PENERAPAN ALGORITMA ADVANCED ENCRYPTION STANDARD PADA APLIKASI PENGAMANAN DATA TEKS BERBASIS WEB

Elvander Hayon[1], Kristina[2], Amok Darmianto[3]
[1]Informatika[23]Sistem Informasi, Fakultas Teknologi Informasi Universitas Widya Dharma Pontianak
e-mail: [1]20421376_elvander_h@widyadharma.ac.id, [2]kristina@widyadharma.ac.id,
[3]amok_d@ widyadharma.ac.id

Abstract

The continuous development of information technology has an impact on the security of sensitive data and information. Cryptography is one of the relevant techniques to maintain data security and confidentiality. The encryption process converts the original data into an unintelligible format called chipertext, while the decryption process converts the chipertext back into the original data or plaintext. This research designs a cryptographic application using 128 bit AES algorithm to increase the security and trust of users in sending and storing text data. This application helps users protect data and provides a high level of security. The research method used is a literature study. The object-oriented system design analysis technique uses UML to model the system structure. The test results show that the encryption and decryption process runs according to the functionality. Overall, this application can provide confidence to users in securing text data through the encryption and decryption process. This research is expected to be an effective solution for individuals and organizations in maintaining the confidentiality of information. This application is also expected to adapt to the ever-changing development of security technology, so that it remains relevant and effective in the future.
Keywords: *Cryptography, Advanced Encryption Standard Algorithm, web*

Abstrak

Perkembangan teknologi informasi yang terus berkembang memberikan dampak terhadap keamanan data dan informasi yang sensitif. Kriptografi sebagai salah satu teknik yang relevan untuk menjaga keamanan dan kerahasiaan data. Proses enkripsi mengubah data asli menjadi format yang tidak dapat dipahami yang disebut *chipertext*, sedangkan proses dekripsi mengubah *chipertext* kembali menjadi data asli atau *plaintext*. Penelitian ini merancang aplikasi kriptografi menggunakan algoritma AES 128 bit untuk meningkatkan keamanan dan kepercayaan pengguna dalam melakukan pengiriman dan penyimpanan data teks. Aplikasi ini membantu pengguna melindungi data dan memberikan tingkat keamanan yang tinggi. Metode penelitian yang digunakan adalah studi literatur. Teknik analisis perancangan sistem berorientasi objek menggunakan UML untuk memodelkan struktur sistem. Hasil pengujian menunjukan proses enkripsi dan dekripsi berjalan sesuai dengan fungsionalitas. Secara keseluruhan, aplikasi ini dapat memberikan kepercayaan kepada pengguna dalam pengamanan data teks melalui proses enkripsi dan dekripsi. Penelitian ini diharapkan dapat menjadi solusi yang efektif bagi individu maupun organisasi dalam menjaga kerahasiaan informasi. aplikasi ini juga diharapkan dapat beradaptasi dengan perkembangan teknologi keamanan yang terus berubah, sehingga tetap relevan dan efektif di masa depan.

Kata kunci: Kriptografi, Algoritma Advanced Encryption Standard, web

1. PENDAHULUAN

Dalam era teknologi informasi yang terus berkembang, perlindungan data dan informasi menjadi hal yang penting. Perlindungan data diperlukan dalam aktivitas pengiriman dan penyimpanan data bersifat rahasia yang sangat rentan terhadap tindakan kejahatan. Oleh karena itu, penggunaan kriptografi sebagai teknik untuk menjaga keamanan dan kerahasiaan data menjadi semakin relevan.

Kriptografi merupakan seni dan ilmu untuk menjaga keamanan data. Kriptografi menggunakan dua proses untuk mengamankan data yaitu proses enkripsi dan dekripsi menggunakan algoritma AES. Algoritma AES adalah algoritma *block chiper* yang menggunakan kunci simetris pada waktu proses enkripsi dan dekripsi.

Proses enkripsi adalah proses mengubah data asli menjadi bentuk yang tidak dapat dipahami. Proses ini menghasilkan *ciphertext* yang merupakan data yang sudah tersandikan sehingga informasi yang bersifat sensitif tidak dapat terbaca oleh pihak yang tidak berwenang. Untuk mengembalikan data tersebut ke bentuk semula harus melakukan proses dekripsi. Proses dekripsi adalah proses untuk mengembalikan *ciphertext* menjadi *plaintext* yang dapat dibaca dan dimengerti dengan menggunakan kunci yang sama pada saat proses enkripsi.

Berdasarkan penelitian yang telah dilakukan, maka diusulkan untuk merancang sebuah aplikasi kriptografi

berbasis *web* untuk pengamanan data teks yang dapat melakukan enkripsi dan dekripsi menggunakan algoritma AES sehingga tingkat keamanan data menjadi lebih baik dan dapat mengurangi risiko kebocoran data. Aplikasi kriptografi ini diharapkan dapat membantu pengguna melindungi data dan informasi pribadi yang dimiliki.

2. METODE PENELITIAN

2. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah studi literatur berdasarkan kajian literatur berupa buku dan jurnal ilmiah yang berkaitan dengan penelitian.

2.1 Teknik Analisis Perancangan Sistem

Teknik analisis sistem yang digunakan adalah teknik *unified Modeling Language* (UML) sebagai pemodelan untuk menjelaskan alur, prosedur, dan proses proses kerja dari aplikasi yang akan dibangun.

2.2 Perancangan Sistem

Perancangan aplikasi menggunakan Visual Studio Code sebagai *code editor,* PHP dan *javascript* sebagai bahasa pemrograman, serta menggunakan MySQL sebagai *database*.

2.3 Landasan Teori

2.3.1 Data

Data merupakan fakta tentang orang, kejadian-kejadian serta subjek lainnya yang dimanipulasi dan diproses untuk menghasilkan informasi. Data bisa berupa angka, karakter, simbol, gambar, suara, atau tanda-tanda yang bisa digunakan untuk dijadikan informasi[1]. Data merupakan sekumpulan keterangan fakta yang dibuat dengan menggunakan kata-kata, kalimat, simbol serta angka yang didapatkan melalui proses pencarian dan pengamatan berdasarkan sumber tertentu[2].

2.3.2 Aplikasi

Aplikasi adalah suatu piranti lunak atau *website* yang kami kembangkan untuk menemukan layanan yang disediakan oleh pihak ketiga dan mengelola penyediaan layanan serta mendukung komunitas layanan[3]. Aplikasi adalah suatu perangkat lunak (*software*) atau program komputer yang beroperasi pada sistem tertentu yang diciptakan dan dikembangkan untuk melakukan perintah tertentu[4].

2.3.3 Perancangan Sistem

Perancangan sistem adalah tahapan dari siklus pengembangan sistem yang didefinisikan sebagai tahap pendefinisian dari kebutuhan fungsional dan menggambarkan sistem yang dibentuk[5]. Perancangan sistem adalah merancang atau mendesain suatu sistem yang baik, yang isinya adalah langkah-langkah operasi dalam proses pengolahan data dan prosedur untuk mendukung operasi sistem[6].

2.3.4 Kriptografi

Algoritma kriptografi adalah cabang matematika terapan (*applied mathematics*) yang fokus pada pada cara pengubahan atau pengacakan (*encrypt*) sebuah pesan menjadi suatu bentuk pesan yang isinya tidak sesuai dengan pesan yang sebenarnya, lalu nantinya akan disusun kembali (*decrypt*) menjadi bentuk pesan yang asli[7]. *Kriptography* berasal dari bahasa Yunani, yakti *Kripto* dan *Grafia*, *Kripto* berarti *secret* (rahasia) dan *Grafia* berarti *writing* (tulisan) [8].

2.3.5 Algoritma Advanced Encryption Standard

AES adalah algoritma simetris yang menggunakan kunci sama persis pada proses enkripsi dan dekripsi yang diimplementasikan dalam teknik tunggal atau gabungan seperti steganografi atau kompresi data[9]. AES adalah sebuah algoritma enkripsi paket berdasarkan kunci simetris, yang tahan terhadap semua jenis serangan yang dikenal selain serangan kekerasan[10].

2.3.6 Website

Website merupakan sebuah media yang memiliki banyak halaman yang saling terhubung (*HyperLink*), dimana *website* memiliki fungsi dalam memberikan informasi berupa teks, gambar, video, suara dan animasi atau penggabungan dari semuanya[11]. *Website* merupakan kumpulan halaman digital yang berisi informasi berupa teks, animasi, gambar, suara, dan video atau gabungan dari semuanya yang terkoneksi oleh internet, sehingga dapat dilihat oleh siapapun yang terkoneksi jaringan internet[12].

2.3.7 Unified Modeling Language (UML)

Unified Modelling Language (UML) adalah sebuah bahasa yang berdasarkan grafik/gambar untuk memvisualisasi, menspesifikasikan, membangun, dan pendokumentasian sebuah sistem pengembangan perangkat lunak berbasis *Object-Oriented* (OO)[13]. UML adalah singkatan dari *Unified Modelling Language*. UML merupakan salah satu alat bantu pengembangan sistem berorientasi obyek[14].

2.3.8 Visual Studio Code

Visual Studio Code merupakan sebuah aplikasi editor kode sumber terbuka yang dibuat oleh *Microsoft* untuk *Windows, Linux*, dan *MacOS*[15]. Visual Studio Code merupakan salah satu aplikasi editor kode yang dikembangkan oleh *Microsoft*[16].

2.3.9 Black Box Testing

BlackBox Testing merupakan pengujian perangkat lunak yang menguji fungsionalitas aplikasi yang bertentangan dengan struktur internal atau kerja[17]. Pengujian *black box* adalah pengujian yang berfokus pada pengujian persyaratan fungsional perangkat lunak untuk meyakinkan bahwa apakah fungsi-fungsi yang ada sudah berfungsi dengan baik dan tidak memperhatikan struktur logika internal perangkat lunak[18].

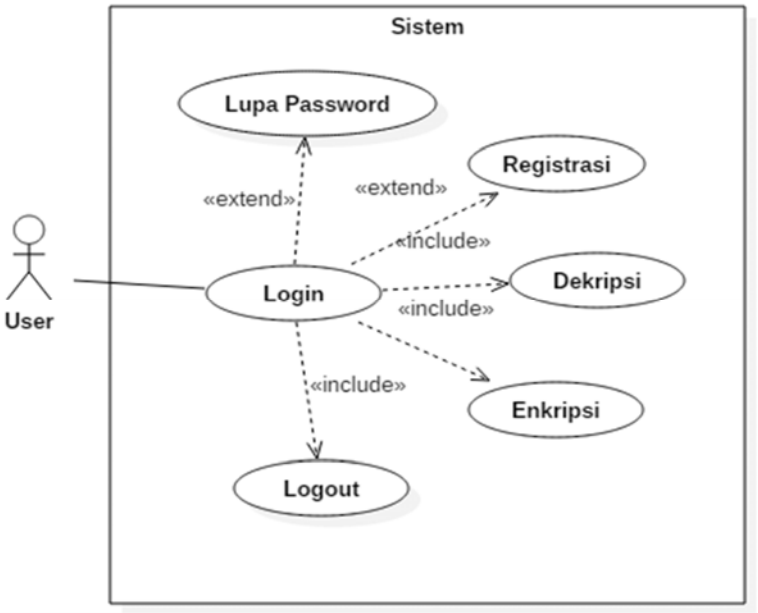
3. HASIL DAN PEMBAHASAN

3.1 Perancangan Unified Modeling Language (UML)

Untuk menggambarkan prosedur, alur, dan proses kerja sistem pada perancangan aplikasi, teknik yang digunakan untuk pemodelan aplikasi adalah *unified modeling language* (UML). Diagram UML yang digunakan dalam perancangan aplikasi yaitu *use case diagram, activity diagram, dan sequence diagram.*

3.1.1 Use Case Diagram

Use Case Diagram merupakan diagram yang berfungsi untuk menggambarkan interaksi antara *user* atau pengguna dengan aplikasi yang akan dikembangkan.



Gambar 1. Use Case Diagram Aplikasi Kriptografi

Tabel 1. Penjelasan Use Case

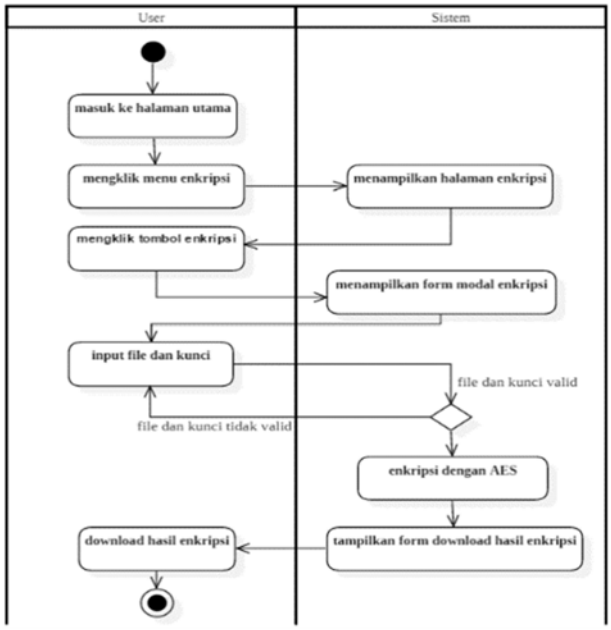
No	Use Case	Keterangan
1	Login	Proses masuknya pengguna ke dalam aplikasi kriptografi
2	Registrasi	Proses pembuatan akun dengan memasukkan data pada form pendaftaran
3	Lupa Password	Proses pembuatan kata sandi baru untuk menggantikan kata sandi sebelumnya
4	Enkripsi	Proses mengubah data menjadi bentuk yang tidak dapat dipahami atau dibaca dengan tujuan untuk menjaga keamanan data
5	Dekripsi	Proses mengembalikan data yang sudah dienkripsi kembali ke bentuk aslinya
6	Logout	Proses pegguna keluar dari aplikasi

3.1.2 Activity Diagram

Activity Diagram menggambarkan berbagai alur aktivitas dalam sistem untuk memberikan gambaran mengenai bagaimana setiap proses berjalan yang sedang dirancang.

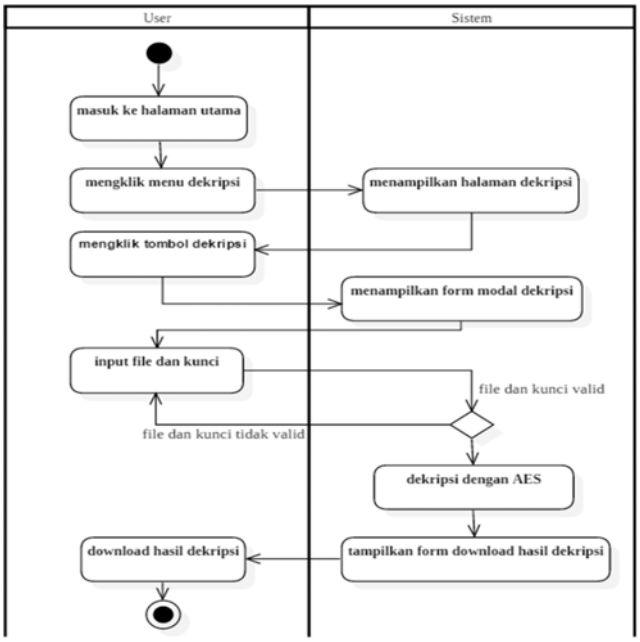
a. Activity Diagram Enkripsi

Gambar 2 merupakan *activity diagram* dari proses enkripsi. Untuk melakukan enkripsi, pada halaman utama pengguna harus memilih menu enkripsi, selanjutnya sistem akan menampilkan halaman enkripsi kepada pengguna. setelah itu, pengguna harus menekan tombol enkripsi terlebih dahulu, kemudian sistem akan menampilkan *form modal* untuk pengguna memasukkan *file* yang ingin dienkripsi dan kunci. Setelah proses enkripsi selesai maka sistem akan menampilkan sebuah *form download* agar pengguna dapat menyimpan *file* hasil enkripsi ke dalam perangkat.



Gambar 2. Activity Diagram Enkripsi

b. Activity Diagram Dekripsi



Gambar 3. Activity Diagram Dekripsi

Gambar 3 merupakan *activity diagram* dari proses dekripsi. Untuk melakukan dekripsi, pada halaman utama pengguna harus memilih menu dekripsi, selanjutnya sistem akan menampilkan halaman dekripsi kepada pengguna. setelah itu, pengguna harus menekan tombol dekripsi terlebih dahulu, kemudian sistem akan menampilkan *form modal* untuk pengguna memasukkan *file* yang sudah terenkripsi dan kunci yang digunakan pada saat proses enkripsi *file* tersebut. Setelah proses dekripsi selesai maka sistem akan menampilkan sebuah *form download* agar pengguna dapat menyimpan *file* hasil dekripsi ke dalam perangkat.

3.2 Perancangan Database

Perancangan *database* merupakan proses merancang struktur *database* yang diperlukan dalam pembuatan aplikasi. Berikut merupakan struktur *database* pada aplikasi yang dirancang.

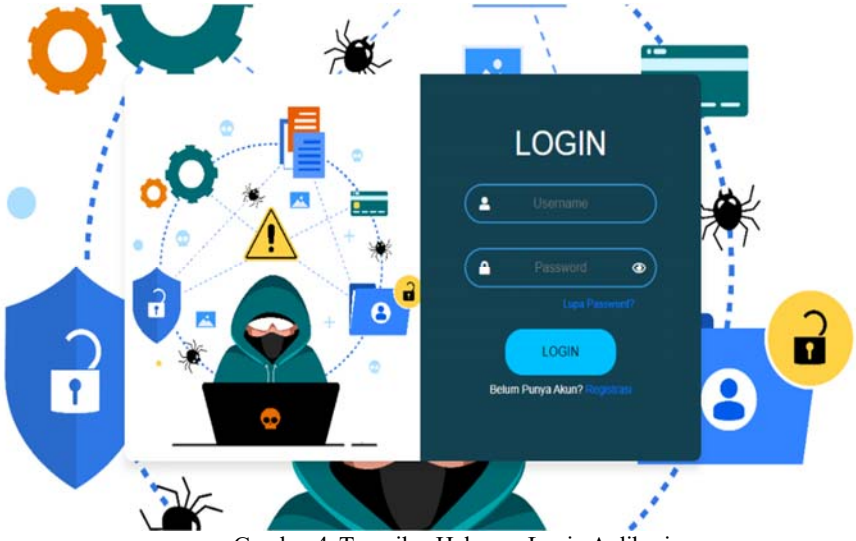
Tabel 2. Struktur Tabel Users

Nama Field	Tipe Data	Ukuran	Keterangan
id	int	11	Auto Increment
username	varchar	255	
password	varchar	255	
email	varchar	255	
reset_token	text		
reset_token_expiration	datetime		
created_datetime	datetime		
aktif	default('N')		
Verification_token	varchar	100	

3.3 Spesifikasi Perangkat

3.3.1 Perangkat Keras

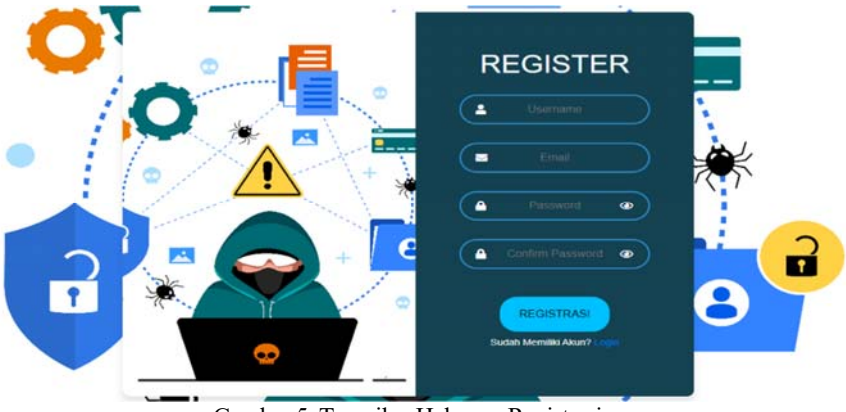
a. Processor AMD Ryzen 3 3200U with Radeon Vega Mobile Gfx 2.60 GHz
b. Minimal RAM 4 GB
c. Kapasitas penyimpanan kosong pada perangkat minimal 200 MB
d. Monitor untuk menampilkan visual aplikasi
e. *Keyboard* dan *mouse* sebagai alat *input* komputer
f. *Wi-Fi adapter* atau kartu jaringan *Wi-Fi*
g. Koneksi internet minimal 2 Mbps



Gambar 4. Tampilan Halaman Login Aplikasi

3.3.2 Perangkat Lunak

a. Aplikasi *browser*
b. Berbagai sistem operasi seperti *windows*, *macOS*, dan *android*.



Gambar 5. Tampilan Halaman Registrasi

3.3 Tampilan Antarmuka Aplikasi Kritografi

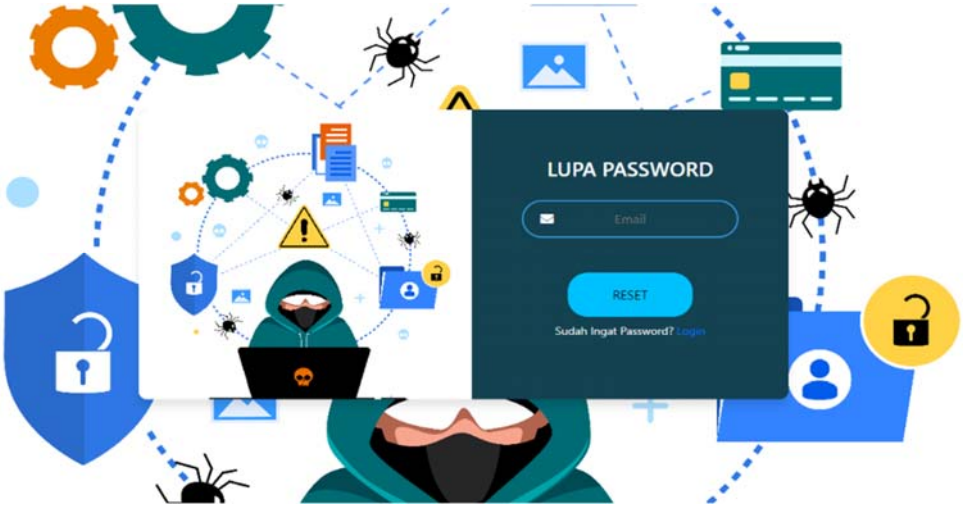
Tampilan antarmuka berfungsi sebagai media untuk menghubungkan pengguna dan sistem untuk dapat saling berinteraksi melalui tampilan visual yang memudahkan pengguna untuk memahami sistem yang dirancang.

3.3.1 Tampilan Halaman Login Aplikasi

Gambar 4 merupakan tampilan halaman *login* pada aplikasi kriptografi. Pada halaman ini pengguna harus memasukkan *username* dan *password* yang sudah didaftarkan sebelumnya untuk masuk ke halaman utama. Setelah itu sistem akan memverifikasi, jika *username* dan *password* yang dimasukkan sudah benar maka pengguna akan langsung diarahkan ke halaman utama aplikasi kriptografi.

3.3.2 Tampilan Halaman Registrasi

Gambar 5 merupakan tampilan dari halaman registrasi akun. Pada halaman ini pengguna yang belum memiliki melakukan registrasi untuk dapat mengakses aplikasi kriptografi. Pengguna diminta untuk memasukkan beberapa informasi yaitu *username*, alamat *email* yang valid, *password* yang kuat, dan konfirmasi *password* yang digunakan untuk proses *login* ketika akun sudah terdaftar.



Gambar 6. Tampilan Halaman Lupa Password

3.3.3 Tampilan Halaman Lupa Password

Gambar 6 merupakan tampilan dari halaman lupa *password*. Pada halaman ini pengguna yang lupa dan ingin membuat *password* baru harus memasukkan terlebih dahulu *email* yang sudah didaftarkan sebelumnya pada *form input*, jika *email* yang dimasukkan sudah benar dan pengguna menekan tombol *reset* maka sistem akan mengirimkan pesan untuk *reset password* ke *email* pengguna untuk mengarahkan ke halaman *reset password*.

3.3.4 Tampilan Halaman Reset Password

Gambar 7 merupakan tampilan dari halaman *reset password*. Pada halaman ini, pengguna harus memasukkan *password* baru dan konfirmasi *password* baru. Setelah kedua *form input* diisi dengan benar dan pengguna mengklik tombol *submit*, maka sistem akan memproses data yang dimasukkan dan *password* pengguna akan diperbarui dan disimpan ke dalam *database* sistem.

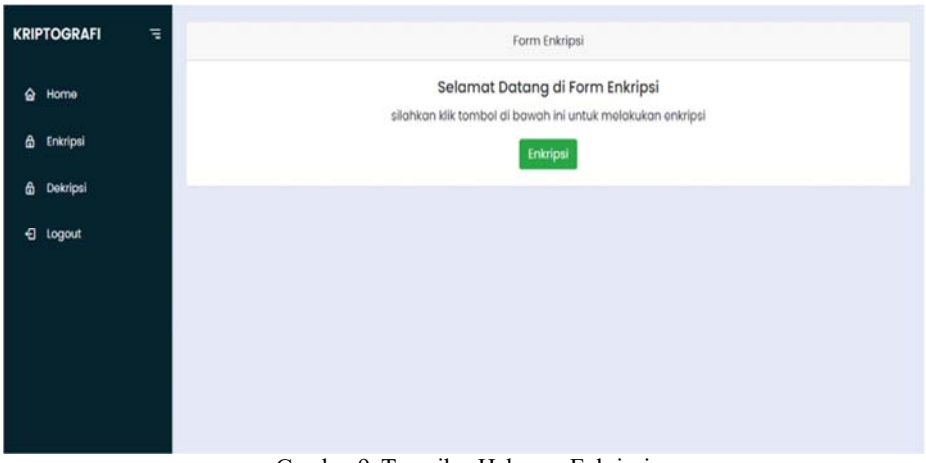
Gambar 7. Tampilan Halaman Reset Password

3.3.5 Tampilan Halaman Utama Aplikasi

Gambar 8. Tampilan Halaman Utama Aplikasi

Gambar 8 merupakan tampilan dari halaman utama aplikasi. Pada halaman utama, terdapat *sidebar navigation* yang berfungsi untuk menampung menu-menu yang terdapat pada aplikasi. Pengguna berpindah dari halaman yang satu ke halaman yang lain melalui *sidebar navigation*. Pada halaman ini juga terdapat tiga *card* yang berisikan informasi singkat tentang *web* kriptografi.

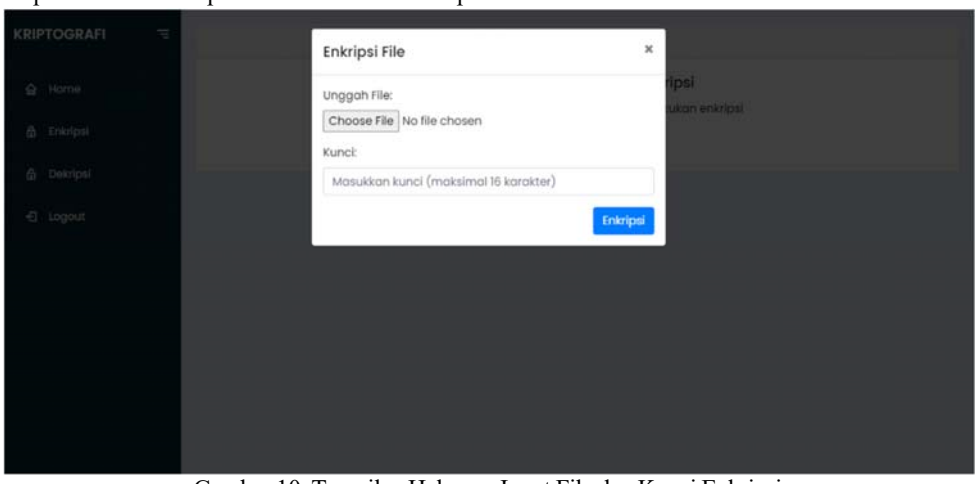
3.3.6 Tampilan Halaman Enkripsi



Gambar 9. Tampilan Halaman Enkripsi

Gambar 9 merupakan tampilan dari halaman enkripsi. Halaman enkripsi merupakan halaman yang digunakan oleh pengguna untuk mengenkripsi *file* yang diinginkan. Pada halaman ini terdapat sebuah tombol "Enkripsi" yang ketika ditekan maka akan menampilkan halaman untuk memasukkan *file* dan kunci untuk dienkripsi.

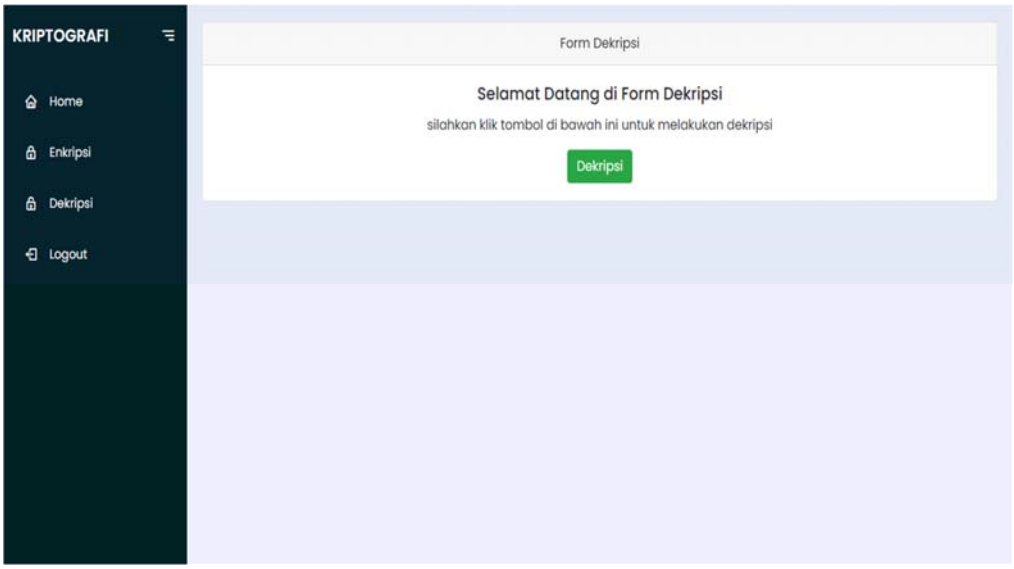
3.3.7 Tampilan Halaman Input File dan Kunci Enkripsi



Gambar 10. Tampilan Halaman Input File dan Kunci Enkripsi

Gambar 10 merupakan tampilan dari halaman *input file* dan kunci yang akan dienkripsi. Halaman ini disebut juga *modal*, pada *modal* tersebut terdapat dua *form input* yang digunakan untuk memasukkan *file* dan kunci enkripsi. *Form input file* digunakan untuk memasukkan *file* yang akan dienkripsi. *Form input* kunci digunakan untuk memasukkan kunci yang diperlukan dalam proses enkripsi dengan panjang maksimal 16 karakter. Selanjutnya dibagian bawah *modal* terdapat sebuah tombol dengan nama enkripsi untuk memproses enkripsi *file* dan kunci. Pada bagian atas *modal* terdapat tombol untuk keluar dari *modal*.

3.3.8 Tampilan Halaman Dekripsi

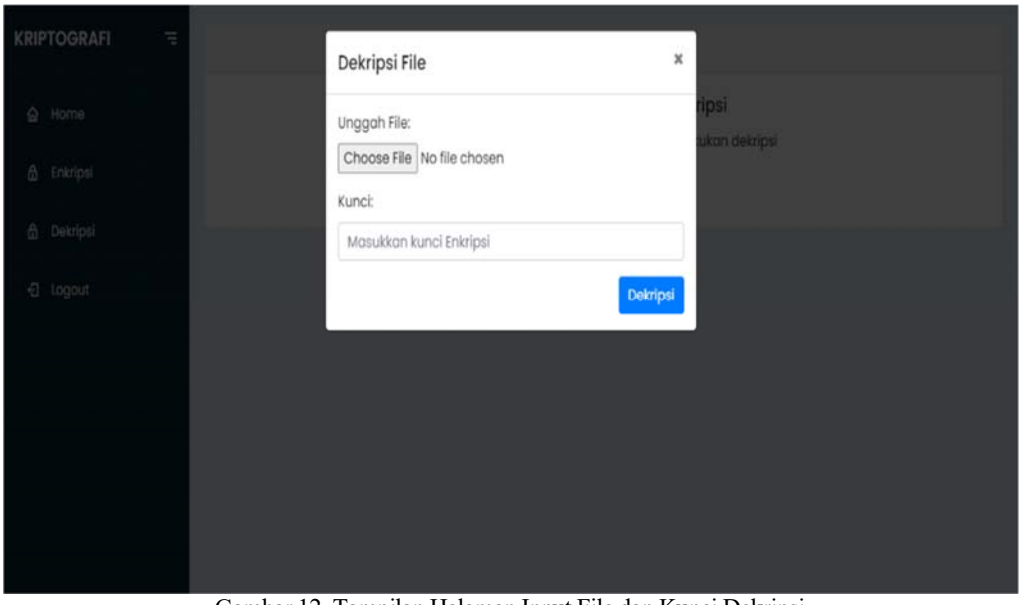


Gambar 11. Tampilan Halaman Dekripsi

Gambar 11 merupakan tampilan dari halaman dekripsi. Halaman dekripsi merupakan halaman yang digunakan oleh pengguna untuk mendekripsi *file* yang sudah dienkripsi. Pada halaman ini terdapat sebuah tombol "Dekripsi" yang ketika ditekan maka akan menampilkan halaman untuk memasukkan *file* yang sudah dienkripsi dan kunci yang digunakan pada proses enkripsi.

3.3.9 Tampilan Halaman Input File dan Kunci Dekripsi

Gambar 12 merupakan tampilan dari halaman *input file* dan kunci dekripsi. Halaman ini disebut juga *modal*, pada *modal* tersebut terdapat dua *form input* yang digunakan untuk memasukkan *file* dan kunci. *Form input file* digunakan untuk memasukkan *file* sudah dienkripsi. *Form input* kunci digunakan untuk memasukkan kunci yang digunakan pada proses. Selanjutnya dibagian bawah *modal* terdapat sebuah tombol dengan nama dekripsi untuk memproses dekripsi *file* dan kunci. Pada bagian atas *modal* terdapat tombol untuk keluar dari *modal*.



Gambar 12. Tampilan Halaman Input File dan Kunci Dekripsi

3.3.10 Pengujian Aplikasi

Pengujian aplikasi merupakan proses mengevaluasi kemampuan dan kinerja aplikasi yang telah dirancang apakah sudah berjalan sesuai dengan hasil yang diharapkan. Pada tahap ini, metode yang diterapkan adalah metode *black box testing*. Pada metode *black box testing*, fokus utama pengujian adalah pada *input* yang diberikan dan *output* yang dihasilkan oleh aplikasi. Proses pengujian menggunakan beberapa skenario kasus untuk memastikan bahwa program berjalan sesuai dengan fungsional yang diharapkan.

3.3.11 Pengujian Pada Halaman Enkripsi

Tabel 2. Pengujian Pada Halaman Enkripsi

No	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil yang Diperoleh	Status Pengujian
1	Mengenkripsi tanpa *file*	*File* kosong	Gagal mengenkripsi	Gagal mengenkripsi	Berhasil
2	Mengenkripsi *file* tanpa kunci	*File* (format yang didukung)	Gagal mengenkripsi	Gagal mengenkripsi	Berhasil
3	Mengenkripsi file dengan ukuran maksimal 30 MB	File(ukuran maksimal 30 MB)	File terenkripsi	File terenkripsi	Berhasil
4	Mengenkripsi *file* dengan panjang kunci melebihi 16 karakter	*File* (format yang didukung)	Gagal mengenkripsi	Gagal mengenkripsi	Berhasil
4	Mengenkripsi *file word* (docx)	*File word* (docx)	File terenkripsi	File terenkripsi	Berhasil
5	Mengenkripsi *file PDF*	*File* (pdf)	File terenkripsi	File terenkripsi	Berhasil
6	Mengenkripsi *file PowerPoint* (ppt)	*File PowerPoint (ppt*)	File terenkripsi	File terenkripsi	Berhasil
7	Mengenkripsi *file* teks (txt)	*File* teks (txt)	File terenkripsi	File terenkripsi	Berhasil
8	Mengenkripsi *file excel* (xlsx)	*File excel* (xlsx)	File terenkripsi	File terenkripsi	Berhasil

Berdasarkan hasil pengujian pada halaman enkripsi yang dapat dilihat pada tabel 2, maka dapat disimpulkan bahwa halaman enkripsi sudah berjalan dengan baik dan sesuai dengan fungsional yang diharapkan. Dapat dilihat dari status pengujian yang menyatakan sistem berhasil mengenkripsi *file* teks yang sudah ditentukan dan fungsi lainnya.

3.3.12 Pengujian Pada Halaman Dekripsi

Tabel 3. Pengujian Pada Halaman Dekripsi

No	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil yang Diperoleh	Status Pengujian
1	Mendekripsi tanpa *file*	*File* kosong	Gagal mendekripsi	Gagal mendekripsi	Berhasil
2	Mendekripsi *file* tanpa kunci	*File* terenkripsi	Gagal mendekripsi	Gagal mendekripsi	Berhasil
3	Mendekripsi file dengan kunci yang salah	*File* terenkripsi	Gagal mendekripsi	Gagal mendekripsi	Berhasil
4	Mendekripsi *file* yang tidak terenkripsi	*File* tidak terenkripsi	Gagal mendekripsi	Gagal mendekripsi	Berhasil
4	Mendekripsi *file word*(docx)	*File* terenkripsi	*File* terdekripsi	*File* terdekripsi	Berhasil
5	Mendekripsi *file PDF*	*File* terenkripsi	*File* terdekripsi	*File* terdekripsi	Berhasil
6	Mendekripsi *file PowerPoint*(ppt)	*File* terenkripsi	*File* terdekripsi	*File* terdekripsi	Berhasil
7	Mendekripsi *file* teks(txt)	*File* terenkripsi	*File* terdekripsi	*File* terdekripsi	Berhasil
8	Mendekripsi *file excel*(xlsx)	*File* terenkripsi	*File* terdekripsi	*File* terdekripsi	Berhasil

Berdasarkan hasil pengujian pada halaman dekripsi yang dapat dilihat pada tabel 3, maka dapat disimpulkan bahwa halaman dekripsi juga berjalan dengan baik sesuai dengan fungsional yang diharapkan. Pada status pengujian, sistem berhasil mendekripsi *file* teks yang sudah terenkripsi dan berhasil menjalankan skenario lainnya.

4. KESIMPULAN

Berdasarkan hasil implementasi dan pengujian pada aplikasi pengamanan data menggunakan algoritma kriptografi AES berbasis *web*, maka dapat disimpulkan beberapa hal sebagai berikut:

a. Pengguna dapat menggunakan aplikasi kriptografi ini untuk melakukan proses enkripsi dan dekripsi terhadap *file* teks.
b. Proses enkripsi dan dekripsi *file*, pengguna harus memiliki *file* dengan format yang sudah ditentukan dan kunci.
c. Kunci enkripsi menggunakan kombinasi 128 bit atau 16 karakter.

5. SARAN

Setelah melakukan implementasi dan pengujian pada aplikasi pengamanan data menggunakan algoritma kriptografi AES berbasis *web*, disimpulkan bahwa aplikasi yang dirancang masih belum sempurna. Sebagai solusinya, disarankan agar aplikasi dapat dikembangkan lebih lanjut dengan menambahkan beberapa hal, yaitu :

a. Menambahkan beberapa fitur untuk melengkapi aplikasi ini agar menjadi lebih baik yaitu fitur seperti kompresi dan conversi data.
b. Menambahkan fitur yang dapat mengamankan berbagai jenis data seperti video dan foto agar dapat lebih bermanfaat kedepannya.
c. Data yang dapat diamankan kedepannya memiliki batasan ukuran lebih dari 30 MB

UCAPAN TERIMA KASIH

Dalam penelitian ini, peneliti telah mendapatkan banyak bantuan berupa bimbingan, petunjuk, dan saran dari berbagai pihak. Pada kesempatan ini, peneliti mengucapkan terima kasih kepada Civitas Akademika Fakultas Teknologi Informasi Universitas Widya Dharma Pontianak serta semua pihak yang telah memberikan bimbingan, petunjuk, dan saran yang berharga untuk penelitian ini. Peneliti juga ingin berterima kasih kepada keluarga tercinta, teman dan dosen yang telah memberikan banyak dukungan dan doa selama menjalani studi dari awal perkuliahan hinggai selesainya penulisan jurnal ini.

DAFTAR PUSTAKA

[1] Jauhari, Achmad, Devie Rosa Anamisa dan Fifin Ayu Mufarroha. (2020). Pengantar Sistem Informasi Model,Siklus, Desain, Sistem Pendukung Keputusan. Media Nusa Creative. Malang.
[2] Manurung, Artha Glory Romey dan Roni Habibi. (2022). Implementasi Data Warehouse Dalam Pengelolaan Barang. Buku Pedia. Bandung.
[3] Supriyadi dan Abi Fajar Fathoni. (2021). Panduan Penggunaan Aplikasi Sport Human Connection Bagi Pelatih Olahraga. Universitas Negeri Malang. Malang.
[4] Juriono. (2023). Panduan Praktis Penggunaan Aplikasi Hadis, Cara Mudah Mencari Dan Meneliti Hadis Versi Digital. Deepublish Digital. Sleman.
[5] Ahmad, Nazaruddin, Erly Krisnanik, Frist Gerit John Rupilele, Anita Muliawati, Nur Syamsiyah, Kraugusteeliana, Bagus Dwi Cahyono, Yesi Sriyeni, Titus Kristanto, Irwanto, Guntoro. (2022). Analisa Perancangan Sistem Informasi Berorientasi Objek. Widina Media Utama. Bandung.
[6] Susanto, Agus. (2022). Pengantar Bisnis. CV Pena Persada. Purwokerto.
[7] Jessica, Patricia. (2024). Cyber Notary Digitalisasi Tanda Tangan. Deepublish. Sleman.
[8] Mukhtar, Harun. (2018). Kriptografi Untuk Keamanan Data. Deepublish. Sleman.
[9] Ravida, Roiya, dan Heru Agus Santoso. (Desember 2020). "Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data Internet of Things (IoT) Tanaman Hidroponik" Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi). Vol. 4, No. 6: hal. 1157-1164.
[10] Shao, Baozhu, Chunhe Song, Zhongfeng Wang, Zhexi Li, Shimao Yu, dan Peng Zeng. (2019). Data Cleaning Based on Multi-sensor Spatiotemporal Correlation. Springer. Switzerland.
[11] Elgamar. (2020). Buku Ajar Konsep Dasar Pemrograman Website Dengan PHP. CV Multimedia Edukasi. Malang.
[12] Ingratubun, Adrian, Ciptono Setyobudi, Frisca Artinus, Dewi Yudho Miranti, Erwin Mulyadi, Ratih Damayanti, Reza Oktavian, Rusman Latief, Safrudiningsih, Suradi, dan Teguh Setiawan. (2023). Perspektif Komunikasi, Media Digital, dan Dinamika Budaya. Kencana. Jakarta.
[13] Sari, Riri Fitri, dan Ardianti Utami S. (2021). Rekayasa Perangkat Lunak Berorientasi Objek Menggunakan PHP. CV ANDI OFSET. Yogyakarta.

[14] Herlinah dan Musliadi. (2019). Pemrograman Aplikasi Android dengan Android Studio, Photoshop, dan Audition. PT Elex Media Komputindo. Jakarta.
[15] Rizky, M, dan Roni Andarsyah. (2023). Komparasi Performa Model Terhadap Klasifikasi Sinyal MIT-BIH Arrhythmia Database. Penerbit Buku Pedia. Bandung.
[16] Sidauruk, Natalya Br, dan Noviana Riza. (2022). Sistem Informasi Koperasi Simpan Pinjam Karyawan. Penerbit Buku Pedia. Bandung.
[17] Ramadhani, Fitriani Dwi dan Maulana Ardhiansyah. (2022). Sistem Prediksi Penjualan Dengan Metode Single Exponential Smoothing Dan Trend Parabolik. Pascal Books. Tangerang.
[18] [Dawis, Mutia, Yusuf Wahyu Setiya Putra, Fitria Fitria, Dini Hamidin, Syifa Nurgaida Yutia, Maniah Maniah, Neneng Rachmalia Feta, Dea Wemona Rahma, dan Fauzan Natsir. (2023). Rekayasa Perangkat Lunak Panduan Praktis Untuk Pengembangan Aplikasi Berkualitas. Widina Media Utama. Bandung.