

PERANCANGAN APLIKASI PENGAMANAN DATA BERBASIS WEB DENGAN PENERAPAN ALGORITMA KRIPTOGRAFI 3DES DAN TWOFISH

Alfred Yulius Arthadi Putra¹, Thommy Willay², Andreas Risky³

¹Informatika, ²Sistem Informasi, Fakultas Teknologi Informasi, Universitas Widya Dharma Pontianak
e-mail: ¹alfredyulius703@gmail.com, ²w.thommy@gmail.com, ³19421281_andreas_r@widyadharma.ac.id

Abstract

In the era of ever-evolving computer technology, the protection of sensitive data and information is becoming increasingly crucial and the main focus. Cryptography as a data disguise technique is increasingly relevant to maintaining the security and confidentiality of information. This study designs cryptographic-based web applications with the 3DES and Twofish algorithms to secure personal data and maintain information integrity. The encryption process converts data into ciphertext which is not easily recognized, while the decryption process returns the ciphertext into readable plaintext. This application makes it easy for users to protect personal data efficiently. The combination of 3DES and Twofish algorithms provides a high level of security and minimizes the risk of data leakage. The research methodology involves the study of literature, analysis of object-oriented systems using UML. For designing web applications, the authors use Visual Studio Code as the Code Editor, PHP and JavaScript as programming languages, and MySQL as the database. The test results show that the encryption and decryption application meets specifications and is able to handle error situations. Overall, this application gives confidence to users in securing document files through efficient encryption and decryption. This research is expected to make a significant contribution in the development of data security systems, becoming an effective solution for individuals and organizations in maintaining the confidentiality of important information.

Keywords: Web, Cryptography, 3DES Algorithm, Twofish Algorithm.

Abstrak

Dalam era teknologi komputer yang terus berkembang, perlindungan data dan informasi sensitif menjadi semakin krusial dan fokus utama. Kriptografi sebagai teknik penyamaran data semakin relevan untuk menjaga keamanan dan kerahasiaan informasi. Penelitian ini merancang aplikasi web berbasis kriptografi dengan algoritma 3DES dan *Twofish* guna mengamankan data pribadi serta menjaga integritas informasi. Proses enkripsi mengubah data menjadi *ciphertext* yang tidak mudah dikenali, sedangkan proses dekripsi mengembalikan *ciphertext* menjadi *plaintext* yang dapat dibaca. Aplikasi ini memudahkan pengguna melindungi data pribadi dengan efisien. Kombinasi algoritma 3DES dan *Twofish* memberikan tingkat keamanan tinggi dan meminimalkan risiko kebocoran data. Metodologi penelitian melibatkan studi literatur, analisis sistem berorientasi objek menggunakan UML. Untuk perancangan aplikasi web, penulis menggunakan Visual Studio Code sebagai *Code Editor*, PHP dan JavaScript sebagai bahasa pemrograman, dan MySQL sebagai basis data. Hasil pengujian menunjukkan aplikasi enkripsi dan dekripsi sesuai spesifikasi dan mampu mengatasi situasi *error*. Secara keseluruhan, aplikasi ini memberikan kepercayaan bagi pengguna dalam mengamankan *file* dokumen melalui enkripsi dan dekripsi yang efisien. Penelitian ini diharapkan memberikan sumbangan signifikan dalam pengembangan sistem keamanan data, menjadi solusi efektif bagi individu dan organisasi dalam menjaga kerahasiaan informasi penting.

Kata Kunci: Web, Kriptografi, Algoritma 3DES, Algoritma *Twofish*,

1. PENDAHULUAN

Dalam era teknologi komputer saat ini, perlindungan data dan informasi yang sensitif menjadi sangat penting. Oleh karena itu, penggunaan kriptografi sebagai Teknik penyamaran data menjadi semakin relevan. Kriptografi melibatkan penggunaan algoritma enkripsi dan dekripsi untuk mengamankan data yang dikirimkan melalui jaringan komunikasi.

Penelitian ini bertujuan untuk merancang sebuah aplikasi enkripsi dan dekripsi data berbasis web menggunakan Teknik kriptografi. aplikasi ini dirancang untuk mengamankan data pribadi dan menjaga kerahasiaan informasi yang dikirimkan atau disimpan dalam sistem. dalam penelitian ini, penulis menggunakan dua jenis algoritma kriptografi, yaitu algoritma 3DES dan *Twofish*.

Pada proses enkripsi, data yang dikirim diubah menjadi bentuk yang tidak mudah dikenali menggunakan algoritma 3DES dan *Twofish*. Proses ini akan menghasilkan *ciphertext*, yang merupakan data yang sudah tersandikan. *Ciphertext* tersebut kemudian dapat dikirim melalui jaringan komunikasi tanpa risiko informasi yang sensitif terbaca oleh pihak yang tidak berwenang.

Saat data yang telah tersandikan tersebut diterima, proses dekripsi dilakukan untuk mengembalikan *ciphertext* menjadi *plaintext* yang dapat dibaca dan dimengerti. Proses dekripsi menggunakan kunci yang sama dengan proses enkripsi sehingga pihak yang memiliki kunci tersebut yang dapat mengakses dan membaca informasi tersebut.

Dengan menggunakan aplikasi enkripsi dan dekripsi berbasis web ini, diharapkan pengguna dapat dengan mudah mengamankan dan melindungi data pribadi mereka. Kombinasi antara algoritma 3DES dan *Twofish* memberikan tingkat keamanan yang lebih tinggi, sehingga risiko kebocoran data dapat diminimalkan.

Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem keamanan data dan menjadi solusi bagi individu maupun organisasi dalam menjaga kerahasiaan informasi penting.

2. METODE PENELITIAN

1.1 Metodologi Penelitian

1.1.1 Rancangan Penelitian

Dalam penelitian ini, menggunakan perancangan penelitian deskriptif, dengan mengkaji literatur-literatur untuk merancang web pengamanan data dengan algoritma 3DES dan *Twofish*.

1.1.2 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah studi literatur, yang dimana penulis mengumpulkan data berdasarkan kajian literatur seperti buku, jurnal, dan laporan penelitian, yang berkaitan dengan objek penelitian.

1.1.3 Teknik Analisis Sistem

Teknik analisis sistem yang digunakan adalah menggunakan teknik berorientasi dengan objek dengan alat pemodelan *Unified Modeling Language (UML)*, yang digunakan peneliti untuk menjelaskan alur, prosedur, dan proses kerja dari website yang akan dibangun.

1.1.4 Teknik Perancangan Sistem

Aplikasi website dirancang menggunakan Visual Studio Code sebagai *code editor*, PHP dan javascript untuk bahasa pemrograman, serta menggunakan MySql sebagai *Database Management System (DBMS)*

1.2 Landasan Teori

1.2.1 Data

Data merupakan sekumpulan informasi atau nilai yang diperoleh dari pengamatan (suatu objek, data dapat berupa angka dan dapat pula merupakan lambang atau sifat, beberapa macam data antara lain: data populasi dan data sampel, data observasi, data primer dan data sekunder^[1]. Data merupakan fakta-fakta mentah yang mewakili kejadian-kejadian yang berlangsung dalam organisasi atau lingkungan fisik sebelum ditata dan diatur kedalam bentuk yang dapat dipahami dan digunakan orang^[2].

1.2.2 Perancangan Sistem

Perancangan Sistem adalah suatu proses memahami sistem kemudian merancang sistem informasi yang berbasis komputer, dimana hasilnya nanti adalah berupa sistem komputerisasi^[3]. Perancangan Sistem merupakan sebuah proses penerapan teknologi informasi dalam rangka mencapai suatu tujuan menyelesaikan suatu masalah. Mengurai permasalahan yang besar dan kompleks menjadi beberapa bagian kecil yang dapat diatur untuk diselesaikan^[4].

1.2.3 Kriptografi

Kriptografi adalah ilmu yang mempelajari teknis matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data, autentikasi entitas dan autentikasi keaslian data^[5]. Kriptografi pada dasarnya terdiri dari dua proses, yaitu proses enkripsi dan proses dekripsi. Proses enkripsi adalah proses penyandian pesan terbuka menjadi pesan rahasia^[6].

1.2.4 Algoritma Triple DES

Algoritma 3DES adalah versi upgrade dari algoritma DES, algoritma ini menerapkan algoritma DES tiga kali untuk setiap blok data. Akibatnya, proses ini membuat 3DES lebih sulit dipecahkan daripada pendahulunya DES^[6]. Algoritma 3DES merupakan proses DES tunggal tiga langkah yang melibatkan pertama-tama pengenkripsian blok masukan menggunakan DES tunggal dengan satu kunci, kemudian pendekripsian blok masukan menggunakan DES tunggal dengan kunci lain, kemudian pengenkripsian blok itu kembali dengan kunci pertama yang digunakan atau kunci lain yang berbeda^[7].

1.2.5 Algoritma Twofish

Algoritma *Twofish* menggunakan jaringan feistel 16 putaran dan 4 kotak-S yang bergantung pada key. Terdapat empat macam *key schedule* dalam implementasinya yaitu: *full keying*, *partial keying*, *minimal keying*, dan *zero keying* dengan perbedaan dalam *key setup*^[8]. Algoritma *Twofish* adalah kode cipher blok kunci simetris. Algoritma ini ditemukan oleh laboratorium counterpane. Algoritma *Twofish* gratis digunakan untuk semua jenis tujuan karena tidak dipatenkan dan kode sumbernya bukan hak cipta^[9].

1.2.6 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^[10]. *Website* atau situs dapat diartikan sebagai kumpulan halaman yang digunakan untuk menampilkan informasi teks, gambar diam atau gerak, animasi, suara atau gabungan dari semuanya baik

yang bersifat statis maupun dinamis yang membentuk suatu rangkaian bangunan yang saling terkait, yang masing-masing dihubungkan dengan jaringan-jaringan halaman^[11].

1.2.7 Unified Modeling Language (UML)

UML merupakan seperangkat diagram dan notasi yang memiliki standar untuk memodelkan sistem yang berorientasi objek, serta menjelaskan semantik yang dijadikan dasar arti dari diagram dan simbol^[12]. *Unified Modeling Language* (UML) merupakan sebuah bahasa visual untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung^[13].

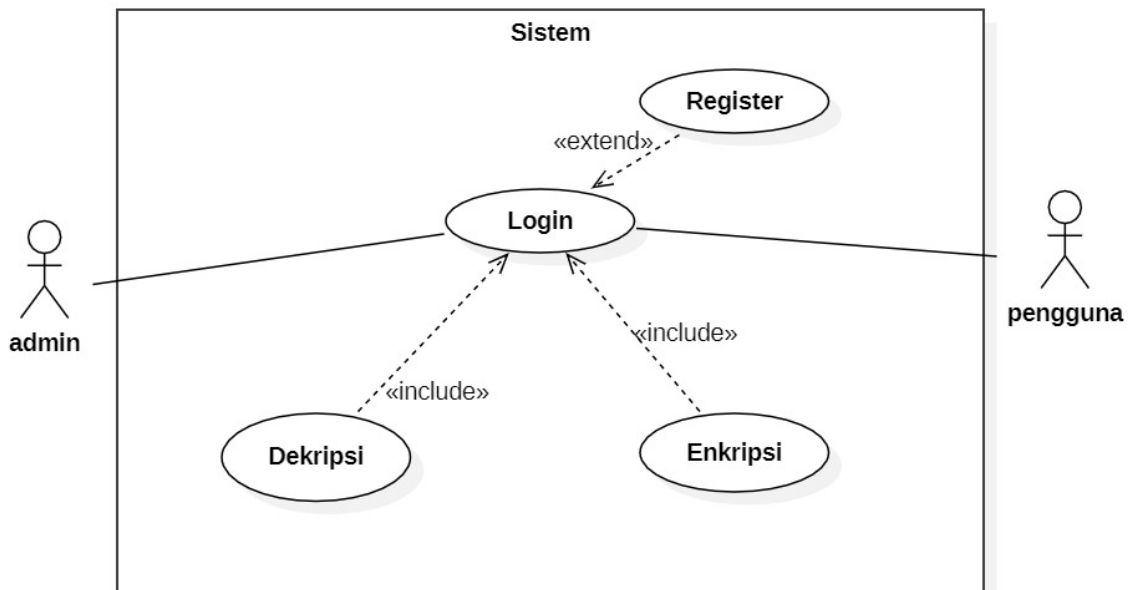
3. HASIL DAN PEMBAHASAN

3.1 Perancangan Unified Modeling Language (UML)

Untuk menggambarkan prosedur, aliran, atau proses kerja sistem pada perancangan aplikasi, penulis menggunakan Teknik pemodelan *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

Diagram use case digunakan untuk mendeskripsikan sebuah interaksi antara salah satu atau lebih aktor dengan website yang akan dibuat. Aktivitas-aktivitas pengguna dengan website diharapkan dapat digambarkan dengan use case diagram.



Gambar 1. Diagram Use Case Website Kriptografi

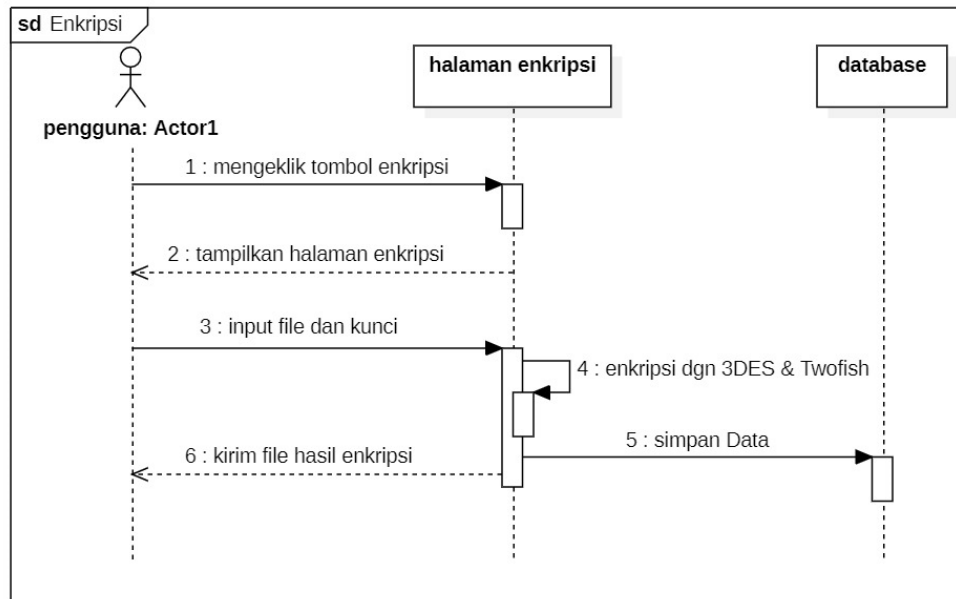
Tabel 1. Penjelasan Use Case

No	Use Case	Deskripsi
1	Login	Proses/kegiatan masuknya pengguna ke dalam website dengan hak ases sebagai pengguna.
2	Register	Proses dimana pengguna menginputkan data dengan mengisi form pendaftaran untuk membuat akun baru.
3	Enkripsi	proses mengubah informasi menjadi kode yang tidak dapat dimengerti atau dibaca dengan tujuan untuk menjaga keamanan informasi.
4	Dekripsi	Proses mengembalikan data atau pesan yang telah dienkripsi ke bentuk asalnya atau <i>plaintext</i> .

3.1.2 Sequence Diagram

Sequence diagram digunakan untuk menggambarkan berbagai alur kerja aktivitas dalam suatu website. Aktivitas yang terjadi dapat digambarkan sebagai berikut:

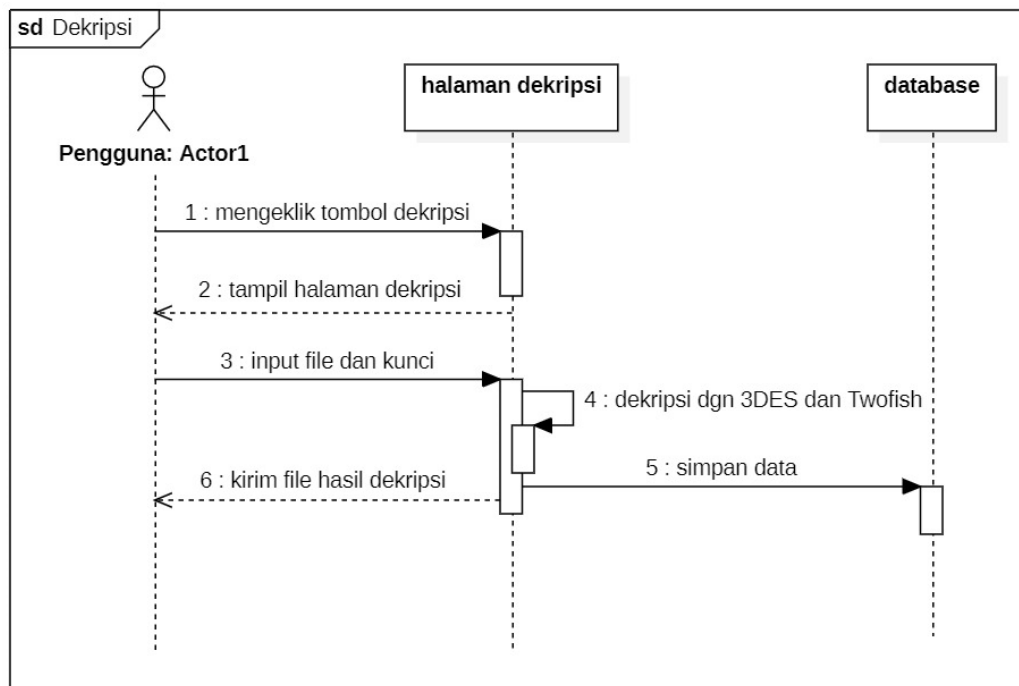
3.1.2.1 Sequence Diagram Enkripsi



Gambar 2. Sequence Diagram Enkripsi

Gambar 2 merupakan *sequence diagram* enkripsi. Untuk dapat melakukan enkripsi, pada menu utama, pengguna harus memilih menu enkripsi, selanjutnya sistem akan memanggil halaman enkripsi. Selanjutnya pengguna menginputkan *file* yang akan dienkripsi dan kunci enkripsi. Setelah *file* dan kunci diinputkan, selanjutnya sistem akan menjalankan proses enkripsi dengan algoritma 3DES dan *Twofish*. Setelah proses enkripsi selesai, selanjutnya data hasil enkripsi akan disimpan ke dalam *database*. *File* hasil enkripsi akan otomatis terunduh pada perangkat yang digunakan pengguna.

3.1.2.2 Sequence Diagram Dekripsi



Gambar 3. Sequence Diagram Dekripsi

Sesuai *sequence diagram* dekripsi di atas, pada menu utama, pengguna memilih menu dekripsi, sistem akan memanggil halaman dekripsi dan akan langsung ditampilkan kepada pengguna. Selanjutnya pada halaman dekripsi tersebut pengguna menginputkan *file* terenkripsi dan kunci enkripsi *file* tersebut. setelah *file* dan kunci dimasukkan, sistem akan menjalankan proses dekripsi dengan algoritma 3DES dan *Twofish*. Ketika proses dekripsi selesai, data

hasil dekripsi tersebut kemudian akan disimpan ke *database* dan *file* hasil enkripsi akan terunduh otomatis pada perangkat yang digunakan oleh pengguna.

3.2 Perancangan Database

Perancangan database merupakan sebuah pembuatan struktur database yang dibutuhkan untuk merancang website yang dirancang oleh penulis.

Tabel 2. Struktur Tabel Enkripsi

Nama Field	Tipe Data	Ukuran	Keterangan
<i>Id</i>	<i>Int</i>		<i>Auto Increment</i>
<i>File</i>	<i>Varchar</i>	100	
Kunci	<i>Varchar</i>	50	MD5
<i>Created_at</i>	<i>Datetime</i>		<i>Current Datetime</i>

Tabel 3. Struktur Tabel Dekripsi

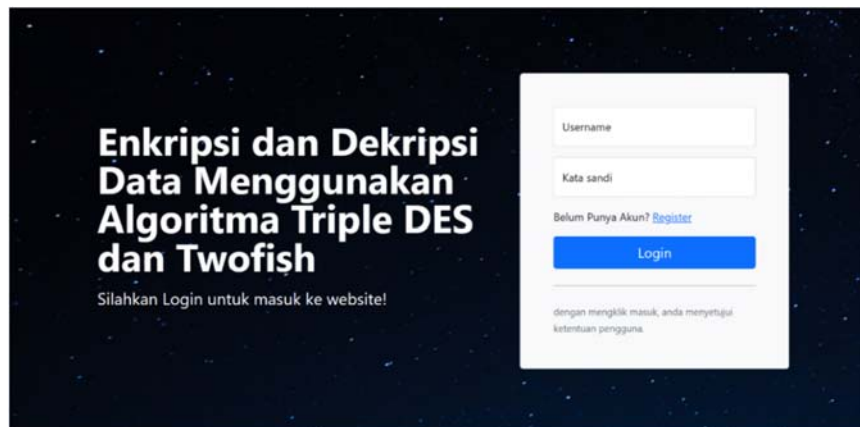
Nama Field	Tipe Data	Ukuran	Keterangan
<i>Id</i>	<i>Int</i>		<i>Auto Increment</i>
<i>File</i>	<i>Varchar</i>	100	
Kunci	<i>Varchar</i>	50	MD5
<i>Created_at</i>	<i>Datetime</i>		<i>Current Datetime</i>

Tabel 4. Struktur Tabel User

Nama Field	Tipe Data	Ukuran	Keterangan
<i>Id</i>	<i>Int</i>		<i>Auto Increment</i>
<i>Username</i>	<i>Varchar</i>	20	
<i>Password</i>	<i>Varchar</i>	20	MD5
<i>Email</i>	<i>Varchar</i>	20	
<i>Verify_token</i>	<i>Varchar</i>	50	
<i>Verify_status</i>	<i>Tinyint</i>	2	<i>Default = 0</i>

3.3 Tampilan Antarmuka Web Kriptografi

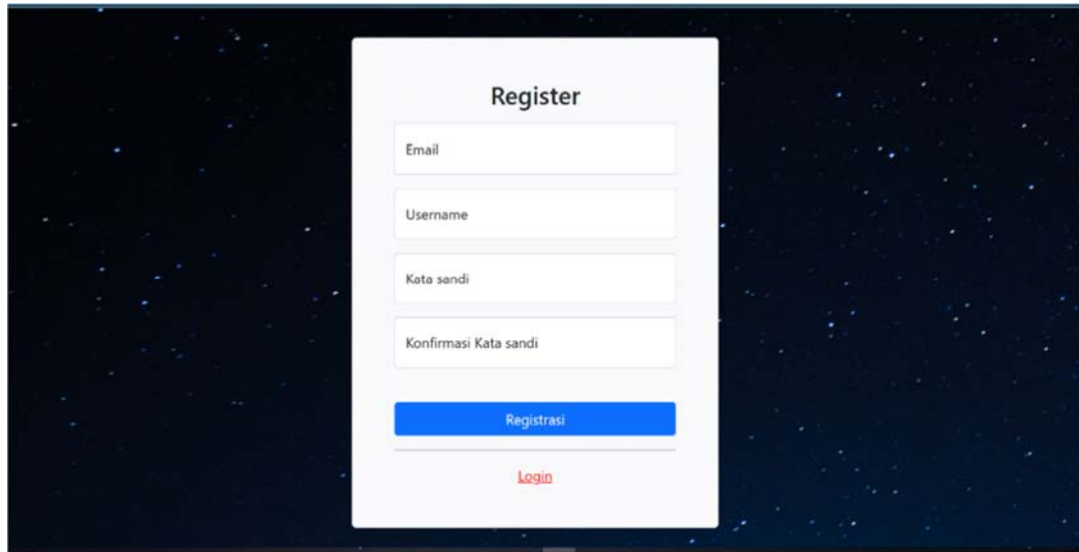
3.3.1 Tampilan Login Website



Gambar 4. Tampilan Login Website

Gambar 4 merupakan tampilan dari halaman login. Halaman login merupakan halaman awal yang akan ditampilkan kepada pengguna ketika membuka website kriptografi. dimana pada halaman ini, pengguna harus memasukkan informasi berupa username dan kata sandi yang benar agar dapat masuk ke dalam website. Setelah login berhasil maka pengguna akan diarahkan ke halaman utama website.

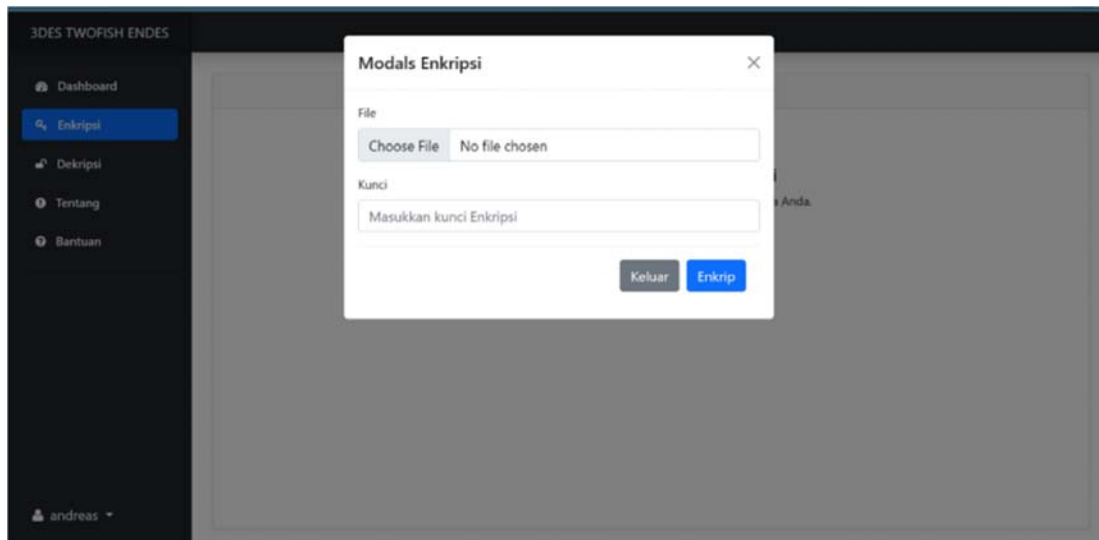
3.3.2 Tampilan Halaman Register



Gambar 5. Tampilan Halaman Register

Gambar 5 merupakan tampilan dari halaman register website kriptografi. pada halaman *register* ini, pengguna mendaftarkan akun untuk dapat mengakses aplikasi kriptografi dan melakukan enkripsi dekripsi *file* dokumen. Pengguna harus memasukkan beberapa data yang harus diisi seperti alamat *email* pengguna, *username* dan kata sandi untuk proses *login* nantinya.

3.3.3 Tampilan Halaman Enkripsi

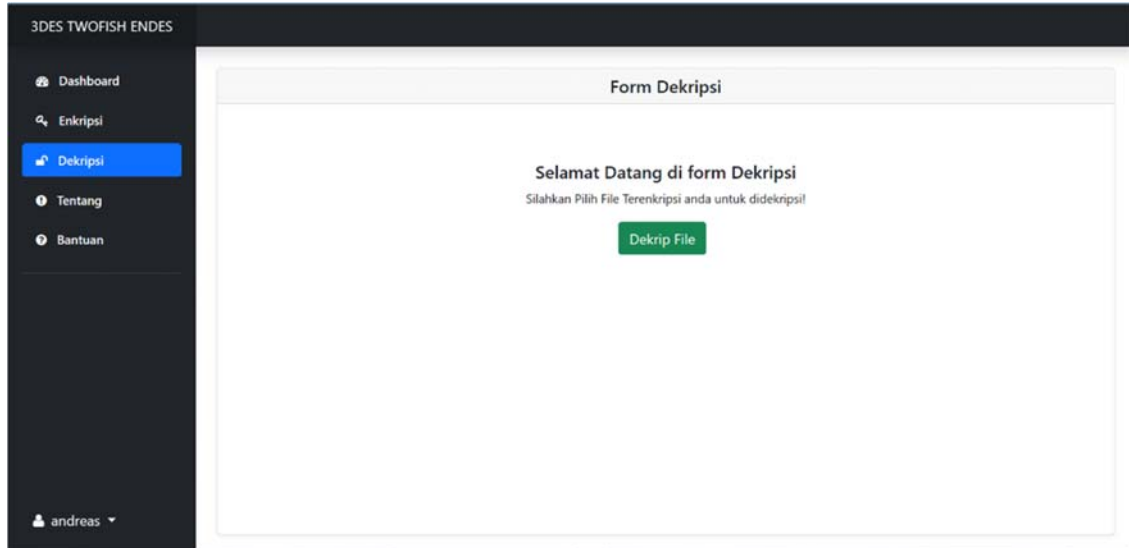


Gambar 6. Tampilan Halaman Enkripsi

Gambar 6 merupakan tampilan dari halaman *input file* dan kunci enkripsi. Pada halaman sebelumnya, ketika tombol Enkrip *File* ditekan maka akan menampilkan halaman seperti pada gambar. Pada halaman ini pengguna memasukkan *file* dokumen yang akan dienkripsi serta memasukkan kunci yang akan digunakan dalam proses pengenkripsian. Kunci ini nantinya akan dipakai ketika akan mendekripsi *file* terenkripsi tersebut. Dalam proses enkripsi, *file* yang boleh dienkripsi adalah *file* word, pdf, ppt/pptx, dan *file* teks sederhana atau txt. Jika pengguna menekan “*Choose File*” maka sistem akan membuka jendela halaman eksplorer sehingga pengguna dapat memilih *file* yang akan mereka lakukan enkripsi. Setelah memilih *file* yang akan dienkripsi, selanjutnya pengguna harus memasukkan kunci berupa kombinasi angka dan huruf yang nantinya kunci ini akan digunakan dalam proses

pengenkripsian. Jika sudah memasukkan *file* dan kunci selanjutnya pengguna harus menekan tombol “Enkrip” dan *file* akan langsung terenkripsi. *File* hasil enkripsi akan otomatis terdownload ke perangkat yang digunakan.

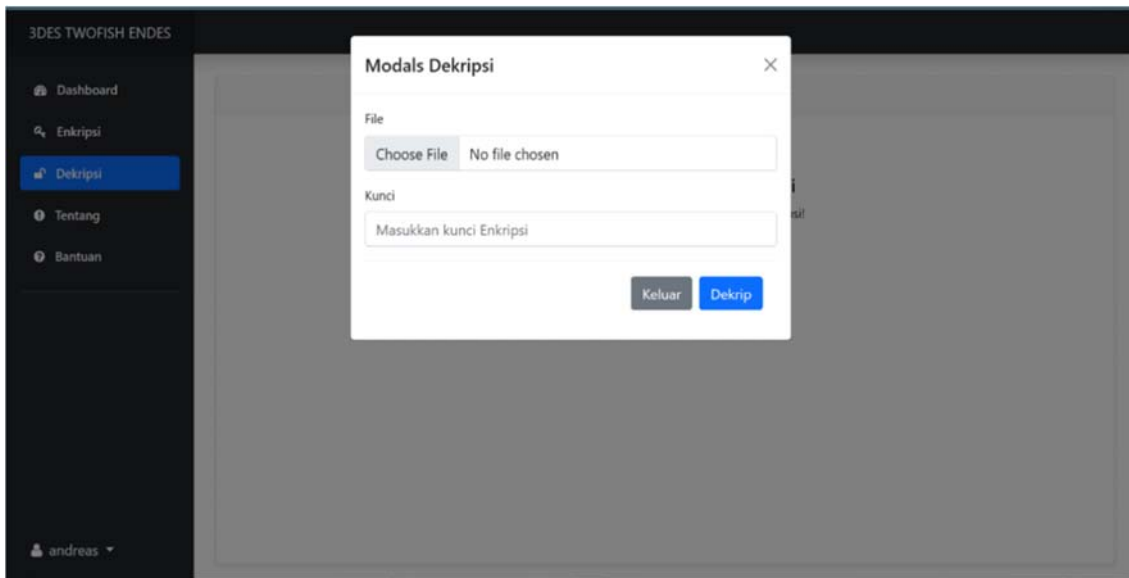
3.3.4 Tampilan Halaman Dekripsi



Gambar 7. Tampilan Halaman Dekripsi

Gambar 7 merupakan tampilan dari halaman dekripsi. Pada halaman ini terdapat sebuah tombol “Dekrip *File*” yang gunanya adalah untuk memanggil dan menampilkan halaman lain yaitu halaman *input file* dan kunci. Pada halaman *input* tersebut pengguna dapat mendekripsi *file* yang sudah terenkripsi sebelumnya. Sama seperti halaman lainnya, pada halaman ini juga terdapat menu *sidebar navigation* yang gunanya untuk navigasi atau berpindah dari satu halaman ke halaman lainnya. Pada bagian bawah navigasi menu terdapat tombol *Logout* yang gunanya untuk keluar dari akun yang sedang aktif atau sedang *login*.

3.3.5 Tampilan Halaman Input File Terenkripsi dan Kunci Enkripsi



Gambar 8. Tampilan Halaman Input File Terenkripsi dan Kunci Enkripsi

Gambar 8 merupakan tampilan dari halaman *input file* terenkripsi dan kunci enkripsi. Halaman ini akan muncul ketika pengguna menekan tombol “Dekrip *File*” pada halaman dekripsi sebelumnya. Pada halaman ini, pengguna memasukkan *file* dokumen yang sudah terenkripsi serta memasukkan kunci yang digunakan pada saat proses enkripsi *file* tersebut. Jika *file* dan kunci sudah diinputkan, selanjutnya pengguna menekan tombol Dekrip untuk memulai proses Dekrip pada *file* yang dipilih. Jika kunci yang diinputkan sudah sesuai maka *file* akan berhasil terdekrip, namun jika kunci yang dimasukkan salah, maka proses Dekrip akan gagal dan muncul pemberitahuan bahwa kunci yang diinputkan tidak valid.

3.3 Pengujian Aplikasi

Pengujian aplikasi merupakan proses mengeksekusi program yang telah dibangun yang bertujuan untuk mengevaluasi kemampuan sebuah program atau sistem dan menentukan apakah program tersebut dapat berjalan sesuai dengan hasil yang diharapkan. Dalam proses pengujian, penulis mencoba beberapa skenario kasus untuk memastikan bahwa program yang dihasilkan sesuai dengan kebutuhan yang sebelumnya sudah ditentukan.

3.3.1 Pengujian Pada Proses Enkripsi

Tabel 5. Pengujian Pada Proses Enkripsi

No	Skenario Pengujian	Nama File	Ukuran file	Hasil yang diharapkan	Waktu pemrosesan	Validasi
1	Mengenkripsi file word (docx)	Full Bab Skripsi - Copy.docx	9,3 MB	File terenkripsi	7,6 Detik	Berhasil
2	Mengenkripsi file word (docx)	Jurnal.docx	2,1 MB	File terenkripsi	2,7 Detik	Berhasil
3	Mengenkripsi file PDF	BAB IV.pdf	1,3 MB	File terenkripsi	5 Detik	Berhasil
4	Mengenkripsi file PDF	Filebaru.pdf	7 MB	File terenkripsi	8 Detik	Berhasil
5	Mengenkripsi file PowerPoint (ppt)	Cryptocurrency.ppt	6,8 MB	File terenkripsi	5,5 Detik	Berhasil
6	Mengenkripsi file PowerPoint (ppt)	PPT.ppt	1,8 MB	File terenkripsi	2,3 Detik	Berhasil
7	Mengenkripsi file teks (txt)	File Test Txt.Txt	1,2 MB	File terenkripsi	1,8 Detik	Berhasil
8	Mengenkripsi file foto	Foto9.jpg	544 Kb	Gagal mengenkripsi	2,8 Detik	Berhasil

3.3.1.1 Hasil Enkripsi File

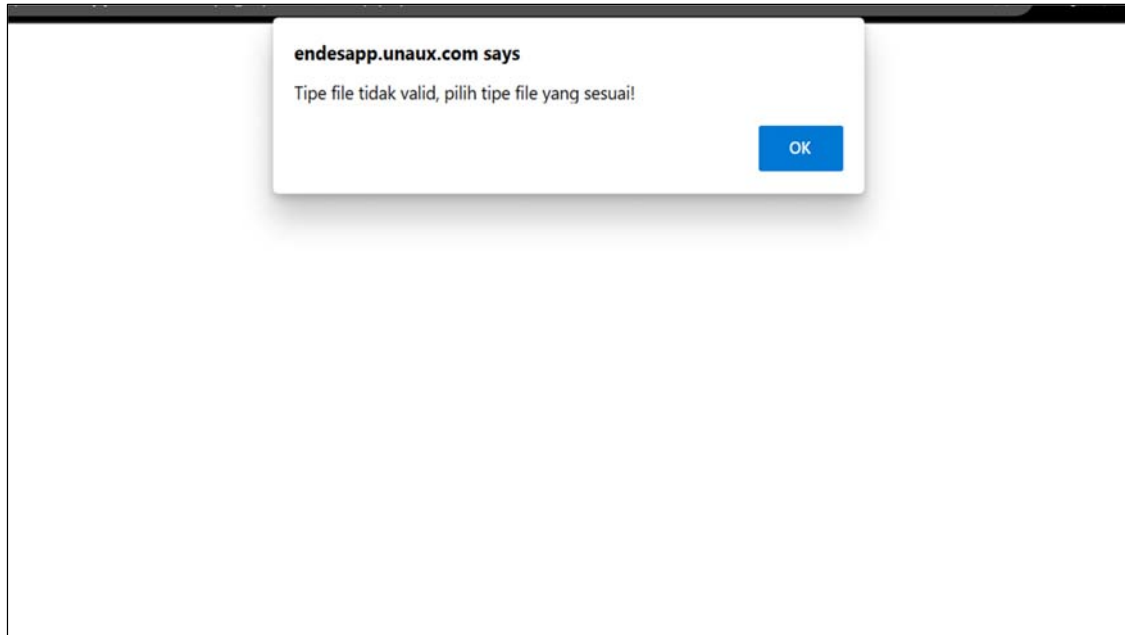


Gambar 9. Hasil Enkripsi File

Berdasarkan hasil pengujian proses Enkripsi yang dapat dilihat pada tabel 5 , maka dapat ditarik kesimpulan bahwa sistem mampu mengenkripsi berbagai file dokumen yang telah ditentukan sebelumnya dan menjalankan

fungsi-fungsi lainnya seperti yang diharapkan. Pengamatan terhadap status pengujian juga mengindikasikan bahwa proses enkripsi dapat diselesaikan dalam waktu yang relatif singkat, menunjukkan kemampuan sistem dalam menangani tugas-tugas tersebut secara efisien. Hasil positif dari pengujian ini memberikan keyakinan bahwa mekanisme enkripsi yang diimplementasikan telah sesuai dengan tujuan fungsional sistem dan telah berhasil memenuhi standar performa yang diharapkan.

3.3.1.2 Hasil Enkripsi File Foto



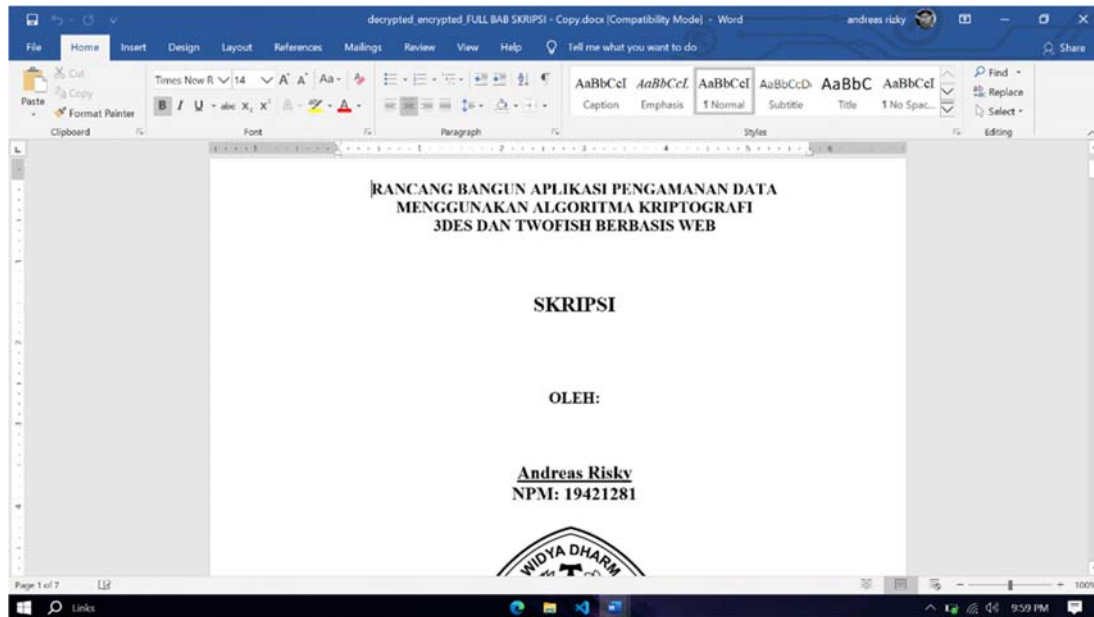
Gambar 10. Hasil Enkripsi File Foto

3.3.2 Pengujian Pada Proses Dekripsi

Tabel 6. Pengujian Pada Proses Dekripsi

No	Skenario Pengujian	Nama File	Ukuran file	Hasil yang diharapkan	Waktu pemrosesan	Validasi
1	Mendenkripsi file word (docx)	encrypted_FULL BAB SKRIPSI - Copy.docx	9,3 MB	File terdekripsi/file asli	9,5 Detik	Berhasil
2	Mendenkripsi file word (docx)	encrypted_jurnal.docx	2,1 MB	File terdekripsi/file asli	3,4 Detik	Berhasil
3	Mendenkripsi file PDF	encrypted_BAB IV.pdf	1,3 MB	File terdekripsi/file asli	7,2 Detik	Berhasil
4	Mendenkripsi file PDF	encrypted_filebaru.pdf	7 MB	File terdekripsi/file asli	11,6 Detik	Berhasil
5	Mendenkripsi file PowerPoint (ppt)	encrypted_Cryptocurrency.pptx	6,8 MB	File terdekripsi/file asli	8 Detik	Berhasil
6	Mendenkripsi file PowerPoint (ppt)	encrypted_PPT.pptx	1,8 MB	File terdekripsi/file asli	3,3 Detik	Berhasil
7	Mendenkripsi file teks (txt)	encrypted_file test txt.txt	1,2 MB	File terdekripsi/file asli	2,4 Detik	Berhasil

3.3.2.1 Hasil Dekripsi File



Gambar 11. Hasil Dekripsi File

Berdasarkan hasil pengujian proses dekripsi yang dapat dilihat pada tabel 6, maka dapat ditarik kesimpulan bahwa proses dekripsi juga sudah berjalan dengan baik dan sesuai dengan spesifikasi fungsional yang diharapkan. pada status pengujian dimana sistem berhasil mendekripsi *file-file* dokumen yang sudah terenkripsi. Dan berhasil menjalankan berbagai skenario kasus lainnya.

4. KESIMPULAN

Berdasarkan hasil implementasi dan pengujian aplikasi pengamanan data menggunakan algoritma kriptografi 3DES dan *Twofish* berbasis web yang sudah dibahas pada bab-bab sebelumnya, maka penulis dapat menarik beberapa kesimpulan sebagai berikut:

- Pengguna dapat menggunakan *website* Kriptografi ini untuk mengenkripsi dan mendekripsi *file* dokumen.
- Aplikasi kriptografi yang dibuat merupakan aplikasi yang dikhususkan untuk mengenkripsi dan dekripsi *file* dokumen.
- semakin besar ukuran *file*, waktu pemrosesan cenderung lebih lama, namun demikian, meskipun pada *file* yang lebih besar, waktu pemrosesan tetap berada dalam kisaran yang cukup cepat.
- metode Enkripsi yang digunakan efektif dalam mengamankan *file* Word dengan waktu pemrosesan yang memadai. Dengan keberhasilan mencapai hasil yang diharapkan dan efisiensi waktu, metode enkripsi ini menjadi pilihan yang baik dalam upaya menjaga kerahasiaan dan keamanan data dalam *file* Word berukuran besar maupun kecil.

5. SARAN

Setelah melakukan implementasi aplikasi pengamana data menggunakan algoritma kriptografi 3DES dan *Twofish* berbasis web, peneliti menyadari bahwa aplikasi yang dirancang dan dibangun masih belum sempurna. Oleh karena itu, peneliti memberikan beberapa saran agar aplikasi dapat dikembangkan lebih lanjut pada penelitian selanjutnya, antara lain:

- Penulis berharap aplikasi ini dapat dikembangkan oleh pembaca yang tertarik untuk mengembangkan fitur enkripsi seperti menambahkan ekstensi *file* lain yang dapat dienkripsi.
- Mengembangkan aplikasi kriptografi pada *platform* android atau IOS sehingga menjadi banyak dikenal dan digunakan.

UCAPAN TERIMA KASIH

Dalam penelitian ini, peneliti telah banyak mendapatkan bantuan berupa bimbingan, petunjuk, dan saran, dan dorongan moral dari berbagai pihak, maka pada kesempatan ini peneliti mengucapkan terima kasih kepada civitas akademika Fakultas Teknologi Informasi Universitas Widya Dharma Pontianak, serta kepada keluarga

tercinta yang telah banyak memberikan dukungan serta doa kepada peneliti selama menjalani studi dari awal perkuliahan hingga selesainya penulisan jurnal ini.

DAFTAR PUSTAKA

- [1] Simarmata, Janner, Sasongko, Dwi, Sihotang, Jannes Ismail, Yuswardi, Rohmah, Miftahul Fadhilah, Umar, Siti Aisyah Hayati, Arni, Siska, Sugianto, Jamaludin, dan Akhriana, Adelia. (2022) *Sistem Keamanan Data*. Yayasan Kita Menulis. Medan.
- [2] Kadir, Abdul. (2020). *Dasar Perancangan dan Implementasi Database Relasional (Edisi Revisi)*. Penerbit Andi. Yogyakarta.
- [3] Santi, Irma Hidayanti. (2020). *Analisa Perancangan Sistem*. Penerbit NEM. Bojong.
- [4] Rozaq, Abdul, dan Fauzan, Riski. (2020). *Konsep Perancangan Sistem Informasi Bisnis Digital*. Poliban Press. Banjarmasin.
- [5] Mukhtar, Harun. (2018). *Kriptografi untuk Keamanan Data*. Deepublish. Yogyakarta.
- [6] Jamaludin, Sulaiman, Oris Krianto, Tandungan, Sofyan, Putra, Lakry Maltaf, Yuswardi, Yulianti, Nia, Sidabutar, Jeckson, Aisa, Sitti, Tantriawan, Hartanto, Arizal, dan Pakpahan, Andrew Fernando. (2022). *Kriptografi: Teknik Keamanan Data*. Yayasan Kita Menulis. Medan.
- [7] Siahaan, Vivian, dan Sianipar, Rismon Hasilolan. (2020). *Java Untuk Keamanan Data*. Balige Publishing. Sumatera Utara.
- [8] Siswanto, Saputro, Arif, Utama, Galih Prasetyo, dan Prasetyo, Bambang Hari. (2021). *Penerapan Algoritma Kriptografi Twofish Untuk Mengamankan Data File*. Jurnal BIT. Vol. 18, no. 1:hal 09-18.
- [9] Ahmad, Khaleel, Singh, Manu Pratap, dan Udzir, Nur Izura. (2019). *Emerging Security Algorithms and Techniques*. CRC press. New York.
- [10] Elgamar. (2020). *Buku Ajar Konsep Dasar Pemrograman Website Dengan PHP*. Ahlimedia Book. Malang.
- [11] Nugroho, Aris, Suprihadi, Umar, dan Jaenul, Ahmad. (2021). *Rancang Bangun Aplikasi Toko Online Berbasis Web Codeigniter 3 Untuk Usaha Mikro Dan UMKM*. Media Sains Indonesia. Bandung.
- [12] Rozaq, Abdul, dan Fauzan, Riski. (2020). *Konsep Perancangan Sistem Informasi Bisnis Digital*. Poliban Press. Banjarmasin.
- [13] Negara, Edi Surya, Romindo, Tanjung, Rahman, Heriyani, Nofitri, Simarmata, Janner, Jamaludin, Putra, Tri Andi Eka, Sudarmanto, Eko, Sudarso, Andriansan, dan Purba, Bonaraja. (2021). *Sistem Informasi Manajemen Bisnis*. Yayasan Kita Menulis. Medan.