1st National Conference on Electrical, Informatics and Industrial Technology (NEIIT-2024)
July 20, 2024

Penerapan Kriptografi Keamanan Data Nilai Leger Siswa SMK Islam Kunjang Menggunakan Algoritma Asimetris RSA

Andryan PutraHidayat[1], Yudo Bismo Utomo[2], Harso Kurniadi[3]
[1,2,3]Teknik Komputer, Fakultas Teknik, Universitas Islam Kadiri
E-mail: [*1]hidayataan12@gmail.com, [2] yudobismo@uniska-kediri.ac.id, [3]harsokurniadi@uniska-kediri.ac.id,

ARTICLE INFO

Article history:

Submited:
July 09, 2024

Accepted:
July 13, 2024

Published:
July 31, 2024

ABSTRACT

One of the most significant concerns in the field of education, and one that affects SMK Islam Kunjang, is information security. Every final exam, SMK Islam Kunjang regularly distributes file leger data—an excel file including the student scores with other schools. File-leger student grade data at SMK Islam Kunjang is susceptible to viral dissemination since people share files via email or Whatsapp. In order to prevent careless people from abusing the information in the leger file including student grades, SMK Islam Kunjang need a solution that can protect its secrecy. In this study, data on the Kunjang Islamic Vocational School students' score leger file was secured using the Rivest Shamir Adleman technique or RSA method. The most used public key encryption algorithm for protecting data is the RSA method. To generate the public and private keys, the method's performance involves selecting two random integers that will be used as keys. Critical student grade data may be encrypted and described with maximum security by utilizing the RSA asymmetric method in cryptography applications. This study demonstrates how well the RSA asymmetric approach maintains data security in the student scoreleger file at SMK Islam Kunjang.

Keywords:

Cryptography, Data Security, RSA Method.

Kata Kunci:

Kriptografi, Keamanan Data, Metode RSA

ABSTRAK

Keamanan informasi merupakan salah satu masalah penting di dunia pendidikan, salah satunya di SMK Islam Kunjang. SMK Islam Kunjang selalu rutin dalam melakukan share file leger data nilai siswa setiap ujian akhir semester berupa file excel. File leger data nilai siswa di SMK Islam Kunjang yang rentan tersebar luas dikarenakan sharing file menggunakan via whatsapp maupun email. Karena itu SMK Islam Kunjang membutuhkan suatu sistem yang dapat menjaga suatu kerahasiaan isi file leger dari nilai siswa agar tidak disalahgunakan oleh oknum yang tidak bertanggung jawab. Dalam penelitian ini, menerapkan metode RSA atau *Rivest Shamir Adleman* dalam mengamankan data pada file leger nilai siswa SMK Islam Kunjang. Metode RSA merupakan sebuah algoritma pada enkripsi public key yang paling banyak digunakan dalam mengamankan data. Kinerja dari metode tersebut yaitu mengambil dua bilangan secara acak yang akan dijadikan kunci, sehingga didapat dua kunci yaitu kunci publik dan kunci private. Dengan menimplementasikan aplikasi kriptografi menggunakan algoritma asimetris RSA, data-data penting nilai siswa dapat diamankan maksimal dengan teknik enkripsi dan deskripsi. Penelitian ini membuktikan bahwa metode asimetris RSA efektif dalam menjaga keamanan data dalam file leger nilai siswa SMK Islam Kunjang.

Corresponding Author:
Andryan Putra Hidayat
Program Studi Teknik Komputer, Fakultas Teknik, Universitas Islam Kadiri
Jalan Sersan Suharmadji No. 38, Kota Kediri, Jawa Timur, Indonesia.
Email: hidayataan12@gmail.com

1. PENDAHULUAN

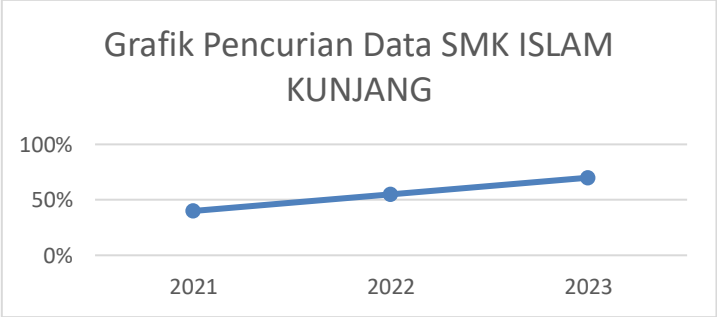
Keamanan informasi merupakan salah satu masalah penting, seiring dengan perkembangan software dan pengguna internet. Keamanan komputer berhubungan dengan pencegahan dari pencurian data atau informasi dari orang yang tidak bertanggung jawab, baik itu mengakses dan memodifikasi informasi[1]. Pengamanan komputer berfungsi untuk melindungi informasi agar tidak dapat diakses bagi orang yang tidak berhak. Banyak cara yang dapat digunakan dalam pengamanan komputer, salah satunya dengan menggunakan kriptografi [2][3].

Kerahasiaan data atau informasi merupakan bagian penting dari pelayanan yang dirancang untuk memastikan bahwa informasi yang tersimpan tidak dapat dibaca atau diakses oleh pihak yang tidak berwenang. Upaya menjaga kerahasiaan informasi telah ada sejak zaman Romawi, menggunakan metode pergeseran huruf atau karakter berdasarkan nilai tertentu [4].

Ilmu yang mempelajari tentang cara-cara mengamankan data atau pesan dikenal dengan istilah Kriptografi, sedangkan dalam langkah-langkah kriptografi disebut algoritma kriptografi. Berdasarkan kunci yang digunakan, algoritma kriptografi dapat dibagi menjadi dua, yaitu algoritma simetrik dan algoritma asimetrik [5]. Dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Proses penyamaran dari plaintext ke ciphertext disebut enkripsi (encryption), dan proses pengembalian dari ciphertext menjadi plaintext kembali disebut dekripsi (decryption) [6].

Enkripsi (encryption) yaitu proses merubah data asli (plaintext) menjadi data samaran (chipertext) dan dekripsi (decryption) yaitu proses pengembalian chipertext menjadi plaintext kembali [7]. Enkripsi itu sendiri adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau chiper. Isu- isu yang terkait dengan keamanan dan kerahasiaan data adalah privacy (kerahasiaan), integrity (keutuhan), authenticity (keaslian), non-repudiation (pembuktian) [8]. Dari sekian banyak algoritma kriptografi dengan kunci-publik yang pernah dibuat, algoritma yang paling populer adalah algoritma rsa. Algoritma rsa yang dibuat oleh Ron Rivest, Adi Shamir dan Leonard Adleman pada tahun 1976. Keamanan algoritma rsa terletak pada sulitnya untuk memfaktorkan bilangan prima yang relatif lebih besar. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama bilangan pemfaktoran prima yang besar besar belum ditemukan algoritma yang berhasil memecahkan, maka selama itu pula algoritma rsa akan tetap terjamin keaananannya [9].

Kerahasiaan data atau file yang dimiliki seseorang menjadi pertimbangan penting dalam berbagi file, sehingga file yang dimaksud hanya boleh diberikan kepada satu orang dalam satu waktu dan hanya dapat diakses oleh orang yang menerima file tersebut. Untuk menganalisis data diperlukan gamanan data yang disebut juga kriptografi. Enkripsi file data semacam ini dapat dilakukan dengan menggunakan metode RSA baik dalam bentuk terenkripsi maupun dekripsi. Oleh karena itu, diperlukan suatu sistem keamanan yang mampu melindungi data sensitif secara efektif dari serangan lain yang dilakukan oleh pihak yang tidak bertanggung jawab. Adapun kasus pencurian data di SMK Islam Kunjang dari tahun ke tahunnya dapat dilihat dari grafik berikut ini.



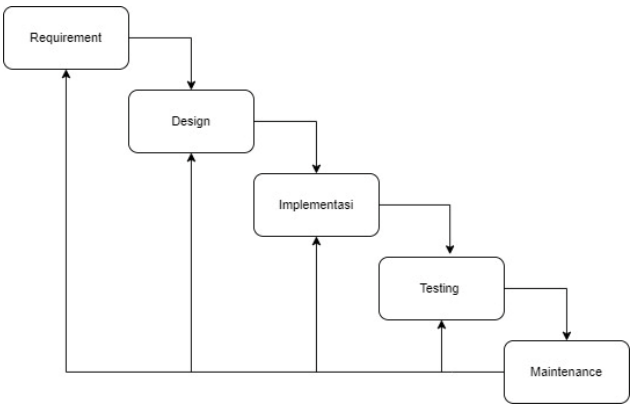
Gambar 1. Grafik Pencurian Data

Untuk menindaklanjuti pencurian data yang semakin banyak diperlukan menggunakan algoritma RSA, karena sistem akan terlebih dahulu mengubah dokumen yang dimasukkan pengguna menjadi chipertext dan kemudian mengenkripsinya sehingga orang yang tidak bertanggung jawab hendak mengubah maupun mencuri tidak bisa melakukannya. Bagi penerima data leger nilai siswa, data tersebut harus diterjemahkan ke dalam teks biasa sehingga penerima file leger siswa dapat lebih mudah memahami dan menggunakan informasi tersebut. Berdasarkan pembahasan latar belakang di atas, maka penulis melakukan penelitian dengan judul "***IMPLEMENTASI***

KRIPTOGRAFI KEAMANAN DATA SISWA SMK ISLAM KUNJANG MENGGUNAKAN ALGORITMA ASIMETRIS RSA".

2. METODE PENELITIAN

Metodologi pengembangan ini digunakan untuk merancang sebuah aplikasi berbasis objek. Oleh karena itu, diperlukan suatu metode perancangan . Metode perancangan sistem yang penulis gunakan untuk mengembangkan sistem ini adalah metodologi Waterfall. Metode Waterfall ini melibatkan perancangan yang dimulai dari spesifikasi kebutuhan pengguna dan perangkat yang akan dikembangkan. Selanjutnya, dilakukan uji validasi dan menunjukkan proses alur yang urut hingga implementasi ke dalam system [10][11].
Berikut ini alur tahapan metode waterfall:



Gambar 2**.** Metode Waterfall

2.1. Metode Pengumpulan Data

Dalam proses pengumpulan data pada Tugas Akhir ini, tujuannya adalah memperoleh hasil yang akurat dan relevan. Penelitian ini menggunakan studi kualitatif dan deskriptif. Penelitian kualitatif melibatkan pengamatan terhadap objek penelitian yang bertujuan untuk menghasilkan konsep atau teori baru. Metode pengumpulan data dalam penelitian kualitatif meliputi Observasi, wawancara, dan studi literatur.

Pengamatan dilakukan dengan melakukan observasi langsung data di lapangan, mulai dari pengenalan data hingga proses dan evaluasi, sehingga data siap untuk mendukung penelitian yang mencerminkan kebenaran di lapangan.

Wawancara dilakukan langsung dengan anggota atau pihak terkait. Wawancara ini dilakukan dengan pengurus dan anggota Smk Islam Kujang untuk mendapatkan informasi atau berita yang tidak ditemukan dalam pustaka. Selain itu, wawancara bertujuan untuk mendapatkan masukan dan solusi terhadap permasalahan yang mungkin belum ditangani oleh sistem sebelumnya, sehingga dapat merancang sistem baru yang sesuai.

Selain itu, Studi pustaka adalah metode yang digunakan untuk mencari dan mengumpulkan informasi yang relevan dalam penyusunan Tugas Akhir. Dalam proses ini, peneliti mencari referensi dan teori dari berbagai sumber tulisan yang berkaitan dengan topik Tugas Akhir yang sedang diteliti. Tujuannya adalah untuk memperoleh pemahaman yang mendalam tentang topik tersebut serta memastikan bahwa Tugas Akhir disusun dengan baik dan didukung oleh literatur yang kuat.

2.2. Implementasi Algoritma RSA Dalam Keamanan File EXCEL

2.2.1 Proses Enkripsi Algoritma RSA

Pilih nilai P dan Q, Nilai P dan Q adalah bilangan prima acak yang panjangnya 4 bit, nilai P ≠ Q. Nilai P dan Q yang dipakai dalam pengujian kedua P = 11, Q = 13.

Tentukan nilai r, N, dan E

N = P . Q = 11 . 13

N = 143 □(r)= (p – 1)(q – 1) = (11-1)(13-1)

= 120

Nilai E merupakan bilangan relatif prima acak bersifat publik, Faktor Persekutuan Terbesar dari r dan nilainya < r. E.gdc(r) = E.gdc(120) = 59

Lakukan transformasi satu ke satu untuk m (terletak pada rentang 0 – (n-1))

hal ini dilakukan agar nilai enkripsi tidak terlampau besar.

Plainteks = Tes atau 84, 101, 115 (dirubah menjadi ASCII desimal)

Rentang setiap blok m = 0 – (n-1) = 0 – 142
m = 84101115 m1 = 84 m2 = 101 m3 = 115
Proses enkripsi:
Y = me mod N
Y1 = m1e mod N ≡ 84 59 mod 143 ≡ 63
Y2 = m2e mod N ≡ 101 59 mod 143 ≡ 17
Y3 = m3e mod N ≡ 115 59 mod 143 ≡ 97
Y (ciphertext)= 63 17 97.

2.2.2. Proses Dekripsi Algoritma RSA

Hitung nilai D, D dengan memasukkan nilai m satu persatu sampai hasilnya bulat, nilai D bersifat rahasia.
E .D mod r = 1
E.D ≡ 1 mod r
D = 1 (x . r)/E = 1 (m. 120)/59
Dengan mencoba nilai x = 1, 2, 3, 4, ... diperoleh nilai x yang menghasilkan D yang bulat adalah 29. Dan nilai D yang didapat adalah 59.
D = 1 (x . r)/E = 1 (29. 120)/E 59
= 3840/59 = 59
Setelah nilai D didapat langkah selanjutnya ialah mengubah ciphertext kembali ke teks awal. Y = 63 17 97 (Y1 = 63 Y2 = 17 Y3 = 97)
m= YD mod N
m1 = Y1 D mod N ≡ 63 59 mod 143 ≡ 84
m2 = Y2 D mod N ≡ 17 59 mod 143 ≡ 101
m3 = Y3 D mod N ≡ 97 59 mod 143 ≡ 115
Sehingga, nilai m = 84 101 115 apabila dikonversikan menjadi string kembali berdasarkan tabel ASCII maka akan menghasilkan teks asli “Tes” [12].

2.3. Perancangan

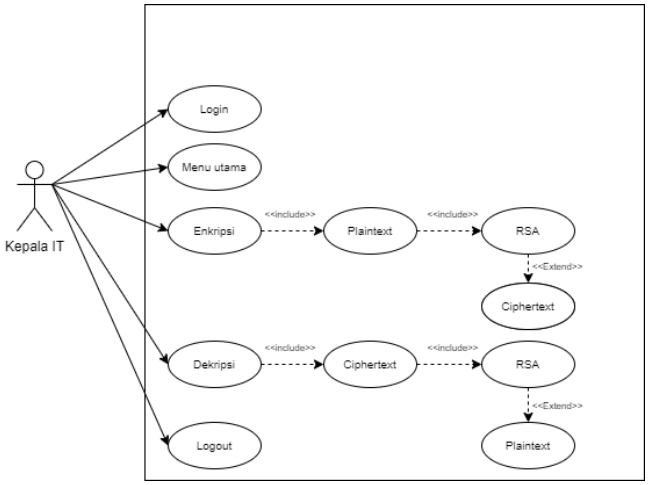
Perancangan aplikasi adalah proses merancang sebuah aplikasi dengan menggunakan bahasa pemrograman PHP. Dalam kasus ini, penulis merancang aplikasi keamanan data file excel dengan menggunakan PHP. Aplikasi ini bersifat kriptografi, dengan tugas utama yaitu enkripsi dan dekripsi file excel.

2.4. Desain Sistem

Perancangan ini akan menjelaskan tentang desain aplikasi serta proses pembentukan dan pembangunan aplikasi untuk menggunakan algoritma kriptografi RSA dalam mengamankan file excel.

2.4.1. Use Case Diagram

Perancangan dimulai dari identifikasi aktor dan bagaimana hubungan antara aktor dan use case didalam sistem. Perancangan Use Case Diagram dapat dilihat pada Gambar 3.

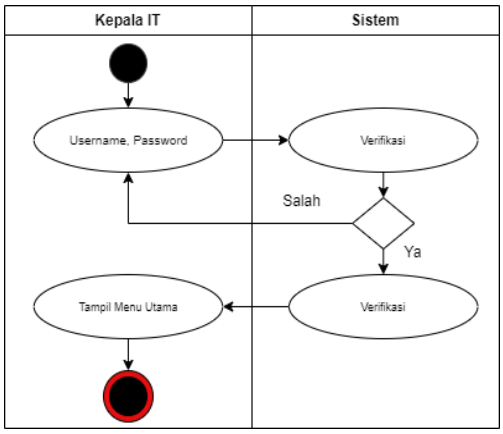


Gambar 3. Use Case Diagram

2.5. Activity Diagram

Diagram Aktivitas menggambarkan berbagai aliran aktivitas, termasuk bagaimana setiap aliran dimulai, keputusan yang mungkin diambil, dan bagaimana sistem tersebut berakhir.

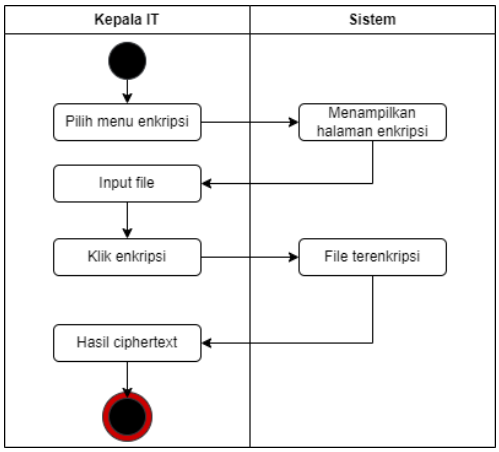
2.5.1. Activity Diagram Login



Gambar 4. Activity Diagram Login

Diagram dimulai dari node bulat berwarna hitam yang menandakan awal dari aktivitas login. Aktivitas pertama yang dilakukan oleh Kepala IT adalah memasukkan "Username" dan "Password" pada sistem. Setelah Admin memasukkan "Username" dan "Password", sistem melakukan aktivitas "Verifikasi". Aktivitas ini berada pada swimlane "Sistem", menandakan bahwa proses ini dilakukan oleh sistem. Setelah proses verifikasi, terdapat simbol diamond yang merepresentasikan keputusan atau kondisi. Sistem akan memeriksa apakah "Username" dan "Password" yang dimasukkan benar atau salah. Salah: Jika verifikasi gagal (salah), alur kembali ke aktivitas memasukkan "Username" dan "Password" oleh Admin. Hal ini digambarkan oleh panah yang kembali ke aktivitas sebelumnya. Ya: Jika verifikasi berhasil (ya), sistem melanjutkan proses. Jika verifikasi berhasil, sistem menampilkan menu utama kepada Kepala IT. Aktivitas ini menunjukkan bahwa Kepala IT telah berhasil login dan sekarang dapat mengakses fitur-fitur yang tersedia dalam menu utama. Diagram berakhir dengan node bulat dengan garis tepi merah yang menandakan akhir dari proses login.

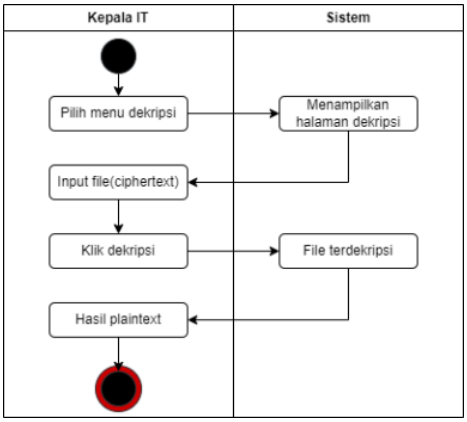
2.5.2. Activity Diagram Enkripsi



Gambar 5. Activity Diagram Enkripsi

Diagram dimulai dari node bulat berwarna hitam yang menandakan awal dari aktivitas enkripsi. Kepala IT memilih menu enkripsi pada sistem. Aktivitas ini berada pada swimlane "Kepala IT". Setelah memilih menu enkripsi, sistem menampilkan halaman enkripsi. Aktivitas ini berada pada swimlane "Sistem", menandakan bahwa sistem yang melakukan perintah ini. kemudian Kepala IT menginput file yang akan dienkripsi ke dalam sistem. Kepala IT mengklik tombol enkripsi untuk memulai proses enkripsi. Sistem melakukan proses enkripsi dan menghasilkan file terenkripsi. Aktivitas ini juga berada pada swimlane Sistem". kemudian menampilkan hasil ciphertext (teks terenkripsi) kepada Kepala IT. Diagram berakhir dengan node bulat dengan garis tepi merah yang menandakan akhir dari proses enkripsi.

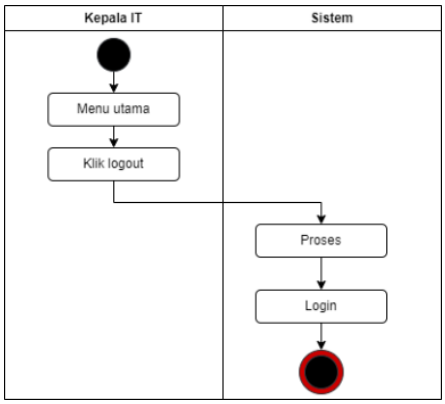
2.5.3. Activity Diagram Dekripsi



Gambar 6. Activity Diagram Dekripsi

Diagram dimulai dari node bulat berwarna hitam yang menandakan awal dari aktivitas dekripsi. Kepala IT memilih menu dekripsi pada sistem. Aktivitas ini berada pada swimlane “Kepala IT. Setelah memilih menu dekripsi, sistem menampilkan halaman dekripsi. Aktivitas ini berada pada swimlane “Sistem”, menandakan bahwa sistem yang melakukan tugas ini. Kepala IT kemudian menginput file yang terenkripsi (ciphertext) ke dalam sistem. Kepala IT mengklik tombol dekripsi untuk memulai proses dekripsi. Sistem melakukan proses dekripsi dan menghasilkan file yang terdekripsi (plaintext). Aktivitas ini juga berada pada swimlane “Sistem”. Sistem kemudian menampilkan hasil plaintext (teks asli) kepada Kepala IT. Diagram berakhir dengan node bulat dengan garis tepi merah yang menandakan akhir dari proses dekripsi.

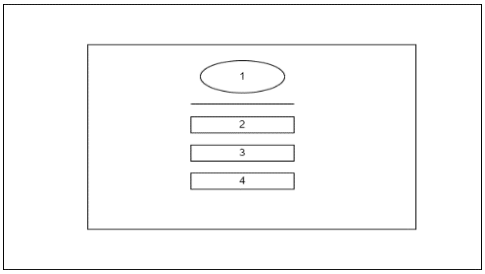
2.5.4. Activity Diagram Logout



Gambar 7. Activity Diagram Logout

diagram ini menunjukkan langkah-langkah dari Kepala IT saat melakukan logout dari sistem, dimulai dari menu utama, mengklik logout, sistem memproses logout, dan akhirnya kembali ke halaman login. Proses ini memastikan bahwa sesi Kepala IT berakhir dengan benar dan siap untuk login berikutnya.

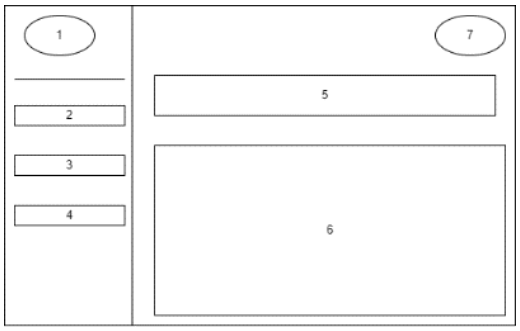
2.6. Rancangan Desain Aplikasi (wireframe)



Gambar 8. Tampilan Form Login

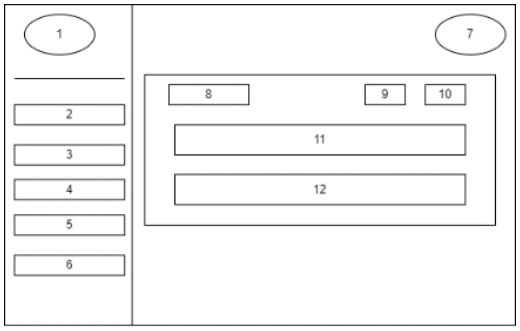
Keterangan pada Gambar 8. :

1. Keterangan pada nomor 1 ialah logo dari aplikasi.
2. Keterangan pada nomor 2 ialah kolom untuk memasukkan email.
3. Keterangan pada nomor 3 ialah kolom untuk memasukkan password.
4. Keterangan pada nomor 4 ialah kolom untuk masuk.



Gambar 9. Tampilan Form Dashboard

Keterangan pada Gambar 9. :
1. Keterangan pada nomor 1 ialah logo dari aplikasi.
2. Keterangan pada nomor 2 ialah kolom tampilan dashboard.
3. Keterangan pada nomor 3 ialah kolom tampilan master.
4. Keterangan pada nomor 4 ialah kolom tampilan pengaturan.
5. Keterangan pada nomor 5 ialah kolom tampilan pengertian algoritma RSA.
6. Keterangan pada nomor 6 ialah kolom tampilan diagram .
7. Keterangan pada nomor 4 ialah logo dari profil.

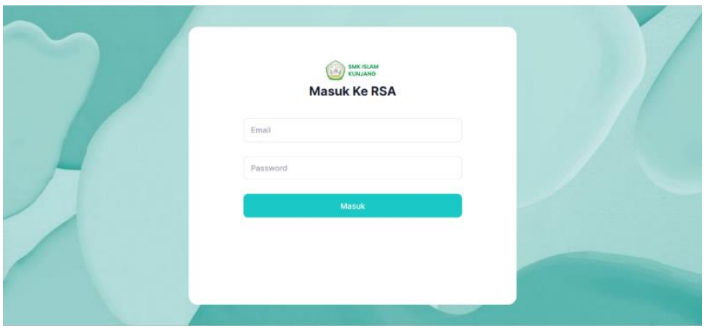


Gambar 10. Tampilan Menu Enkripsi Dan Dekripsi

Keterangan pada Gambar 10. :
1. Keterangan pada nomor 1 ialah logo dari aplikasi.
2. Keterangan pada nomor 2 ialah kolom tampilan dashboard.
3. Keterangan pada nomor 3 ialah kolom tampilan master.
4. Keterangan pada nomor 4 ialah kolom tampilan dokumen enkripsi.
5. Keterangan pada nomor 5 ialah kolom tampilan dokumen dekripsi
6. Keterangan pada nomor 6 ialah kolom tampilan pengaturan .
7. Keterangan pada nomor 7 ialah logo dari profil.
8. Keterangan pada nomor 8 ialah kolom tampilan cari dokumen.
9. Keterangan pada nomor 9 ialah kolom tampilan penyaringan.
10. Keterangan pada nomor 10 ialah kolom tambah dokumen.
11. Keterangan pada nomor 11 ialah kolom ceklis file.
12. Keterangan pada nomor 12 ialah kolom ceklis file.

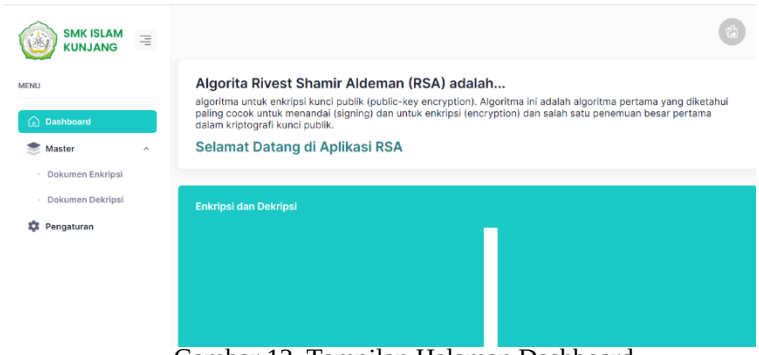
3. Hasil Dan Pembahasan

Setelah menyelesaikan tahap perancangan konsep sistem dengan menggunakan wireframe, langkah selanjutnya adalah mengembangkan tampilan aplikasi berdasarkan konsep yang telah dirancang. Rincian tampilan aplikasi yang telah dibuat adalah sebagai berikut:



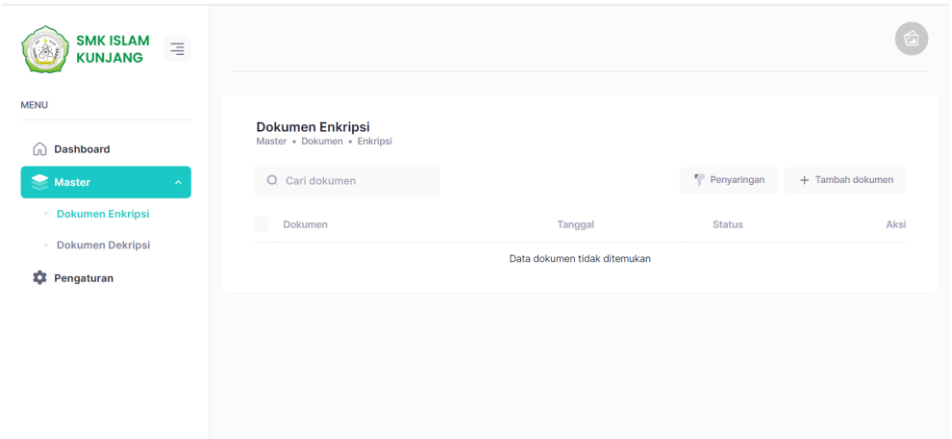
Gambar 11. Tampilan Halaman *Login*

Pada gambar 11. menampilkan halaman login untuk sistem RSA di SMK Islam Kunjang. Halaman ini minta kepala IT untuk memasukkan alamat email dan kata sandi mereka untuk masuk ke dalam sistem. Terdapat dua kolom input untuk memasukkan email dan password, serta satu tombol hijau tosca bertuliskan "Masuk" yang digunakan untuk mengirimkan informasi login.



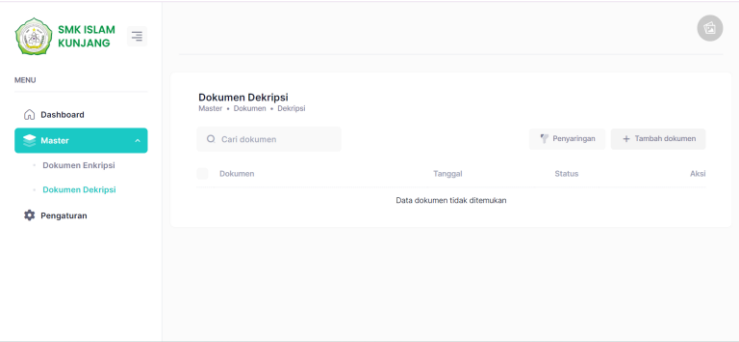
Gambar 12. Tampilan Halaman Dashboard

Pada gambar 12. tersebut menampilkan halaman dashboard dari aplikasi RSA di SMK ISLAM KUNJANG. Pada bagian atas halaman, penjelasan singkat mengenai algoritma RSA (Rivest Shamir Adleman). Pada menu sebelah kiri memeiliki beberapa opsi yaitu dashboard, master data, dokumen enkripsi, dokumen dekripsi, dan pengaturan. Serta tombol dibagian kanan atas untuk melihat profil dan keluar dari menu dashboard untuk Kembali ke laman login.



Gambar 13. Tampilan menu enkripsi

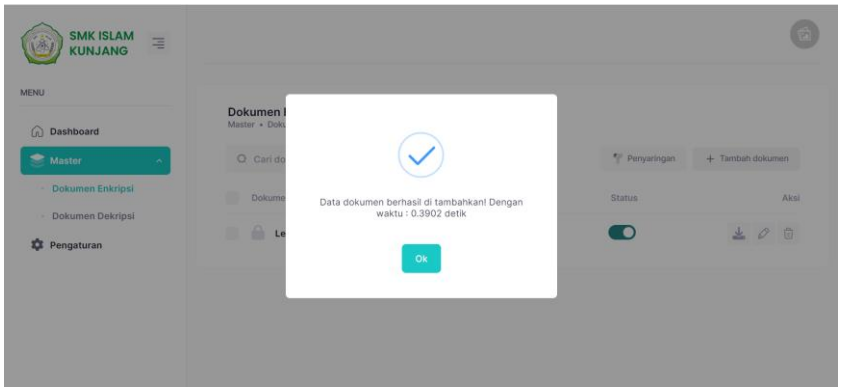
Pada Gambar 13. tersebut menunjukkan tampilan antarmuka dari aplikasi web untuk mengelola dokumen enkripsi di SMK Islam Kunjang. Di sisi kiri, terdapat menu navigasi dengan opsi Dashboard, Master (terdiri dari Dokumen Enkripsi dan Dokumen Dekripsi), serta Pengaturan. Di tengah halaman, pengguna berada pada halaman Dokumen Enkripsi, dengan fitur pencarian dokumen, penyaringan, dan tombol untuk menambahkan dokumen baru. Tabel di bawahnya akan menampilkan daftar dokumen, tetapi saat ini menunjukkan pesan "Data dokumen tidak ditemukan," yang berarti belum ada dokumen yang tersedia.



Gambar 14. Tampilan Menu Dekripsi

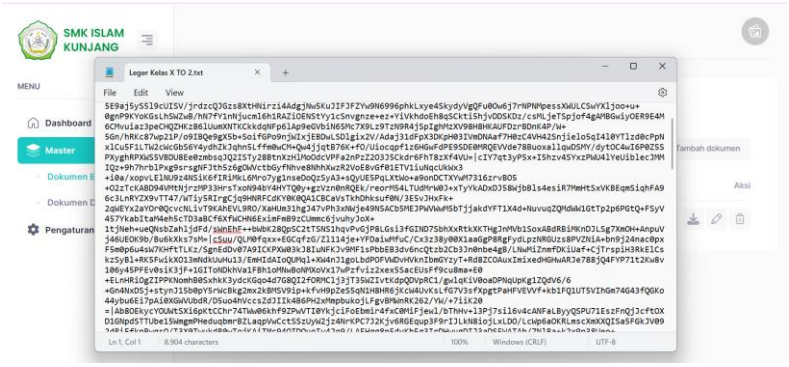
Pada Gambar 14. tersebut menunjukkan tampilan antarmuka dari aplikasi web untuk mengelola dokumen dekripsi di SMK Islam Kunjang. Di sisi kiri, terdapat menu navigasi dengan opsi Dashboard, Master (terdiri dari Dokumen Enkripsi dan Dokumen Dekripsi), serta Pengaturan. Di tengah halaman, pengguna berada pada halaman Dokumen Dekripsi, dengan fitur pencarian dokumen, penyaringan, dan tombol untuk menambahkan dokumen baru. Tabel di bawahnya akan menampilkan daftar dokumen, tetapi saat ini menunjukkan pesan "Data dokumen tidak ditemukan," yang berarti belum ada dokumen yang tersedia

3.2. Tampilan Dokumen Setelah Enkripsi Dan Deskripsi



Gambar 15. Tampilan Proses Enkripsi

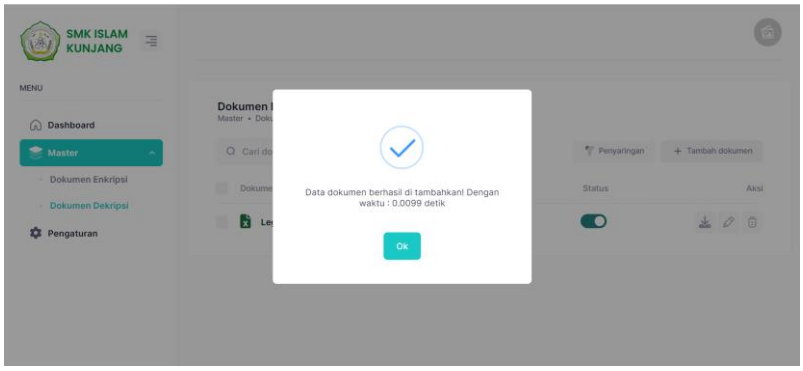
Pada Gambar 15. menunjukkan bahwa proses enkripsi file berhasil. Pada jendela pop-up bagian Tengah layer terdapat sebuah pesan dengan tanda centang dan bertuliskan “Data dokumen berhasil ditambahkan!” yang menandakan bahwa data dokumen telah berhasil dienkripsi dan ditambahkan ke sistem lalu tekan tombol “OK” untuk menutup pesan konfirmasi tersebut.



Gambar 16. Tampilan Dokumen Dienkripsi

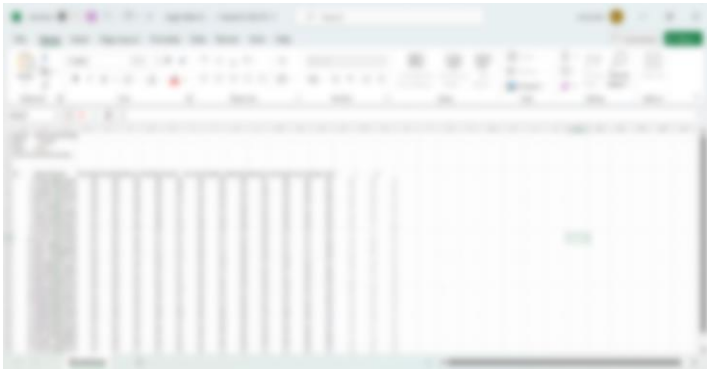
Setelah melewati proses enkripsi dokumen menghasilkan sebagaimana pada Gambar 16. tersebut menunjukkan hasil dari proses enkripsi dokumen menggunakan algoritma RSA. Pada jendela yang terbuka, terlihat sebuah file teks berbentuk txt yang berisi deretan karakter acak yang panjang. Ini merupakan teks terenkripsi yang

dihasilkan dari algoritma RSA, di mana setiap blok teks asli telah diubah menjadi format yang tidak bisa dibaca tanpa kunci dekripsi yang sesuai akan menampilkan data yang bersifat acak atau kode-kode.



Gambar 17. Tampilan Proses Dekripsi

Pada Gambar 17. menunjukkan bahwa proses dekripsi file berhasil. Pada jendela pop-up bagian Tengah layer terdapat sebuah pesan dengan tanda centang dan bertuliskan "Data dokumen berhasil ditambahkan!" yang menandakan bahwa data dokumen telah berhasil didekripsi dan ditambahkan ke sistem lalu tekan tombol "OK" untuk menutup pesan konfirmasi tersebut.



Gambar 18. Tampilan Dokumen Didekripsi

Setelah dokumen berupa txt yang berisikan teks kode acak tak beraturan di dekripsi akan kembali lagi ke dokumen berupa excel serta pulih Kembali seperti dokumen semula pada Gambar 18 diatas.

3.3. Pengujian Sistem

pengujian sistem waktu enkripsi dan dekripsi seberapa cepat proses enkripsi file dibandingkan dengan dekripsi file. Berdasarkan hasil pengujian pada tabel 1. dibawah, dapat disimpulkan bahwa ukuran file berpengaruh terhadap waktu yang dibutuhkan untuk proses enkripsi dan dekripsi. Semakin besar ukuran file, semakin lama waktu enkripsi yang diperlukan. Waktu untuk enkripsi dan dekripsi biasanya hampir sama, karena ukuran file tetap tidak berubah selama proses tersebut. Meskipun demikian, ada beberapa faktor yang dapat menyebabkan sedikit perbedaan dalam waktu enkripsi dan dekripsi, seperti spesifikasi perangkat keras laptop, koneksi internet, dan faktor lainnya [13].

Tabel 1. Pengujian Enkripsi Dan Dekripsi

No.	Nama File	Tipe File	Size File	Waktu Enkripsi (s)	Waktu Dekripsi (s)
1	Leger-Nilai-Akhir-Kelas-X-TO-2	Xls	10kb	0.3902 detik	0.0099 detik
2	Leger-Nilai-Akhir-Kelas-X-TJKT-2	Xls	10kb	0.3830 detik	0.0060 detik

4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa aplikasi Keamanan Data Siswa SMK Islam Kunjang Menggunakan Algoritma Asimetris RSA memiliki beberapa keunggulan sebagai berikut:

1. Aplikasi berbasis web ini sangat mudah digunakan untuk mengamankan file leger nilai siswa. Dari serangkaian penelitian yang telah dilakukan, aplikasi ini dapat beroperasi dengan baik dan membantu Kepala IT dalam mengamankan dokumen-dokumen file leger siswa yang bersifat rahasia.

2. Dengan adanya aplikasi ini, Kepala IT dapat mengamankan dokumen file leger siswa SMK Islam Kunjang sehingga tidak dapat disalahgunakan oleh oknum siswa maupun orang yang tidak bertanggung jawab.
3. Penggunaan aplikasi ini cukup mudah, terbukti dari hasil pengujian blackbox testing yang menunjukkan bahwa aplikasi ini dapat berfungsi dengan baik.

Adapun saran yang dapat menjadi bahan pertimbangan untuk pengembangan sistem di masa yang akan datang, yaitu:

1. Untuk penelitian selanjutnya, diharapkan agar aplikasi yang dikembangkan dapat memproses gambar dalam file excel yang diproses.
2. Saat ini file yang bisa diproses hanya berekstensi excel dan txt saja, maka dari itu dapat ditambahkan ekstensi yang lain agar lebih lengkap.
3. Diharapkan fitur-fitur yang ada di aplikasi harus ditambahkan sehingga kedepannya sudah banyak fitur yang menarik.

DAFTAR PUSTAKA

[1] Firda Nurelia Syah Putri, Yudo Bismo Utomo, and Harso Kurniadi, "Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux," Online, 2023.

[2] S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, and S. Srinjiwi, "ANALISIS PERFORMA KRIPTOGRAFI HYBRID ALGORITMA BLOWFISH DAN ALGORITMA RSA," *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)*, vol. 6, no. 1, pp. 1–10, Dec. 2019, doi: 10.33330/jurteksi.v6i1.395.

[3] Y. B. Utomo and D. Erwanto, "Analisa Teknik Steganografi dan Steganalysis Pada File Multimedia Menggunakan Net Tools dan Hex Editor," 2019.

[4] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika*, vol. 8, no. 1, p. 52, 2018, doi: 10.30864/eksplora.v8i1.139.

[5] B. Nuansyah, "Penerapan Kriptografi Dengan Algoritma Rivest Shamir Adleman (Rsa) Untuk Keamanan Pesan Text," vol. 1, no. 16, pp. 1–12, 2021.

[6] K. Andriani and B. H. Hayadi, "Pengamanan Data Penjualan Dengan Kriptografi Algoritma Rivest Shamir Adleman (Rsa) Pad a Toko Baju Family," *Journal of Science and Social Research*, vol. 5, no. 3, p. 664, 2022, doi: 10.54314/jssr.v5i3.1018.

[7] A. Khamsyar and Muh. Basri, "Aplikasi Enkripsi Gambar Menggunakan Metode (Rivest Shamir Adleman) Rsa," *Jurnal Sintaks Logika*, vol. 2, no. 3, pp. 39–45, 2022, doi: 10.31850/jsilog.v2i3.1850.

[8] Azlin, F. Musadat, and J. Nur, "Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64," *Jurnal Informatika*, vol. 7, no. 2, pp. 1–5, 2018.

[9] I. Gunawan, "Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk pengamanan File Dokumen dan Pesan Teks," *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)*, vol. 2, no. 2, pp. 124–129, 2018, doi: 10.30743/infotekjar.v2i2.266.

[10] A. Abdul Wahid, "Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi," *Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK*, no. November, pp. 1–5, 2020.

[11] N. Moch Bachrudin, Y. Bismo Utomo, and I. Kurniasari, "Perancangan Aplikasi E-Archive Untuk Penyimpanan Laporan Tugas Akhir (Studi Kasus: Fakultas Teknik Uniska Kediri)," 2023.

[12] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.

[13] A. N. Agustina, Aryanti, and Nasron, "Pengamanan Dokumen Menggunakan Kombinasi Metode Rsa (Rivest Shamir Adleman) Dan Vigenere Cipher," *Prosiding Seminar Nasional Multi Disiplin Ilmu & Call For Papers UNISBANK*, pp. 14–19, 2017.