PENERAPAN TANDA TANGAN DIGITAL MENGGUNAKAN ALGORITMA *RSA* DAN *SHA* 256 DENGAN QR CODE PADA SERTIFIKAT ELEKTRONIK

Gagah Rizky Mulyawan[1], Asmunin[2]

Manajemen Informatika, Fakultas Vokasi, Universitas Negeri Surabaya
Jl. Ketintang, Kec. Wonokromo, Kota Surabaya, Jawa Timur 60231

[1]gagah.20045@mhs.unesa.ac.id

[2] asmunin@unesa.ac.id

Abstrak **- *Sistem otentikasi dokumen yang diterapkan dalam penelitian ini mengintegrasikan teknologi Quick Response (QR) code dan tanda tangan digital untuk memverifikasi keaslian dokumen digital, seperti sertifikat siswa. Proses pembuatan tanda tangan digital melibatkan penggunaan fungsi hash, khususnya Secure Hash Algorithm-256 (SHA-256), untuk menghasilkan inti pesan dari dokumen yang akan ditandatangani. Selain itu, algoritma Rivest-Shamir-Adleman (RSA) digunakan untuk enkripsi dan dekripsi, serta pembentukan kunci publik dan kunci privat yang diperlukan dalam proses tanda tangan digital. Penelitian ini melakukan pengujian terhadap beberapa sertifikat yang menggunakan QR code sebagai tanda tangan digitalnya, serta sertifikat lain yang menggunakan generator QR code lain. Hasil pengujian menunjukkan bahwa sistem otentikasi dokumen dengan QR code dan tanda tangan digital dapat memastikan keaslian dan integritas dokumen, sehingga dapat mencegah pemalsuan dokumen. Sertifikat yang menggunakan QR code yang dihasilkan oleh sistem ini berhasil diverifikasi sebagai asli, sedangkan yang menggunakan QR code dari sumber lain diidentifikasi sebagai palsu.***

Kata kunci-Tanda tangan digital, Sertifikat elektronik, Qr Code, Metode RSA, Metode Sha-256

Abstract **- *The document authentication system implemented in this research integrates Quick Response (QR) code technology and digital signatures to verify the authenticity of digital documents, such as student certificates. The process of creating a digital signature involves the use of a hash function, specifically Secure Hash Algorithm-256 (SHA-256), to generate the message core of the document to be signed. In addition, the Rivest-Shamir-Adleman (RSA) algorithm is used for encryption and decryption, as well as the formation of public keys and private keys required in the digital signature process. This research tested several certificates that use QR codes as digital signatures, as well as other certificates that use other QR code generators. The test results show that the document authentication system with QR codes and digital signatures can ensure the authenticity and integrity of documents, thereby preventing document forgery. Certificates using QR codes generated by this system were successfully verified as genuine, while those using QR codes from other sources were identified as fake.***

Keywords-Digital signature, electronic certificate, Qr Code, RSA method, Sha-256 method

I. PENDAHULUAN

Di era digital saat ini, pemanfaatan teknologi informasi semakin meluas. Oleh karena itu, keamanan menjadi kebutuhan dasar yang sangat penting, terutama ketika data sensitif dikirim dan disimpan, karena ada ancaman pencurian dan perusakan data. Saat ini, lembaga-lembaga yang menyediakan layanan kursus kompetensi secara online dan mengeluarkan sertifikat elektronik sebagai bukti partisipasi dalam kegiatan tersebut juga menghadapi tantangan ini [1].

Sertifikat elektronik akan mempermudah dalam pendistribusian sehingga persebarannya lebih luas dan dapat dijangkau ke seluruh tempat tanpa harus meminta bantuan kurir. Selain itu, penggunaan sertifikat elektronik lebih hemat kertas. Namun, keberadaan sertifikat elektronik tidak menutup kemungkinan adanya penggandaan dokumen tersebut. Otentikasi dokumen dapat menggunakan sistem enkripsi dengan teknik tanda tangan digital. Oleh karena itu, sertifikat elektronik harus disertakan tanda tangan digital untuk memastikan kredibilitas dan keasliannya [1] [2].

Menurut Labolo & Senung pada tahun 2022, tanda tangan digital mempunyai kekuatan hukum setara tanda tangan basah. Tanda tangan digunakan sebagai alat untuk memeriksa atau memvalidasi keaslian sebuah dokumen, memastikan apakah dokumen tersebut benar-benar berasal dari pembuatnya atau telah dipalsukan [3].

Selain tanda tangan digital, otentikasi dokumen saat ini juga dapat memanfaatkan skema kode QR, yang dapat menyimpan data numerik yang memiliki ruang penyimpanan lebih besar dibandingkan barcode. Kode QR juga bisa digunakan untuk menyembunyikan pesan di balik kode, memastikan keamanan dan privasi seseorang yang mengirim pesan. Namun pembuatan QR-Code belum menyediakan kunci untuk menyembunyikan perubahan parameter data asli, sehingga untuk keamanan data yang lebih tinggi, data dapat dienkripsi menggunakan metode *SHA 256* sebelum dibuat QR *Code* [1].

Kode QR sangat menyederhanakan proses pembuatan dan validasi dokumen digital. Untuk menghasilkan kode QR yang unik dan berbeda, perlu adanya algoritma enkripsi SHA yang

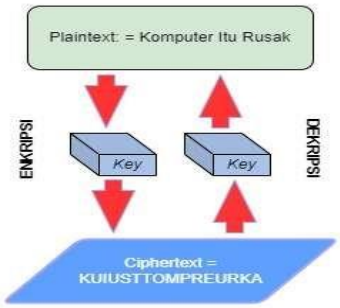
dapat menjaga keamanan kode QR agar tidak mudah disalin dari dokumen. Menurut Nuraeni (2020), bahwa pemakaian QR *Code* pada sertifikat elektronik bisa mempermudah dalam proses verifikasi sertifikat dan pemberian tanda tangan digital yang kemungkinan mempunyai kode cukup panjang.

Berdasarkan penjelasan yang diberikan, dapat disimpulkan bahwa penggunaan tanda tangan digital pada sertifikat elektronik berbentuk QR Code sangatlah penting. Hal ini mempermudah proses penandatanganan secara tidak langsung serta proses validasi, yang diperlukan untuk mencegah ancaman penipuan dan perubahan data.

II. KAJIAN PUSTAKA

A. *Kriptografi*

Kriptografi berasal dari kata Yunani "cryptos" yang berarti "rahasia" dan "graphein" yang berarti "menulis". Dengan demikian, kriptografi dapat didefinisikan sebagai proses "penulisan pesan secara rahasia". Enkripsi merupakan bidang ilmu dan seni untuk mengamankan komunikasi dengan mengubah teks atau data menjadi bentuk yang tidak dapat dimengerti (ciphertext), menggunakan teknik dan algoritma matematika khusus. Tujuan utama *kriptogarafi* antara lain untuk menjaga *confidentiality*, *authentication*, dan data *integrity*, dan *nonrepudiation* [4].



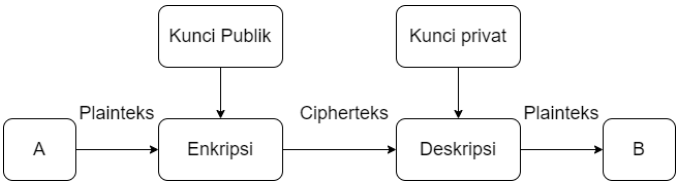
Gambar 1**.** Ilustrasi Kriptograsi

Istilah-istilah pada ilmu kriptografi diantaranya [5].

1) *Plain text* adalah pesan atau disebut juga sumber daya yang pertama kali dibuat oleh pengguna; Pesan yang dapat dibaca oleh semua orang.
2) *Ciphertext* adalah pesan teks biasa yang telah diubah ke bentuk yang lebih aman sehingga tidak dapat dibaca.
3) Algoritma kriptografi adalah langkah-langkah yang digunakan dalam operasi matematika dasar untuk mengubah teks biasa menjadi teks tersandi.
4) *Key* adalah kunci yang digunakan berdasarkan algoritma enkripsi untuk memproses enkripsi dan dekripsi pesan yang dikirim. Artinya hanya pengguna yang memiliki kunci yang dapat mendekripsi pesan dalam bentuk ciphertext.
5) *Message Digest* merupakan suatu algoritma kriptografi yang menghasilkan rangkuman (digest) dari pesan (file, aliran data) dengan menggunakan fungsi hash yang akan menghasilkan suatu intisari.
6) Enkripsi adalah suatu metode enkripsi data agar informasi tetap aman.
7) Dekripsi adalah proses mengubah kembali data yang telah dienkripsi ke bentuk aslinya yang dapat dibaca, sehingga teks atau gambar yang sebelumnya tidak dapat dipahami oleh orang lain atau penerima dapat dikembalikan ke bentuk yang dapat dipahami.

B. *RSA (Rivest-Shamir-Adlemen)*

RSA (Rivest-Shamir-Adlemen) adalah algoritma enkripsi asimetris yang menggunakan pasangan kunci publik dan kunci pribadi. RSA diciptakan oleh tiga orang dari Massachusetts Institute of Technology (MIT), Ron Rivest, Adi Shamir, dan Leonard Adelman pada tahun 1977. Nama *RSA* dapat diambil dari nama belakang mereka bertiga [6].



Gambar 2. Skema Kriptografi

Pada algoritma RSA, terdapat dua jenis kunci dalam enkripsi: kunci publik yang bisa dibagikan secara bebas, dan kunci privat yang hanya diketahui oleh pemiliknya. Kunci publik digunakan untuk mengenkripsi pesan, sementara kunci privat digunakan untuk mendekripsinya [7].

Berikut beberapa komponen dari algoritma kunci publik RSA:

- p dan q adalah bilangan prima dan harus dijaga kerahasiaannya.
- n adalah hasil perkalian p dan q, tetapi nilainya tidak perlu dirahasiakan.
- $\phi(n)$ adalah hasil dari (p-1)*(q-1) dan nilainya harus dirahasiakan.
- e adalah kunci enkripsi dan nilainya tidak perlu dirahasiakan.
- d adalah kunci dekripsi dan harus dijaga kerahasiaannya.
- m adalah teks biasa (plaintext) dan harus dirahasiakan.
- c adalah teks terenkripsi (ciphertext) dan nilainya tidak perlu dirahasiakan.

Setelah mendapatkan kunci publik dan kunci privat dari algoritma RSA, kunci privat dapat digunakan untuk mengenkripsi pesan, sementara kunci publik akan digunakan untuk mendekripsi pesan [8].

Menurut Hidayat (2023), Keamanan algoritma RSA didasarkan pada kesulitan faktorisasi bilangan bulat besar. Keamanannya sangat tergantung pada kompleksitas proses faktorisasi dua bilangan prima. Algoritma ini dianggap aman jika bilangan prima yang digunakan memiliki nilai yang besar. Proses utama dalam RSA meliputi pembangkitan kunci, enkripsi, dan dekripsi yang dijelaskan sebagai berikut:

1. Cara Pembangkitan Pasangan Kunci
   a. Memilih dua bilangan prima besar, p dan q.
   b. Hitung nilai n, di mana n = p*q.
   c. Hitung nilai fungsi Euler totient φ(n), yaitu φ(n) = (p - 1) * (q - 1).
   d. Pilih bilangan bulat e yang lebih kecil dari φ(n) dan relatif prima dengan φ(n).
   e. Temukan bilangan bulat d yang memenuhi persamaan (d * e) mod φ(n) = 1.
   f. Dengan langkah-langkah ini, Anda akan mendapatkan pasangan kunci yang terdiri dari kunci publik (e,n) dan kunci privat (d,n) dalam algoritma RSA.
2. Cara Enkripsi
   a. Ambil pesan atau plaintext (p) yang akan dienkripsi
   b. Bagi kedalam beberapa blok yang lebih kecil: m1, m2, ... (syarat 0 mi< n)
   c. Repesentasikan dalam bentuk angka m, dengan 0 ≤ m < n.
   d. Hitung ciphertext (ci) untuk setiap blok pesan menggunakan rumus ci = (mi^e) mod n, di mana mi adalah blok pesan, e adalah eksponen kunci publik, dan n adalah modulus dari kunci publik.
3. Cara Dekripsi
   a. Untuk setiap blok ciphertext (ci), hitung nilai plaintext mi menggunakan kunci privat d dengan rumus mi = (ci^d) mod n.

C. *SHA 256* ***(Secure Hash Algoritm-256)***

SHA merupakan algoritma hashing yang digunakan untuk menghasilkan representasi tetap dari teks atau data, yang disebut nilai hash atau pesan hash [9].

SHA-256 adalah algoritma hash kriptografi satu arah yang dikembangkan oleh NSA dan diterbitkan oleh NIST sebagai bagian dari FIPS di AS. Ini adalah bagian dari standar hash aman, yang juga mencakup SHA-1, SHA-256, SHA-384, dan SHA-512. [10].

TABEL 1.
Jenis SHA

Algoritma		**Ukuran Pesan (bit)**	**Ukuran Blok (bit)**	**Ukuran Kata (bit)**	**Ukuran *message digest* (bit)**
SHA-1	SHA-1	<264	512	32	160
SHA-2	SHA-256	<264	512	32	256
	SHA-384	<2128	1024	64	384
	SHA-521	<2128	1024	64	512

Nilai fungsi hash digunakan untuk mengautentikasi pesan dengan menghitung nilai hash sebagai representasi bit dari pesan tersebut. Menurut standar tanda tangan aman, jika panjang pesan kurang dari 264 bit, fungsi hash menghasilkan hash 512-bit dan mengkompreskannya menjadi message digest 256-bit [10].

D. *Qr-Code*

Kode QR, atau kode respons cepat, awalnya dikembangkan oleh peneliti Jepang pada tahun 1994. Pengembangan lebih lanjut dari kode batang yang menggunakan dua dimensi untuk menyimpan lebih banyak informasi [11].

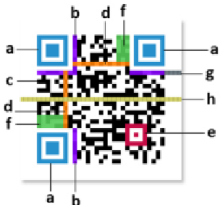
Secara umum, QR Code terdiri dari kotak-kotak hitam yang diatur dalam grid persegi dengan latar belakang putih. Sekarang, QR Code telah berkembang menjadi lebih bervariasi dengan penggunaan berbagai warna, bentuk yang tidak selalu kotak sempurna, dan bahkan kemampuan untuk menyisipkan gambar atau logo [12].

Gambar 3. Contoh Qr Code

Kode QR memiliki kemampuan untuk menyimpan data dalam berbagai panjang dan tingkat ketelitian yang berbeda. Kode QR versi terbaru memiliki ukuran 177 x 177 yang dapat menampung lebih dari 1852 karakter data. Tingkat ketelitian Kode QR bervariasi, di mana pada tingkat ketelitian tinggi, kode QR masih dapat dibaca meskipun ada sebagian yang hilang atau rusak [13].

1. Anatomi Kode QR

Berikut Gambar anatomi Kode QR pada gambar 4.



Gambar 1 Anatomi Kode QR

Berikut adalah beberapa penjelasan tentang struktur QR Code menurut [14]:

a. *Finder Pattern* Adalah formasi tiga kotak persegi yang ditempatkan di tiga sudut QR Code dan berfungsi untuk membantu perangkat pemindai atau pembaca QR *Code* mengidentifikasi letak QR *code* dalam gambar atau media dimana QR *code* ditempatkan.
b. *Format Information* adalah bagain dari QR *code* yang menyimpan informasi tentang tingkat

koreksi kesalahan dan pola maker yang digunakan untuk mengenkripsi data pada QR *code*.

c. Data merupakan bagian dari QR *code* yang sebenarnya menyimpan data yang telahh dikodekan, seperti teks, Url, atau informasi lainnya yang ingin disimpan dalam QR *code.*
d. *Timming Pattern* adalah pola garis hitam putih yang terletak di sepanjang tepi QR *code* dan berfungsi sebagai referensi untuk perangkat pembaca dalam mengidentifikasi koordinat pusat QR *code.*
e. *Alignment Pattern* adalah pola kotak persegi yang terletak di dalam kode QR yang mengoreksi penyimpangan kode QR, terutama distorsi non-linier yang mungkin terjadi pada kode QR saat dicetak atau dipindai.
f. *Version Information* adalah informasi tentang versi QR Code yang digunakan, yang menentukan jumlah modul (kotak hitam atau putih) yang ada dalam QR Code dan kapasitas penyimpanan data yang dapat diakomodasi.
g. *Quiet Zone* adalah informasi tentang versi QR *Code* yang digunakan, yang menentukan jumlah modul (kotak hitam atau putih) yang ada dalam QR *Code* dan kapasitas penyimpanan data yang dapat diakomodasi.
h. QR Code Version adalah tingkat kepadatan atau versi QR Code yang menentukan jumlah modul dan ukurannya. Semakin tinggi versi QR Code, semakin banyak modul yang digunakan dan kapasitas penyimpanan data yang dapat ditampung oleh QR Code tersebut.

E. *Tanda Tangan Digital*

Tanda tangan digital adalah mekanisme keamanan jaringan yang memungkinkan pengirim data untuk "menandatangani" data secara elektronik, sehingga penerima dapat memverifikasi tanda tangan secara elektronik. Tanda tangan digital diterapkan pada unit data untuk menunjukkan sumber pengirim dan mencegah pemalsuan [15].

Menurut Bansal Tanda Tangan Digital pada dasarnya adalah aplikasi matematika dari kriptografi asimetris pada dokumen yang didigitalkan untuk mengesahkan keabsahan dan integritasnya kepada para penggunanya. Dokumen yang didigitalkan untuk menyatakan keabsahan dan integritasnya kepada penggunanya. Tanda tangan digital dapat digunakan untuk memberikan pernyataan bahwa pihak yang diklaim mengesahkan informasi tersebut [16].

F. *Sertifikat Elektronik*

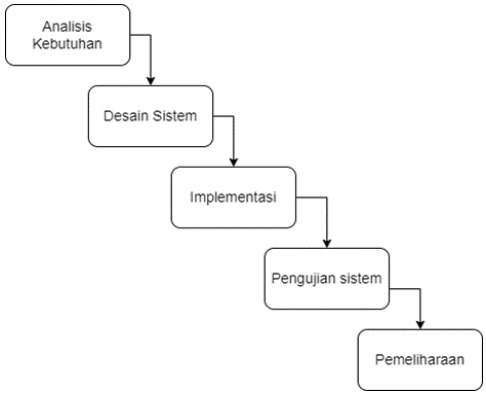
Sertifikat elektronik adalah dokumen elektronik yang berisi tanda tangan elektronik dan informasi identitas untuk menegaskan status hukum subjek dalam transaksi elektronik. Dokumen ini diterbitkan oleh penyedia layanan sertifikasi elektronik [17].

Sertifikat elektronik sangat penting untuk memastikan keaslian dokumen elektronik, baik dari segi konten maupun identitas penandatanganannya. Tanda tangan elektronik pada sertifikat elektronik sulit untuk dipalsukan. Pada Pasal 1 Angka 9 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), menjelaskan bahwa sertifikat elektronik adalah dokumen elektronik yang memuat tanda tangan elektronik dan informasi identitas yang menunjukkan status hukum subjek dalam suatu transaksi elektronik, yang diterbitkan oleh badan yang berwenang untuk sertifikasi elektronik. Pasal 1 Angka 12 UU ITE menjelaskan bahwa tanda tangan elektronik yang terdiri dari informasi elektronik yang dihubungkan atau dihubungkan dengan informasi elektronik lainnya, yang digunakan untuk keperluan verifikasi atau autentikasi. [18].

G. *Metode Waterfall*

Salah satu metode pengembangan perangkat lunak. Pendekatan ini adalah kerangka kerja yang sering digunakan untuk mengelola proses pengembangan sistem informasi dengan terstruktur dan terorganisir [19].

Metode pengembangan ini seperti mengikuti alur kehidupan yang terstruktur secara berurutan. Tahapan dalam metode air terjun adalah sebagai berikut [19]:



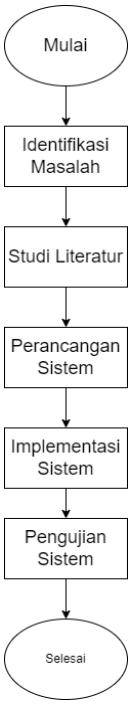
Gambar 5. Metode Waterfall

H. *Blackbox Testing*

Metode pengujian perangkat lunak yang berfokus pada fungsionalitasnya tanpa mempedulikan struktur internal atau kode sumbernya. Tujuannya adalah untuk mengidentifikasi dan menemukan berbagai jenis kesalahan atau ketidakcocokan dalam fungsi perangkat lunak. Ini termasuk masalah seperti fungsi yang tidak berjalan dengan benar, kesalahan antarmuka pengguna, masalah struktur data, kinerja yang buruk, masalah dalam proses inisialisasi dan terminasi, serta ketidaksesuaian dengan kebutuhan yang diinginkan [20].

III. METODOLOGI PENELITIAN

Berikut Alur Penelitian:



Gambar 6. Alur Penelitian

Gambar tersebut mengilustrasikan alur dan proses penelitian yang dimulai dengan mendefinisikan masalah, yaitu implementasi sistem otentikasi dokumen yang menggunakan kode QR berbasis tanda tangan digital. Langkah berikutnya adalah melakukan studi literatur untuk mengumpulkan data dari sumber-sumber yang relevan. Setelah itu, dilakukan perancangan sistem, di mana aplikasi dirancang berdasarkan analisis kebutuhan sistem. Tahap selanjutnya adalah implementasi sistem dengan menggunakan bahasa pemrograman PHP. Intinya, pengujian system yang berfokus untuk memastikan aplikasi dapat bekerja dengan baik.

A. Identifikasi Masalah

Pada tahap awal penelitian ini, dimulai dengan mendefinisikan masalah yang relevan dengan topik yang dipilih oleh peneliti, yakni mengenai implementasi tanda tangan digital menggunakan algoritma RSA dan SHA-256 dengan QR Code pada sertifikat elektronik.

Tanda tangan digital dianggap dapat diandalkan karena menggunakan sistem kriptografi asimetris yang terdiri dari pasangan kunci publik dan kunci privat. Kunci privat disimpan secara rahasia oleh pihak yang menerbitkan dokumen, sementara kunci publik dapat digunakan oleh pihak penerima untuk memverifikasi keaslian dokumen. Keamanan sistem kriptografi dipastikan dengan kompleksitas operasi algoritma yang tinggi, membuatnya sulit untuk dipecahkan. Oleh karena itu, untuk meningkatkan keamanan tanda tangan digital, digunakan algoritma RSA.

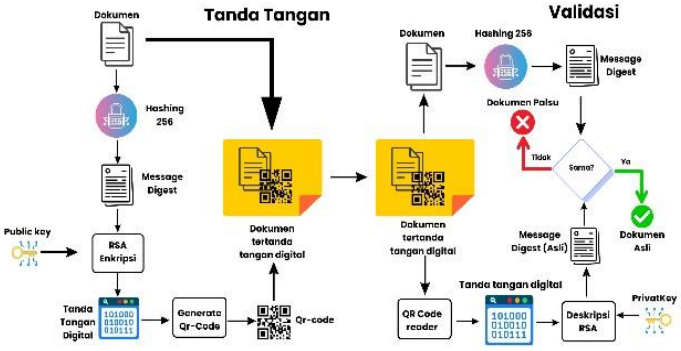
B. Studi Literatur

Penelitian ini menggunakan acuan rancangan berdasarkan dari studi literatur yang diakses melalui situs seperti Google Scholar, Science Direct serta sumber-sumber literatur lain. Tujuan dari penggunaan studi literatur ialah untuk meningkatkan pemahaman terkait Penerapan Tanda Tangan Digital Menggunakan Algoritma *RSA* dan *SHA 256* Dengan Qr-code Pada Sertifikat Elektronik. Hal tersebut dilakukan dengan mempelajari dasar penelitian serta melakuakan research melalui jurnal, artikel dan penelitian terdahulu. Dari penelitian terdahulu dimanfaatkan untuk menambah wawasan mengenai metode *RSA* dan *SHA 256*

C. Perancangan Sistem

Dilakukannya analisis dan perancangan sistem yang akan digunakan dalam penelitian untuk menerapkan tanda tangan digital menggunakan algoritma RSA dan SHA-256 dengan QR Code pada sertifikat elektronik.

1. Desain Sistem



Gambar 7. Proses Tanda Tangan dan Validasi Pada Dokumen Elektronik

Proses tanda tangan dimulai dengan penggunaan proses hashing, di mana data asli dari dokumen diambil inti sarinya (message digest) menggunakan fungsi hash SHA-256. Hashing ini merupakan proses satu arah di mana hasilnya tidak dapat dikembalikan untuk mendapatkan data asli seperti dalam proses dekripsi pada kriptografi. Salah satu kelemahan fungsi hash adalah kemungkinan terjadinya tabrakan hash, di mana data yang berbeda dapat menghasilkan nilai hash yang sama. Setelah itu, *message digest* (md0) dari dokumen dienkripsi menggunakan kunci publik yang dihasilkan dari algoritma RSA. Tanda tangan digital yang dihasilkan kemudian diubah menjadi kode QR untuk memudahkan penyisipannya pada dokumen sertifikat elektronik sebelum dikirimkan kepada pihak-pihak yang berwenang.

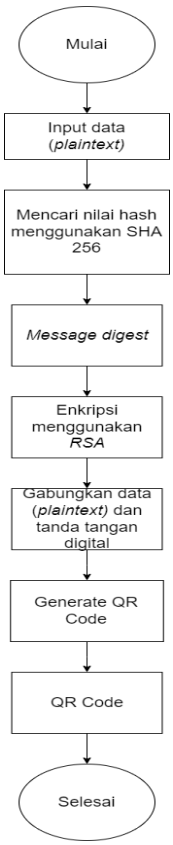
Untuk memverifikasi keaslian sertifikat elektronik, langkah pertama adalah memindai kode QR untuk mendapatkan kode tanda tangan digital. Kode ini kemudian di-dekripsi menggunakan kunci pribadi dalam algoritma RSA, yang mengembalikan inti pesan asli (md0) yang digunakan dalam proses penandatanganan. Untuk memvalidasi dokumen, data dari sertifikat elektronik dijalankan melalui proses hashing untuk menghasilkan message digest (md1). Jika message digest yang dihasilkan oleh sertifikat elektronik (md1) sama dengan message digest asli

(md0), maka dapat dipastikan bahwa integritas data dokumen terjaga sehingga sertifikat tersebut asli. Namun, jika message digest yang dihasilkan (md1) berbeda dengan md0, maka dapat disimpulkan bahwa terjadi modifikasi pada data dalam sertifikat.

2. Flowchart Tanda Tangan Digital

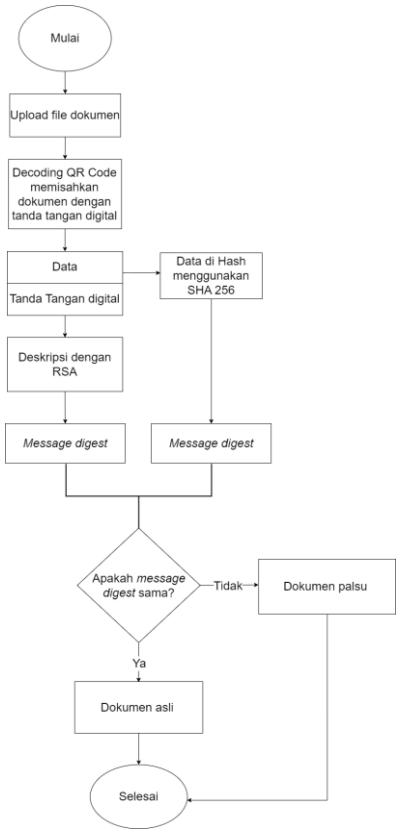
Penelitian dimulai dengan memasukkan data yang akan disimpan dalam sistem. Data ini kemudian diolah menggunakan fungsi hash SHA-256 untuk menghasilkan ringkasan pesan. Langkah berikutnya mencakup pembuatan pasangan kunci publik dan kunci privat menggunakan algoritma RSA, yang diikuti dengan proses penggunaan kunci privat untuk mengenkripsi ringkasan pesan. Hasil dari proses enkripsi ini adalah tanda tangan digital dari data yang dimasukkan ke dalam sistem. Proses ini mengandalkan algoritma RSA untuk menghasilkan kunci dan melakukan enkripsi ringkasan pesan.

Kemudian, teks yang telah ditambahkan dengan tanda tangan digital diinputkan ke dalam pembuat kode QR. Proses ini menghasilkan kode QR yang memuat informasi tanda tangan digital tersebut. Kode QR yang telah dibuat dapat dimasukkan ke dalam dokumen sertifikat, yang selanjutnya dapat dicetak atau digunakan sesuai dengan kebutuhan.



Gambar 8. Pembangkitan Tanda Tangan Digital

3. Flowchart Validasi dokumen



Gambar 9. Flowchart Validasi Dokumen

Proses validasi dokumen pada sistem ini dimulai dengan mengunggah dokumen sertifikat dalam format PDF ke platform. Ketika dokumen diunggah, sistem menggunakan decoder kode QR untuk memisahkan tanda tangan digital dari data dalam kode QR. Teks biasa kemudian di-hash dengan fungsi hash SHA-256 untuk menghasilkan intisari pesan.

Berikutnya melakukan dekripsi terhadap bagian tanda tangan digital menggunakan kunci publik, sehingga intisari pesan yang dienkripsi saat kode QR dibuat dapat diambil. Proses verifikasi dilanjutkan dengan membandingkan intisari pesan yang dihasilkan dari data dengan intisari pesan yang terkandung dalam tanda tangan digital. Jika hasil perbandingannya sama, maka dokumen dianggap asli dan tidak mengalami perubahan atau modifikasi. Namun, jika hasil perbandingannya tidak sama, maka dokumen dianggap tidak asli dan telah mengalami perubahan pada dokumen atau tanda tangan digital.

D. Implementasi Sistem

Tahap Implementasi Sistem adalah langkah di mana aplikasi dikembangkan sesuai dengan rancangan yang telah disiapkan sebelumnya. Proses ini melibatkan pembuatan aplikasi menggunakan framework Laravel untuk memastikan bahwa hasil akhir sesuai dengan tahapan yang telah direncanakan sebelumnya.

E. Pengujian Sistem

Pengujian dilakukan menggunakan metode blackbox testing untuk mengevaluasi apakah fungsi-fungsi yang telah diimplementasikan dalam aplikasi web berjalan sesuai dengan harapan atau terdapat kesalahan. Blackbox testing berfokus pada pengujian input dan output sistem tanpa memperhatikan detail implementasi internal kode atau struktur sistem. Selama pengujian, berbagai skenario pengujian digunakan untuk menguji berbagai situasi dan kondisi yang mungkin terjadi dalam penggunaan aplikasi. Hasil dari pengujian tersebut divalidasi untuk memastikan respons sistem sesuai dengan yang diharapkan. Hasil dari pengujian ini akan memudahkan dalam penentuan kelayakan aplikasi web untuk dianalisis ke publik atau perlu dilakukan perbaikan secara lanjut sebelum peluncuran.

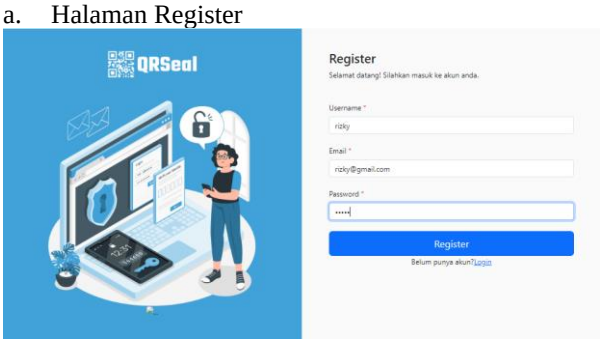
IV. HASIL DAN PEMBAHASAN

A. Hasil Penelitian

1. Implementasi Sistem

Pada implementasi sistem, setelah desain tanda tangan digital dibuat, selanjutnya akan dibuat aplikasi perwujudan dari rancangan yang telah dipaparkan sebelumnya. Tahap ini akan menjelaskan mengenai hasil dari website yang dibuat. Hasil yang didapatkan antara lain:

a. Halaman Register



Gambar 10. Halaman Register

Halaman Halaman registrasi pada gambar tersebut digunakan oleh pengguna untuk mendaftar jika mereka belum memiliki akun. Pengguna dapat membuat akun baru dengan

b. Halaman Login

Gambar 11. Halaman Login

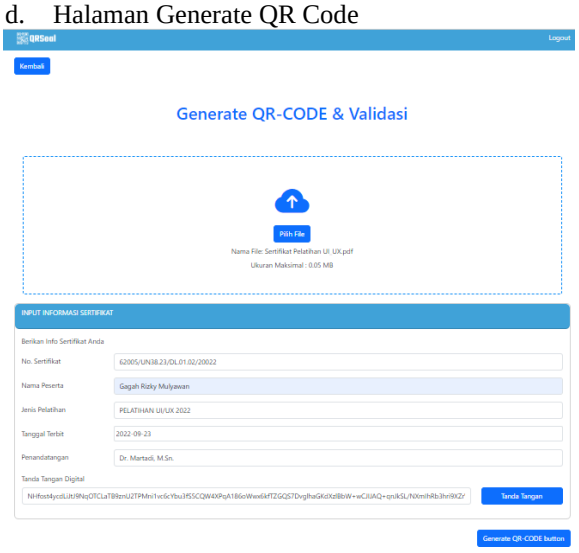
Halaman Login pada gambar diatas digunakan oleh pengguna untuk masuk ke akun yang sudah dibuat sebelumnya dengan memasukkan informasi yang sesuai, seperti email beserta kata sandi yang terkait dengan akun mereka. Setelah proses login berhasil, pengguna dapat menggunakan layanan yang tersedia dengan pada website.

c. Halaman Home

Halaman 12. Halaman Home

Halaman Home berisi menu Generate QR code dan Validasi Dokumen. Ketika pengguna menekan Generate QR code, mereka akan diarahkan ke menu tersebut di mana mereka dapat membuat kode QR sesuai dengan kebutuhan mereka. Begitu juga, ketika pengguna akan memilih menu Validasi Dokumen, mereka diarahkan ke halaman untuk memvalidasi dokumen.

d. Halaman Generate QR Code

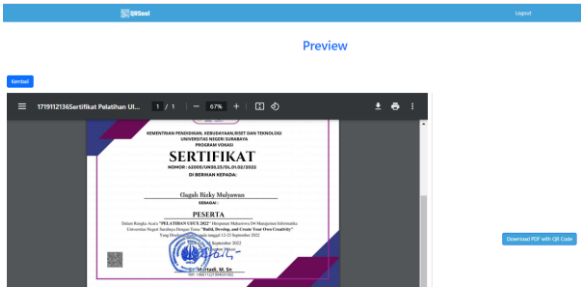


Gambar 13. Halaman Generate QR Code

Halaman Generate QR Code digunakan oleh pengguna untuk mengunggah file sertifikat dan mengisi informasi terkait dengan sertifikat tersebut. Dan fitur tanda tangan digital nantinya akan menghasilkan berupa kode dari

gabungan RSA dan SHA 256. Setelah semua data sudah diinputkan, selanjutnya sistem akan meng*generate* Qr *code.*

e. Halaman Preview



Gambar 14. Halaman Preview

Halaman Preview digunakan oleh pengguna untuk menarik dan menyimpan QR code ke dalam sertifikat dengan cara yang mudah. Selanjutnya Qr code yang sudah ditempelkan ke dalam sertifikat dan selatah itu sertifikat akan diunduh yang telah ditambahkan kode QR dan menyimpan sertifikat dalam bentuk file digital untuk keperluan lebih lanjut

f. Halaman Validasi Sertifikat

Gambar 15. Halaman Validasi Sertifikat

Halaman preview digunakan oleh pengguna untuk melihat hasil proses validasi yang telah dilakukan oleh sistem. Agar pengguna dapat mengetahui hasil dari pengecekan dokumen untuk memastikan keaslian dan validitas sertifikat tersebut.

2. Pengujian Sistem

Pengujian black box dilakukan untuk mengevaluasi fungsionalitas setiap tombol yang ada di semua halaman aplikasi tanpa memerhatikan struktur internal kode. Tujuan utamanya adalah untuk memverifikasi apakah respons yang diberikan oleh sistem sesuai dengan skenario pengujian yang telah ditetapkan sebelumnya serta untuk mengidentifikasi potensi kesalahan dalam fungsi tombol tersebut. Hasil dari pengujian ini menunjukkan bahwa sistem beroperasi sesuai dengan ekspektasi dan memenuhi skenario pengujian yang telah diatur sebelumnya, mengonfirmasi keberhasilan implementasinya.

TABEL 2.
Blackbox Testing

No	Menu	Skenario	Hasil yang diharapkan	Valid
1	*Register*	Masukan *Username*, *Email* dan *Password*	Menampilkan pemberitahuan *register* berhasil	**V**
2	*Login*	Masukkan *Username* dan *password*	*Login* berhasil dan menampilan halaman beranda	**V**
3	*Home*	Menampilkan generate Qr code Menampilkan validasi	Menampilkan halaman *home*	**V**
4	*Generate QR code*	- Tambah data (upload file pdf, input form, kode otomatis generate) - Tombol generate	Menampilkan hasil dari tambah data ke menu *preview*	**V**
5	*Preview*	- Menambah Qr Code ke dalam sertifikat - Tombol download sertifikat pdf	Mendowload sertifikat yang sudah tertandatangan oleh Qr *code*	**V**
6	Validasi File	Menampilkan pemberitahuan scan di perangkat lain	Menampilkan hasil scan Qr code dari perangkat lain	**V**

B. Pembahasan

1. Hipotesis

Tes ini melibatkan validasi enam dokumen sertifikasi yang berisi kode QR. Tiga sertifikat menyertakan kode QR yang dihasilkan oleh sistem sebagai tanda tangan digital, sementara tiga sertifikat lainnya menggunakan kode QR yang dihasilkan oleh generator lain sebagai tanda tangan digital. Tabel 4 menampilkan contoh validasi dokumen menggunakan kode QR sebagai tanda tangan yang dihasilkan oleh sistem otentikasi. Hasil verifikasi menunjukkan dokumen asli tanpa kerusakan. Pengujian dilakukan pada tiga sertifikat, semuanya diverifikasi sebagai sah.

Semakin tinggi tingkat koreksi kesalahan, semakin banyak cacat yang dapat diperbaiki pada kode QR sebelum menjadi tidak terbaca.

TABEL 3. Level Koreksi

Level	Kemampuan Koreksi Kesalahan
L (L*ow)*	7%
M (*Medium)*	15%
Q (*Quartile)*	25%
H (*High)*	30%

Sistem ini menggunakan QR code dengan tingkat koreksi kesalahan tinggi (level H). Pada level H, QR code memiliki kemampuan untuk mengoreksi kesalahan hingga 30%.

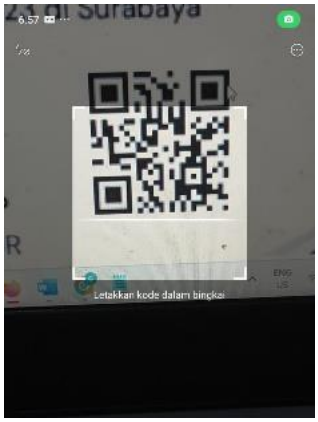
TABEL 4.
Contoh Validasi Dokumen

Validasi Berkas	Hasil Validasi
	
	

Selanjutnya dilakukan pengujian terhadap dokumen sertifikat dengan menggunakan tanda tangan kode QR yang tidak dihasilkan oleh sistem yang diterapkan. Dari tiga dokumen sertifikasi yang digunakan dalam pengujian ini, hasilnya menunjukkan semuanya palsu atau tidak valid. Tabel 4 memberikan gambaran validasi dokumen sertifikat yang berisi tanda tangan kode QR dari sumber di luar sistem.

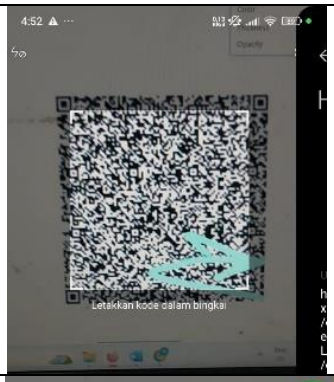
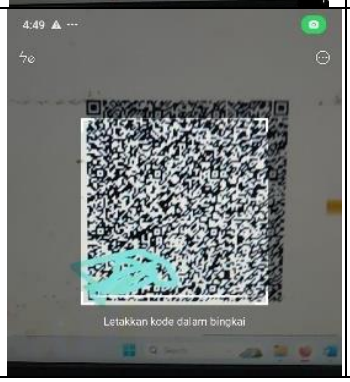
TABEL 5.
Contoh Validasi Dokumen

Validasi Berkas	**Hasil Validasi**
	Tidak ada data ditemukan
	Tidak ada data ditemukan

	Tidak ada data ditemukan

Seperti Sistem otentikasi dokumen menghasilkan kode QR dengan tingkat koreksi kesalahan tinggi. Pengujian dilakukan dengan dua kode QR untuk data yang sama, satu dengan koreksi kesalahan tinggi dan satu dengan koreksi rendah. Kedua kode QR kemudian diuji untuk membaca setelah diubah. Hasil menunjukkan bahwa kode QR dengan koreksi kesalahan tinggi masih dapat diverifikasi, sementara kode QR dengan koreksi kesalahan rendah tidak terbaca. Informasi lebih lanjut terdapat pada Tabel 5.

TABEL 5.
Validasi Level Koreksi Kesalahan QR Code

Level koreksi kesalahan	**Validasi Berkas**	**Hasil Validasi**
H(high)		
L(low)		QR code tidak terbaca

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Penelitian ini menekankan pada metode verifikasi keaslian dokumen menggunakan tanda tangan digital dan kode QR. Metode ini diimplementasikan dalam sistem autentikasi dokumen (sertifikat) dengan perangkat pengkodean dan dekoding kode QR. Sistem ini mencakup fitur pembuatan tanda tangan digital, konversi tanda tangan menjadi kode QR, serta verifikasi dokumen. Hasil pengujian menunjukkan bahwa sistem ini efektif dalam menjaga keaslian dokumen yang dilengkapi dengan tanda tangan digital atau kode QR. Penggunaan tanda tangan digital dengan perangkat keras enkripsi dan dekoding kode QR berfungsi sebagai mekanisme pencegahan pemalsuan dokumen, kecuali jika pihak lain memiliki akses ke kunci privat untuk membuat tanda tangan digital.

B. Saran

Saran untuk penelitian lebih lanjut dan pengembangan aplikasi adalah sebagai berikut:

1. Website yang telah dibangun masih memerlukan studi lebih lanjut, penyesuaian, dan perbaikan yang lebih mendalam. Diperlukan pengembangan website yang dapat mengakomodasi semua kebutuhan yang diperlukan secara optimal.
2. Dapat menggunakan berbagai metode kriptografi lain untuk mengamankan data pada tanda tangan digital

REFERENSI

[1] F. Nuraeni dkk., “Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik,” 2020.

[2] B. Renaldy Suteja, R. Victor Imbar, dan M. Christianti Johan, “e-Certificate system based on Portable Document Format and QR Code for Academic Activities”, doi: 10.5281/zenodo.4431081.

[3] I. Labolo dan B. Senung, “Penerapan QrCode dan Digital Signature Menggunakan Algoritma SHA Untuk Lembar Disposisi Elektronik,” JURIKOM (Jurnal Riset Komputer), vol. 9, no. 6, hlm. 1707, Des 2022, doi: 10.30865/jurikom.v9i6.5006.

[4] K. Adiyasa Bachtiar -13519001, “Implementasi Tanda Tangan Digital pada Surat Keterangan Sakit.”

[5] N. Wachid Hidayatulloh, M. Tahir, H. Amalia, N. Afdlolul Basyar, A. F. Prianggara, dan M. Yasin, “Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data,” Digital Transformation Technology (Digitech) | e, vol. 3, no. 1, 2023, doi: 10.47709/digitech.v3i1.2293.

[6] R. Hidayat, “Implementasi Algoritma RSA dan Fungsi Hash SHA-3 Untuk Pembangkitan Tanda Tangan Digital Pada Faktur Elektronik (Electronic Invoice).”

[7] M. Raihan Aulia, “Implementasi Algoritma RSA dan SHA-3 sebagai Digital Signature Hasil Karya Anggota Unit Genshiken ITB.” [Daring]. Tersedia pada: https://keccak.team/sponge_duplex.html

[8] V. Finnegan Dyell, “Implementasi Tanda Tangan Digital untuk Pengamanan Sertifikat yang Didigitisasi Terkhusus untuk Kegiatan Internal Institut Teknologi Bandung.”

[9] Z. Panjaitan dan E. Fahmi Ginting, “Modifikasi SHA-256 dengan Algoritma Hill Cipher untuk Pengamanan Fungsi Hash dari Upaya Decode Hash *#1,” Jurnal Sains Manajemen Informatika dan Komputer, vol. 19, no. 1, hlm. 53–61, 2020, [Daring]. Tersedia pada: https://ojs.trigunadharma.ac.id/

[10] F. M. Rangkuti, N. Budi Nugroho, dan Z. Panjaitan, “Implementasi Digital Signature Pada E-Invoice Di Uniqa Digital Invitation Menggunakan Algoritma SHA-256 (Secure Hash Algorithm-256) Dan RSA (Rivest Shamir Adleman),” Jurnal CyberTech, vol. x. No.x, 2019, [Daring]. Tersedia pada: https://ojs.trigunadharma.ac.id/

[11] S. H. Hung dkk., “Micrography QR Codes,” IEEE Trans Vis Comput Graph, vol. 26, no. 9, hlm. 2834–2847, Sep 2020, doi: 10.1109/TVCG.2019.2896895.
[12] J. Dermawan Ikhsan, “Implementasi Algoritma RSA dan Hash SHA-256 untuk Tanda Tangan Digital dalam Membangkitkan Kode QR Akses Masuk Kampus.”
[13] Y. S. Fatmala, A. Kusyanti, dan M. Data, “Implementasi Algoritme Speck untuk Enkripsi dan Dekripsi pada QR Code,” 2018. [Daring]. Tersedia pada: http://j-ptiik.ub.ac.id
[14] D. Husnaa Dhiyaulhaq dan S. Armandiva Usman, “Comparative Performance of Digital Signature Security Using Cryptography AES 192 BIT and RSA 512 BIT Algorithm Model,” Journal of Advances in Information Systems and Technology, vol. 2, no. 2, 2020, [Daring]. Tersedia pada: https://journal.unnes.ac.id/sju/index.php/jaist
[15] D. Bansal, M. Tech Scholar, M. Sharma, dan A. Mishra, “Analysis of Digital Signature based Algorithm for Authentication and Privacy in Digital Data,” Int J Comput Appl, vol. 161, no. 5, hlm. 975–8887, 2017, doi: 10.1007/s13389.
[16] P. P. Bandung dan P. Praktisi, “Kedudukan Hukum Tanda Tangan Elektronik Yane Mayasari.”
[17] M. H. Khairinif dan Z. Aidi, “KAJIAN YURIDIS KEKUATAN SERTIFIKAT ELEKTRONIK SEBAGAI ALAT BUKTI DALAM PENYELESAIAN PERKARA PERDATA DI PENGADILAN NEGERI,” 2022.
[18] M. Badrul, “PENERAPAN METODE WATERFALL UNTUK PERANCANGAN SISTEM INFORMASI INVENTORY PADA TOKO KERAMIK BINTANG TERANG,” vol. 8, no. 2, 2021.
[19] Y. Dwi Wijaya dan M. Wardah Astuti, “PENGUJIAN BLACKBOX SISTEM INFORMASI PENILAIAN KINERJA KARYAWAN PT INKA (PERSERO) BERBASIS EQUIVALENCE PARTITIONS BLACKBOX TESTING OF PT INKA (PERSERO) EMPLOYEE PERFORMANCE ASSESSMENT INFORMATION SYSTEM BASED ON EQUIVALENCE PARTITIONS,” Jurnal Digital Teknologi Informasi, vol. 4, hlm. 2021.