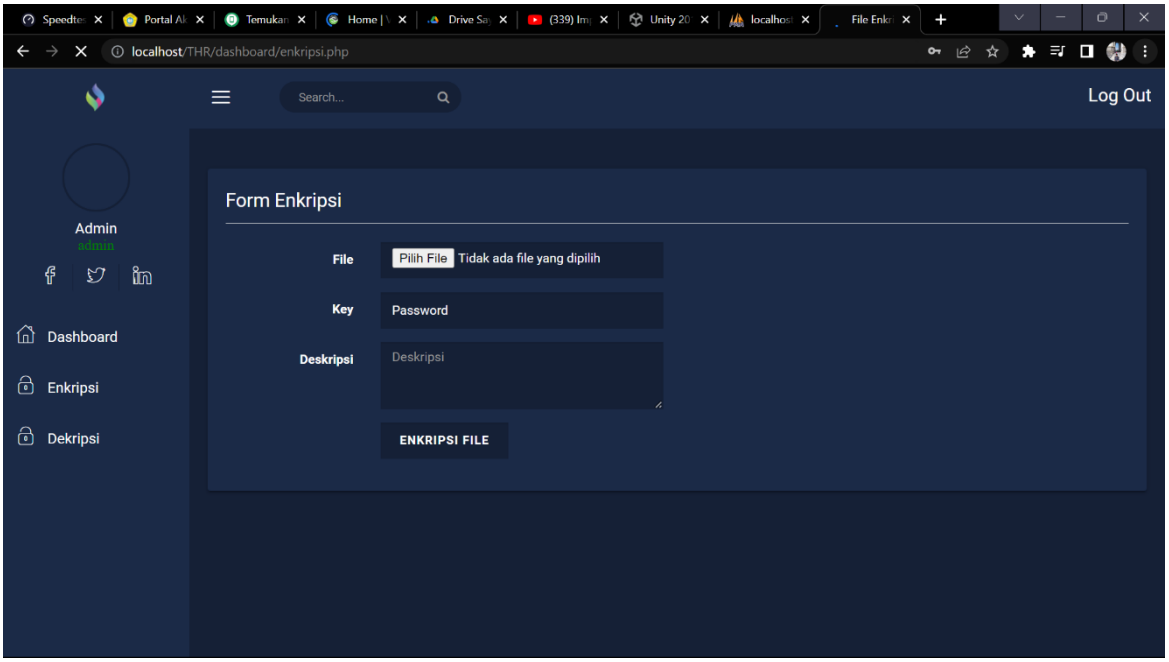
Laman enkripsi file berisi beberapa kolom. kolom-kolom tersebut adalah kolom file, kolom kata sandi (password), dan dekripsi. Berikut tampilan laman enkripsi:



Gambar 6. Tampilan Layar Login

c. Tampilan Layar Dashboard

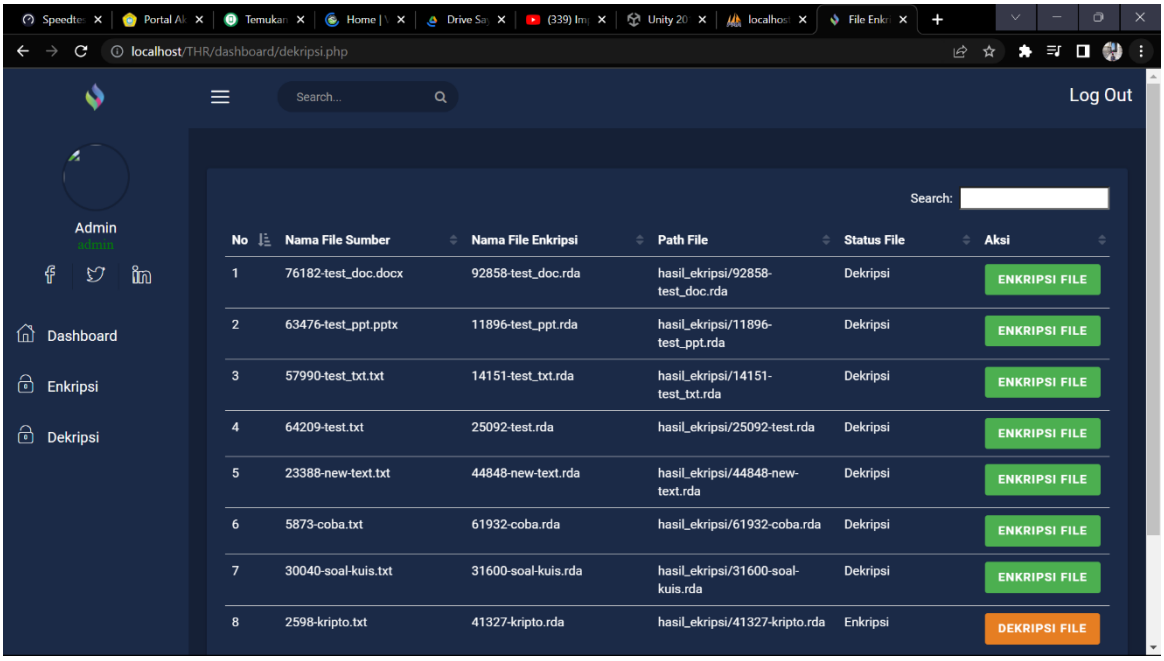
Pada tampilan layar dashboard terdapat beberapa menu yang ada di bagian kiri, yaitu enkripsi dan dekripsi. Tampilan layar dashboard seperti pada gambar di bawah ini.



Gambar 8. Tampilan Layar Enkripsi File

d. Tampilan Layar Dekripsi File

Laman dekripsi berisikan daftar dari file-file dari pengguna, dimana file ini dibedakan menjadi file yang telah dan belum didekripsikan. Berikut tampilan laman dekripsi:



Gambar 9. Tampilan Layar Dekripsi File

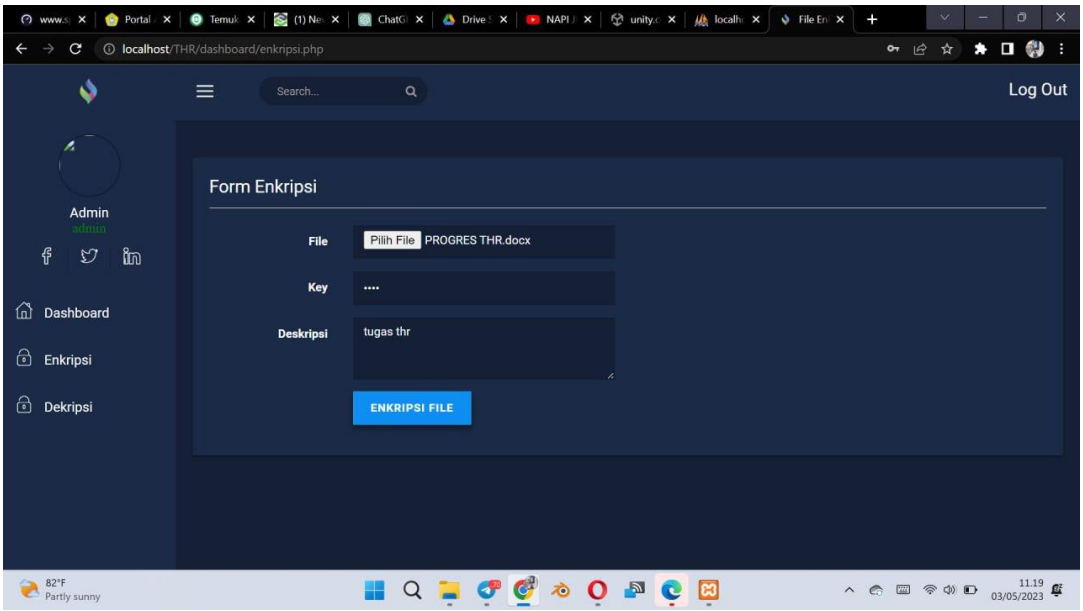
e. Implementasi

a. Enkripsi File

Pengujian tahap 1 dilakukan dengan mengenkripsi file dari pengguna, file ini memiliki format.tx

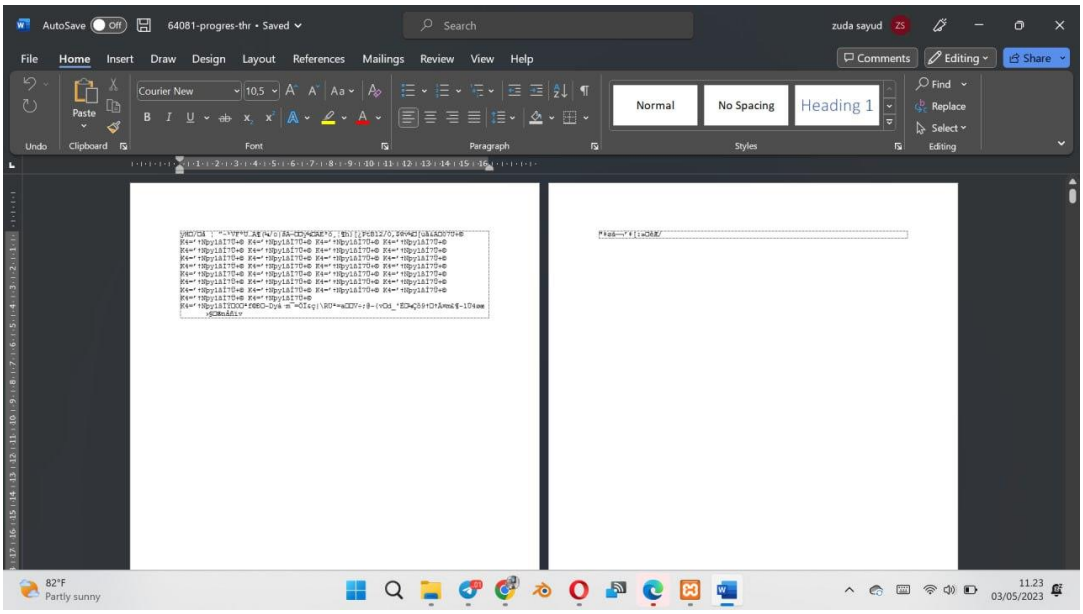
File : “PROGRES THR.docx”

Password : kel3



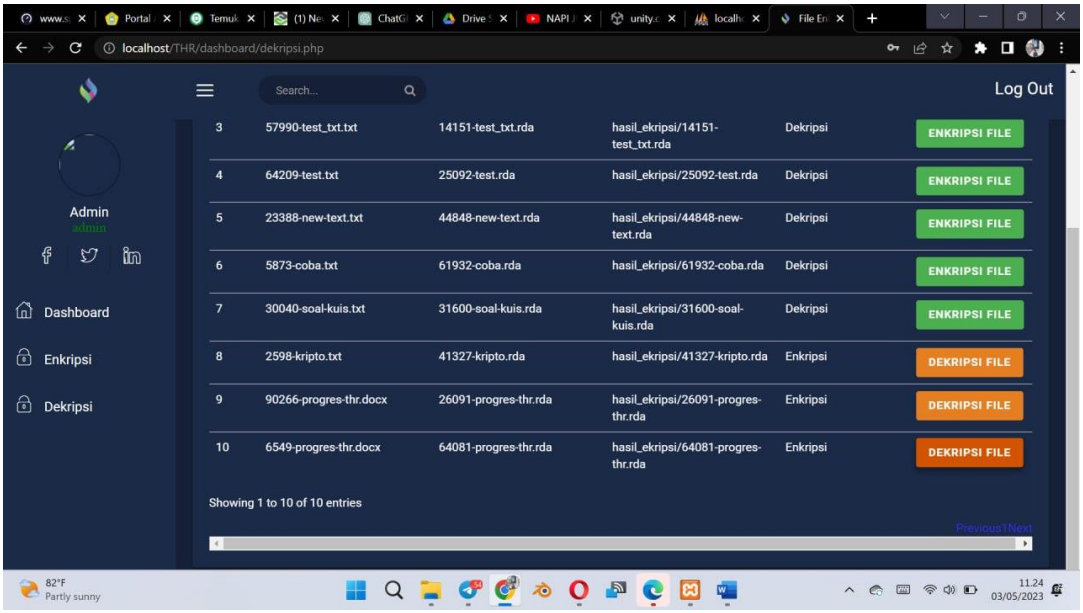
b. Isi File

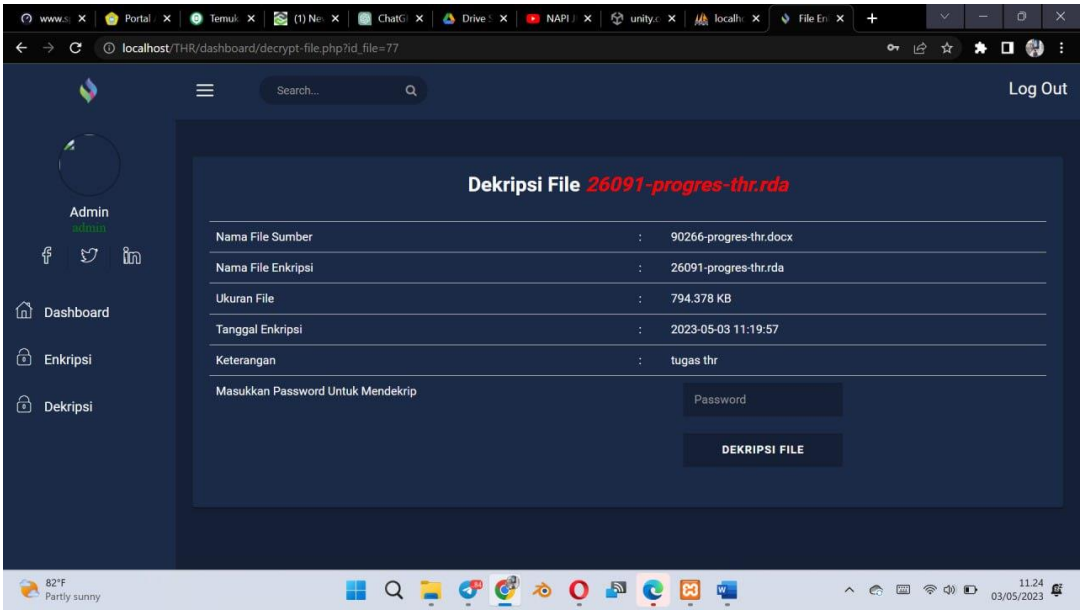
Jika sudah dienkripsikan, selanjutnya membuka file tadi. Berikut hasil enkripsinya:



c. Dekripsi File

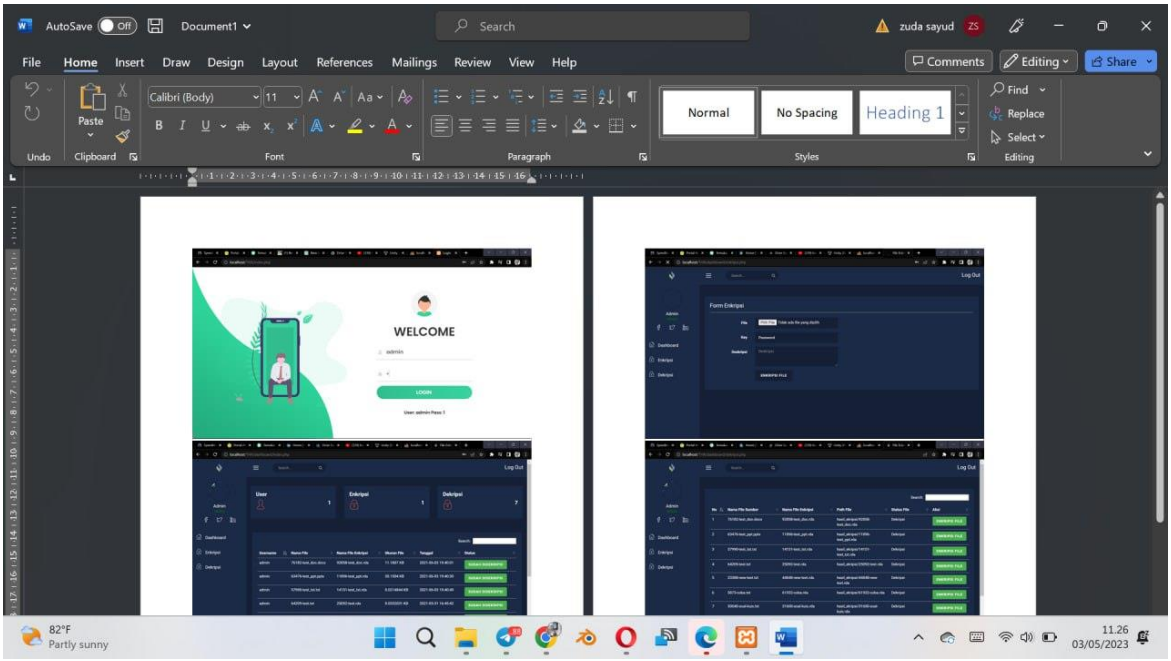
Langkah selanjutnya adalah dengan dekripsikan file. Klik pada tombol enkripsi dan dikolom password dimasukkan kata sandi yang dimasukkan ketika proses enkripsi. Berikut hasilnya:





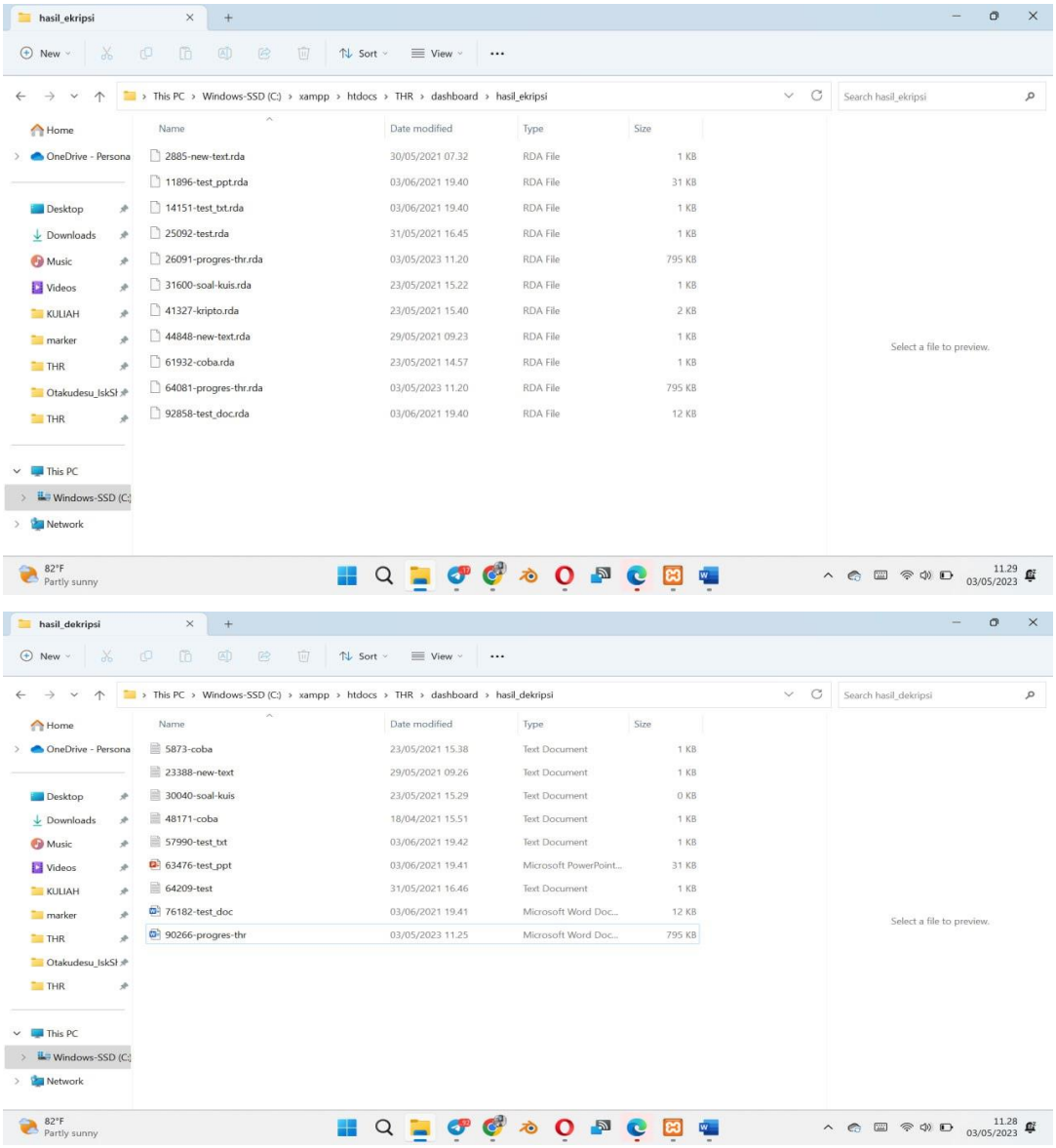
d. Isi file dekripsi

Apabila sudah melakukan dekripsi, maka selanjutnya buka file yang telah didekripsikan. Maka file akan kembali menjadi bentuk ketika belum dienkripsikan, berikut hasilnya:



f. Testing Waktu Enkripsi dan Dekripsi AES-128

Uji coba dilakukan dengan menggunakan 9 file dengan format serta setiap file memiliki ukuran beragam. Untuk daftar hasil uji coba seperti berikut:



KESIMPULAN

Dari penelitian yang sudah dilaksanakan terdapat hasil dari uji coba file dan deskripsi aplikasi dengan menggunakan metode AES-128, peneliti menyimpulkan penelitian sebagai berikut :

a. Terciptanya aplikasi enkripsi dan deskripsi file diharapkan dapat memudahkan pengguna dalam mengamankan file yang bersifat rahasia sehingga data-data yang terdapat didalamnya ini tidak mudah bocor.
b. Mampu menerapkan metode Advanced Encryption Standard (AES-128) dengan menggunakan bahasa prmrograman yaitu PHP melalui pencetakan aplikasi web

dan MySQL sebagai databasenya. Melalui penggunaan aplikasi ini dapat sekaligus menjaga keamanan data file yang dimiliki.

c. Dalam penelitian yang telah dilakukan, peneliti telah berhasil melakukan enkripsi dan dekripsi pada file dalam format file docx, ppt-, dan txt.
d. Peneliti telah menciptakan desain menu yang mempermudah pengguna dalam menggunakan aplikasi tersebut dengan memberikan alur yang jelas dan spesifik berupa gambar.
e. Peneliti membuat aplikasi enkripsi dan dekripsi file ini dengan memperhatikan langkah-langkah dan pengujian yang tepat sehingga tidak mudah diakses oleh orang lain.
f. Uji coba yang dilakukan telah berhasil mengamankan file dari pengguna dengan menggunakan 9 file sebagai eksperimen penelitian tersebut.

DAFTAR PUSTAKA

Andi Inayah Auliyah, Implementasi Kombinasi Algoritma Enkripsi Rivest Shamir Adleman (Rsa) dan Algoritma Kompresi Huffman Pada File Document, *"Indonesian Journal of Data and Science (IJODAS)",* vol 1, no 1, pp. 23-28, 2020.

Asri Prameshwari1, Nyoman Putra Sastra2, Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen, *"Jurnal Eksplora Informatika"*, Vol.8, No.1, pp. 52-58, September 2018

Natanael Sijabat1, Nurul Hayaty2, Eka Suswaini3, Implementasi Kriptografi Hybrid Menggunakan Algoritma AES-128 DAN Algoritma Rabin Untuk Mengamankan Data Dalam Database, *"Student Online Jurnal"*, vol.3, no.1, pp. 178-183, 2022.

Niolinda Cristy1, Fristi Riandari2, Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan, *"Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)"*, vol.4, no.2, pp. 75-85, 2021.

Muhammad Azhari1, Dadang Iskandar Mulyana2, Faizal Joko Perwitosari3, Firhan Ali4, 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.

Megawati1, Muhammad Fitra Hamidy2, Sasqia Ismi Aulia3, Yuhendri Putra4, Mhd Arief Hasan, M. Kom5, Enkripsi dan Deskripsi File Menggunakan Kombinasi Vigenere dan Shift Cipher di Python, *"Sains dan Teknologi Informasi (SATIN)"*, vol. 07, no. 01, pp. 102-111, 2021.

Binanda Wicaksana1*, Ma'mun Setiawan2, Penerapan Algoritma Advanced Encryption Standard (AES) untuk Pengamanan Berkas Soal Ujian, *"Jurnal Ilmiah Teknologi Informasi & Sains (TEKNOIS)"*, vol. 10, no. 1, pp. 25-34, 2020.

Arther Ignasius Suranta1, Dolly Virgian Shaka Yudha Sakti2*, Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi, *"Sistem Komputer dan Teknik Informatika (SKANIKA)"*, vol. 5, no. 1, pp. 1-10, 2022.

Imelda Asih Rohani Simbolon1*, Indra Gunawan1, Ika Okta Kirana1, Rafiqa Dewi2, S. Solikhun2, 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.

Nayuni Dwitri1, Sukma Sindi2, Irma Agustika Sihombing3, Indra Gunawan4, Pengamanan Data File Document Menggunakan Kriptografi Encryption System (DES), *"Journal of Information System, Informatics and Computing (JISICOM)"*, vol.4, no.1, pp. 40-45, 2020.