**Journal of Information and Information Security (JIFORTY)**
**Vol. 4, No. 1, Juni 2023, 91 – 104**
**e-ISSN : 2722-4058**
**Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty**

# Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web

**Dika Alfiani Fauzan [1], Ahmad Fathurrozi [1,*], Sugiyatno [1]**

[1]Informatika; Universitas Bhayangkara Jakarta Raya; Jl Raya Perjuangan No. 81 Bekasi Utara, (021) 889558822; e-mail: dika.alfiani.fauzan19@mhs.ubharajaya.ac.id, fathur@dsn.ubharajaya.ac.id, sugiyatno@ dsn.ubharajaya.ac.id

* Korespondensi: e-mail: fathur@dsn.ubharajaya.ac.id

Diterima: 22 Juni 2023; Review: 18 Juli 2023; Disetujui: 12 Agst 2023; Diterbitkan: 12 Agst 2023

## *Abstract*

*Cryptography is a method of manipulating a secret message into an unknown form to many people, with the aim of protecting the secret message from unauthorized individuals. Various types of cryptographic algorithms can be applied to protect data and information. Among them are the RSA (Rivest Shamir Adleman) and AES cryptographic algorithms. AES and RSA are often used together to provide optimal security. AES is used for efficient data encryption, while RSA is used for key exchange and digital signatures. In this research, AES is used for encrypting and decrypting documents/data, while RSA serves as the encryption and decryption for the AES key, which acts as the encryptor and decryptor for the documents/data. With this combination, the strengths of both algorithms can be utilized to achieve strong data security and confidentiality. The author aims to implement data security at XYZ Company. In this research, the author focuses on securing procedure documents and calibration methods.*

***Keywords**: Data Protection, Key Generation, Encryption, Description, Algorithm AES, Algorithm RSA*

## Abstrak

Kriptografi adalah sebuah metode untuk memanipulasi suatu pesan rahasia ke dalam bentuk yang tidak diketahui oleh banyak orang dengan tujuan pesan rahasia tersebut terlindungi dari orang yang tidak berhak mengetahuinya. Berbagai jenis algoritma kriptografi dapat diterapkan untuk melindungi data dan informasi. Diantaranya adalah algoritma kriptografi RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard). AES dan RSA sering digunakan bersama-sama untuk memberikan keamanan yang optimal. AES digunakan untuk enkripsi data yang efisien, sedangkan RSA digunakan untuk pertukaran kunci dan tanda tangan digital. Pada penelitian ini, AES digunakan untuk mengenkripsi dan mendekripsi dokumen/data, sementara RSA berperan sebagai enkripsi dan dekripsi untuk kunci AES yang berperan sebagai enkriptor dan dekriptor dokumen/data. Dengan kombinasi ini, kelebihan keduanya dapat dimanfaatkan untuk mencapai keamanan dan kerahasiaan data yang kuat. Untuk itu penulis berupaya mewujudkan implementasi keamanan data pada PT.XYZ. Pada penelitian ini, penulis melakukan pengamanan dokumen prosedur dan metode kalibrasi.

**Kata kunci:** Pengamanan Data, Pembangkitan Kunci, Enkripsi, Deskripsi, Algoritma RSA, Algoritma AES

## 1. Pendahuluan

Kriptografi adalah sebuah metode untuk memanipulasi suatu pesan rahasia ke dalam bentuk yang tidak diketahui oleh banyak orang dengan tujuan pesan rahasia tersebut terlindungi dari orang yang tidak berhak mengetahuinya. Maka dari itu, kriptografi dijadikan sebagai salah satu cara untuk mengamankan data atau informasi dari tindak kejahatan, yang akan menyebabkan kerugian bagi pemilik informasi (Amin, 2017). Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto artinya secret (rahasia) dan graphia artinya writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Sugiyatno & Atika, 2018). Khususnya pada sebuah perusahaan, terdapat banyak dokumen penting yang berisi data-data rahasia milik perusahaan yang hanya dapat dilihat oleh pihak tertentu. Dengan adanya kriptografi, maka pertukaran data dapat terjaga keamanan dan kerahasiaannya, sehingga data tersebut tidak jatuh pada pihak yang tidak berwenang dan tidak bertanggung jawab. Fokus bidang ilmu komputer dan matematika adalah teknologi yang digunakan untuk mengamankan komunikasi antara dua pihak di hadapan pihak ketiga (Bin Idris et al., 2017).

Salah satunya pada PT. XYZ, dimana perusahaan ini bergerak dalam bidang penyediaan pelayanan jasa, diantaranya kalibrasi, pengujian material, pelatihan, konsultan manajemen mutu, dan pelayanan jasa *maintenance*. Dimana perusahaan tersebut memiliki data penting seperti data terkait prosedur dan metode kalibrasi, dokumen akreditasi dan sertifikasi, laporan hasil pengujian/kalibrasi pelanggan, informasi tentang pelanggan dan proyek, riset dan pengembangan (R&D) *internal*, dan dokumen penting lainnya. Mengingat data ini tidak boleh diketahui oleh pihak yang tidak berkepentingan, terutama kompetitor, karena bisa merugikan. Oleh karena itu diperlukan sebuah pengamanan data agar pertukaran data pun dapat dilakukan secara aman sehingga terhindar dari pencurian data, untuk ini diperlukan sebuah aplikasi dengan metode yang dapat melindungi data dan informasi yang berada didalamnya. Metode yang dimaksud adalah kriptografi.

Kriptografi terbangun dalam blok-blok tertentu dan hanya bisa dipecahkan dengan sejumlah besar daya komputasi. Kriptografi secara khusus dibedakan ke dalam tiga metode kerja yang berbeda. Ketiganya dikembangkan dengan mempertimbangkan kebutuhan keamanan yang berbeda. Ketiga jenis metode kriptografi tersebut adalah asimetris, simetris, dan homorfik. Kriptografi asimetris merupakan kriptografi kunci berbasis publik yang mengenkripsi dan mendekripsi data menggunakan dua kunci asimetris kriptografi secara terpisah. Kedua kunci ini dikenal sebagai "*public key*" dan "*private key*" Kriptografi simetris merupakan jenis kriptografi di mana hanya ada satu kunci simetris yang bersifat rahasia dan digunakan untuk mengenkripsi plaintext dan mendekripsi ciphertext. Kriptografi homomorfik merupakan teknik kriptografi atau enkripsi yang didukung oleh jenis algoritma khusus yang memungkinkan jenis operasi tertentu dilakukan pada ciphertext tanpa memerlukan akses ke sebuah kunci rahasia.

Berbagai jenis algoritma kriptografi dapat diterapkan untuk melindungi data dan informasi. Diantaranya adalah algoritma kriptografi RSA dan AES. Dalam penilitian ini menggunakan algoritma. Algoritma RSA dipilih karena keamanannya terletak pada sulitnya pemfaktoran bilangan prima, semakin besar jumlah bilangan prima dalam pembangkitan kunci maka semakin sulit untuk dipecahkan (Rizkyansyah & Saifudin, 2018). Algoritma RSA (Rivest Shamir Adleman) merupakan salah satu metode dalam cabang ilmu kriptografi, dimana RSA adalah jenis kriptografi asimetris yang menggunakan 2 kunci, yaitu kunci publik dan private. Algoritma kriptografi RSA didesain sesuai fungsinya sehingga kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi. Kunci untuk enkripsi pesan disebut publik, sedangkan kunci untuk mendekripsi pesan yang diterima disebut private (Apdilah & Swanda, 2018) (Susanto & Trisusilo, 2018) (Sumarno, 2018). Kunci AES (*Advanced Encryption Standard*) adalah nilai rahasia yang digunakan dalam algoritma enkripsi AES untuk mengamankan data. AES adalah salah satu algoritma enkripsi yang paling umum digunakan dalam keamanan komputer dan komunikasi data. Algoritma AES mendukung berbagai variasi ukuran kunci yang digunakannya. Jenis ukuran kunci yang algoritma AES terbagi tiga, yaitu AES-128, AES-193 dan AES-256. Perbedaan jenis ukuran block dan kunci yang algoritma AES miliki yaitu karena perbedaan ukuran kunci yang akan menentukan jumlah proses yang harus dilalui pada saat pengenkripsian dan pendeskripsian atau lebih mudahnya dan dapat disimpulkan perbedaan pada banyaknya round atau putaran yang dipakai pada proses enkripsi dan dekripsi Semakin panjang kunci yang digunakan, semakin tinggi tingkat keamanannya (Fathurrozi, 2021).

Dalam praktiknya, AES dan RSA sering digunakan bersama-sama untuk memberikan keamanan yang optimal. AES digunakan untuk enkripsi data yang efisien, sedangkan RSA digunakan untuk pertukaran kunci dan tanda tangan digital. Dengan kombinasi ini, kelebihan keduanya dapat dimanfaatkan untuk mencapai keamanan dan kerahasiaan data yang kuat. Untuk itu penulis berupaya mewujudkan implementasi keamanan data pada sebuah perusahaan dengan menggunakan metode enkripsi RSA dan AES ke dalam suatu aplikasi yang mudah digunakan.

## 2. Metode Penelitian

Penelitian ini berfokus pada perusahaan kalibrasi PT.XYZ yang bertujuan untuk pengamanan data/dokumen. PT.XYZ merupakan perusahaan jasa yang menyediakan layanan kalibrasi, pengujian material, pelatihan, konsultan manajemen mutu, dan maintenance. Pendekatan penelitian yang digunakan adalah perancangan aplikasi yang dimulai dari analisis sistem, termasuk konsep, objek, keterkaitan, solusi algoritma, dan kebutuhan aplikasi. Analisis ini diwujudkan dalam pemodelan UML, seperti use case diagram, activity diagram, dan sequence diagram, sebagai perancangan aplikasi. Pengumpulan data untuk penelitian ini dilakukan melalui metode studi literatur, dengan mengacu pada penelitian yang telah ada, serta metode studi pustaka, dengan membaca referensi, e-book, dan mencari tambahan dari internet.

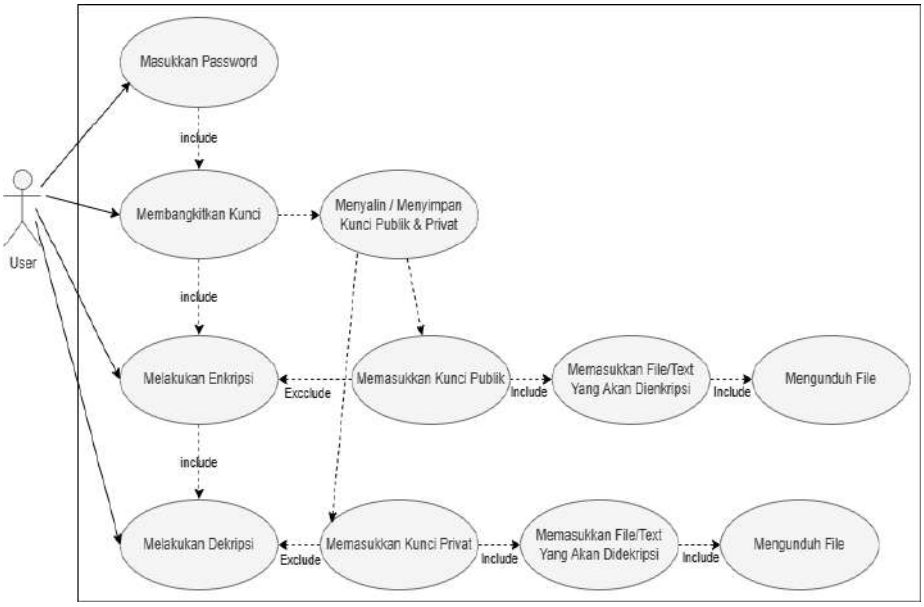
## 3. Hasil dan Pembahasan

Penerapan AES (Advanced Encryption Standard) dan RSA (Rivest Shamir Adleman) dalam ini melibatkan penggunaan dua algoritma kriptografi yang berbeda. AES digunakan untuk melakukan enkripsi data menggunakan kunci simetris AES, sementara RSA digunakan untuk mengamankan kunci simetris AES dengan menggunakan enkripsi kunci publik RSA. AES berperan dalam melindungi kerahasiaan data dengan mengenkripsi data menggunakan kunci simetris AES yang dihasilkan. Kunci simetris AES digunakan untuk memastikan bahwa hanya pihak yang memiliki kunci yang sesuai dapat mengakses dan membaca data yang dienkripsi. Sementara itu, RSA digunakan untuk mengamankan kunci simetris AES dengan menggunakan enkripsi kunci publik RSA.

Melalui enkripsi kunci publik RSA, kunci simetris AES dapat dikirimkan secara aman kepada penerima yang memiliki kunci privat RSA yang sesuai untuk melakukan dekripsi kunci simetris. Penerapan RSA juga mencakup pengelolaan pasangan kunci publik dan privat yang digunakan dalam skema enkripsi RSA-OAEP. Kunci publik RSA digunakan untuk enkripsi kunci simetris AES, sementara kunci privat RSA digunakan untuk dekripsi kunci simetris dan mengakses data yang telah dienkripsi. Dengan memadukan AES dan RSA, penerapan ini menggabungkan keuntungan dari kedua algoritma tersebut. AES efisien untuk mengenkripsi data yang lebih besar, sementara RSA cocok untuk enkripsi kunci simetris dan pengiriman kunci secara aman.

Pada tahap ini aplikasi mulai dirancang dengan pemodelan UML (*Unified Modelling Language*), membuat struktur yang ada didalam menu dan tampilan antar muka atau yang sering disebut User Interface dengan mempertimbangkan keefisienan suatu aplikasi yang dibangun oleh peneliti. Rancangan aplikasi ini mencakup ;

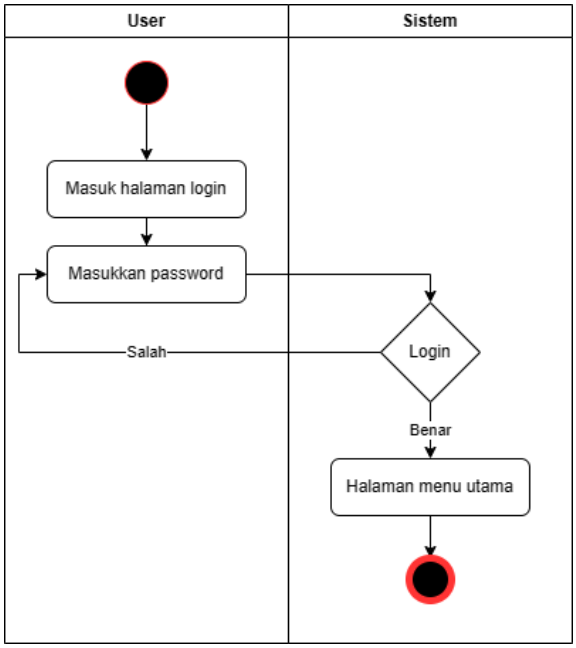
a. Sistem yang ada di dalam aplikasi yaitu tampilan menu utama yang berisikan halaman untuk akses aplikasi, dimana user harus memasukkan password terlebih dahulu. Lalu setelah masuk ke sistem aplikasi, terdapat 4 menu lainnya, diantaranya pembangkitan kunci, yang digunakan untuk membangkitkan kunci RSA publik dan privat, lalu ada menu enkripsi teks, enkripsi file, dekripsi text, dan dekripsi file.
b. Pemodelan aplikasi menggunakan *Unified Modelling Language* (UML). Unifield Modeling Language merupakan salah satu metode pemodelan visual yang digunakan dalam perancangan dan pembuatan sebuah software yang berorientasikan pada objek. UML menyediakan beberapa diagram visual yang menunjukan beberapa aspek dalam sistem (Ismai, 2019). UML merupakan sebuah standar penulisan atau semacam blue print diamna didalamnya termasuk sebuah bisnis proses, penulisan kelas-kelas dalam sebuah bahasa yang spesifik. Terdapat beberapa diagram UML yang sering digunakan dalam pengembangan sebuah sistem, yaituyang terdiri dari Use Case Diagram, Activity Diagram dan Class Diagram (M Teguh Prihando, 2018).




Sumber: Hasil Penelitian (2023)

Gambar 1. Use Case Diagram Aplikasi Pengamanan Data

Gambar 1 menjelaskan tingkat fungsionalitas tertinggi dari suatu sistem yang akan menggambarkan bagaimana aktor akan menggunakan dan memanfaatkan sistem. Diagram ini mendeskripsikan apa yang hendak dilakukan sistem. Pada use case ini terdapat aktor user, dimana user ini sebagai penerima dan pengirim file yang dienkripsi.

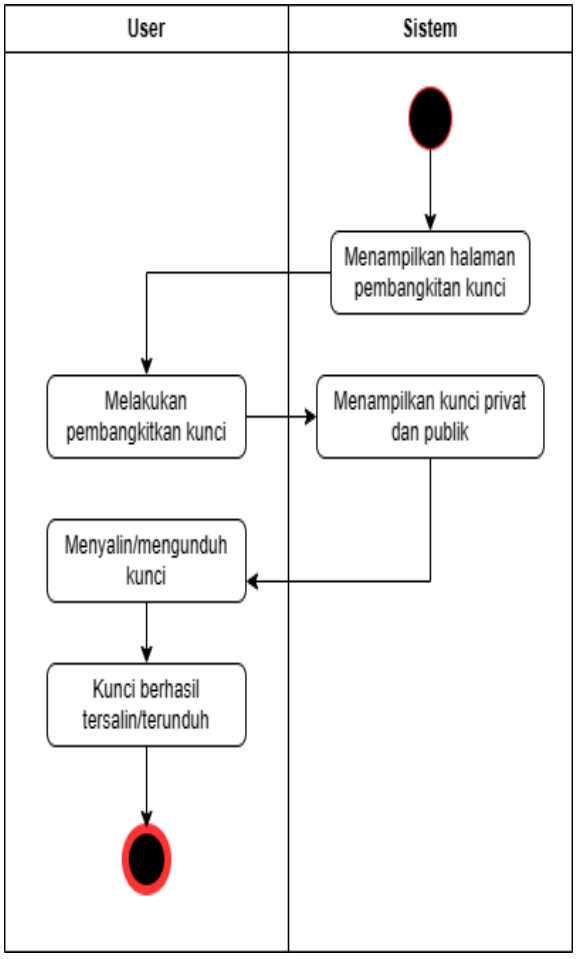



Sumber: Hasil Penelitian (2023)

Gambar 2. Activity Diagram Login Aplikasi Pengamanan Data

Gambar 2 menjelaskan aktivitas user untuk melakukan login lalu sistem akan menampilkan halaman pembangkitan kunci, berikut adalah detail prosesnya:

1. User melakukan login dengan memasukkan password.
2. Sistem akan melakukan pengecekkan login, jika gagal user akan dikembalikan ke halaman utama login, jika benar sistem akan menampilkan halaman pembangkitan kunci aplikasi.

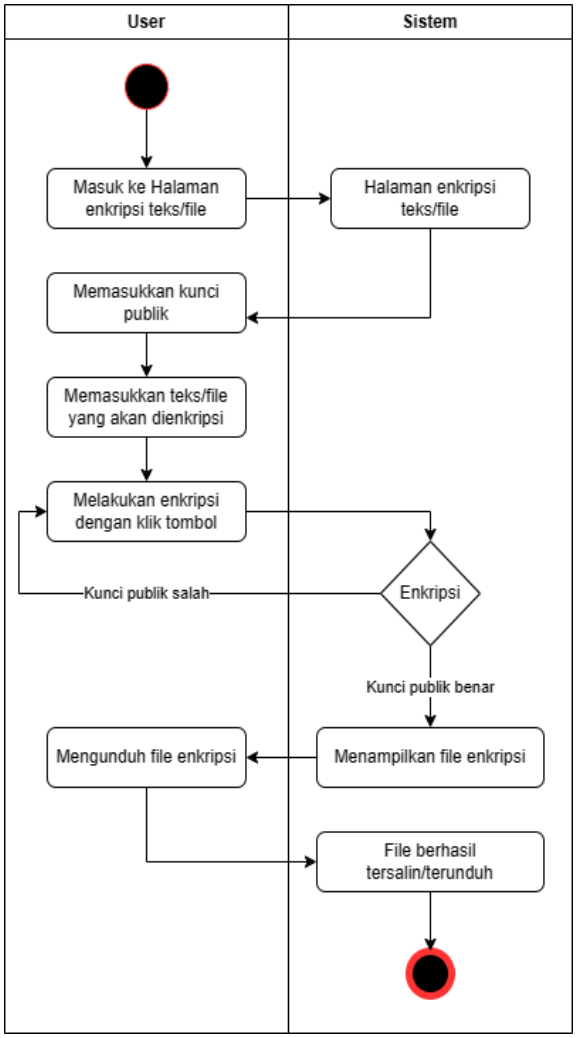



Sumber: Hasil Penelitian (2023)

Gambar 3. Activity Diagram Pembangkitan Kunci Aplikasi Pengamanan Data

Gambar 3 menjelaskan aktivitas user untuk melakukan pembangkitan kunci, berikut adalah detail prosesnya:

1. Sistem menampilkan halaman pembangkitan kunci
2. User membangkitkan kunci dengan mengklik tombol yang tersedia pada halaman.
3. Sistem akan menampilkan kunci privat dan publik yang akan digunakan untuk proses enkripsi dan dekripsi.
4. User menyalin atau mengunduh kunci yang telah dibangkitkan untuk nanti digunakan saat proses enkripsi dan dekripsi.

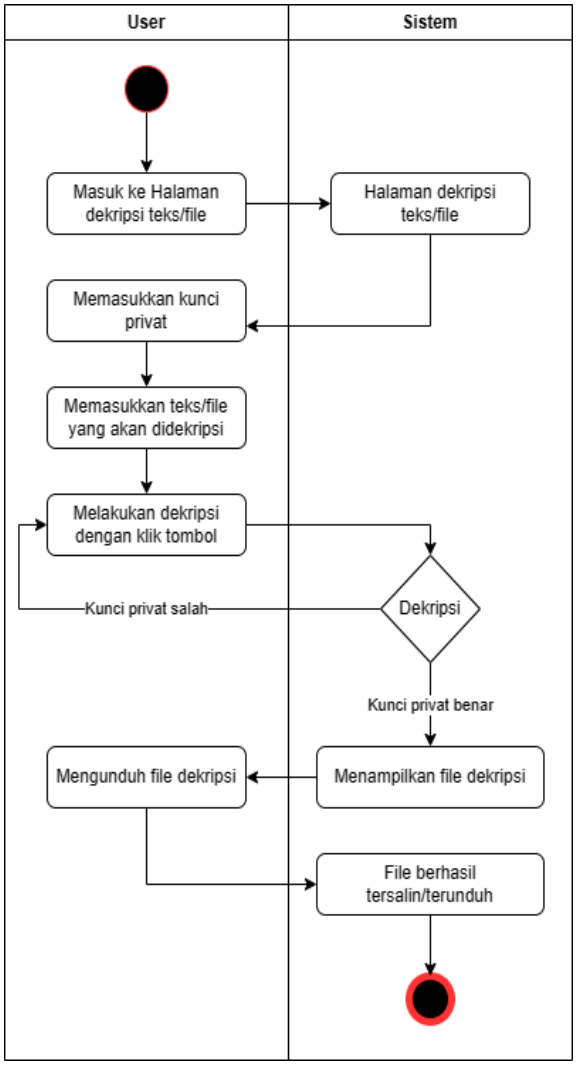



Sumber: Hasil Penelitian (2023)

Gambar 4. Activity Diagram Enkripsi Teks/File Aplikasi Pengamanan Data

Gambar 4 menjelaskan aktivitas user untuk melakukan enkripsi teks maupun file, berikut adalah detail prosesnya:

1. User masuk ke halaman enkripsi dan sistem menampilkan halaman enkripsi.
2. User memasukkan kunci publik dan memasukkan teks maupun file yang hendak dienkripsi.
3. User melakukan enkripsi dengan mengklik tombol yang tersedia pada halaman, apabila kunci publik benar, maka sistem akan menampilkan teks maupun file yang dapat diunduh dari teks/file yang berhasil dienkripsi oleh user. Apabila kunci publik yang dimasukkan salah, maka sistem akan memberitahu bahwa kunci yang dimasukkan tidak benar.
4. User dapat menyalin ataupun melakukan pengunduhan terhadap teks/file yang berhasil dienkripsi.

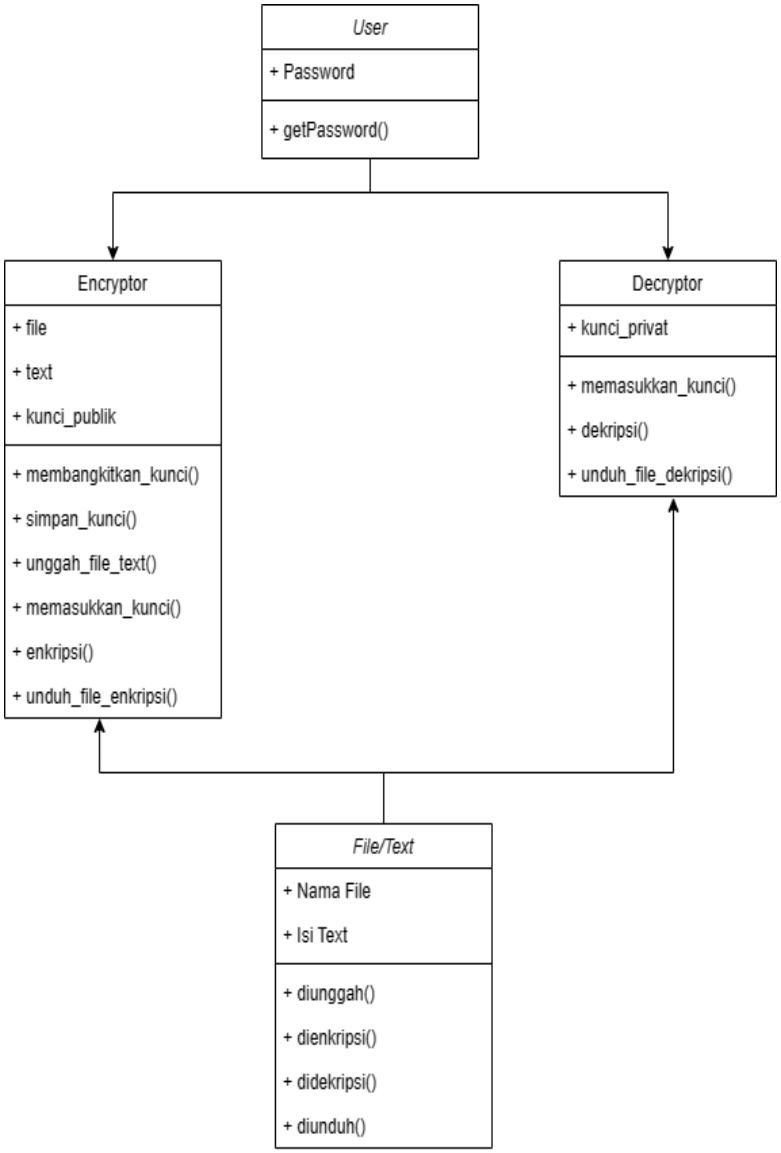



Sumber: Hasil Penelitian (2023)

Gambar 5. Activity Diagram Dekripsi Teks/File Aplikasi Pengamanan Data

Gambar 5 menjelaskan aktivitas user untuk melakukan dekripsi teks maupun file, berikut adalah detail prosesnya:

1. User masuk ke halaman dekripsi dan sistem menampilkan halaman enkripsi.
2. User memasukkan kunci privat dan memasukkan teks maupun file yang hendak didekripsi.
3. User melakukan dekripsi dengan mengklik tombol yang tersedia pada halaman, apabila kunci privat benar, maka sistem akan menampilkan teks maupun file yang dapat diunduh dari teks/file yang berhasil didekripsi oleh user.
4. Apabila kunci privat yang dimasukkan salah, maka sistem akan memberitahu bahwa kunci yang dimasukkan tidak benar. User dapat menyalin ataupun melakukan pengunduhan terhadap teks/file yang berhasil didekripsi.




Sumber: Hasil Penelitian (2023)

Gambar 6. Class Diagram Dekripsi Teks/File Aplikasi Pengamanan Data

Gambar 6 menjelaskan struktur dan hubungan antar objek-objek yang ada pada sistem. Struktur itu meliputi atribut-atribut dan metode-metode yang ada pada masing-masing kelas. Pada diagram ini dijelaskan proses database pada sebuah pemrograman. Ini sangat penting karena setiap kelas dalam sistem tersebut wajib dilaporkan secara berkala supaya tidak terjadi error berkepanjangan.

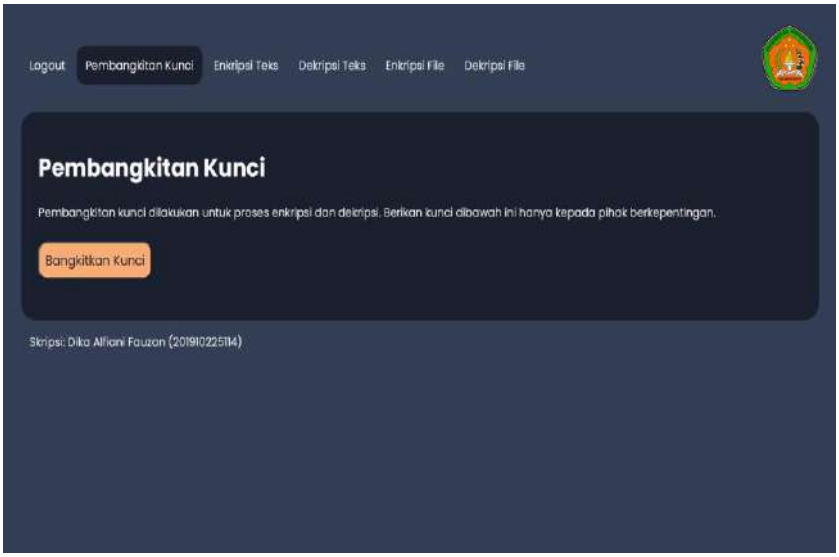
### 3.2. Implementasi

Implementasi antar muka aplikasi yaitu tampilan menu menu yang dibuat dan ditampilkan di dalam aplikasi yang dibangun.


Sumber: Hasil Penelitian (2023)

Gambar 7. Halaman *Login* Aplikasi Pengamanan Data

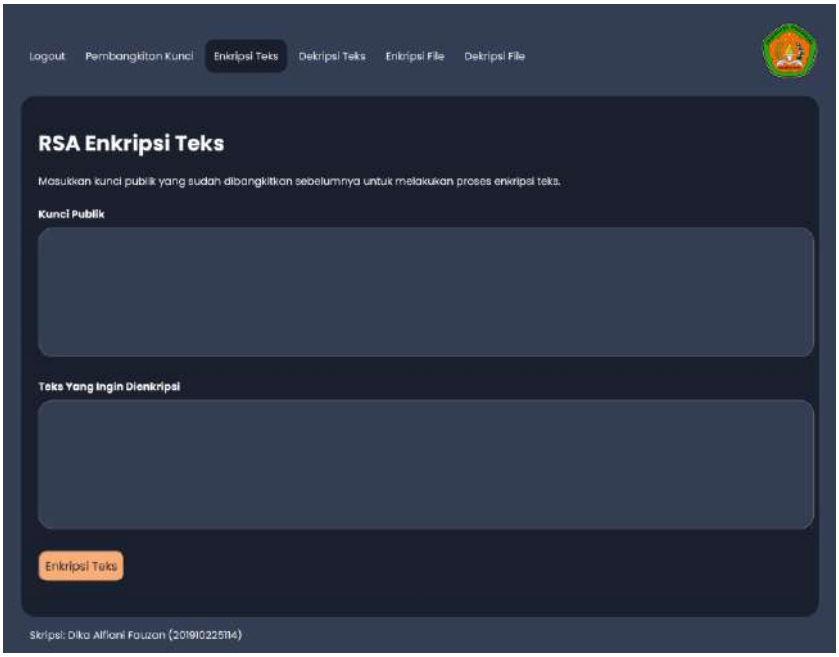
Gambar 7 menjelaskan tampilan aplikasi saat pengguna mengakses aplikasi tersebut, dimana pada tampilan ini, pengguna diminta untuk mengisi password yang diperlukan untuk mengakses aplikasi pengamanan data.




Sumber: Hasil Penelitian (2023)

Gambar 8. HalamanPembangkitan Kunci Aplikasi Pengamanan Data

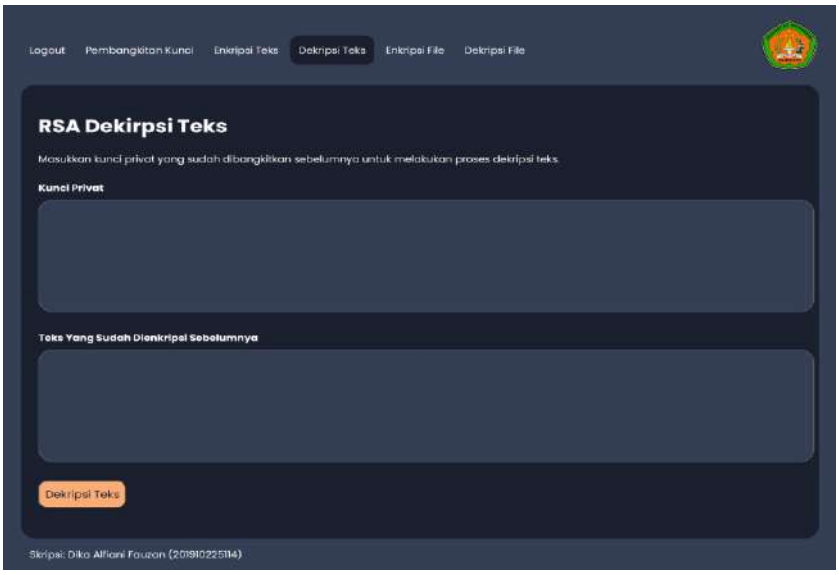
Gambar 8 menjelaskan halaman pembangkitan kunci, dimana pengguna dapat mendapatkan kunci publik dan kunci privat yang digunakan untuk proses enkripsi dan dekripsi.




Sumber: Hasil Penelitian (2023)

Gambar 9. Halaman Enkripsi Teks Aplikasi Pengamanan Data

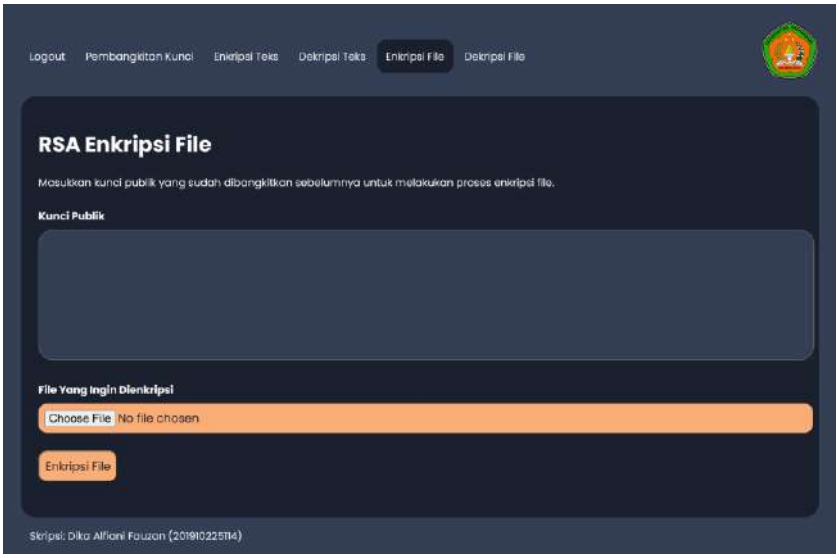
Gambar 9 menjelaskan halaman enkripsi teks, dimana pengguna dapat memasukkan teks yang hendak dienkripsi dan selanjutnya mengunduh file yang berhasil dienkripsi.




Sumber: Hasil Penelitian (2023)

Gambar 10. Halaman Dekripsi Teks Aplikasi Pengamanan Data

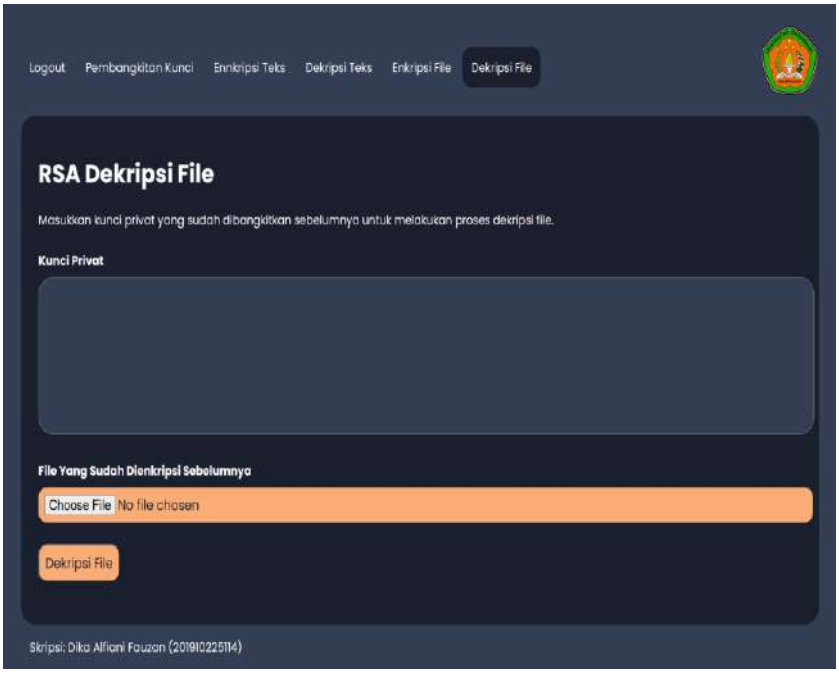
Gambar 10 menjelaskan halaman dekripsi teks, dimana pengguna dapat memasukkan teks yang telah dienkripsi sebelumnya dan selanjutnya mengunduh file yang berhasil didekripsi.




Sumber: Hasil Penelitian (2023)

Gambar 11. Halaman Enkripsi File Aplikasi Pengamanan Data

Gambar 11 menjelaskan halaman enkripsi file, dimana pengguna dapat memasukkan file yang hendak dienkripsi dan selanjutnya mengunduh file yang berhasil dienkripsi.




Sumber: Hasil Penelitian (2023)

Gambar 12. Halaman Dekripsi File Aplikasi Pengamanan Data

Gambar 12 menjelaskan halaman dekripsi file, dimana pengguna dapat memasukkan teks yang telah dienkripsi sebelumnya dan selanjutnya mengunduh file yang berhasil didekripsi.

## 4. Kesimpulan

Aplikasi pengamanan data ini berhasil mengimplementasikan metode Rivest Shamir Adleman dalam mengamankan file atau text perusahaan. Hal ini dibuktikan melalui hasil pengujian pada tabel 4.1 yang memperlihatkan bahwa semua file dan teks yg dienkripsi dapat berubah menjadi file berekstensi (.encrypted) yang tidak dapat dibuka tanpa kunci privat, serta dapat dikembalikan ke file aslinya dalam proses dekripsi dan tidak mengalami perubahan, dengan tingkat keberhasilan 100%. Selain itu, waktu proses pengenkripsian dan pendekripsian sangat cepat, semua proses dengan berbagai macam ukuran dan jenis file dienkripsi dan didekripsi tidak lebih dari 0.5 detik. Proses pengamanan data ini pun tidak mengubah ukuran file dengan dengan signifikan, bahkan cenderung sama untuk file asli sebelum dienkripsi dan file sesudah dienkripsi atau didekripsi.

## Daftar Pustaka

Amin, M. M. (2017). Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks. *Pseudocode*, *3*(2), 129–136. https://doi.org/10.33369/pseudocode.3.2.129-136

Apdilah, D., & Swanda, H. (2018). Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP. *Jurnal Teknologi Informasi*, *2*(1), 45. https://doi.org/10.36294/jurti.v2i1.407

Bin Idris, Y., Adli Ismail, S., Mohd Azmi, N. F., Azmi, A., & Azizan, A. (2017). Enhancement Data Integrity Checking Using Combination MD5 and SHA1 Algorithm in Hadoop Architecture. *Journal of Computer Science & Computational Mathematics*, *7*(3), 99–102. https://doi.org/10.20967/jcscm.2017.03.007

Fathurrozi, A. (2021). Penerapan Algoritma Advanced Encryption Standard (AES-256) Dengan Mode CBC DanSecure Hash Algorithm (SHA-256) Untuk Pengamanan Data File. *Journal of Information and Information Security (JIFORTY)*, *2*(2), 227–238. http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Ismai. (2019). Evolusi : Jurnal Sains dan Manajemen Vol 7 No . 2 September 2019 ISSN : 2338-8161 E-ISSN : 2657-0793. *Jurnal Sains dan Manajemen*, *7*(2), 6–14.

M Teguh Prihando. (2018). Unified Modeling Language (UML) Model Untuk Pengembangan Sistem Informasi Akademik Berbasis Web. *Jurnal Informatika: Jurnal Pengembangan IT*, *3*(1), 126–129.

Rizkyansyah, Y. F., & Saifudin, A. (2018). Integrasi Algoritma RSA (Rivest Shamir Adleman) dan Caesar Cipher untuk Meningkatkan Keamanan Enkripsi SMS (Short Message Service). *Jurnal Informatika Universitas Pamulang*, *3*(3), 208. https://doi.org/10.32493/informatika.v3i3.2238

Sugiyatno, & Atika, P. D. (2018). Digital Signature Dengan Algoritma Sha-1 Dan Rsa Sebagai Autentikasi. *Jurnal Cendikia*, *16*(2), 74–83.

Sumarno. (2018). Analisis Kinerja Kombinasi Algoritma Message-Digest Algortihm 5 (MD5),

Rivest Shamir Adleman (RSA ) dan Rivest Cipher 4 (RC4) Pada Keamanan E-Dokumen. *Tesis*, *2*(1), 1–71. http://jurnal.unprimdn.ac.id/index.php/JUSIKOM/article/view/140

Susanto, S., & Trisusilo, A. A. (2018). Penerapan Algoritma Asimetris Rsa Untuk Keamanan Data Pada Aplikasi Penjualan Cv. Sinergi Computer Lubuklinggau Berbasis Web. *Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, *9*(2), 1043–1052. https://doi.org/10.24176/simet.v9i2.2537