wPENERAPAN TANDA TANGAN DIGITAL DALAM PENGAMANAN DATA IJAZAH BEBRASIS QR CODE DENGAN ALGORITMA RSA PADA YAYASAN ISLAMIC CENTRE SUMUT

SKRIPSI

DISUSUN OLEH

MUHAMMAD RIZKY ANANDA RANGKUTI

NPM. 2009010101

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

MEDAN

2025

PENERAPAN TANDA TANGAN DIGITAL DALAM PENGAMANAN DATA IJAZAH BEBRASIS QR CODE DENGAN ALGORITMA RSA PADA YAYASAN ISLAMIC CENTRE SUMUT

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) dalam Program Studi Sistem Informasi pada Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara

Muhammad Rizky Ananda Rangkuti
NPM. 2009010101

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2025

LEMBAR PENGESAHAN

Judul Skripsi	:	PENERAPAN TANDA TANGAN DIGITAL DALAM PENGAMANAN DATA IJAZAH BEBRASIS QR CODE DENGAN ALGORITMA RSA PADA YAYASAN ISLAMIC CENTRE SUMUT
Nama Mahasiswa	:	MUHAMMAD RIZKY ANANDA RANGKUTI
NPM	:	2009010101
Program Studi	:	SISTEM INFORMASI

Menyetujui
Komisi Pembimbing

(Wilda Rina Hasibuan, S.T., M.Kom)
NIDN. 0105017703

Ketua Program Studi	Dekan
(Martiano S.Pd, S.Kom., M.Kom)	**(Dr. Al-Khowarizmi, S.Kom., M.Kom)**
NIDN. 0128029302	**NIDN. 0127099201**

ii

PERNYATAAN ORISINALITAS

PENERAPAN TANDA TANGAN DIGITAL DALAM PENGAMANAN DATA IJAZAH BEBRASIS QR CODE DENGAN ALGORITMA RSA PADA YAYASAN ISLAMIC CENTRE SUMUT

SKRIPSI

Saya menyatakan bahwa karya tulis ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya.

Medan, April 2025

Yang membuat pernyataan

Muhammad Rizky Ananda Rangkuti

NPM. 2009010101

iii

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Muhammadiyah Sumatera Utara, saya bertanda tangan dibawah ini:

Nama	: Muhammad Rizky Ananda Rangkuti
NPM	: 2009010101
Program Studi	: Sistem Informasi
Karya Ilmiah	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Sumatera Utara Hak Bedas Royalti Non-Eksekutif *(Non-Exclusive Royalty free Right)* atas penelitian skripsi saya yang berjudul:

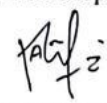
PENERAPAN TANDA TANGAN DIGITAL DALAM PENGAMANAN DATA IJAZAH BEBRASIS QR CODE DENGAN ALGORITMA RSA PADA YAYASAN ISLAMIC CENTRE SUMUT

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksekutif ini, Universitas Muhammadiyah Sumatera Utara berhak menyimpan, mengalih media, memformat, mengelola dalam bentuk database, merawat dan mempublikasikan Skripsi saya ini tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemegang dan atau sebagai pemilik hak cipta.

Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, April 2025

Yang membuat pernyataan



Muhammad Rizky Ananda Rangkuti
NPM. 2009010101

iv

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap	: Muhammad Rizky Ananda Rangkuti
Tempat dan Tanggal Lahir	: Medan, 23 Oktober 2002
Alamat Rumah	: Jl. Sempurna Gg. Melati 45 Tembung
Telepon/Faks/HP	: +6285143138391
E-mail	: rizkyanandarkt@gmail.com
Instansi Tempat Kerja	: -
Alamat Kantor	: -

DATA PENDIDIKAN

SD	: MIN 2 Medan	TAMAT: 2014
SMP	: MTS Tahfizhil Qur'an Medan	TAMAT: 2017
SMA	: MAS Tahfizhil Qur'an Medan	TAMAT: 2020

KATA PENGANTAR

Puji syukur atas kehadiran Allah SWT, berkat limpahan rahmat, hidayah dan karunianya, penulis bisa menyelesaikan skripsi dengan judul "**PENERAPAN TANDA TANGAN DIGITAL DALAM PENGAMANAN DATA IJAZAH BEBRASIS QR CODE DENGAN ALGORITMA RSA PADA YAYASAN ISLAMIC CENTRE SUMUT**". Skripsi ini adalah salah satu dari beberapa persyaratan untuk menyelesaikan pendidikan dan memperoleh gelar sarjana pada program studi S1 Sistem Informasi di Universitas Muhammadiyah Sumatera Utara.

Penulis tentunya berterima kasih kepada berbagai pihak dalam dukungan serta doa dalam penyelesaian skripsi. Penulis juga mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Agussani, M.AP., Rektor Universitas Muhammadiyah Sumatera Utara (UMSU)
2. Bapak Dr. Al-Khowarizmi, S.Kom., M.Kom. Dekan Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
3. Bapak Martiano, S.Pd., S.Kom., M.Kom selaku Ketua Program Studi Sistem Informasi
4. Ibu Yoshida Sary, S.E., S.Kom., M.Kom selaku Sekretaris Program Studi Sistem Informasi
5. Ibu Wilda Rina Hasibuan, S.T., M.Kom selaku Dosen Pembimbing
6. Papa tercinta, bapak Ridwan Rangkuti, terima kasih sebesar-besarnya penulis ucapkan karena telah menjadi panutan dalam mengenalkan arti kasih sayang dan pengorbanan. Kehadiran papa telah menjadi sumber semangat penulis dalam setiap langkah perjalanan akademik penulis.
7. Mama Tercinta, Ibu Rosmina Lubis, S.H, terima kasih sebesar-besarnya penulis ucapkan atas cinta, doa, dan dukungan tanpa batas, baik moral maupun material, yanag selalu diberikan dalam setiap langkah saya.

8. Teman-teman seperjuangan, yang telah menemani perjalanan ini dari awal hingga akhir. Terima kasih atas kebersamaan, diskusi, tawa, bahkan tangisan yang telah kita lewati bersama.
9. Kepada semua keluarga yang tidak dapat disebutkan satu persatu yang telah banyak membantu dan dukungan serta memberikan pemikiran demi kelancaran dan keberhasilan penyusunan skripsi ini.

PENERAPAN TANDA TANGAN DIGITAL DALAM PENGAMANAN DATA IJAZAH BERBASIS QR CODE DENGAN ALGORITMA RSA PADA YAYASAN ISLAMIC CENTRE SUMUT

ABSTRAK

Pemalsuan ijazah menjadi permasalahan serius dalam dunia pendidikan karena dapat merusak integritas akademik dan menurunkan kepercayaan terhadap lembaga pendidikan. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem pengamanan ijazah menggunakan tanda tangan digital berbasis QR Code dengan algoritma RSA pada Yayasan Islamic Centre Sumut. Metode yang digunakan adalah pendekatan kuantitatif dengan studi kasus yang dilaksanakan di Madrasah Aliyah Hifdzil Qur'an. Sistem yang dibangun bekerja dengan cara mengenkripsi data ijazah menggunakan algoritma RSA, lalu menyimpan hasil enkripsi dalam bentuk QR Code yang dapat diverifikasi keasliannya. Hasil penelitian menunjukkan bahwa proses enkripsi dan dekripsi berjalan dengan baik, dan QR Code mampu menyimpan tanda tangan digital yang dapat diverifikasi secara cepat dan efisien. Dengan sistem ini, keaslian data ijazah dapat terjamin, dan potensi pemalsuan dokumen dapat diminimalisir.

Kata Kunci: Tanda Tangan Digital, RSA, QR Code, Pengamanan Ijazah, Kriptografi

IMPLEMENTATION OF DIGITAL SIGNATURE IN SECURING DATA OF DIPLOMAS BASED ON QR CODE WITH RSA ALGORITHM AT THE ISLAMIC CENTER FOUNDATION OF SUMUT

ABSTRACT

Diploma forgery is a serious issue in the field of education as it undermines academic integrity and reduces trust in educational institutions. This research aims to design and implement a diploma security system using digital signatures based on QR Code and the RSA algorithm at Yayasan Islamic Centre Sumut. The method used is a quantitative approach with a case study conducted at Madrasah Aliyah Hifdzil Qur'an. The system encrypts diploma data using the RSA algorithm and stores the encrypted result in a QR Code that can be verified for authenticity. The results show that the encryption and decryption processes work effectively, and the QR Code can securely store digital signatures that are verifiable quickly and efficiently. This system ensures the authenticity of diploma data and minimizes the potential for document forgery.

Keywords: Digital Signature, RSA, QR Code, Diploma Security, Cryptography

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Ijazah merupakan dokumen atau surat yang memiliki harga yang diberikan pada peserta didik setelah selesai menjalankan studinya dan dinyatakan lulus dari suatu institusi pendidikan (Sukardi, et al. 2021). Ijazah biasanya diperoleh sesudah tamat belajar dari Sekolah, Sekolah Tinggi, Politeknik, Universitas atau Perguruan Tinggi yang diterbitkan oleh pihak yang berwenang yaitu Dinas Pendidikan melalui jalur pendidikan yang tercantum didalam undang undang (Sinabutar, 2022). Sudah sepantasnya ijazah disimpan baik-baik dan dapat sebebas-bebasnya digunakan untuk kepentingan pemiliknya agar pemiliknya dapat menikmati hak yang timbul dari ijazah tersebut. Pemalsuan ijazah tidak hanya termasuk dalam jenis kejahatan atau tindak pidana yang dapat dikenakan pidana, tetapi juga merupakan pelanggaran dalam etika akademis. Tindakan yang melanggar etika akademis merupaka perbuatan yang salah dan tindakan yang semestinya tidak dilakukan (Nugroho, 2022).

Melihat begitu pentingnya ijazah bagi pemiliknya, tidaklah heran banyak oknum-oknum yang tidak bertanggung jawab melakukan pemalsuan ijazah Salah satunya yang dilakukan oleh Kepala desa untuk memenuhi syarat administrasi untuk pencalonan Pemilihan Kepala desa. Dalam pencalonan Kepala desa, ada oknum yang menghalalkan segala cara agar dapat lolos dalam masalah pengadministrasian yaitu dengan memalsukan dokumen seperti ijazah (Sinabutar, 2022). Hal ini tentu menjadi masalah, bukan hanya merugikan individu yang

bersangkutan, tetapi juga dapat merusak reputasi lembaga pendidikan serta kepercayaan masyarakat terhadap ijazah sebagai bukti pencapaian pendidikan.

Dalam menghadapi fenomena ini, Yayasan Islamic Centre SUMUT sebuah lembaga pendidikan yang menggabungkan pendidikan akademis, agama, dan teknologi, sangat memperhatikan masalah pemalsuan data ijazah karena kemajuan teknologi dapat digunakan untuk memalsukan data ijazah yang lebih akurat. Oleh karena itu, untuk mengatasi masalah ini diperlukan solusi yang efektif dan dapat diandalkan. Untuk meningkatkan pengamanan data ijazah, Yayasan Islamic Centre SUMUT menggunakan pendeketan kriptografi yang memakai konsep tanda tangan digital dan teknologi Quick Response Code (QR Code) dengan menggunakan algoritma Rivest Shamir Adleman (RSA). Dengan menyertakan QR Code yang ditempelkan pada dokumen ijazah yang dihasilkan melalui algoritma RSA akan meningkatkan pengamanan data ijazah.

Kriptografi merupakan bidang ilmu pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi dan dekripsi pesan. Teknik ini dipakai untuk mengubah pesan kedalam kode-kode tertentu sehingga informasi yang ditransmisikan melalui jaringan yang mungkin tidak aman (misalnya saja internet) tidak dapat dibaca oleh pihak manapun kecuali orang-orang yang berhak (Rizki & Ariyani, 2021). Fungsi utama kriptografi adalah merahasiakan kunci dan mengubah plaintext menjadi ciphertext, sehingga plaintext menjadi password yang tidak diketahui orang lain, tanpa harus merahasiakan algoritma yang digunakan (sari, et al. 2022).

RSA merupakan salah satu algoritma kriptografi yang menggunakan dua kunci berbeda untuk melakukan enkripsi dan dekripsi. Dalam pengamanan keaslian ijazah, RSA digunakan untuk menghasilkan tanda tangan digital yang unik dan sulit dipalsukan, Tanda tangan ini berfungsi sebagai bukti otentikasi, di mana setiap verifikasi keaslian dokumen dilakukan melalui proses kriptografi yang hanya dapat divalidasi dengan kunci yang sah. RSA masih digunakan secara luas dalam protokol-protokol perdagangan elektronik dan dipercayai sangat aman karena diberikan kunci-kunci yang cukup panjang dan penerapan-penerapannya yang sangat mutakhir (Indriani, et al. 2022). Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima, pemfaktoran dilakukan untuk memperoleh kunci private. Selama pemfaktoran bilangan besar menjadi bilangan prima belum tentu menemukan algoritma yang benar, maka selama itu pula keamanan algoritma RSA terjamin (Rahayu, et al. 2024).

Tujuan dari penelitian ini adalah untuk membuat aplikasi yang dapat memverifikasi keaslian ijazah yang menggunakan teknologi QR Code dan algoritma RSA di Yayasan Islamic Centre SUMUT. Dengan cara ini diharapkan dapat membantu menjamin keaslian data ijazah secara digital, mengurangi peluang pemalsuan, dan memberikan kepercayaan kepada semua pihak yang terlibat dalam pendidikan dan penerimaan di jenjang selanjutnya. Berdasarkan latar belakang tersebut, maka diangkatlah sebuah judul skripsi yaitu "**PENERAPAN TANDA TANGAN DIGITAL DALAM PENGAMANAN DATA IJAZAH BERBASIS QR CODE DENGAN ALGORITMA RSA PADA YAYASAN ISLAMIC CENTRE SUMUT**".

1.2. Rumusan Masalah

Berdasarkan latar belakang penelitian yang telah dijelaskan sebelumnya, maka rumusan masalahnya yaitu sebagai berikut:

1. Bagaimana merancang sistem dengan menggunakan algoritma RSA berbasis QR Code agar dapat mengatasi masalah pengamanan data ijazah pada Yayasan Islamic Centre SUMUT?
2. Bagaimana menerapkan tanda tangan digital dalam pengamanan data ijazah pada Yayasan Islamic Centre SUMUT?
3. Bagaimana menguji sistem yang telah dirancang untuk menilai sejauh mana sistem tersebut dapat menyelesaikan masalah p engamanan data ijazah pada Yayasan Islamic Centre SUMUT?
4. Apakah sistem yang telah diuji dapat diimplementasikan sebagai solusi efektif untuk masalah pengamanan data ijazah pada Yayasan Islamic Centre SUMUT?

1.3. Basatan Masalah

Agar topik penelitian tidak terlalu luas, maka dilakukan pembatasan. Adapun batasan masalahnya sebagai berikut:

1. Penelitian ini menggunakan algoritma RSA (*Rivest Shamir Adleman*) yang diintegrasikan dengan website.
2. Penelitian ini hanya fokus pada pengamanan data ijazah, tidak mencakup data akademik lainnya.
3. Penelitian ini hanya diperuntukkan untuk Madrasah Aliyah (MA) atau setara Sekolah Menengah Atas (SMA) di Yayasan Islamic Centre SUMUT
4. Sistem yang dibuat hanya memberikan akses kepada pihak berwenang di

Yayasan Islamic Centre Sumut serta pemegang ijazah. Pengguna dari luar atau publik tidak termasuk.

5. Pengujian keamanan yang dilakukan terbatas pada pengujian dasar validasi keaslian data ijazah. Risiko keamanan terkait serangan siber atau kebocoran data dari sistem secara lebih luas tidak dibahas secara mendalam.

1.4. Tujuan Penelitian

Tujuan dari penelitian yang dilakukan yaitu sebagai berikut:

1. Merancang sebuah sistem keamanan yang dapat mengamankan data ijazah untuk menyelesaikan masalah di Yayasan Islamic Centre SUMUT.
2. Menerapkan sistem berbasis *QR Code* yang menyimpan informasi tanda tangan digital untuk mempermudah verifikasi data ijazah oleh pihak-pihak berwenang.
3. Menguji dan mengevaluasi sistem yang dikembangkan untuk memastikan bahwa sistem tersebut dapat melindungi ijazah dari pemalsuan dan modifikasi yang tidak sah.
4. Untuk meningkatkan kepercayaan pihak terkait bahwa data ijazah yang dikeluarkan oleh Yayasan Islamic Centre SUMUT itu asli.

1.5. Manfaat Penelitian

Penelitian ini memiliki banyak manfaat, tetapi beberapa manfaat utamanya adalah sebagai berikut:

1. Dapat membantu Yayasan Islamic Centre SUMUT, bahwa setiap data ijazah yang diterbitkan dapat terjamin keasliannya.

2. Bagi para lulusan, sistem ini memberikan jaminan bahwa ijazah mereka memiliki nilai yang sah dan diakui.
3. Mengurangi pemalsuan ijazah, memberikan manfaat untuk masyarakat umum dengan menjaga kepercayaan terhadap dokumen pendidikaan.

BAB II

LANDASAN TEORI

2.1. Dokumen Ijazah

Menurut Permendikbudristek No. 6 Tahun 2022, Ijazah adalah dokumen yang diberikan kepada lulusan pendidikan akademik dan pendidikan vokasi sebagai pengakuan terhadap prestasi belajar dan/atau penyelesaian program studi terakreditasi yang diselenggarakan oleh perguruan tinggi. Selain menjadi bukti bahwa seseorang telah menyelesaikan program pendidikan tertentu Ijazah menjadi salah satu bukti otentik yang menunjukkan bahwa pemegangnya telah memenuhi syarat-syarat akademis dan administrasi yang ditetapkan oleh lembaga pendidikan tersebut. Keaslian ijazah adalah jaminan bahwa dokumen tersebut dibuat dan diakui oleh lembaga pendidikan yang sah. Keaslian ijazah sering kali dilindungi dengan berbagai macam keamanan termasuk hologram, tanda air, dan tanda tangan digital untuk mencegah pemalsuan (Vasi Waruwu, et al. 2020). Ini dilakukan untuk menjaga agar ijazah tidak dipalsukan dan disalahgunakan, dan untuk memastikan bahwa orang yang menggunakannya adalah orang yang sah.

Pemalsuan ijazah adalah tindakan yang melanggar hukum dan dapat berdampak negatif pada individu, masyarakat, dan lembaga terkait. Sesuai dengan Pasal 69 ayat 1 UU No. 20 Tahun 2003 tentang Sistem Pendidikan Nasional yang mengatur bahwa “setiap orang yang menggunakan ijazah, sertifikat kompetensi, gelar akademik, profesi, dan/atau vokasi yang terbukti palsu dipidana dengan pidana penjara paling lama lima tahun dan/atau pidana denda paling

banyak Rp. 500.000.000,00 (lima ratus juta rupiah)". Selain merugikan individu yang bersangkutan, pemalsuan ijazah dapat merusak reputasi lembaga pendidikan dan kepercayaan masyarakat terhadap ijazah sebagai bukti pencapaian pendidikan.

2.2. Kriptografi

Kriptografi atau kriptologi berasal dari bahasa Yunani yaitu *kryptos* yang berarti tersembunyi atau rahasia dan *graphein* yang berarti menulis atau ilmu (Rangkuti & Fahmi, 2020). Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain (M. Hidayat, et al. 2023). Menurut Kamus Besar Bahasa Indonesia (KBBI), kriptografi berarti penyelidikan kode rahasia. Ini juga berarti teknik yang menggunakan algoritma matematika untuk mengubah data menjadi berbeda dari aslinya, sehingga orang yang tidak tahu kuncinya tidak akan dapat membongkar data tersebut.

2.2.1. Tujuan Kriptografi

Ada beberapa tujuan mendasar memanfaatkan ilmu kriptografi dalam pengamanan pesan yaitu (Ziliwu, et al. 2022):

a. Kerahasiaan

   Kerahasiaan (*Confiedentiality*), adalah layanan yang bertujuan untuk menjaga isi pesan agar tidak dapat dibaca oleh orang lain selama pengiriman selain dari penerima pesan yang telah ditentukan oleh pengirim yang memiliki kunci atau kode untuk membuka pesan tersandi. Didalam kriptografi layanan ini diimplementsikan dengan cara mengenkripsi pesan menjadi cipherteks.

b. Kelengkapan data

Kelengkapan *(Data integrity*), adalah layanan berkaitan dengan penjagaan isi pesan agar tidak ada perubahan selama pengiriman berlangsung. Tujuan kriptografi lainnya yaitu menjamin bahwa pesan masih asli/utuh atau belum pernah diubah/manipulasi selama proses pengirimanan. Keutuhan isi pesan selama pengiriman bisa dibuktikan saat peneriman mengubah pesan tersandi dengan cara melakukan deskripsi dengan kunci yang sama sehingga mengembalikan isi pesan yang bisa dimengerti.

c. Otentikasi

Otentikasi (*authentication*), adalah layanan yang berhubungan dengan identifikasi, yang mengidentifikasikan kebenaran pihak-pihak yang berkomunikasi. Dalam menjaga keaslian data, pihak yang melakukan pertukaran informasi terlebih dahulu melakukan autentikasi terhadap sumber, server dan orang yang ingin menggunakan data.

d. Anti penyangkalan

Anti penyangkalan (*non-repudiation*), adalah layanan untuk mencegah entitas yang berkomunikasi melalukan penyangkalan, yaitu pengirim pesan membantah telah mengirim pesan, atau penerima pesan menyangkal telah menerima pesan.

2.2.2. Algoritma Kriptografi

Dalam kriptografi, algoritma adalah prosedur matematis yang digunakan untuk mengamankan informasi dengan cara mengubah (enkripsi) dan mengembalikan (dekripsi) data (Andriani & Hayadi, 2022). Tujuannya adalah untuk menjaga kerahasiaan, integritas, dan otentikasi informasi yang ditransmisikan atau disimpan. Algoritma kriptografi bekerja dengan memanipulasi

data menggunakan kunci yang disepakati, sehingga hanya penerima yang memiliki kunci yang benar dapat membaca atau memproses data tersebut. Algoritma kriptografi memiliki tiga fungsi, yaitu (Utomo & Haryanti, 2024):

a. Enkripsi

   Enkripsi adalah proses menjaga kerahasiaan data yang dikirim dengan mengubah pesan asli menjadi kode-kode yang tidak dapat dimengerti.

b. Dekripsi

   Dekripsi adalah proses mengembalikan pesan yang telah dienkripsi menjadi bentuk aslinya.

c. Kunci

   Kunci yang dimaksud adalah kunci yang digunakan untuk melakukan enkripsi dan dekripsi data. Kunci terbagi menjadi dua jenis: kunci publik (public key) dan kunci pribadi (private key).

Keamanan algoritma kriptografi bergantung pada cara mereka bekerja. Oleh karena itu, algoritma seperti ini disebut algoritma terbatas. Algoritma kriptografi bekerja seperti kunci untuk mengunci pesan kita sehingga hanya orang yang memiliki kunci yang tepat bisa membukanya. Dengan begitu, kita bisa merasa lebih aman saat berkomunikasi online atau menyimpan data sensitif seperti informasi bank atau kata sandi.

2.2.3. Jenis Kriptografi

Bedasarkan jenis kuncinya, dalam kriptografi ada dua jenis algoritma yang digunakan untuk mengamankan data, yaitu algoritma kriptografi simetris dan algoritma kriptografi asimetris.

a. Algoritma Simetris

(Arif & Nurokhman, 2023) Algoritma kriptografi simetris, juga dikenal sebagai kunci rahasia, adalah metode enkripsi dan dekripsi yang menggunakan satu kunci. Pada algoritma kriptografi simetris, kunci yang digunakan untuk proses enkripsi maupun dekripsi adalah kunci yang sama. Algoritma yang menggunakan kunci simetris diantaranya:

1. AES *(Advanced Encryption Standard)*.
2. DES *(Data Encryption Standard)*.
3. *IDEA (International Data Encryption Algorithm*).
4. RC4 (*Rivest Cipher 4*).

b. Algoritma Asimetris

(Arif & Nurokhman, 2023) Algoritma kriptografi asimetris, juga dikenal sebagai kriptografi kunci publik. Pada algoritma kriptografi asimetris menggunakan sepasang kunci yang berbeda tetapi terkait secara matematis, kunci publik dan kunci privat. Kunci publik dapat dibagikan secara bebas dan digunakan untuk mengenkripsi data, sementara kunci privat harus dijaga kerahasiaannya dan digunakan untuk mendekripsi data. Algoritma yang menggunakan kunci asimetris diantaranya:

1. RSA *(Rivest-Shamir-Adleman*).
2. DSA *(Digital Signature Algorithm*).
3. ECC (*Elliptic Curve Cryptography*).
4. NTRUEncrypt.

2.3. Algoritma RSA (*Rivest Shamir Adleman*)

Di antara banyak algoritma kriptografi kunci publik yang telah diciptakan, algoritma RSA adalah yang paling populer. RSA bekerja dengan memfaktorkan

bilangan yang sangat besar, yang membuatnya dianggap aman. Untuk menghasilkan dua kunci, dipilih dua bilangan prima acak yang besar. Algoritma RSA dikembangkan oleh tiga peneliti dari MIT (Massachusetts Institute of Technology) pada tahun 1976, yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman. Kekuatan RSA terletak pada kesulitan memfaktorkan bilangan besar menjadi faktor-faktor bilangan primanya, semakin besar bilangan prima yang digunakan semakin baik dan aman algoritma ini. Dalam penggunaan algoritma RSA dalam kriptografi, terdapat tiga proses yaitu pembangkitan kunci publik dan kunci privat, enkripsi, dan dekripsi (Syahputra, A. 2021).

Penemuan algoritma RSA menyarankan bahwa nilai p dan q harus memiliki panjang lebih dari 100 digit, sehingga hasil perkalian r = p x q akan menghasilkan bilangan dengan lebih dari 200 digit. Menurut Rivest dan rekan-rekannya, upaya untuk memfaktorkan bilangan dengan 200 digit memerlukan waktu komputasi sekitar 4 miliar tahun, dengan asumsi penggunaan algoritma faktorisasi tercepat saat ini dan komputer dengan kecepatan 1 milidetik. Karena belum ditemukan metode yang efisien untuk memfaktorkan bilangan bulat besar menjadi faktor primanya, algoritma RSA tetap menjadi pilihan utama untuk mengamankan pesan. Keamanan yang tinggi yang ditawarkan oleh RSA berdasarkan kesulitan matematis dalam faktorisasi bilangan besar menjadikannya pilihan yang andal dalam kriptografi modern (A. C. Putra, et al. 2021). Algoritma RSA memiliki besaran-besaran yang sifatnya rahasia dan tidak rahasia, besaran tersebut sebagai berikut (D. W. T. Putra & Andriani, 2020):

1. p dan q bilangan prima (rahasia)
2. n = p x q (tidak rahasia)

3. (n) = (p - 1) . (q - 1) (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)
6. P (plainteks) (rahasia)
7. C (cipherteks) (tidak rahasia)

2.3.1. Tahapan Algoritma RSA

(Christian, et al. 2023) Algoritma RSA terdiri dari tiga tahap yaitu tahap pembangkitan kunci, tahap enkripsi dan dekripsi pesan. Berikut merupakan tahapan dari algoritma RSA.

a. Pembangkitan Kunci

Berikut merupakan tahapan prosedur pembangkitan kunci pada algoritma RSA.

1. Memilih dua bilangan prima *p* dan *q*.
2. Menghitung $n = p \times q$.
3. Menghitung nilai $m = (p\text{-}1) \times (q\text{-}1)$.
4. Memilih sebuah bilangan bulat (e) dimana $1 < e < m$ yang relatif prima terhadap (m).
5. Menghitung nilai (d), dimana $1 < d < m$ dimana $e \times d = 1 \pmod m$.

Berdasarkan tahapan pembangkitan kunci diatas maka dapat diperoleh kunci publik dari variabel (n) dan (e) sedangkan kunci privat diperoleh dari variabel (d).

b. Enkripsi

Berikut merupakan tahapan prosedur enkripsi pada algoritma RSA.

1. Membentuk pesan kedalam blok–blok pesan (p1, p2, …., pn) dan mengkonversi blok pesan tersebut kedalam bilangan integer.
2. Melakukan enkripsi pada blok–blok pesan tersebut menggunakan persamaan berikut: $C=P^e$ (*mod n*).

c. Dekripsi

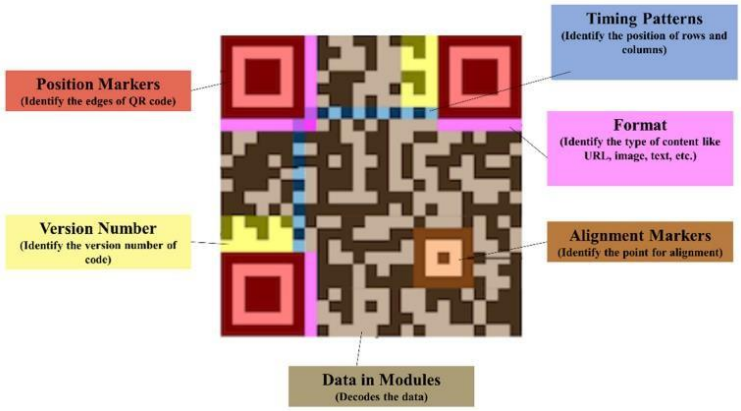
Berikut merupakan tahapan prosedur enkripsi pada algoritma RSA.

1. Membentuk pesan chiperteks kedalam blok–blok pesan (p1, p2, …., pn) dan mengkonversi blok pesan tersebut kedalam bilangan integer.
2. Melakukan enkripsi pada blok–blok pesan tersebut menggunakan persamaan berikut: $M=C^d$ (*mod n*).

2.4. Quick Response code (QR Code)

*Quick Response Cod*e (QR Code) adalah bentuk evolusi *barcode* dari satu dimensi menjadi dua dimensi (2D). Di Jepang QR Code sudah sangat umum digunakan. Hal ini dikarenakan QR Code dapat menyimpan data yang lebih besar dibanding *barcode* sehingga mampu mengkodekan informasi dalam bahasa Jepang sebab dapat menampung huruf kanji. QR Code pertama kali dikembangkan oleh Denso Wave, yang merupakan sebuah perusahaan Jepang. Perbedaan Barcode dengan QR Code adalah kemampuan QR Code yang mampu menyimpan informasi secara horisontal dan vertikal sehingga QR Code dapat menyimpan informasi lebih banyak dibandingkan dengan Barcode (Muhammad, et al. 2021).

(Huo, et al. 2021) QR Code dapat distrukturkan menjadi modul yang berbeda seperti position markers, timing patterns, version number, format identifier, alignment marker, dan data indicator.



Gambar 2.1 Struktur QR Code

a. *Position markers:* Ini adalah indikator deteksi posisi dari kode QR, yang diwakili oleh persegi kecil dikombinasikan dengan persegi yang lebih terang dan lebih gelap. Ini menentukan posisi dan orientasi kode QR.
b. *Timing pattern:* Pola yang saling terkait yang terbentuk oleh urutan alterasi elemen gelap dan cahaya. *Timing pattern* bertugas untuk menentukan ukuran, jumlah baris dan kolom, dan identifikasi distorsi yang hadir dalam kode QR.
c. *Version number:* Indikator ini dalam kode QR membantu untuk mengidentifikasi nomor versi kode.
d. *Format identifier:* Indikator ini berisi informasi tentang nomor pola masker dan tingkat koreksi kesalahan, yang diperlukan untuk mendekodkan kode QR untuk mengidentifikasi jenis konten seperti URL, teks, gambar, dll.
e. *Alignment marker:* menentukan kemungkinan distorsi dalam kode QR dengan mengidentifikasi titik persesuaian dalam kode.

f. *Data indicator*: Data yang dikodekan di dalam kode QR didekodekan dengan menggunakan indikator ini. Jika kode QR rusak, masih bisa dipulihkan dan dibaca dengan menggunakan metode koreksi kesalahan.

2.5 UML

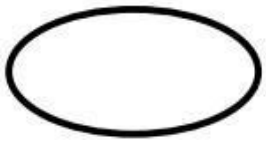
UML (*Unified Modeling Language*) adalah sebuah bahasa yang berdasarkan grafik dan gambar yang digunakan untuk memvisualisasi, menspesifikasikan, membangun, dan mendokumentasikan sistem pengembangan software berbasis OO (*ObjectOriented*) (Mangadi, et al. 2022). UML juga memberikan standar penulisan sistem blue print, yang mencakup konsep bisnis proses, skema database, kelas-kelas yang ditulis dalam bahasa program tertentu, dan komponen-komponen yang diperlukan untuk sistem software.

2.5.1 Use Case Diagram

Diagram *use case* memodelkan perilaku sistem informasi yang akan dibuat. *Use case* bekerja dengan mendeskripsikan interaksi khas antara pengguna suatu sistem dan sistem itu sendiri melalui cerita tentang bagaimana sistem tersebut digunakan. Berikut merupakan simbol-simbol yang terdapat didalam *use case diagram* yang dapat dilihat pada tabel berikut (Suharni, et al. 2023).

Tabel 2.1 Simbol *Use Case Diagram*

Simbol	Nama	Deskripsi
	Actor	Digunakan untuk menjelaskan sesuatu atau seseorang

		yang sedang berinteraksi dengan sistem.
	Use Case	Menggambarkan suatu perilaku dari sistem tanpa mengungkapkan struktur internal dari sistem tersebut.
	Assosiation	Jalur komunikasi antar actor dengan use case yang saling berpartisipasi.
<<extend>>	Extend	Penambahan perilaku ke dalam use case dasar yang tidak tahu tentang hal tersebut.
	Use case generalization	Hubungan antara use case umum dengan use case yang lebih spesifik, yang mewarisi dan

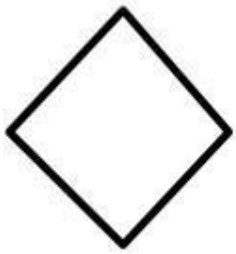
		menambah fitur terhadapnya.
 <<include>>	Include	Penambahan perilaku ke dalam use case dasar yang secara eksplisit menjelaskan penambahannya.

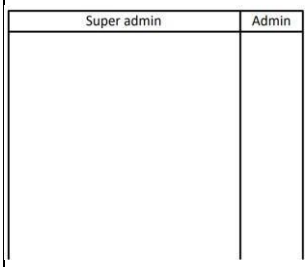
2.5.2. Activity Diagram

Activity Diagram atau diagram aktivitas menunjukkan aktivitas atau aliran kerja dari sistem, proses bisnis, atau menu perangkat lunak. Ini menunjukkan aktivitas sistem bukan apa yang dilakukan oleh aktor. Berikut merupakan simbol-simbol yang terdapat didalam *acivity diagram* yang dapat dilihat pada tabel berikut.

Tabel 2.2 Simbol *Activity Diagram*

Simbol	Nama	Deskripsi
	Status Awal/ Initial State	Status Awal atau Initial State adalah suatu keadaan awal pada saat sistem mulai hidup.

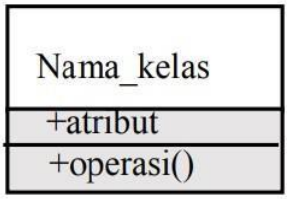
	Status Akhir/ Final State	Status Akhir atau Final State adalah suatu keadaan akhir dari daur hidup.
	Aktivasi	Aktivasi adalah suatu kegiatan yang dilakukan didalam sistem, biasanya diawali dengan kata kerja.
	Percabangan / Decision	Percabangan adalah suatu kegiatan dimana terdapat pilihan kegiatan didalamnya.
	Penggabungan / Join	Asosiasi penggabungan dimana lebih dari satu aktivitas digabung menjadi satu.

	Swimlane	Digunakan untuk memisahkan organisasi bisnis yang bertanggung jawab terhadap aktivitas yang terjadi.
Atau 		

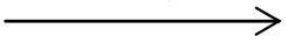
3.5.3. Class Diagram

Class Diagram atau diagram kelas menggambarkan struktur sistem dalam kaitannya dengan definisi kelas-kelas yang dibuat untuk membangun sistem. Kelas memiliki atribut dan metode atau operasi. Berikut adalah simbol-simbol dari class diagram yang dapat dilihat pada tabel berikut.

Tabel 2.3 Simbol *Class Diagram*

Simbol	**Nama**	**Deskripsi**
	Kelas	Kelas pada struktur sistem.

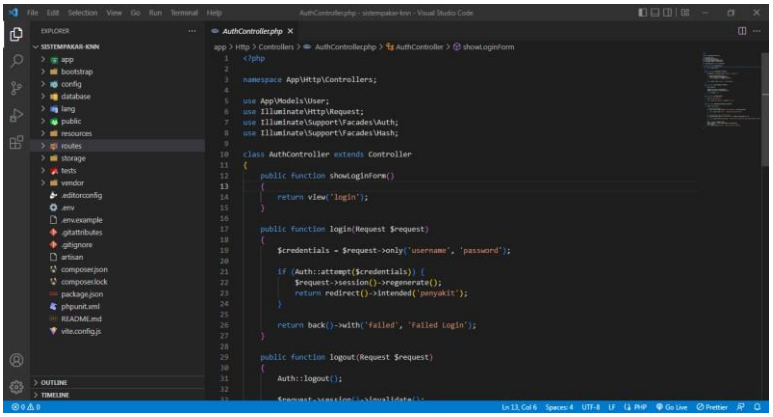
	Antar muka/ Interface	Sama dengan konsep interface dalam pemrograman berorientasi objek.
	Asosiasi/ association	Relasi antar kelas dengan makna umum, asosiasi biasanya juga disertai dengan *multiplicity*.
	Asosiasi berarah / directed association	Relasi antar kelas dengan makna kelas yang satu digunakan oleh kelas yang lain, asosiais biasanya juga disertai dengan *multiplicity*.
	Generalisasi	Relasi antar kelas dengan makna gener alisasi-generalisasi-spesialisasi (umum khusus).

	Kebergantungan / dependency	Relasi antar kelas dengan makna kebergan tungan antar kelas.
	Agregasi/aggregation	Relasi antar kelas dengan makna semua- bagian (whole- part).

2.6. Aplikasi Pengembangan Sistem

2.6.1. Visual Studio Code

Visual Studio Code merupakan aplikasi editor kode sumber terbuka yang dikembangkan oleh Microsoft untuk sistem operasi Windows, Linux, dan MacOS. Mendukung untuk berbagai bahasa pemrograman seperti C++, C#, Java, Python, PHP, dan GO. Visual Studio Code dapat mengidentifikasi jenis bahasa pemrograman yang digunakan dan mengubah warna kode sesuai dengan fungsinya. Selain itu, Visual Studio Code telah diintegrasikan ke platform Github. Salah satu fitur tambahan adalah kemampuan untuk menambah ekstensi, yang memungkinkan pengembang menambahkan fitur yang tidak ada di Visual Studio Code (Ulfah & Nurdin, 2023). Berikut adalah tampilan ruang kerja (workspace) dari Visual Studio Code.



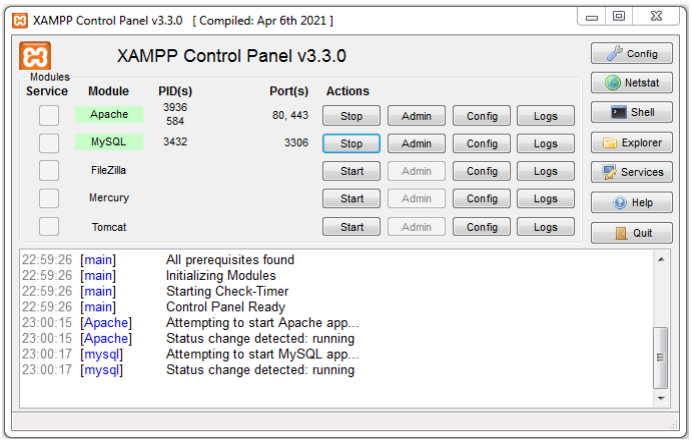
Gambar 2.2 Tampilan Visual Studio Code

2.6.2. Xampp

XAMPP adalah sebuah aplikasi web server instan yang memiliki semua yang dibutuhkan untuk membuat situs web dengan *Content Management System* (Joomla) di dalamnya. XAMPP adalah sebuah paket installer AMP (Apache, MySQL, dan Php) yang sangat mudah digunakan dalam komputer yang belum memiliki server, sehingga komputer dapat menampilkan situs yang dibuat menggunakan bahasa server dan database server tersebut (A. Hidayat, et al. 2020).

Apache adalah web server yang dapat digunakan di berbagai sistem operasi, seperti Windows, Linux, dan MAC. Berfungsi untuk melayani dan mengelola situs web. Protokol yang digunakan untuk melayani fasilitas web/www ini adalah HTTP (Kesuma Astuti & Sri Agustina, 2022). MySql adalah *Relational Database Management System* (RDBMS) gratis yang berlisensi dibawah GNU *General Public License* (GPL), yang berarti bisa digunakan oleh siapa saja dengan syarat tidak boleh diperjualbelikan. MySql dapat digunakan dalam *Text mode*, *Command prompt* atau PHPMyAdmin. PHP (*Hypertext Preprocessor*) adalah bahasa pemrograman web berbasis teks yang bersifat *open source* dan digunakan untuk mengolah data dan mengirimkannya kembali ke web browser menjadi kode

HTML (Hypertext Markup Language) (Alfarizi, et al. 2020). Berikut adalah tampilan *control panel* dari XAMPP.



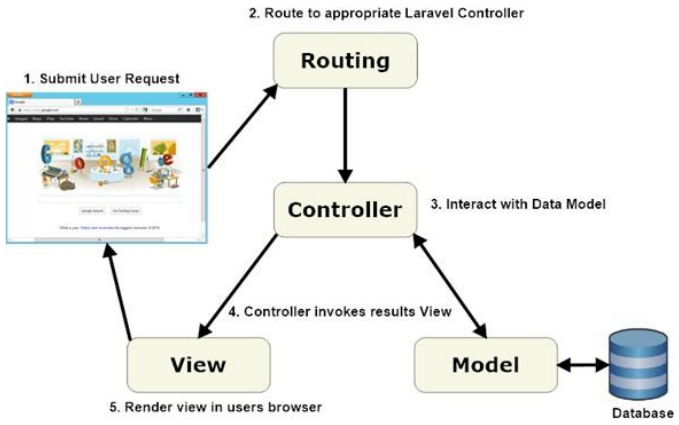
Gambar 2.3 *Control Panel* XAMPP

2.6.3. Laravel

Laravel, yang dikembangkan oleh Taylor Otwell, adalah framework web berbasis PHP yang tidak berbayar dan *opensource* yang dirancang untuk membangun aplikasi web yang menggunakan pola MVC. Struktur pola MVC Laravel sedikit berbeda dari struktur pola MVC biasa. Di Laravel, terdapat routing yang menghubungkan user dan controller. Dengan demikian, controller tidak langsung menerima permintaan dari user (Agustian & Yuliana, 2024).

MVC adalah arsitektur perangkat lunak yang mengorganisir struktur dan logika suatu aplikasi. Arsitektur ini terdiri dari tiga komponen utama: Model, View, dan Controller. Bagian yang bertanggung jawab untuk mengelola logika dan data bisnis adalah model. Tampilan, atau antarmuka pengguna, menangani presentasi data untuk pengguna dan menerima input dari mereka. Controller berfungsi sebagai perantara antara Model dan Tampilan, mengelola alur logika aplikasi, dan merespons input pengguna dengan mengubah data dalam Model atau Tampilan. Konsep MVC memungkinkan pengembang untuk meningkatkan

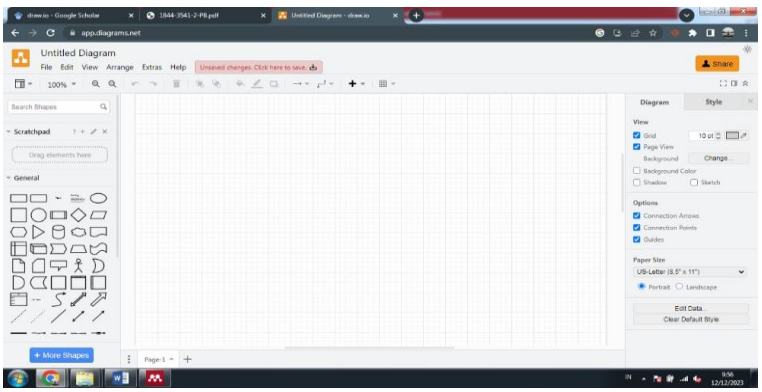
modularitas, mempermudah pemeliharaan kode, dan memungkinkan pengembangan paralel (Santoso, et al. 2021). Berikut adalah tampilan *control panel* dari XAMPP.



Gambar 2.4 Ilustrasi MVC Laravel

2.6.4. Draw.io

Draw.io adalah aplikasi yang dapat membuat rancangan diagram yang memiliki banyak paket untuk merancang dan membuat diagram, termasuk UML, Flowchart, dan 12 Entity Relation (Berliana & Purtiningrum, 2023). Draw.io sudah terintegrasi dengan Google Drive untuk penyimpanan file selain mengekspor dalam bentuk JPG/PNG/SVG/XML. Berikut merupakan gambar halaman kerja dengan draw.io.



Gambar 2.5 Halaman Kerja Draw

BAB III

METODOLOGI PENELITIAN

3.1. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode studi kasus untuk memahami implementasi tanda tangan digital dan QR code dalam pengamanan data ijazah pada Yayasan Islamic Centre SUMUT. Pendekatan kuantitatif dipilih karena memungkinkan peneliti untuk mendalami dan mengeksplorasi secara rinci proses implementasi teknologi serta memahami perspektif dan pengalaman para pengguna di lapangan. Dengan menggunakan metode studi kasus, penelitian ini berfokus pada satu lokasi spesifik, yakni Madrasah Aliyah Hifdzil Qur'an, pendidikan formal setara dengan sekolah SMA yang berada di Yayasan Islamic Centre SUMUT, memungkinkan pengumpulan data yang mendalam dan kontekstual. Kerangka kerja adalah struktur dasar yang sistematis untuk menganalisis dan mengatasi suatu masalah yang dibahas. Adapun kerangka kerja penelitian dapat dilihat pada gambar berikut.

Gambar 3.1 Kerangka Kerja

Kerangka kerja pada gambar 3.1 akan menjelaskan langkah-langkah yang perlu dilakukan dalam membangun sistem untuk mengamankan data ijazah, antara lain:

a. Identifikasi Masalah

   Suatu tindakan atau proses meneliti, mencari, menemukan, mencatat informasi dan mencari permasalahan di Yayasan Islamic Centre SUMUT.

b. Analisis Masalah dan Kebutuhan

   Menganalisis permasalahan yang ada di Yayasan Islamic Centre SUMUT, yaitu tentang penerapan tanda tangan digital pada data ijazah serta kebutuhan apa saja di dalam pemecahan masalahnya.

c. Studi Literatur

   Mencari referensi terkait kasus yang diangkat dan tentang kriptografi untuk membantu dalam penelitian ini.

d. Perancangan Sistem

   Merupakan tahapan dimana aplikasi akan dirancang kedalam sebuah bahasa pemodelan dan pemrograman. Dalam penelitian ini, menggunakan UML sebagai bahasa pemodelan dan PHP sebagai bahasa pemrogramannya.

e. Implementasi

   Penerapan Kriptografi dalam sebuah aplikasi yang akaan dijadikan sebuah solusi dalam penelitian ini.

3.1. Waktu dan Tempat Penelitian

Penelitian ini dilaksanakan selama periode lima bulan, mulai dari April 2024 hingga Agustus 2024. Tempat penelitian adalah Madrasah Aliyah Hifdzil Qur'an, sebuah madrasah unggul yang memiliki program Tahfidz Qur’an.

Pemilihan lokasi ini didasarkan pada ketersediaan teknologi yang digunakan dan kesiapan institusi untuk berpartisipasi dalam penelitian. Penelitian dilakukan di lingkungan sekolah, yang melibatkan interaksi langsung dengan staf IT, guru, dan pihak administrasi yang bertanggung jawab atas pengelolaan data ijazah.

3.3. Algoritma Sistem

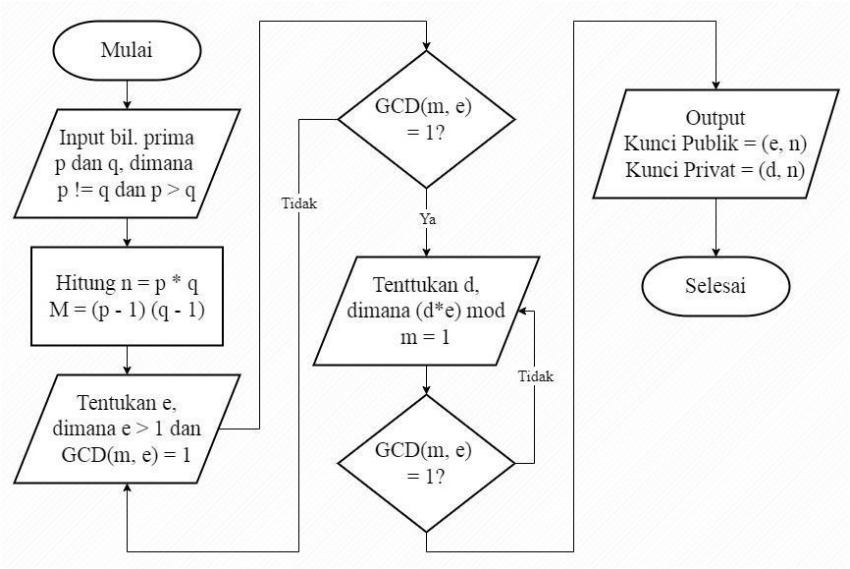
Algoritma sistem menjelaskan langkah-langkah penyelesaian suatu masalah dalam merancang sistem menggunakan algoritma RSA.

3.3.1. Algoritma RSA

Algoritma RSA memiliki beberapa tahapan yang akan dijelaskan sebagai berikut:

a. Tahap Pembangkitan Kunci

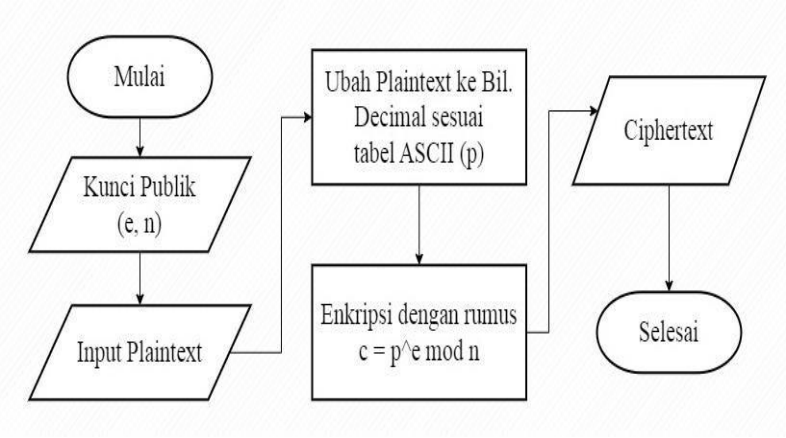
Pada tahap ini akan dihasilkan sepasang kunci, yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk proses enkripsi sementara kunci publik untuk proses dekripsi. Berikut adalah *flowchart* pembangkitan kunci.



Gambar 3.2 *Flowchart* Pembangkitan Kunci

b. Enkripsi

Proses enkripsi merupakan proses untuk mengubah informasi atau data menjadi bentuk yang tidak dapat dibaca atau dimengerti tanpa kunci atau metode khusus. Berikut adalah *flowchart* enkripsi pada algoritma RSA.



Gambar 3.3 *Flowchart* Enkripsi

3.3.2. Perhitungan Algoritma RSA

a. Tahap Pembangkitan Kunci RSA

Algoritma RSA memiliki dua buah kunci yaitu public key dan private key. Berikut adalah langkah langkah dalam proses pembangkitan kunci RSA.

1. Pilih dua buah bilangan prima p dan q. $p \neq q$

   Missal, $p = 11$, dan $q = 7$

2. Hitung $n = p * q$

   $n = 11 * 7$

   $n = 77$

3. Hitung $m = (p - 1)(q - 1)$

$m = (11 - 1)(7 - 1)$

   $m = (10)(6)$

$m = 60$

4. Pilih nilai e dengan syarat $e > 1$ dan $GCD(m, e) = 1$

   Nilai e yang diambil adalah 17

   Bukti : $(60, 17)$

   $60\ mod\ 17 = 9$

   $17\ mod\ 9 = 8$

   $9\ mod\ 8 = 1$

5. Hitung d dengan persamaan $(d * e)\ mod\ m = 1$

   $d * 17\ mod\ 60 = 1$

   $d = 53$

   Bukti : $53 * 17\ mod\ 60 = 1$

   Sehingga pasangan kunci yang didapatkan adalah

   Kunci enkripsi $(public\ key)(e, n) = (17, 77)$ dan

   Kunci dekripsi $(private\ key)(d, n) = (53, 77)$

b. Tahap Enkripsi

Pada tahap ini informasi atau data diubah menjadi bentuk yang tidak dapat dibaca atau dimengerti oleh orang yang tidak memiliki kunci. Sebagai contoh pesan yang akan dienkripsi adalah HAI. Sebelum melakukan enkripsi, pesan tersebut diubah terlebih dahulu menjadi bilangan decimal berdasarkan table ASCII.

Table 3.1 Karakter untuk dienkripsi

Pi	*Plaintext*	*Decimal*
1	H	72
2	A	65
3	I	73

Kemudian enkripsi dengan rumus $C_i = {P_i}^e \ mod\ n$. Dengan kunci enkripsi $(e, n) = (17, 77)$.

Plaintext 1 (P_1) :

$P_1 = 72$

$C_1 = 72^{17} \ mod\ 77$

Sederhanakan perpangkatan,

$72^1 \ mod\ 77 = 72$

$72^2 \ mod\ 77 = (72 * 72) \ mod\ 77 = 25$

$72^4 \ mod\ 77 = (25 * 25) \ mod\ 77 = 9$

$72^8 \ mod\ 77 = (9 * 9) \ mod\ 77 = 4$

$72^{16} \ mod\ 77 = (4 * 4) \ mod\ 77 = 16$

Sehingga,

$C_1 = 72^{16+1} \ mod\ 77$

$C_1 = (72^{16} * 72^1) \ mod\ 77$

$C_1 = (16 * 72) \ mod\ 77$

$C_1 = 74$

Plaintext 2 (P_2) :

$P_2 = 65$

$C_2 = 65^{17} \ mod\ 77$

$C_2 = 32$

Plaintext 3 (P_3) :

$P_3 = 73$

$C_3 = 73^{17} \ mod\ 77$

$C_3 = 61$

Berikut adalah tabel hasil enkripsi (*ciphertext*) dengan algoritma RSA.

Tabel 3.2 Hasil Enkripsi

Plaintext	*Decimal*	*Encrypt*
H	72	74
A	65	32
I	73	61

c. Tahap Dekripsi

Tahap dekripsi adalah langkah untuk mengubah data atau informasi yang telah dienkripsi kembali ke bentuk asalnya sehingga teks dapat dibaca dan dimengerti.

Tabel 3.3 Karakter untuk didekripsi

Ci	*Decimal*
1	74
2	32
3	61

Dekripsi dengan rumus $P_i = {C_i}^d \ mod \ n$. Dengan kunci dekripsi $(d, n) = (53, 77)$.

Ciphertext 1 (C_1) :

$C_1 = 74$

$P_1 = 74^{53} \ mod \ 77$

Sederhanakan perpangkatan,

$74^1 \ mod \ 77 = 74$

$74^2 \ mod \ 77 = (74 * 74) \ mod \ 77 = 9$

$74^4 \ mod \ 77 = (25 * 25) \ mod \ 77 = 4$

$74^8 \ mod \ 77 = (4 * 4) \ mod \ 77 = 16$

$74^{16} \ mod \ 77 = (16 * 16) \ mod \ 77 = 25$

$74^{32}\ mod\ 77 = (25 * 25)\ mod\ 77 = 9$

Sehingga,

$P_1 = 74^{32+16+4+1}\ mod\ 77$

$P_1 = (74^{32} * 74^{16} * 74^{4} * 74^{1})\ mod\ 77$

$P_1 = (9 * 25 * 4 * 74)\ mod\ 77$

$P_1 = \big(((9 * 25)\ mod\ 77) * ((4 * 74)\ mod\ 77)\big)\ mod\ 77$

$P_1 = (71 * 65)\ mod\ 77$

$P_1 = 72$

Ciphertext 2 (C_2) :

$C_2 = 32$

$P_2 = 32^{53}\ mod\ 77$

$P_2 = 65$

Ciphertext 3 (C_3) :

$C_3 = 61$

$P_3 = 61^{53}\ mod\ 77$

$P_3 = 73$

Setelah didekripsi, hasilnya dikonversi Kembali kedalam karakter berdasarkan tabel ASCII untuk mengetahui pesan aslinya.

Tabel 3.4 Hasil Dekripsi

Ciphertext	*Decrypt*	*Plaintext*
74	72	H
32	65	A
61	73	I

3.3.3. Generate QR Code

Dalam penelitian ini, QR Code dimanfaatkan sebagai media untuk

menyimpan tanda tangan digital hasil enkripsi data ijazah menggunakan algoritma RSA. QR Code dipilih karena memiliki kemampuan menyimpan data dalam jumlah cukup besar, tahan terhadap kerusakan sebagian, serta dapat diakses dengan cepat melalui pemindaian menggunakan perangkat digital. Penggunaan QR Code juga mendukung sistem verifikasi dokumen secara otomatis, aman, dan efisien. Adapun tahapan generate QR Code dalam penelitian ini dijelaskan sebagai berikut:

a. Enkripsi Data

   Langkah pertama adalah melakukan enkripsi terhadap data penting pada ijazah, seperti nama siswa, nomor induk, program studi, dan tahun kelulusan, menggunakan algoritma RSA. Proses ini dilakukan dengan menggunakan kunci privat (*private key*) milik institusi penerbit ijazah. Hasil dari proses enkripsi tersebut berupa tanda tangan digital (*digital signature*), yang menjamin integritas dan keaslian data. Tanda tangan digital ini bersifat unik untuk setiap ijazah karena bergantung pada isi data dan kunci privat yang digunakan.

b. Pembangkitan *QR Code*

   Setelah tanda tangan digital diperoleh, tanda tangan digital yang dihasilkan akan disimpan didalam *QR Code* yang dibangkitkan melalui API (*Application Programming Interface*) yang dapat membangkitkan *QR Code*. Data yang dimasukkan ke dalam QR Code bisa berupa string terenkripsi secara langsung, atau dapat juga berupa URL yang mengarah ke halaman validasi yang menyimpan referensi terhadap tanda tangan digital di basis data. Penggunaan *QR Code* sebagai pembawa tanda tangan

digital membuat proses distribusi dan verifikasi data menjadi lebih praktis dan aman.

c. Penerapan QR Code

Setelah *QR Code* didapatkan, kemudian disematkan kedalam sertifikat keaslian data ijazah. Sertifikat ini sebagai bukti bahwasannya data ijazah telah dilakukan tanda tangan digital. Penyematan ini dapat dilakukan secara digital (pada ijazah berbasis PDF) maupun cetak. Dengan adanya *QR Code*, dokumen ijazah tidak hanya menjadi representasi fisik data, tetapi juga terintegrasi dengan sistem keamanan digital. Hal ini memungkinkan pihak ketiga, seperti institusi pendidikan lanjutan atau perusahaan, untuk melakukan verifikasi keaslian ijazah secara langsung dan real-time.

d. Verifikasi

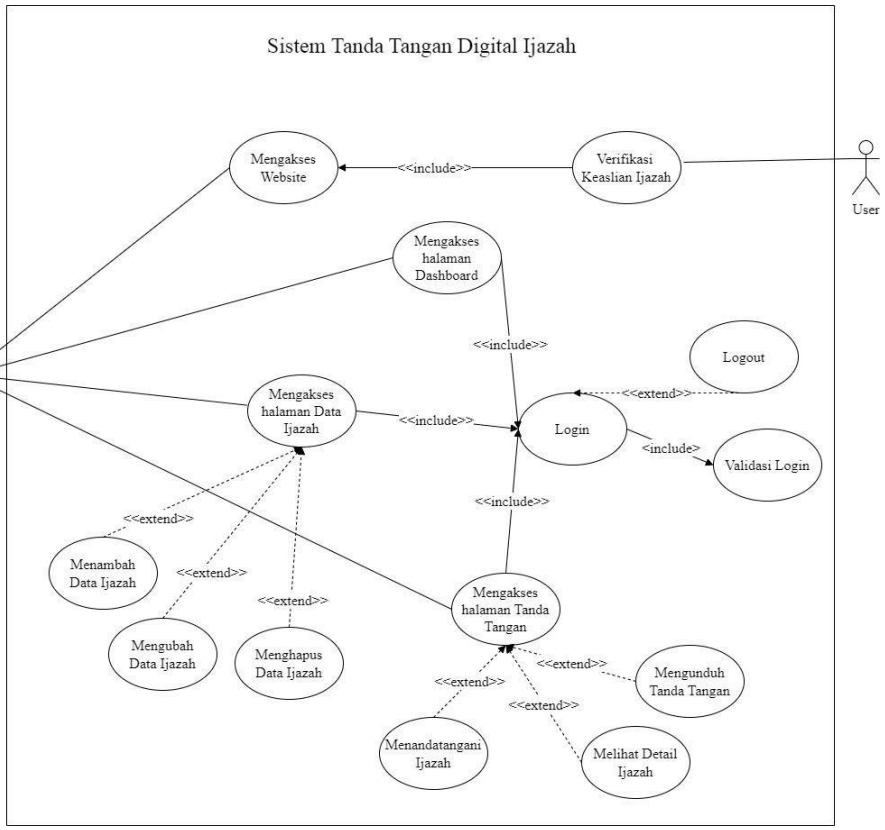
Tahap akhir adalah proses verifikasi. Pengguna atau institusi yang ingin memverifikasi ijazah cukup melakukan pemindaian *QR Code* menggunakan smartphone atau pemindai QR. Setelah dipindai, pengguna akan diarahkan ke URL sistem validasi data ijazah, di mana sistem akan menampilkan data hasil dekripsi dari tanda tangan digital, kemudian mencocokkannya dengan data ijazah yang tersimpan di basis data. Jika data yang diperoleh cocok dengan data asli, maka ijazah dinyatakan valid dan tidak mengalami pemalsuan. Proses ini memperkuat keamanan data ijazah dan mencegah penyalahgunaan dokumen.

3.4. UML

UML (*Unified Modelling Languange*) merupakan suatu bahasa pemodelan yang menggambarkan suatu sistem.

3.4.1. Use Case Diagram

Use case diagram menggambarkan berbagai *use case* yang mungkin terjadi dalam suatu sistem, serta hubungan antara aktor dan *use case* tersebut. Berikut merupakan gambaran *use case diagram* dari sistem yang akan dikembangkan.

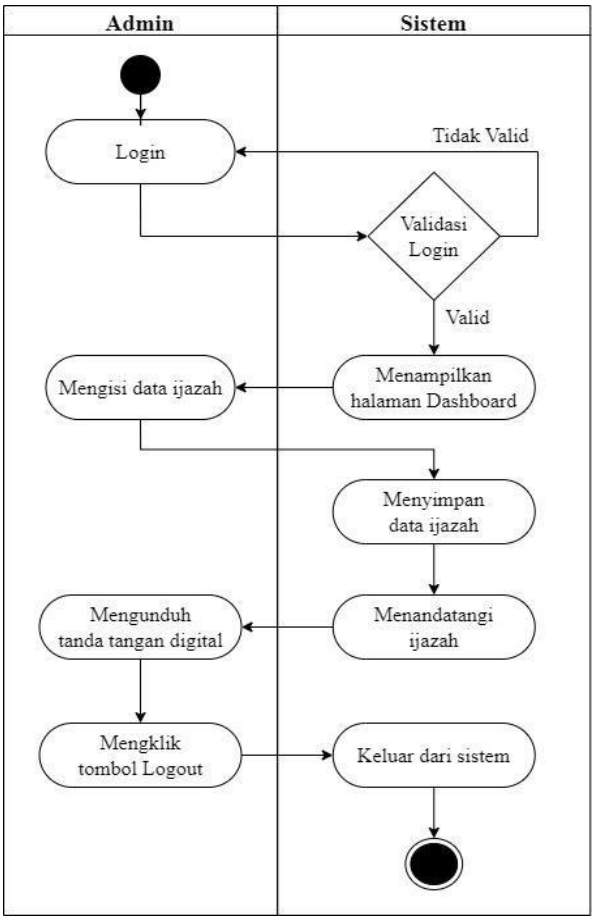


Gambar 3.4 *Use Case* Diagram

3.4.2. *Activity* Diagram

Activity diagram menggambarkan alur kerja atau aktivitas dari sistem, menunjukkan urutan langkah-langkah yang dilakukan dalam proses tertentu.

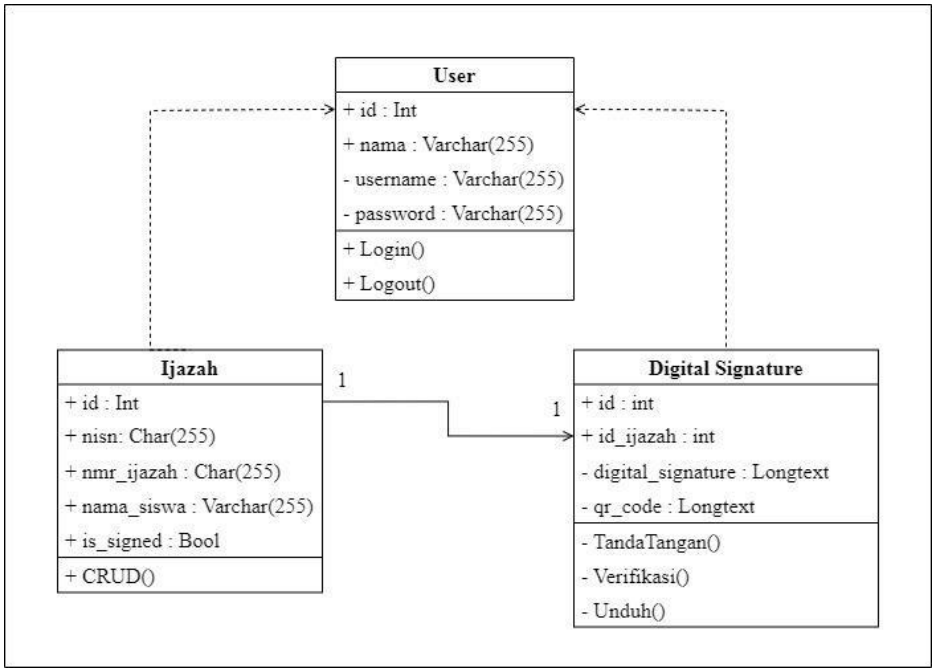
Berikut adalah gambar *activity* diagram dari sistem.



Gambar 3.5 *Activity* Diagram

3.4.3. *Class* Diagram

Class diagram adalah representasi visual yang digunakan untuk memodelkan struktur statis suatu sistem dengan menampilkan kelas, atribut, dan hubungan antar kelas. Berikut adalah gambar *class* diagramnya.



Gambar 3.6 *Class* Diagram

3.5. Rancangan Tabel

Pada sistem yang akan dikembangkan menggunakan sistem manajemen basis data MySQL. Berikut adalah rancangan tabel dalam basis data.

a. Tabel *User*

Tabel *user* digunakan untuk menyimpan data pengguna sistem.

Tabel 3.5 Tabel *User*

Nama Field	Tipe Data	Ukuran Data
id	Int	
nama	Varchar	255
username	Varchar	255
password	Varchar	255

b. Tabel Ijazah

Tabel ijazah digunakan untuk menyimpan data ijazah yang akan diterapkan tanda tangan digital.

Tabel 3.6 Tabel Ijazah

Nama Field	Tipe Data	Ukuran Data
id	Int	
nomor_ijazah	Char	255
nisn	Char	255
nama_siswa	Varchar	255
is_signed	Bool	

c. Tabel *Sign*

Tabel *sign* digunakan untuk menyimpan hasil dari proses tanda tangan digital.

Tabel 3.7 Tabel *Sign*

Nama Field	Tipe Data	Ukuran Data
id	Int	
id_ijazah	Int	
digital_signature	Longtext	
qr_code	Longtext	

3.6. Rancangan Antarmuka

Berikut merupakan rancangan tampilan antarmuka dari aplikasi yang akan dibangun.

a. Halaman Utama

Halaman utama adalah halaman yang pertama tampil saat sistem diakses.

Gambar 3.7 Halaman Utama

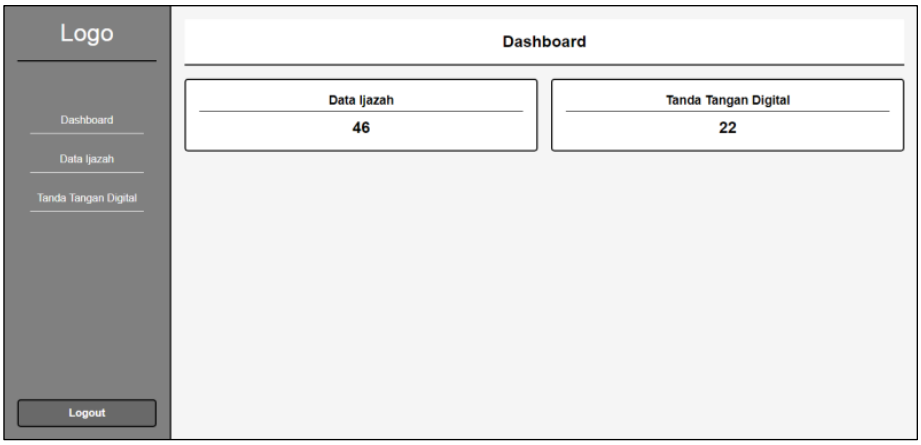
b. Halaman Login

Halaman ini berfungsi sebagai proses login *user* untuk masuk ke sistem.

Gambar 3.8 Halaman Login

c. Halaman Dashboard

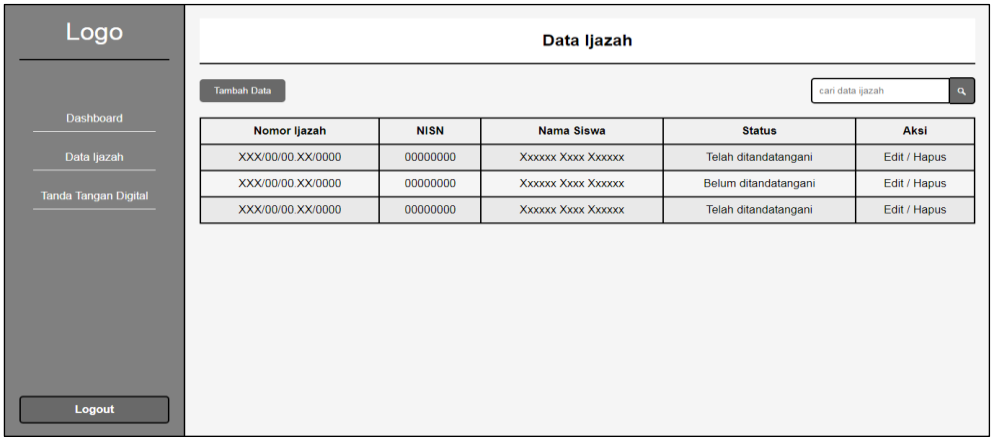
Pada halaman ini akan menampilkan informasi terkait sistem.



Gambar 3.9 Halaman Dashboard

d. Halaman Data Ijazah

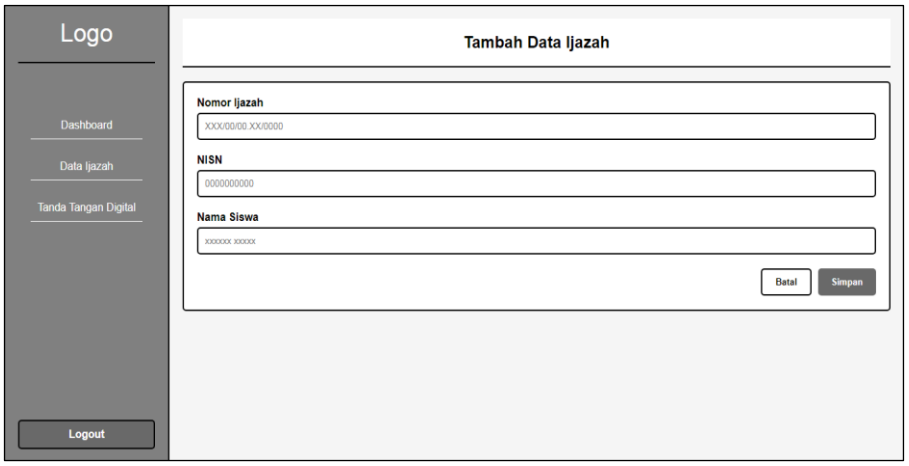
Halaman ini akan menyajikan data ijazah yang telah ditambah.



Gambar 3.10 Halaman Data Ijazah

e. Halaman Tambah Data Ijazah

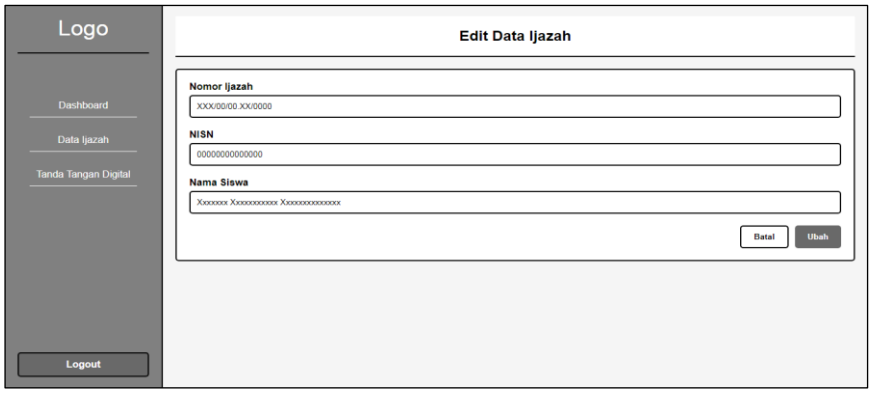
Halaman ini akan menampilkan formulir tambah data ijazah.



Gambar 3.11 Halaman Tambah Data Ijazah

f. Halaman Edit Data Ijazah

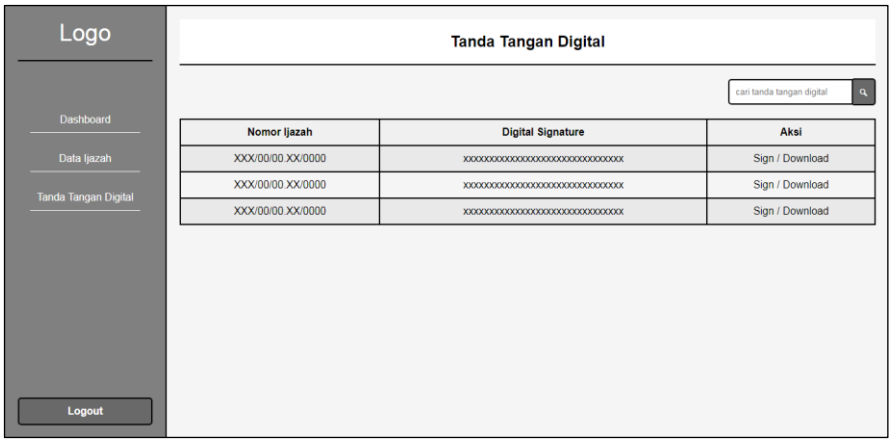
Halaman ini berfungsi untuk mengubah data ijazah.



Gambar 3.12 Halaman Edit Data Ijazah

g. Halaman Tanda Tangan Digital

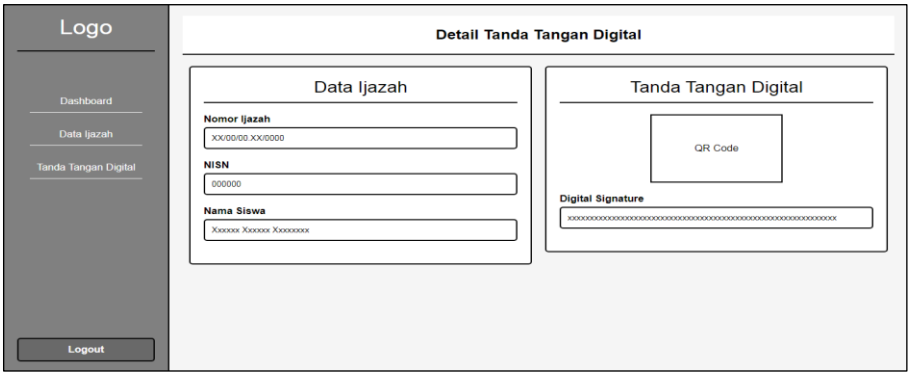
Pada halaman ini akan menampilkan data ijazah yang belum dilakukan tanda tangan digital, dan juga dapat melakukan tanda tangan serta mendownload.



Gambar 3.13 Halaman Tanda Tangan Digital

h. Halaman Detail Tanda Tangan Digital

Halaman ini akan menampilkan detail dari data ijazah yang telah dilakukan tanda tangan digital.



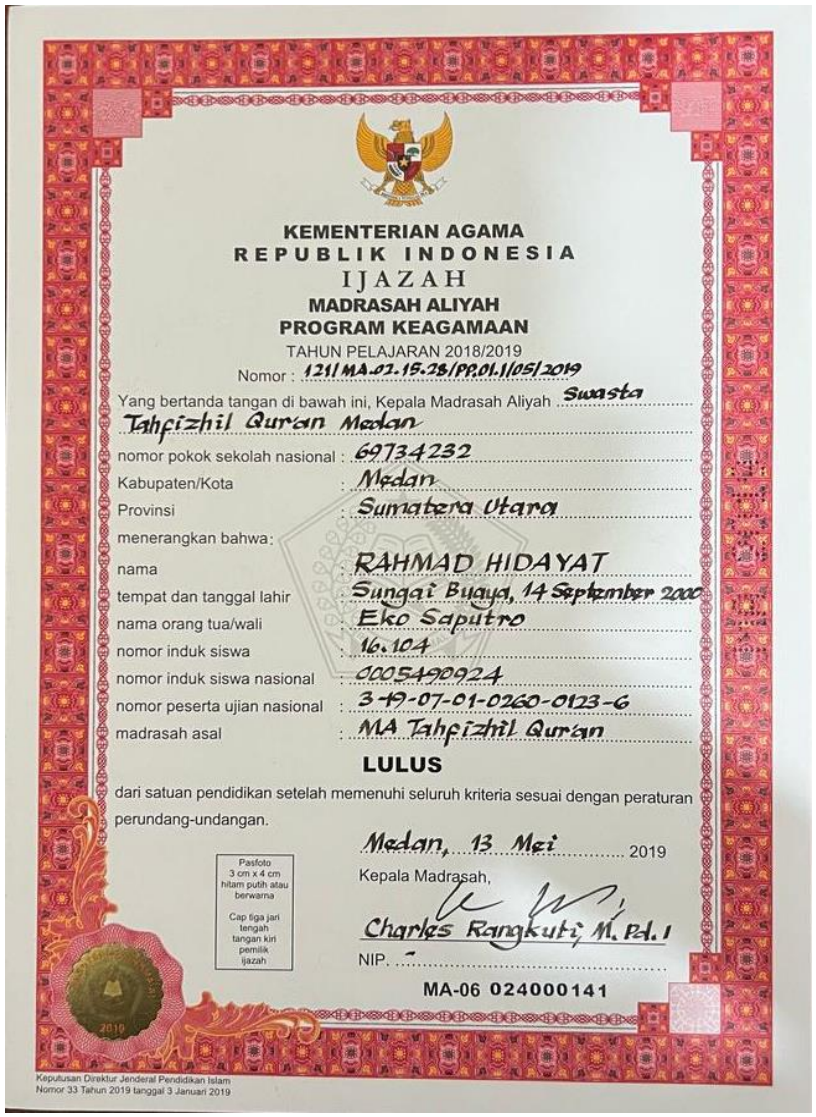
Gambar 3.14 Halaman Detail Tanda Tangan Digital

BAB IV

HASIL DAN PEMBAHASAN

4.1. Analisis Data

Dalam penelitian ini akan dilakukan pengamanan terhadap data ijazah menggunakan Algoritma RSA. Berikut merupakan sampel data yang akan diamankan.



KEMENTERIAN AGAMA
REPUBLIK INDONESIA
IJAZAH
MADRASAH ALIYAH
PROGRAM KEAGAMAAN
TAHUN PELAJARAN 2018/2019
Nomor : 121/MA.02.15.28/PP.01.1/05/2019

Yang bertanda tangan di bawah ini, Kepala Madrasah Aliyah : Swasta
Tahfizhil Quran Medan
nomor pokok sekolah nasional : 69734232
Kabupaten/Kota : Medan
Provinsi : Sumatera Utara
menerangkan bahwa:
nama : RAHMAD HIDAYAT
tempat dan tanggal lahir : Sungai Buaya, 14 September 2000
nama orang tua/wali : Eko Saputro
nomor induk siswa : 16.104
nomor induk siswa nasional : 0005499024
nomor peserta ujian nasional : 3-49-07-01-0260-0123-6
madrasah asal : MA Tahfizhil Quran

LULUS

dari satuan pendidikan setelah memenuhi seluruh kriteria sesuai dengan peraturan perundang-undangan.

Pasfoto 3 cm x 4 cm hitam putih atau berwarna
Cap tiga jari tengah tangan kiri pemilik ijazah

Medan, 13 Mei 2019
Kepala Madrasah,
Charles Rangkuti, M.Pd.I
NIP. -

MA-06 024000141

Keputusan Direktur Jenderal Pendidikan Islam
Nomor 33 Tahun 2019 tanggal 3 Januari 2019

Gambar 4.1 Sampel Ijazah

4.1.1. Penerapan Algoritma RSA

a. Pembangkitan Kunci RSA

Pembangkitan kunci akan menghasilkan dua buah kunci, yaitu kunci publik untuk mengenkripsi dan kunci privat untuk mendekripsi. Berikut pembangkitan kunci RSA.

1. Missal, $p = 23$, dan $q = 17$
2. Hitung $n = p * q$

   $n = 23 * 17$

   $n = 391$
3. Hitung $m = (p - 1)(q - 1)$

   $m = (23 - 1)(17 - 1)$

   $m = (22)(16)$

   $m = 352$
4. Pilih nilai e dengan syarat $e > 1$ dan $GCD(m, e) = 1$

   Nilai e yang diambil adalah 23

   Bukti : $(352, 23)$

   $352\ mod\ 23 = 7$

   $23\ mod\ 7 = 2$

   $7\ mod\ 2 = 1$
5. Hitung d dengan persamaan $(d * e)\ mod\ m = 1$

   $d * 23\ mod\ 352 = 1$

   $d = 199$

   Bukti : $199 * 23\ mod\ 352 = 1$

Sehingga pasangan kunci yang didapatkan adalah Kunci publik $(e, n) = (23{,}391)$ dan Kunci dekripsi $(d, n) = (199, 391)$

b. Enkripsi

Enkripsi akan mengubah informasi atau data menjadi tidak dapat dibaca jika tidak memiliki kunci untuk mendekripsi ke informasi aslinya. Pada proses enkripsi ini data yang akan dienkripsi adalah data ijazah. Sebagai contoh nama siswa dari pemilik ijazah.

Karakter yang akan dienkripsi diubah terlebih dahulu kedalam bentuk decimal sesuai dengan tabel ASCII dan dibagi menjadi blok-blok plainteks.

Tabel 4.1 Konversi Karakter ke Bilangan Desimal

Pi	Plainteks	Desimal	Pi	Plainteks	Desimal
1	R	82	8	H	72
2	A	65	9	I	73
3	H	72	10	D	68
4	M	77	11	A	65
5	A	65	12	Y	89
6	D	68	13	A	65
7		32	14	T	84

Enkripsi semua blok plainteks dengan rumus $C_i = P_i^{\,e} \; mod \; n$. Menggunakan kunci enkripsi (e, n) = (23, 391). Berikut hasil perhitungan enkripsinya.

Plainteks 1 (P_1) :

$P_1 = 82$

$C_1 = 82^{23} \; mod \; 391$

Sederhanakan perpangkatan,

$82^1 \; mod \; 391 = 82$

$82^2 \; mod \; 391 = (82 * 82) \; mod \; 391 = 77$

$82^4 \ mod \ 391 = (77 * 77) \ mod \ 391 = 64$

$82^8 \ mod \ 391 = (64 * 64) \ mod \ 391 = 186$

$82^{16} \ mod \ 391 = (186 * 186) \ mod \ 391 = 188$

Sehingga,

$C_1 = 82^{16+4+2+1} \ mod \ 391$

$C_1 = \ (82^{16} * 82^4 * 82^2 * 82^1) \ mod \ 391$

$C_1 = (188 * 64 * 77 * 82) \ mod \ 391$

$C_1 = \Big(((188 * 64) \ mod \ 391) * ((77 * 82) \ mod \ 391)\Big) \ mod \ 391$

$C_1 = (302 * 58) \ mod \ 391$

$C_1 = 312$

Plainteks 2 (P_2) :

$P_2 = 65$

$C_2 = 65^{23} \ mod \ 391$

$C_2 = 295$

Plainteks 3 (P_3) :

$P_3 = 72$

$C_3 = 72^{23} \ mod \ 391$

$C_3 = 302$

Plainteks 4 (P_4) :

$P_4 = 77$

$C_4 = 77^{23} \ mod \ 391$

$C_4 = 376$

Plainteks 5 (P_5) :

$P_5 = 65$

$C_5 = 65^{23}\ mod\ 391$

$C_5 = 295$

Plainteks 6 (P_6) :

$P_6 = 68$

$C_6 = 68^{23}\ mod\ 391$

$C_6 = 68$

Plainteks 7 (P_7) :

$P_7 = 32$

$C_7 = 32^{23}\ mod\ 391$

$C_7 = 331$

Plainteks 8 (P_8) :

$P_8 = 72$

$C_8 = 72^{23}\ mod\ 391$

$C_8 = 302$

Plainteks 9 (P_9) :

$P_9 = 73$

$C_9 = 73^{23}\ mod\ 391$

$C_9 = 27$

Plainteks 10 (P_{10}) :

$P_{10} = 68$

$C_{10} = 68^{23}\ mod\ 391$

$C_{10} = 68$

Plainteks 11 (P_{11}) :

$P_{11} = 65$

$C_{11} = 65^{23}\ mod\ 391$

$C_{11} = 295$

Plainteks 12 (P_{12}) :

$P_{12} = 89$

$C_{12} = 89^{23}\ mod\ 391$

$C_{12} = 319$

Plainteks 13 (P_{13}) :

$P_{13} = 65$

$C_{13} = 65^{23}\ mod\ 391$

$C_{13} = 295$

Plainteks 14 (P_{14}) :

$P_{14} = 84$

$C_{14} = 84^{23}\ mod\ 391$

$C_{14} = 84$

Setelah hasil enkripsi sudah didapat kemudian dikonversi ke heksadesimal untuk dijadikan tandatangan digital.

Tabel 4.2 Hasil Enkripsi

Desimal (plainteks)	Enkrip	Heksadesimal	Desimal (plainteks)	Enkrip	Heksadesimal
82	312	138	72	302	178
65	295	127	73	27	1B
72	302	12E	68	68	44
77	376	178	65	295	127
65	295	127	89	319	13F
68	68	44	65	295	127
32	331	14B	84	84	54

c. Dekripsi

Dekripsi adalah cara merubah informasi yang telah dienkripsi menjadi kebentuk awalnya yang dapat dibaca dan dimengerti.

Karakter yang akan didekripsi diubah terlebih dahulu kedalam bentuk decimal sesuai dengan tabel ASCII dan dibagi menjadi blok-blok ciperteks.

Tabel 4.3 Konversi Karakter Heksa ke Bilangan Desimal

Ci	Heksa	Desimal	Ci	Heksa	Desimal
1	138	312	8	178	302
2	127	295	9	1B	27
3	12E	302	10	44	68
4	178	376	11	127	295
5	127	295	12	13F	319
6	44	68	13	127	295
7	14B	331	14	54	84

Dekripsi semua blok plainteks dengan rumus $P_i = {C_i}^d \ mod\ n$. Menggunakan kunci dekripsi (d, n) = (199, 391). Berikut hasil perhitungan dekripsinya.

Ciperteks 1 (C_1) :

$C_1 = 312$

$P_1 = 312^{199}\ mod\ 391$

Sederhanakan perpangkatan,

$312^1\ mod\ 391 = 312$

$312^2\ mod\ 391 = (312 * 312)\ mod\ 391 = 376$

$312^3\ mod\ 391 = (376 * 312)\ mod\ 391 = 12$

$312^4\ mod\ 391 = (376 * 376)\ mod\ 391 = 225$

$312^8\ mod\ 391 = (225 * 225)\ mod\ 391 = 186$

$312^{16}\ mod\ 391 = (186 * 186)\ mod\ 391 = 188$

$312^{32}\ mod\ 391 = (188 * 188)\ mod\ 391 = 154$

$312^{64}\ mod\ 391 = (154 * 154)\ mod\ 391 = 256$

$312^{128}\ mod\ 391 = (256 * 256)\ mod\ 391 = 239$

Sehingga,

$P_1 = 312^{128+64+4+3}\ mod\ 391$

$P_1 = \ (312^{128} * 312^{64} * 312^{4} * 312^{3})\ mod\ 391$

$P_1 = (239 * 256 * 225 * 12)\ mod\ 391$

$P_1 = \Big(((239 * 256)\ mod\ 391) * \big((225 * 12)\ mod\ 391\big)\Big)\ mod\ 391$

$P_1 = (188 * 354)\ mod\ 391$

$P_1 = 82$

Ciperteks 2 (C_2) :

$P_2 = 295$

$P_2 = 295^{199}\ mod\ 391$

$P_2 = 65$

Ciperteks 3 (C_3) :

$P_3 = 302$

$P_3 = 302^{199}\ mod\ 391$

$P_3 = 72$

Ciperteks 4 (C_4) :

$P_4 = 376$

$P_4 = 376^{199}\ mod\ 391$

$P_4 = 77$

Ciperteks 5 (C_5) :

$P_5 = 295$

$P_5 = 295^{199}\ mod\ 391$

$P_5 = 65$

Ciperteks 6 (C_6) :

$P_6 = 68$

$P_6 = 68^{199}\ mod\ 391$

$P_6 = 68$

Ciperteks 7 (C_7) :

$P_7 = 331$

$P_7 = 331^{199}\ mod\ 391$

$P_7 = 32$

Ciperteks 8 (C_8) :

$P_8 = 302$

$P_8 = 302^{199}\ mod\ 391$

$P_8 = 72$

Ciperteks 9 (C_9) :

$P_9 = 27$

$P_9 = 27^{199}\ mod\ 391$

$P_9 = 73$

Ciperteks 10 (C_{10}) :

$P_{10} = 68$

$P_{10} = 68^{199}\ mod\ 391$

$P_{10} = 68$

Ciperteks 11 (C_{11}) :

$P_{11} = 295$

$P_{11} = 295^{199}\ mod\ 391$

$P_{11} = 65$

Ciperteks 12 (C_{12}) :

$P_{12} = 319$

$P_{12} = 319^{199}\ mod\ 391$

$P_{12} = 89$

Ciperteks 13 (C_{13}) :

$P_{13} = 295$

$P_{13} = 295^{199}\ mod\ 391$

$P_{13} = 65$

Ciperteks 14 (C_{14}) :

$P_{14} = 84$

$P_{14} = 84^{199}\ mod\ 391$

$P_{14} = 84$

Setelah dilakukan dekripsi, hasil dekripsi diubah kedalam Karakter berdasarkan tabel ASCII untuk mendapatkan pesan aslinya. Berikut adalah tabel hasil dekripsi.

Tabel 4.4 Hasil Dekripsi

Desimal (ciperteks)	Dekrip	Karakter	Desimal (ciperteks)	Dekrip	Karakter
312	82	R	302	72	H
295	65	A	27	73	I
302	72	H	68	68	D
376	77	M	295	65	A
295	65	A	319	89	Y
68	68	D	295	65	A
331	32		84	84	T

4.1.2. Generate QR Code

QR Code digunakan untuk menyimpan tanda tangan digital yang dihasilkan dari proses enkripsi sebelumnya, sehingga dapat mempermudah penyimpanan informasi dan pemindaiannya. Maka hasil generate qr code dari tanda tangan digital sebelumnya adalah sebagai berikut.

Gambar 4.2 QR Code Tanda Tangan Digital

4.2. Tampilan Halaman WEB

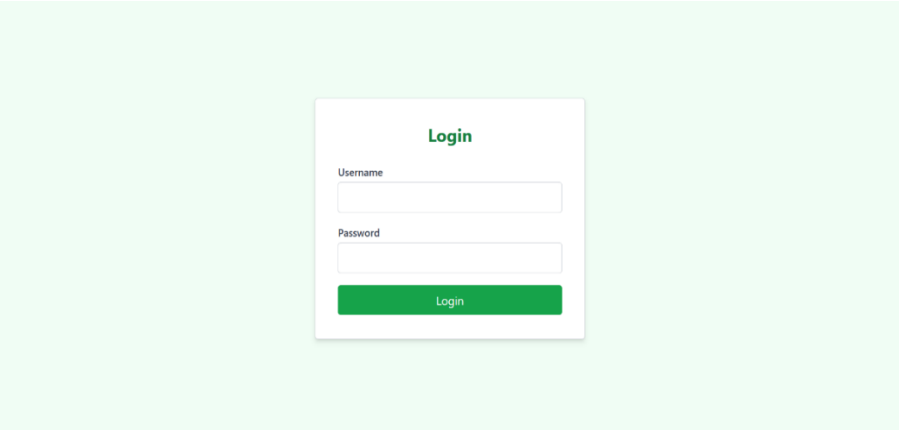
1. Halaman Utama

   Halaman Utama merupakan halaman yang akan pertama kali tampil saat aplikasi dijalankan.

Gambar 4.3 Tampilan Halaman Utama

2. Halaman Login

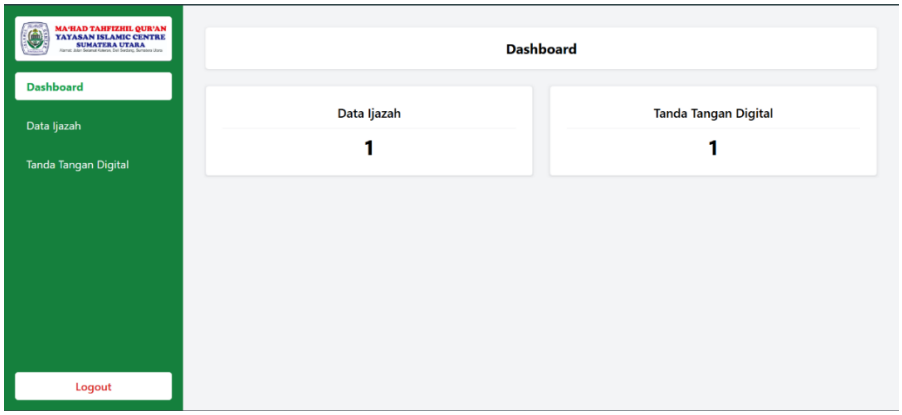
Halaman Login akan menampilkan form login untuk mengautentikasi pengguna yang akan menggunakan system.



Gambar 4.4 Tampilan Halaman Login

3. Halaman Dashboard

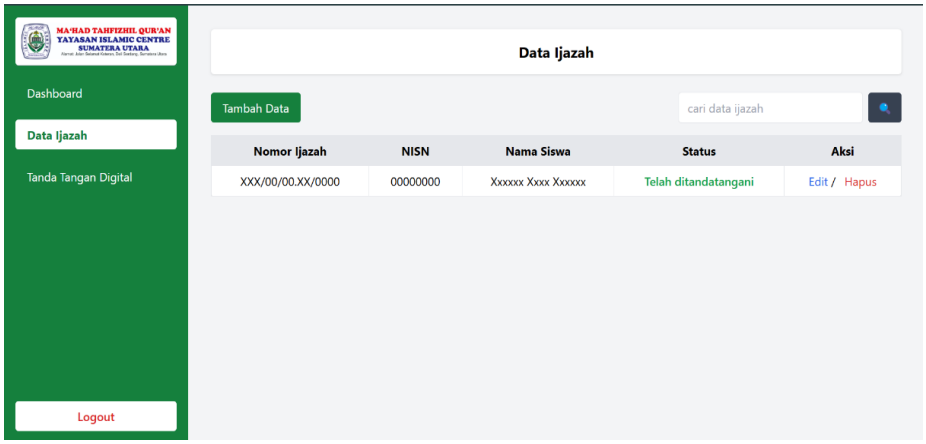
Halaman Dashboard akan tampil Ketika pengguna berhasil login. Halaman ini akan menyajikan informasi penting terkait sistem.



Gambar 4.5 Tampilan Halaman Dashboard

4. Halaman Data Ijazah

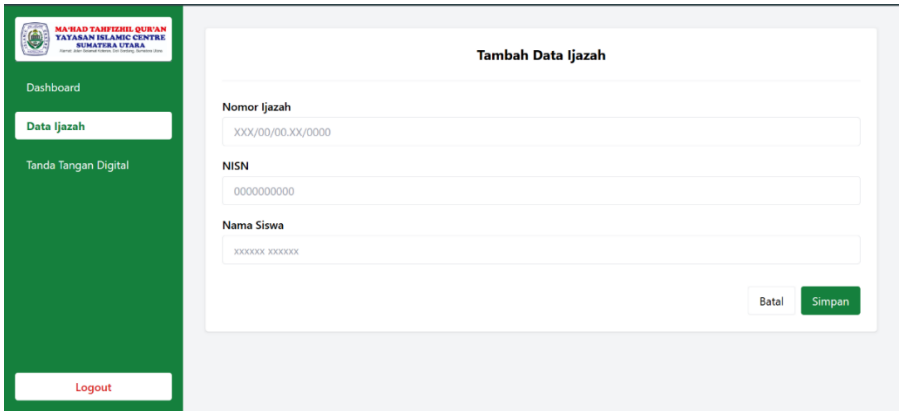
Halaman Ijazah akan menampilkan seluruh data ijazah yang diambil dari database dan disajikan dalam bentuk tabel.



Gambar 4.6 Tampilan Halaman Data Ijazah

5. Halaman Tambah Data Ijazah

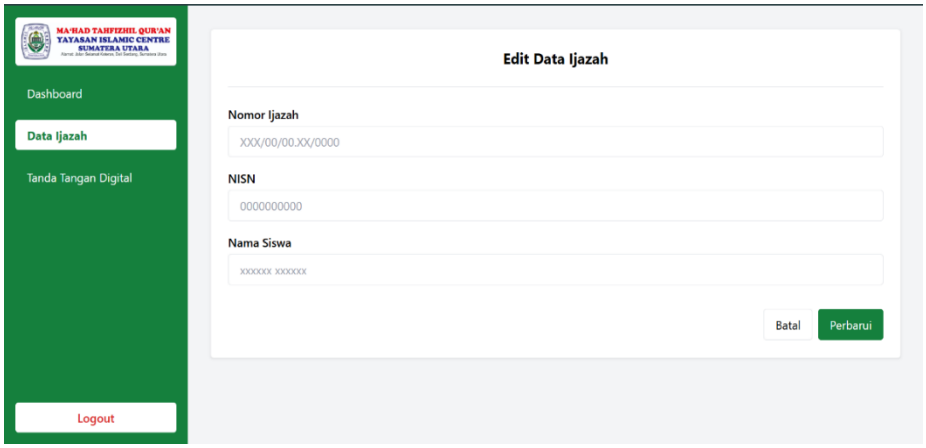
Halaman Tambah Data Ijazah merupakan halaman yang menampilkan form untuk menambah data ijazah.



Gambar 4.7 Tampilan Halaman Tambah Data Ijazah

6. Halaman Edit Data Ijazah

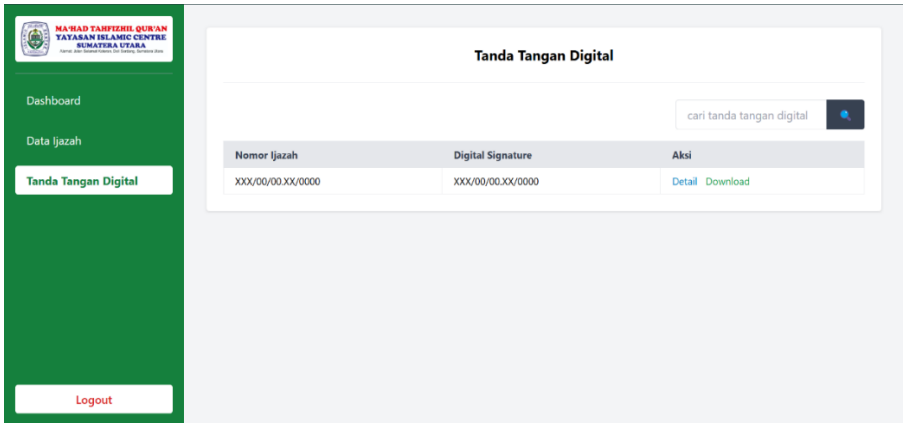
Halaman Edit Data Ijazah akan menampilkan form untuk mengubah data ijazah jika terjadi kesalahan data ijazah.



Gambar 4.8 Tampilan Halaman Edit Data Ijazah

7. Halaman Tanda Tangan Digital

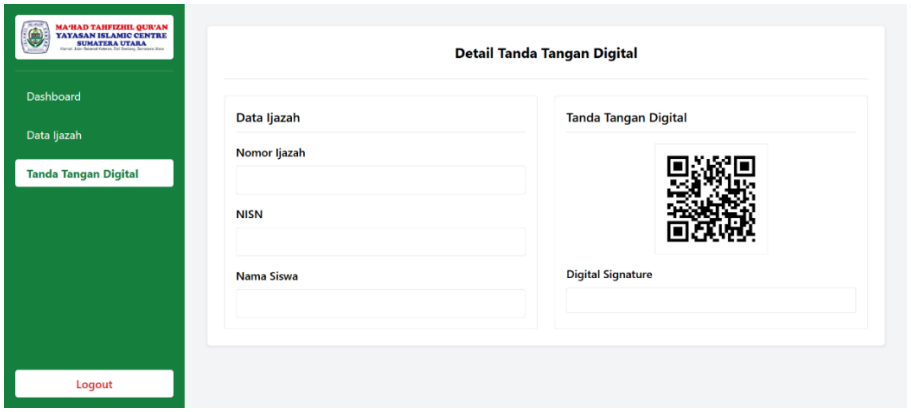
Halaman Tanda Tangan Digital akan menampilkan seluruh data ijazah yang sudah dilakukan tanda tangan digital.



Gambar 4.9 Tampilan Halaman Tanda Tangan Digital

8. Halaman Detail Tanda Tangan Digital

Halaman Detail Tanda Tangan Digital akan menampilkan detail dari tanda tangan digital, mulai dari data asli ijazah, digital signature dan juga qr code dari tanda tangan digital.



Gambar 4.10 Tampilan Halaman Detail Tanda Tangan Digital

9. Laporan

Berikut adalah gambar dari bentuk laporan hasil data ijazah yang sudah dilakukan tanda tangan digital.

Laporan Tanda Tangan Digital Data Ijazah

Nomor Ijazah : YICSU/IJAZAH/MA-2017/0218
Nama Siswa : Muhammad Rizky Ananda Rangkuti
NISN : 120901212
Tanda Tangan Digital : 0xbf6a7d25ae

Kode QR

Gambar 4.11 Tampilan Laporan Tanda Tangan Digital

BAB V

PENUTUP

5.1. Kesimpulan

Penelitian ini dilakukan untuk merancang dan mengimplementasikan sistem pengamanan data ijazah berbasis QR Code dengan menggunakan algoritma RSA di Yayasan Islamic Centre Sumut. Berdasarkan hasil yang diperoleh, dapat disimpulkan bahwa sistem yang dibangun mampu memberikan solusi atas permasalahan pemalsuan ijazah. Dengan menggunakan metode kriptografi RSA, informasi penting dalam ijazah dienkripsi sehingga hanya dapat diakses oleh pihak yang memiliki kunci dekripsi yang sesuai. Hal ini memberikan jaminan keaslian serta keamanan data ijazah.

Penerapan QR Code sebagai media penyimpanan tanda tangan digital juga terbukti efektif dalam mempermudah proses verifikasi dokumen. Cukup dengan memindai QR Code, pengguna dapat mengakses halaman validasi yang berisi data asli dari ijazah tersebut. Hasil enkripsi dan dekripsi yang konsisten menunjukkan bahwa sistem ini berjalan dengan baik dan akurat. Dengan demikian, sistem yang dikembangkan telah memenuhi tujuan utama penelitian, yaitu memberikan solusi praktis dan aman terhadap pengamanan dokumen ijazah secara digital.

5.2. Saran

Meskipun sistem yang dibangun telah berjalan sesuai dengan harapan, ada beberapa hal yang dapat menjadi saran untuk pengembangan lebih lanjut. Pertama, sistem ini sebaiknya tidak hanya digunakan pada jenjang Madrasah Aliyah saja, melainkan bisa diperluas ke seluruh unit pendidikan di bawah naungan Yayasan Islamic Centre Sumut agar manfaatnya lebih merata. Kedua,

perlu dilakukan peningkatan pada sisi keamanan sistem, seperti penambahan fitur autentikasi ganda (two-factor authentication) serta pencatatan log aktivitas pengguna.

Selanjutnya, penting juga untuk melakukan pengujian sistem terhadap berbagai potensi serangan siber guna memastikan ketahanan dan keamanannya dalam jangka panjang, pelatihan bagi staf atau operator yang akan menggunakan sistem juga sangat disarankan agar implementasi sistem dapat dilakukan secara maksimal dan sesuai dengan prosedur yang telah ditetapkan.

Terakhir, bahwasanya aplikasi yang di rancang belum terverifikasi oleh BSE (Balai Sertifikasi Elektronik), sehingga harapan kedepannya program yang di rancang dapat di kombinasikan dengan sistem sertifikasi surat elektronik.

DAFTAR PUSTAKA

Sukardi, E., Pasaribu, D., & Kaliye, V. X. (2021). *Penahanan ijazah pekerja oleh pemberi kerja dalam perspektif teori keadilan bermartabat*. Fakultas Hukum, Universitas Pelita Harapan.

Sinabutar, K. N. (2022). *Perancangan sistem informasi pengarsipan ijazah menggunakan metode Waterfall pada SMK Swasta Teladan Pematangsiantar* (Skripsi, Universitas HKBP Nommensen). Universitas HKBP Nommensen Repository.

Nugroho, Y. (2022). TINDAK PIDANA TERHADAP PENGGUNAAN IJAZAH PALSU. *MIMBAR INTEGRITAS : Jurnal Pengabdian, 1*(2), 168-177. doi:10.36841/mimbarintegritas.v1i2.2071.

Rizki, M., & Farida Ariyani, P. (2021). PENERAPAN KRIPTOGRAFI DENGAN MENGGUNAKAN ALGORITMA RSA UNTUK PENGAMANAN DATA BERBASIS DESKTOP PADA PT TRIAS MITRA JAYA MANUNGGAL. *SKANIKA: Sistem Komputer Dan Teknik Informatika*, *4*(2), 77–82.

Sari, Maya, et al. "Review : Cryptographic Algorithm for SMS Security System on Android." *Journal of Information Technology*, vol. 2, no. 1, 2022, pp. 11-15, doi:10.46229/jifotech.v2i1.292.

Ulfah Indriani, Ommi Alfina, & Nita Syahputri. (2022). Penerapan Algoritma RSA Dalam Keamanan File Ms Word . *Journal of Machine Learning and Data Analytics*, *1*(2), 95-100.

Rahayu, A. ., Putri Ardana, A. ., Pramudhita , C. ., Syafitri, D. ., & Zabitha Sirega, R. . (2024). Perbandingan Algoritma RSA dengan Algoritma Blowfish Pada Perancangan Aplikasi Keamanan Data. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, *7*(1), 203-207.

Vasi Waruwu, E., Sonata, F., & Zulkarnain, I. (2020). J-SISKO TECH Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD PENERAPAN DIGITAL SIGNATURE MENGGUNAKAN METODE RSA UNTUK MENVALIDASI KEASLIAN IJAZAH SMA SWASTA BINA ARTHA. *45*(2), 45–55. ,

Rangkuti, A. Z. F., & Fahmi, H. (2020). Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5. Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI), 3(2), 170– 175.

Hidayat, M. ., Tahir, M. ., Sukriyadi , A. ., Sulton , A., A, C. A. S., & F, . S. A. . (2023). PENERAPAN KRIPTOGRAFI CAESAR CHIPER DALAM PENGAMANAN DATA. *Jurnal Ilmiah Multidisiplin*, *2*(03), 35–41.

Ziliwu, K. B., Maslan, A., & Kremer, H. (2022). IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN. *Computer and Science Industrial Engineering (COMASIE)*, *7*(2), 117–126.

Utomo, N. P., & Haryanti, T. (2024). Requirement Engineering Sistem Kriptografi RSA Pada GMail. *Computing Insight : Journal of Computer Science*, *4*(2), 40–46. https://doi.org/10.30651/comp_insight.v4i2.21735.

Syahputra, A. (2021). Implementasi Algoritma Freivlds Untuk Pembangkitan Kunci Algoritma RSA Pada Pengamanan Data Video. *vol*, *10*, 70-77.

Putra, A. C., Simanjuntak, M., & Nurhayati, N. (2021). PENERAPAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) UNTUK MENGAMANKAN DATABASE PROGRAM KELUARGA HARAPAN (PKH). *JTIK (Jurnal Teknik Informatika Kaputama)*, *5*(1), 76–84. https://doi.org/10.59697/jtik.v5i1.588.

Putra, D. W. T., & Andriani, R. (2019). Unified modelling language (uml) dalam perancangan sistem informasi permohonan pembayaran restitusi sppd. *Jurnal Teknoif Teknik Informatika Institut Teknologi Padang*, *7*(1), 32-39.

Christian, C., Sitorus, S. H., & Nirmala, I. (2023). Implementasi Algoritma RSA Dan One Time Password (OTP) Untuk Pengamanan Data Pengguna dan Proses Transaksi pada Website E-Commerce. *Coding Jurnal Komputer dan Aplikasi*, *11*(1), 62-72.

Ismail, M., Syam, A. G., & Masnur, M. (2021). Aplikasi Qr Code Sebagai Sarana Penyampaian Informasi Pohon Dikebun Raya Jompie Informasi Artikel. *J. Sintaks Log*, *1*(1), 2775-412.

Huo, L., Zhu, J., Singh, P. K., & Pavlovich, P. A. (2021). Research on QR image code recognition system based on artificial intelligence algorithm. *Journal of Intelligent Systems*, *30*(1), 855-867.

Suharni, E. S., & Pakusadewa, F. (2023). Perancangan Website Rumah Makan Ninik Sebagai Media Promosi Menggunakan Unified Modelling Language. *Rekayasa Inf*, *12*(1), 1-12.

Ulfah, J., & Nurdin, N. (2023). Implementasi Metode Deteksi Tepi Canny Untuk Menghitung Jumlah Uang Koin Dalam Gambar Menggunakan Opencv. *Jurnal Informatika dan Teknik Elektro Terapan*, *11*(3).

Kesuma Astuti, F., & Sri Agustina, D. (2022). Membangun Website MTS Negeri 01 OKU Timur Menggunakan Php dan Mysql. *JIK : Jurnal Informatika Dan Komputer* , *13*(1), 7-14.

Alfarizi, S., Mulyawan, A. R., Gunawan, D., & Aryanti, R. (2020). Implementasi Unified Modelling Language Pada Sistem Informasi Nasgor Delivery Berbasis Web. *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, *15*(2), 84–93. https://doi.org/10.35969/interkom.v15i2.71.

Safira, Y. B., & Purtiningrum, S. W. (2023). Sistem Pendukung Keputusan Penilaian Ketidakdisiplinan Siswa Menggunakan Metode SAW Berbasis Web (Studi Kasus: MA Al-Muddatsiriyah). *IKRA-ITH Informatika: Jurnal Komputer dan Informatika*, *7*(1).

Santoso, G. B., Sinaga, T. M., & Zuhdi, A. (2021). MVC Implementation In Laravel Framework For Development Web-Based E-Commerce Applications. Intelmatics, 1(1).

Agustian, F., & Yuliana, A. (2024). APLIKASI CHATBOT PELAYANAN PUBLIK BERBASIS WEBSITE (STUDI KASUS SEKRETARIAT DPRD KOTA CIMAHI). *Jurnal Informatika dan Teknik Elektro Terapan*, *12*(3S1).

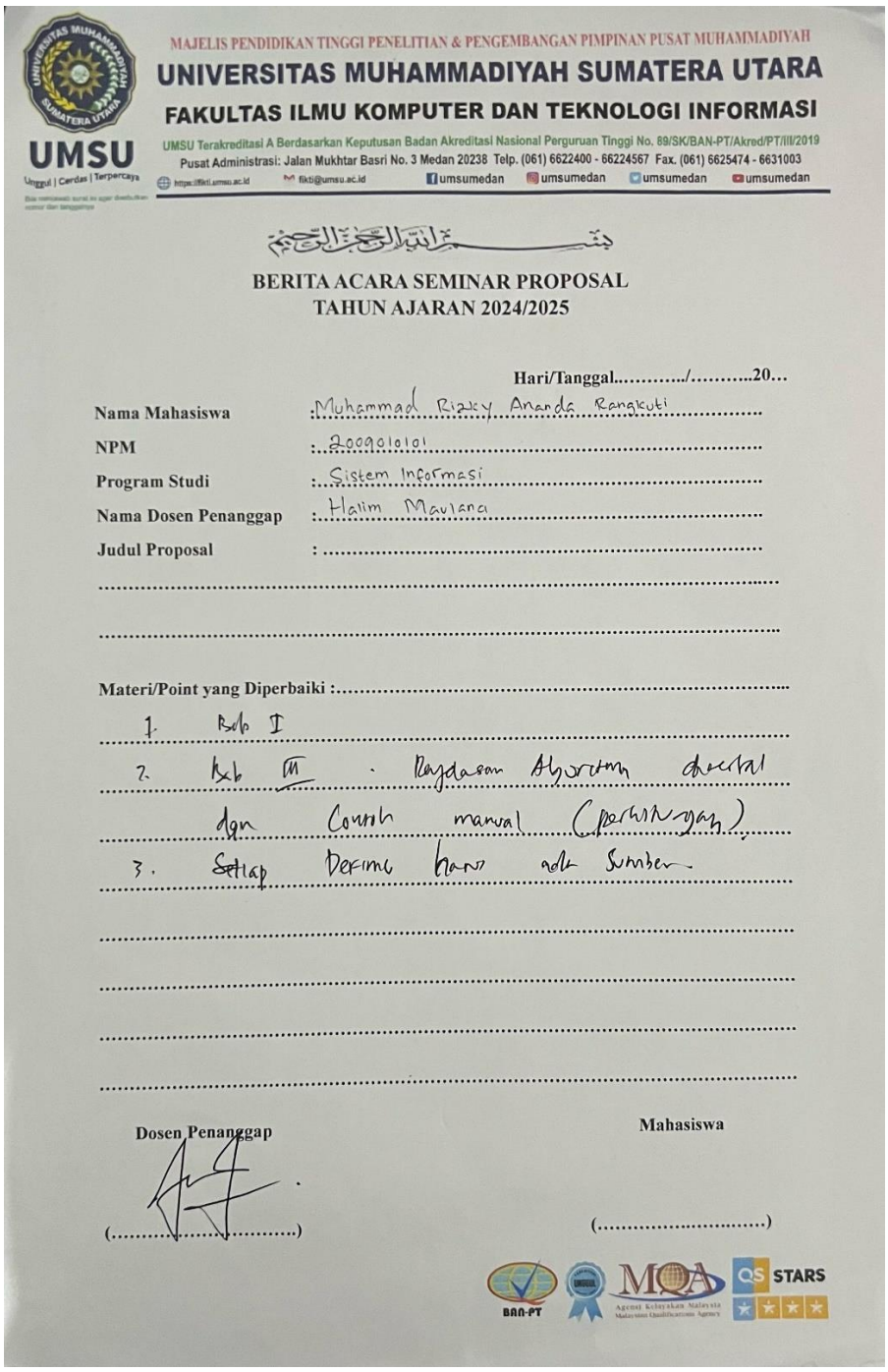
Mangadi, E. P., Mirfan, M., & Rismayani, R. (2022). Desain Sistem Informasi Pengenalan Jenis Tanaman Obat Berbasis Web. *Dipanegara Komputer Sistem Informasi*, *16*(1), 71-76.

Arif, Z., & Nurokhman, A. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi. *Jurnal Teknologi Sistem Informasi*, *4*(2), 394-405.

Andriani, K., & Hayadi, B. H. (2022). Pengamanan Data Penjualan Dengan Kriptografi Algoritma Rivest Shamir Adleman (Rsa) Pad a Toko Baju Family. *Journal of Science and Social Research*, *5*(3), 664-670.

LAMPIRAN-LAMPIRAN

Lampiran 1 Berita Acara Seminar Proposal



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
https://fikti.umsu.ac.id fikti@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

بسم الله الرحمن الرحيم

BERITA ACARA SEMINAR PROPOSAL
TAHUN AJARAN 2024/2025

Hari/Tanggal...../.....20...

Nama Mahasiswa : Muhammad Rizky Ananda Ranakuti
NPM : 2009010101
Program Studi : Sistem Informasi
Nama Dosen Penanggap : Halim Maulana
Judul Proposal : .....

.....

.....

Materi/Point yang Diperbaiki :.....

1. Bab I
2. Isi Bab III . Berdasarkan Algoritma Journal dan Contoh manual (perhitungan)
3. Setiap Definisi harus ada Sumber.

.....

.....

.....

.....

Dosen Penanggap

(.....)

Mahasiswa

(.....)

Lampiran 2 Surat Izin Riset

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
https://fikti.umsu.ac.id fikti@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Nomor : 542/II.3-AU/UMSU-09/F/2025
Lampiran : -
Perihal : **IZIN RISET PENDAHULUAN**

Medan, 17 Sawwal 1446 H
15 April 2025 M

Kepada Yth.
Bapak/Ibu Pimpinan
MAS Tahfizil Quran Yayasan Islamic Centre Sumatera Utara
Jl. Selamat Ketaren, Deli Serdang, Sumatera Utara

Di Tempat

Assalamu'alaikum Warahmatullahi Wabarakatuh

Dengan hormat, sehubungan mahasiswa kami akan menyelesaikan studi,untuk itu kami memohon kesediaan Bapak / Ibu untuk memberikan kesempatan pada mahasiswa kami melakukan riset di **Perusahaan / Instansi** yang Bapak / Ibu pimpin, guna untuk penyusunan skripsi yang merupakan salah satu persyaratan dalam menyelesaikan Program **Studi Strata Satu (S-1)**

Adapun Mahasiswa/i di Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara tersebut adalah:

Nama	**: Muhammad Rizky Ananda Rangkuti**
Npm	**: 2009010101**
Jurusan	**: Sistem Informasi**
Semester	**: X (Sepuluh)**
Judul	**: Penerapan Tanda Tangan Digital Dalam Pengamanan Data Ijazah Berbasis QR Code Dengan Algoritma RSA Pada Yayasan Islamic Centre Sumut**
Email	**: rizkyanandarkt@gmail.com**
Hp/Wa	**: 085143138391**

Demikianlah surat kami ini, atas perhatian dan kerjasama yang Bapak / Ibu berikan kami ucapkan terimaksih

Wassalamu 'alaikum Warahmatullahi Wabarakatuh

Dekan

Dr. Al-Khowarizmi,M.Kom.
NIDN : 0127099201

Cc.File

Lampiran 3 Dokumentasi Di MAS Islamic Centre