JIKTEKS : Jurnal Ilmu Komputer dan Teknologi Informasi
Vol. 04, No. 03, Agustus 2026, hlm. 92 - 103
ISSN : 2986-5417
DOI : doi.org/10.70404/jikteks.v4i03.680
Laman Jurnal: jurnal.faatuatua.com/index.php/JIKTEKS

Implementasi Sistem Verifikasi Keaslian Ijazah Berbasis Tanda Tangan Digital Menggunakan RSA dan SHA-256

Ainus Sya'adah[1*], Yusnia Budiarti[2], Aprillia Ayu Fadhilah[3], Elvita Febrianti[4], Fadillah Akbar[5], Rangga Adi Saputra[6], Rio Singgih Daniswara[7]

[1*, 2, 3, 4, 5, 6, 7]Teknologi Informasi, Universitas Bina Sarana Informatika, DKI Jakarta, Indonesia.
e-mail: [1*]ainusaicc@gmail.com, [2]yusnia.ybi@bsi.ac.id, [3]17230876@bsi.ac.id, [4]17230566@bsi.ac.id , [5]17231037@bsi.ac.id, [6]17231165@bsi.ac.id, [7]17230551@bsi.ac.id

Keywords:

Digital Diploma;
Digital Signature;
Document Verification;
RSA;
SHA-256.

ABSTRACT

The digitalization of academic documents has improved the efficiency of educational data management but has also increased the risk of document forgery and unauthorized modification, particularly for diploma documents in Portable Document Format (PDF). Therefore, a security mechanism is required to ensure document authenticity and integrity in digital environments. This study aims to implement a diploma authenticity verification system based on digital signatures using the Rivest-Shamir-Adleman (RSA) algorithm and Secure Hash Algorithm 256 (SHA-256). The research employed an experimental-implementation approach consisting of problem identification, literature review, system design, implementation, testing, and result analysis. During the digital signature generation process, the PDF document is processed using SHA-256 to produce a hash value, which is then signed using an RSA private key and stored in a signature file with a .sig extension. The verification process is performed by recalculating the document hash and comparing it with the hash value obtained from signature verification using the RSA public key. The testing results demonstrate that the system successfully validates authentic documents, detects modified documents, rejects mismatched signature files, and handles invalid file formats appropriately. Therefore, the combination of RSA and SHA-256 is proven effective in maintaining the integrity and authenticity of digital diploma documents and can be utilized as a practical solution for electronic academic document verification.

Kata Kunci:

Ijazah Digital;
RSA;
SHA-256;
Tanda Tangan Digital;
Verifikasi Dokumen.

ABSTRAK

Digitalisasi dokumen akademik telah meningkatkan efisiensi pengelolaan data pendidikan, namun juga menimbulkan risiko pemalsuan dan manipulasi dokumen, khususnya ijazah dalam format Portable Document Format (PDF). Oleh karena itu, diperlukan mekanisme keamanan yang mampu menjamin keaslian dan integritas dokumen secara digital. Penelitian ini bertujuan untuk mengimplementasikan sistem verifikasi keaslian ijazah berbasis tanda tangan digital menggunakan kombinasi algoritma Rivest-Shamir-Adleman (RSA) dan Secure Hash Algorithm 256 (SHA-256). Metode penelitian yang digunakan adalah pendekatan eksperimental-implementatif yang meliputi identifikasi masalah, studi literatur, perancangan sistem, implementasi, pengujian, dan analisis hasil. Pada tahap pembentukan tanda tangan digital, dokumen PDF diproses menggunakan SHA-256 untuk menghasilkan nilai hash, kemudian hash tersebut ditandatangani menggunakan kunci privat RSA dan disimpan dalam berkas signature berekstensi .sig. Proses verifikasi dilakukan dengan menghitung ulang nilai hash dokumen dan membandingkannya dengan nilai hash hasil verifikasi signature menggunakan kunci publik RSA. Hasil pengujian menunjukkan bahwa sistem mampu mengenali dokumen asli, mendeteksi dokumen yang telah dimodifikasi, menolak penggunaan signature yang tidak sesuai, serta menangani file dengan format yang tidak valid. Dengan demikian, kombinasi RSA dan SHA-256 terbukti efektif dalam menjaga integritas dan keaslian dokumen ijazah digital serta dapat diterapkan sebagai solusi verifikasi dokumen akademik secara elektronik.

Korespondensi Penulis *):

Ainus Sya'adah
Universitas Bina Sarana Informatika
Jl. Kramat Raya No.98, Kwitang, Kec. Senen, Jakarta Pusat, DKI Jakarta 10450

Diajukan: 13-06-2026 | Direvisi: 24-06-2026 | Diterima: 05-07-2026 | Diterbitkan: 14-07-2026

1. PENDAHULUAN

Perkembangan teknologi informasi yang masif di era transformasi digital telah mendorong institusi pendidikan tinggi untuk mengadopsi sistem administrasi tanpa kertas *(paperless system).* Transformasi dokumen fisik ke dalam format digital, seperti *Portable Document Format (PDF)*, memudahkan institusi pendidikan dalam mendistribusikan dokumen penting melalui berbagai media komunikasi elektronik. Namun, fleksibilitas dokumen digital juga menimbulkan tantangan pada aspek keamanan, khususnya yang berkaitan dengan integritas data dan autentikasi dokumen. Dokumen akademik digital rentan terhadap berbagai ancaman, seperti modifikasi tanpa izin, penyadapan, pencegatan data, serta pemalsuan dokumen oleh pihak yang tidak bertanggung jawab untuk kepentingan tertentu. Oleh karena itu, penerapan mekanisme pengamanan berbasis kriptografi yang andal menjadi sangat penting untuk menjaga kerahasiaan, keutuhan, dan keabsahan dokumen di lingkungan digital [1][2].

Fenomena yang terjadi di lapangan menunjukkan bahwa ijazah merupakan salah satu dokumen akademik yang paling sering menjadi sasaran manipulasi, duplikasi, dan pemalsuan [3]. Ijazah memiliki nilai hukum dan ekonomi yang tinggi sebagai bukti resmi kelulusan seseorang sehingga keasliannya harus senantiasa terjamin [4]. Dalam praktiknya, banyak instansi maupun perusahaan yang masih memerlukan waktu cukup lama untuk melakukan verifikasi keaslian ijazah secara manual karena proses tersebut umumnya hanya mengandalkan hasil pemindaian tanda tangan basah atau cap stempel fisik. Metode semi-manual semacam ini memiliki tingkat keamanan yang rendah karena hasil pemindaian tanda tangan dapat dengan mudah disalin dan ditempelkan pada dokumen palsu menggunakan perangkat lunak pengolah gambar [5]. Kerentanan tersebut dapat menimbulkan sengketa hukum, kerugian finansial, serta menurunkan kredibilitas institusi pendidikan akibat beredarnya ijazah palsu yang sulit dibedakan dari ijazah asli secara visual.

Berbagai penelitian sebelumnya telah berupaya mengatasi permasalahan tersebut melalui penerapan teknologi tanda tangan digital. Salah satu penelitian menerapkan tanda tangan digital pada faktur elektronik dengan memanfaatkan kombinasi fungsi hash SHA-256 dan algoritma kunci publik RSA [6]. Penelitian lain mengembangkan sistem pengamanan Surat Keterangan Lulus (SKL) menggunakan kombinasi SHA-256 dan RSA yang terintegrasi dengan kode Respons Cepat (QR Code) [4]. Selain itu, terdapat penelitian yang menerapkan kombinasi RSA dan *Advanced Encryption Standard (AES)* untuk mengamankan sertifikat elektronik [7]. Meskipun berbagai pendekatan tersebut berhasil mendeteksi perubahan pada dokumen, masih terdapat kesenjangan penelitian yang perlu diperhatikan. Sebagian besar penelitian terdahulu hanya berfokus pada proses enkripsi ringkasan pesan tanpa memberikan perhatian yang memadai terhadap keamanan penyimpanan kunci privat milik penandatanganan. Apabila kunci privat disimpan dalam bentuk teks biasa pada perangkat lokal, pihak yang berhasil memperoleh akses tidak sah terhadap sistem dapat menyalahgunakan kunci tersebut untuk membuat tanda tangan digital palsu yang tampak sah tanpa mengubah integritas dokumen [3]. Selain itu, sebagian besar penelitian hanya menilai performa sistem berdasarkan kecepatan proses, tanpa melakukan pengukuran lebih mendalam terhadap aspek efek longsoran (avalanche effect) dan tingkat entropi untuk menilai ketahanan terhadap analisis frekuensi.

Untuk mengatasi kesenjangan penelitian tersebut, penelitian ini menawarkan implementasi sistem verifikasi keaslian ijazah berbasis tanda tangan digital dengan mengombinasikan algoritma RSA dan fungsi hash SHA-256. Kebaruan penelitian ini terletak pada penerapan arsitektur keamanan yang tidak hanya berfokus pada pembentukan tanda tangan digital dari ringkasan dokumen ijazah, tetapi juga mendukung proses validasi dokumen melalui pemanfaatan berkas tanda tangan eksternal. Dalam prosesnya, fungsi hash SHA-256 digunakan untuk menghasilkan ringkasan pesan sepanjang 256 bit yang unik dari isi dokumen ijazah. Ringkasan pesan tersebut kemudian dienkripsi menggunakan kunci privat RSA milik institusi untuk menghasilkan berkas tanda tangan digital berekstensi .sig. Sistem ini dikembangkan dalam bentuk aplikasi berbasis web yang memungkinkan proses verifikasi dokumen dilakukan secara cepat, akurat, dan tanpa mengubah tampilan visual dokumen akademik asli.

Berdasarkan latar belakang tersebut, permasalahan utama yang dirumuskan dalam penelitian ini adalah bagaimana mengimplementasikan kombinasi algoritma RSA dan fungsi hash SHA-256 ke dalam sistem berbasis web untuk mengamankan dokumen ijazah digital. Selain itu, penelitian ini juga mengkaji efektivitas sistem yang dikembangkan dalam mendeteksi manipulasi atau ketidaksesuaian data pada dokumen ijazah berformat PDF [1]. Sejalan dengan rumusan masalah tersebut, tujuan utama penelitian ini adalah merancang dan membangun sistem tanda tangan digital menggunakan kombinasi algoritma RSA dan fungsi hash SHA-256 untuk mengamankan dokumen ijazah akademik. Tujuan berikutnya adalah menguji dan menganalisis kemampuan sistem dalam memvalidasi keaslian dokumen serta mendeteksi setiap bentuk perubahan yang tidak sah pada berkas ijazah berformat PDF [4]. Selain itu, penelitian ini juga bertujuan mengukur kinerja dan efisiensi waktu komputasi yang dibutuhkan dalam proses pembangkitan serta verifikasi tanda tangan digital pada berbagai ukuran berkas PDF [1].

Secara teoretis, penelitian ini diharapkan dapat memberikan kontribusi ilmiah bagi perkembangan ilmu pengetahuan di bidang teknologi informasi, khususnya pada bidang keamanan komputer dan kriptografi modern. Penelitian ini memperkaya kajian mengenai integrasi dan implementasi fungsi hash SHA-256 serta algoritma RSA dalam proses autentikasi dokumen akademik digital. Selain itu, hasil analisis terhadap parameter kinerja komputasi

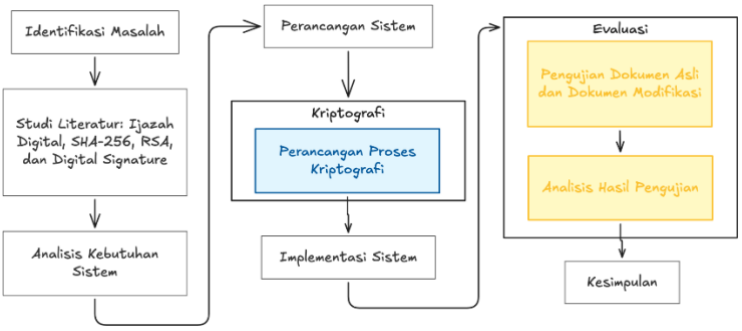
dapat menjadi referensi bagi penelitian selanjutnya yang berfokus pada pengembangan sistem tanda tangan digital maupun penerapan teknologi kunci publik pada berbagai jenis dokumen elektronik.

Secara praktis, penelitian ini diharapkan dapat memberikan solusi bagi institusi pendidikan dalam menyediakan sistem verifikasi ijazah yang aman sehingga mampu melindungi reputasi institusi dari permasalahan pemalsuan dokumen kelulusan. Bagi masyarakat dan dunia industri, sistem ini dapat mempermudah proses verifikasi keaslian ijazah secara mandiri, cepat, dan akurat tanpa memerlukan proses korespondensi manual yang memakan waktu antarlembaga. Sementara itu, bagi pembuat kebijakan, hasil penelitian ini dapat dijadikan sebagai bahan pertimbangan dalam penyusunan standar keamanan dokumen elektronik serta penerapan tanda tangan elektronik di lingkungan pendidikan guna menekan angka pemalsuan dokumen akademik di Indonesia.

2. METODE PENELITIAN

2.1 Desain Penelitian

Penelitian ini menerapkan pendekatan eksperimental-implementatif yang terstruktur untuk merancang, membangun, dan menguji sistem verifikasi keaslian ijazah digital dengan menerapkan algoritma SHA-256 dan RSA. Tahapan penelitian disusun agar proses pengembangan sistem dapat dilakukan secara terarah, mulai dari identifikasi masalah hingga analisis hasil pengujian. Alur penelitian ditunjukkan pada Gambar 1.



Gambar 1. Alur Penelitian

Tahap pertama adalah identifikasi masalah, yaitu mengamati permasalahan terkait keaslian dokumen ijazah digital yang dapat mengalami perubahan atau modifikasi setelah diterbitkan. Tahap kedua adalah studi literatur, yaitu mengumpulkan referensi yang berkaitan dengan tanda tangan digital, fungsi hash SHA-256, algoritma RSA, serta penelitian terdahulu mengenai verifikasi dokumen digital. Studi literatur digunakan untuk memahami konsep dasar integritas dokumen, proses pembentukan nilai hash, proses enkripsi hash, dan mekanisme verifikasi menggunakan pasangan kunci RSA. Tahap ketiga adalah perancangan sistem, yaitu menyusun alur kerja sistem verifikasi keaslian ijazah. Perancangan dilakukan dengan menentukan proses utama yang akan dibangun, yaitu proses pembentukan tanda tangan digital dan proses verifikasi dokumen. Tahap keempat adalah implementasi sistem, yaitu membangun sistem berdasarkan rancangan yang telah dibuat. Sistem dibuat dengan fitur utama berupa unggah file PDF, unggah file signature .sig, serta proses pengecekan status dokumen. Tahap kelima adalah pengujian sistem. Pengujian dilakukan dengan beberapa skenario, yaitu menggunakan dokumen asli, dokumen yang telah dimodifikasi, signature asli, dan signature yang tidak sesuai. Pengujian ini bertujuan untuk mengetahui apakah sistem dapat membedakan dokumen yang asli dan dokumen yang telah mengalami perubahan. Tahap terakhir adalah analisis hasil, yaitu membandingkan hasil verifikasi dari setiap skenario pengujian. Dokumen dinyatakan valid apabila nilai hash dari PDF yang diuji sama dengan nilai hash hasil dekripsi file signature. Sebaliknya, dokumen dinyatakan tidak valid apabila kedua nilai hash tersebut berbeda.

2.2 Objek Data dan Penelitian

Objek dalam penelitian ini adalah dokumen ijazah digital dalam format PDF dan file tanda tangan digital dengan ekstensi .sig. File PDF digunakan sebagai dokumen utama yang akan diverifikasi keasliannya, sedangkan file .sig digunakan sebagai hasil enkripsi nilai hash dari dokumen PDF asli. Kedua file tersebut menjadi pasangan data yang digunakan dalam proses verifikasi. Data utama yang digunakan dalam penelitian ini terdiri dari dua jenis, yaitu data dokumen dan data dokumen uji. Data dokumen asli merupakan file PDF ijazah yang belum mengalami perubahan setelah proses pembentukan tanda tangan digital. File ini digunakan sebagai sumber awal untuk menghasilkan nilai hash menggunakan SHA-256. Nilai hash tersebut kemudian dienkripsi menggunakan RSA dan disimpan ke dalam file signature .sig [8].

Untuk memperkuat pemrosesan data di atas, objek-objek digital tersebut diolah menggunakan parameter Kriptografi. Kriptografi merupakan cabang ilmu matematika dan komputer yang mempelajari teknik-teknik untuk mengamankan data serta pesan, guna menjamin aspek kerahasiaan *(confidentiality)*, integritas data *(data integrity)*, serta autentikasi *(authentication)* [9]. Dalam menjamin integritas objek dokumen ijazah digital, diterapkan fungsi SHA-256 *(Secure Hash Algorithm 256)*. SHA-256 adalah sebuah fungsi hash kriptografi searah *(one-way*

cryptographic hash function) yang menerima masukan data dengan ukuran acak dan mentransformasikannya menjadi keluaran nilai unuk (message digest) berupa string sepanjang 256 bit [10]. Sifat khas SHA-256 yang sangat peka terhadap perubahan data sekecil satu bit sekalipun *(avalanche effect)* menjadikannya standar ideal untuk mendeteksi keaslian isi file PDF ijazah [8].

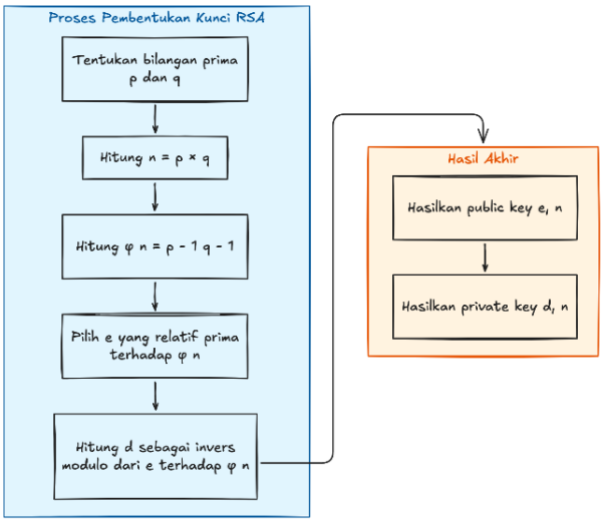
Selanjutnya, untuk mengamankan nilai hash tersebut, digunakan algoritma kriptografi kunci publik atau asimetris yang dikenal sebagai RSA (Rivest-Shamir-Adleman). RSA merupakan algoritma kriptografi asimetris yang beroperasi menggunakan sepasang kunci matematis yang berbeda, yakni kunci privat *(private key)* yang dipegang oleh institusi untuk mengenkripsi nilai hash (membuat tanda tangan digital) dan kunci publik *(public key)* yang disebarkan secara bebas untuk proses dekripsi (verifikasi tanda tangan digital) [11]. Kekuatan keamanan algoritma RSA bertumpu pada tingkat kesulitan komputasi dalam memfaktorkan perkalian dua bilangan prima yang berukuran sangat besar [12]. Kombinasi kedua metode kriptografi ini secara teoretis melahirkan struktur digital signature yang kuat dan valid untuk mengamankan objek data dalam penelitian ini.

2.3 Prosedur Penelitian

Prosedur penelitian dilakukan untuk menghasilkan sistem verifikasi keaslian ijazah digital menggunakan kombinasi algoritma RSA dan SHA-256. Tahapan penelitian dimulai dari pembentukan pasangan kunci RSA, proses pembentukan tanda tangan digital, hingga proses verifikasi dokumen.

2.3.1 Pembentukan Kunci RSA

Proses pembentukan pasangan kunci dikendalikan melalui komponen antarmuka Streamlit pada panel "Manajemen Kunci RSA". Operasi ini diperlukan untuk menghasilkan kunci privat institusi untuk mengamankan proses penyegelan ijazah, serta kunci publik institusi yang diekspor untuk didistribusikan secara terbuka pada proses pembuktian keaslian berkas oleh pihak ketiga [13].



Gambar 1. Alur Pembentukan Kunci RSA

Langkah operasional pertama adalah melakukan pemilihan dua bilangan prima acak berukuran besar yang bersifat rahasia, yang disimbolkan sebagai variabel p dan q. Setelah kedua bilangan prima tersebut ditetapkan, sistem akan melakukan operasi perkalian aritmatika untuk menghitung nilai modulus RSA (n) dengan rumus sebagai berikut:

$$n = p \times q \qquad (1)$$

Nilai modulus (n) ini mendefiniskan panjang bit kunci (2048-bit) yang akan membatasi ruang numerik pada saat kalkulasi modular eksponensial dilakukan. Tahap sekuensial berikutnya sesuai dengan blok proses pada diagram alir adalah menghitung nilai fungsi totient Euler atau fungsi phi (n). Komponen ini dihitung dengan mengacu pada persamaan matematika berikut:

$$\varphi\,(n) = (p-1) \times (q-1) \qquad (2)$$

Setelah variabel (n) didapatkan, sistem melangkah ke tahap penentuan eksponen publik (e). Karakteristik nilai e yang dipilih harus berupa bilangan bulat yang relatif prima terhadap (n), di mana relasi pembatas keduanya diatur melalui kondisi matematis berikut:

$$1 < e < \varphi\,(n) \; dan \; FPB\big(e, \varphi(n)\big) = 1 \; (3)$$

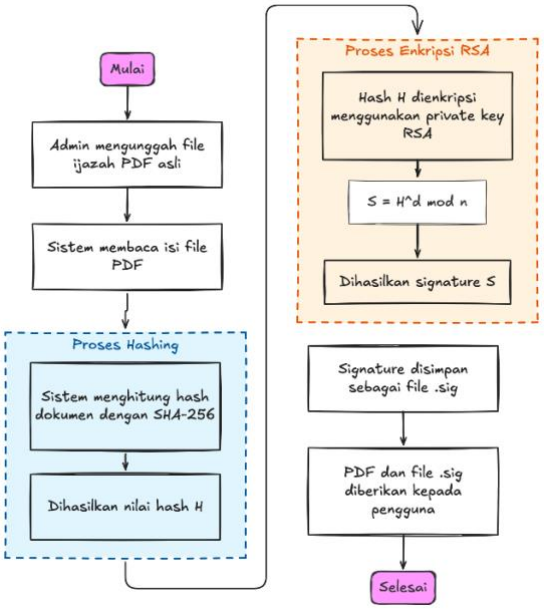
Nilai eksponen publik menggunakan bilangan prima Fermat e = 65537 untuk mengoptimalkan kecepatan proses verifikasi tanpa mengorbankan kekuatan enkripsi. Langkah komputasi terakhir adalah mencari eksponen privat (d). Komponen kunci rahasia ini diperoleh melalui perhitungan invers multiplikatif dari eksponen publik (e) terhadap modulo φ (n), yang secara sistematis dituliskan dalam kongruensi berikut:

$$d = e^{-1} mod\ \varphi(n) \qquad (4)$$

Komponen yang memuat parameter rahasia (p,q,d) diekspor ke dalam direktori lokal dengan nama berkas private.pem. Komponen publik yang berisi parameter (n,e) diekstraksi ke dalam berkas terpisah bernama public.pem.

2.3.2 Pembentukan Tanda Tangan Digital

Pada tahap ini, sistem menghasilkan sebuah tanda tangan digital yang berfungsi sebagai bukti keaslian dokumen sekaligus menjamin bahwa isi dokumen tidak mengalami perubahan setelah diterbitkan [14]. Pembentukan tanda tangan digital dilakukan melalui dua tahapan kriptografi. Tahapan pertama adalah proses hashing menggunakan algoritma SHA-256, algoritma ini membaca seluruh isi berkas PDF dan mengubahnya menjadi sebuah nilai hash berupa karakter sepanjang 256 bit yang unik. Tahap kedua, yaitu proses enkripsi menggunakan algoritma RSA. Nilai hash yang telah diperoleh tidak langsung disimpan, melainkan dienkripsi menggunakan kunci privat (private key) milik institusi penerbit ijazah. Hasil enkripsi tersebut kemudian menjadi tanda tangan digital (digital signature) yang akan disematkan atau dikaitkan dengan dokumen PDF.



Gambar 2. Alur Pembentukan Tanda Tangan Digital

a. Pembentukan nilai Hash (*hashing*)
Proses dimulai ketika sistem menerima dokumen ijazah asli yang direpresentasikan sebagai pesan (M). Dokumen tersebut kemudian diproses menggunakan fungsi hash SHA-256 untuk menghasilkan nilai message digest (H). Proses tersebut dinyatakan sebagai berikut:

$$H = SHA - 256(M) \qquad (5)$$

Keterangan:
H = nilai hash dokumen
M = dokumen PDF Ijazah

Fungsi SHA-256 bekerja dengan memetakan berkas dokumen berukuran apa pun menjadi sebuah untaian string unik sepanjang 256-bit (64 karakter heksadesimal). Melalui pemrosesan modul biner pada aplikasi, berkas (M) memproduksi nilai hash seperti diatas. Nilai hash berfungsi sebagai sidik jari digital dokumen. Sifat searah (one-way) dari algoritma SHA-256 menjamin bahwa data nilai hash tidak dapat dikembalikan lagi untuk membentuk dokumen asli, namun sangat sensitif terhadap perubahan sekecil apapun pada struktur berkas ijazah.

b. Enkripsi Hash Menggunakan RSA
Setelah nilai H terbentuk, tahap selanjutnya adalah melakukan operasi enkripsi asimetris. Nilai hash dokumen (H) ditandatangani secara digital dengan cara dipangkatkan terhadap eksponen kunci privat RSA milik institusi

(d) dan dihitung sisa pembagiannya terhadap nilai modulus (n). Rumus penandatanganan digital RSA sebagai berikut:

$$S = H^d (mod\ n) \qquad (6)$$

Keterangan:
S = tanda tangan digital (signature)
H = nilai hash dokumen
d = kunci privat RSA
n = modulus RSA

Untuk mempermudah pemahaman logika kalkulasi dari formula di atas, disimulasikan contoh perhitungan menggunakan parameter di bawah ini:

1) Diasumsikan nilai prima penyusun kunci p = 7 dan q = 13
2) Maka nilai modulus RSA n = p q = 7 13 = 91
3) Nilai totient Euler φ(n) = (7-1) (13-1) = 6 12 =72
4) Dipilih eksponen publik e = 5
5) Dihitung eksponen privat d = 29 (karena (29 5) (mod 72) = 1)

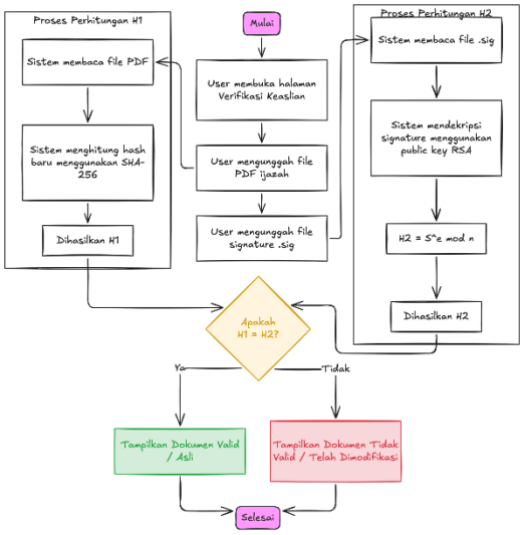
Apabila potongan nilai hash asli (H) direpresentasikan ke dalam bentuk nilai angka sederhana yaitu 48, maka substitusi angka-angka tersebut ke dalam formula enkripsi tanda tangan digital menghasilkan operasi matematika berikut:

$$S = H^d\ (mod\ n)$$
$$S = 48^{29}\ (mod\ 91)$$
$$S = 55$$

Nilai angka 55 inilah yang menjadi kode tanda tangan digital kriptografis dari dokumen ijazah. Pada implementasi sistem yang sesungguhnya, nilai tanda tangan biner hasil enkripsi asimetris standar pkcs1_15. Pembuatan tanda tangan digital dilakukan setelah file ijazah PDF asli tersedia. Tujuan dari proses ini adalah menghasilkan file signature .sig yang menjadi bukti kriptografis dari dokumen asli. File signature tersebut nantinya digunakan pada proses verifikasi untuk menentukan apakah dokumen PDF yang diuji masih sama dengan dokumen asli.

2.3.3 Verifikasi Keaslian Dokumen

Proses verifikasi tanda tangan digital merupakan mekanisme kriptografi yang bertujuan untuk membuktikan keaslian *(authenticity)* sumber dokumen sekaligus memastikan integritas data dokumen ijazah yang diuji. Sistem melakukan pemeriksaan terhadap berkas PDF ijazah yang direpresentasikan sebagai (M') untuk menentukan apakah dokumen benar-benar berasal dari institusi penerbit dan tidak mengalami perubahan setelah proses penandatanganan digital dilakukan.



Gambar 3 Alur Verifikasi Keaslian Dokumen

Proses verifikasi keaslian ijazah dilakukan dengan membandingkan nilai hash dari dokumen PDF yang diuji dengan nilai hash hasil dekripsi file signature. Pada tahap ini, pengguna mengunggah file PDF ijazah dan file signature .sig melalui halaman verifikasi. Sistem kemudian melakukan dua proses utama, yaitu menghitung ulang nilai hash dari file PDF dan mendekripsi file signature menggunakan kunci publik RSA. Tahap pertama adalah menghitung nilai hash dari file PDF yang diuji menggunakan algoritma SHA-256. Proses tersebut dapat dituliskan sebagai berikut.

$$H1 = SHA - 256(M') \quad (7)$$

Keterangan:
H1 = nilai hash dokumen yang diuji
M'= dokumen PDF hasil unggahan

Tahap kedua adalah mendekripsi file signature menggunakan kunci publik RSA. Signature yang sebelumnya dihasilkan dari proses enkripsi hash dokumen asli akan dikembalikan menjadi nilai hash. Proses dekripsi signature dapat dituliskan sebagai berikut.

$$H2 = S^e \ mod \ n \quad (8)$$

Keterangan:
H2 = hash hasil verifikasi signature
S = tanda tangan digital
e = kunci publik RSA
n = modulus RSA

Guna membuktikan validitas matematis dari formula dekripsi di atas,diimplementasikan pengujian lanjutan menggunakan parameter numerik, di mana:

1) Modulus RSA (n) = 91
2) Eksponen publik (e) = 5
3) Nilai Tanda Tangan (S) hasil ekstraksi = 55

$$H2 \ = \ 55\text{^}\ 5 \ (mod \ 91)$$
$$H2 \ = \ 503.284.375 \ (mod \ 91)$$
$$H2 \ = \ 48$$

Setelah nilai H_1 dan H_2 diperoleh, sistem melakukan proses perbandingan. Jika nilai H_1 sama dengan H_2, maka dokumen dinyatakan valid karena hash dokumen yang diuji sesuai dengan hash dokumen asli yang tersimpan dalam signature. Sebaliknya, jika nilai H_1 berbeda dengan H_2, maka dokumen dinyatakan tidak valid karena terdapat perbedaan antara dokumen yang diuji dan dokumen asli.

$$H1 = H2 \quad (9)$$

Sebaliknya, apabila:

$$H1 \neq H2 \quad (10)$$

Maka dokumen dinyatakan tidak valid karena telah mengalami perubahan atau menggunakan file signature yang tidak sesuai.

2.4 Prosedur Pengujian

Pengujian sistem dilakukan untuk memastikan bahwa seluruh fungsi pada sistem verifikasi keaslian ijazah digital dapat berjalan sesuai dengan kebutuhan yang telah ditetapkan. Metode pengujian yang digunakan dalam penelitian ini adalah *Black-Box Testing,* yaitu metode pengujian yang berfokus pada pengujian sistem berdasarkan masukan (*input*) dan keluaran (*output*) tanpa memperhatikan struktur kode program yang digunakan.

Pengujian dilakukan terhadap fitur-fitur utama yang terdapat pada sistem, meliputi proses autentikasi administrator, pembangkitan kunci RSA, pembentukan tanda tangan digital, serta verifikasi keaslian dokumen ijazah. Setiap fitur diuji menggunakan beberapa skenario masukan untuk mengetahui apakah sistem mampu menghasilkan keluaran yang sesuai dengan rancangan sistem. Pada proses verifikasi dokumen, pengujian dilakukan menggunakan beberapa skenario. Pengujian ini bertujuan untuk mengetahui kemampuan sistem dalam menjaga integritas dokumen dan mendeteksi perubahan yang tidak sah pada berkas digital.

Hasil pengujian kemudian dibandingkan dengan hasil yang diharapkan pada setiap skenario. Sistem dinyatakan berhasil apabila keluaran yang dihasilkan sesuai dengan tujuan fungsional masing-masing fitur. Seluruh hasil pengujian selanjutnya dianalisis untuk mengevaluasi tingkat keberhasilan implementasi algoritma RSA dan SHA-256 dalam proses verifikasi keaslian dokumen ijazah.

3. HASIL DAN ANALISIS

3.1 Gambaran Umum Sistem

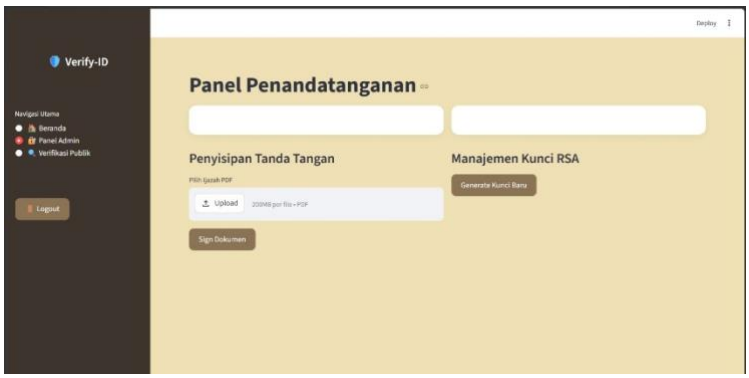
Sistem yang dibangun pada penelitian ini merupakan sistem verifikasi keaslian ijazah digital berbasis tanda tangan digital. Sistem ini dirancang untuk memeriksa apakah file ijazah dalam format PDF masih sama dengan dokumen asli yang telah ditandatangani secara digital. Proses verifikasi dilakukan dengan memanfaatkan nilai hash dokumen dan file signature yang menjadi pasangan dari dokumen tersebut [15][16]. Secara umum, sistem memiliki dua proses utama, yaitu proses pembuatan tanda tangan digital dan proses verifikasi keaslian ijazah. Proses pembuatan tanda tangan digital dilakukan terhadap file PDF ijazah asli. File tersebut diproses menggunakan algoritma SHA-256 untuk menghasilkan nilai hash. Nilai hash yang dihasilkan kemudian dienkripsi menggunakan algoritma RSA sehingga membentuk file tanda tangan digital dengan ekstensi .sig [17].

Aplikasi ini dibangun menggunakan bahasa pemrograman Python dengan kerangka kerja Streamlit sebagai fondasi antarmuka web, serta diperkuat oleh pustaka PyCryptodome untuk komputasi kriptografi dan pustaka pypdf untuk manipulasi objek berkas. Verify-ID diwujudkan ke dalam bentuk platform web interaktif modern yang membagi seluruh fungsionalitas sistem ke dalam dua halaman operasional utama pada bilah navigasi sidebar, yaitu menu "Panel Admin" dan menu "Verifikasi Publik". Pembagian halaman ini merepresentasikan pemisahan hak akses antara otoritas penerbit dokumen dan masyarakat luas sebagai penguji dokumen.

Halaman "Panel Admin" dikunci oleh sebuah gate autentikasi berupa kecocokan nama pengguna (username) dan kata sandi (password) untuk mengamankan kunci privat dari manipulasi pihak luar. Di dalam halaman admin ini, sistem menyediakan dua panel kontrol utama. Panel pertama adalah panel penandatanganan dokumen yang menyediakan fitur seret dan letakkan (drag and drop file uploader) untuk memproses berkas ijazah asli, memicu fungsi pengkodean tanda tangan digital di latar belakang, dan menyediakan tombol unduh berkas PDF yang telah tersegel oleh Base64. Panel kedua adalah panel manajemen kunci RSA yang menyediakan tombol interaktif untuk melakukan regenerasi pasangan kunci baru apabila terjadi kebocoran kode keamanan. Sementara itu, halaman "Verifikasi Publik" disediakan secara terbuka tanpa autentikasi log masuk untuk memudahkan pihak ketiga (seperti lembaga perusahaan) melakukan pengujian keaslian ijazah secara mandiri. Pengguna hanya perlu mengunggah berkas PDF ijazah yang ingin diuji ke dalam kotak file uploader. Sistem yang telah terimplementasi akan langsung mengeksekusi fungsi pembacaan / ekstraksi metadata.

3.2 Implementasi Pembentukan Kunci RSA

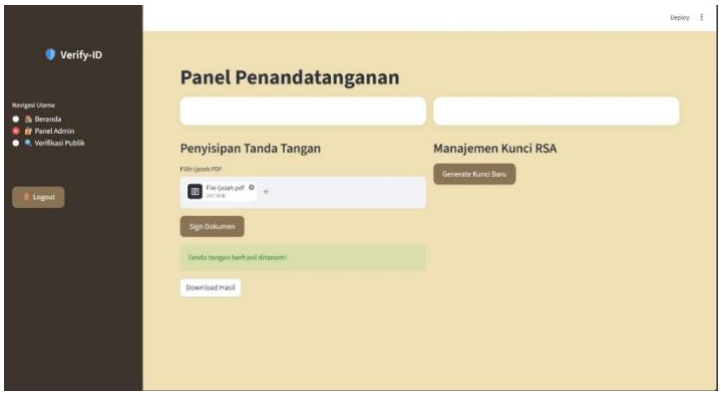
Implementasi pembentukan pasangan kunci RSA dilakukan melalui fitur manajemen kunci yang hanya dapat diakses oleh administrator. Fitur ini digunakan untuk menghasilkan pasangan kunci yang terdiri dari kunci privat (private key) dan kunci publik (public key) yang digunakan pada proses penandatanganan dan verifikasi dokumen. Ketika administrator menekan tombol Generate Kunci Baru, sistem secara otomatis membentuk pasangan kunci RSA 2048-bit dan menyimpannya ke dalam dua berkas, yaitu private.pem dan public.pem. Kunci privat digunakan untuk membuat tanda tangan digital, sedangkan kunci publik digunakan dalam proses verifikasi keaslian dokumen oleh pengguna.



Gambar 4 Halaman Manajemen Kunci RSA

3.3 Implementasi Pembentukan Tanda Tangan Digital

Proses pembentukan tanda tangan digital dilakukan pada halaman administrator setelah dokumen ijazah dalam format PDF berhasil diunggah ke sistem. Sistem kemudian melakukan proses hashing menggunakan algoritma SHA-256 dan menghasilkan nilai hash yang merepresentasikan identitas unik dokumen. Nilai hash yang dihasilkan selanjutnya diproses menggunakan kunci privat RSA sehingga menghasilkan tanda tangan digital yang disimpan dalam file berekstensi .sig. File signature tersebut menjadi bukti autentikasi dokumen dan digunakan pada tahap verifikasi.

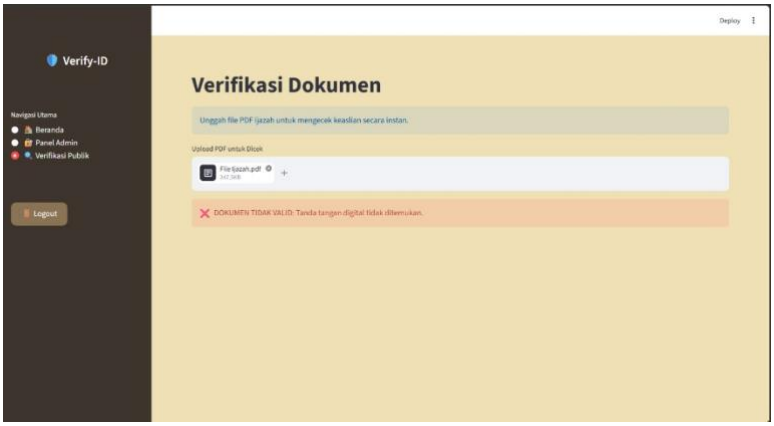


Gambar 5 Halaman Penandatanganan Dokumen

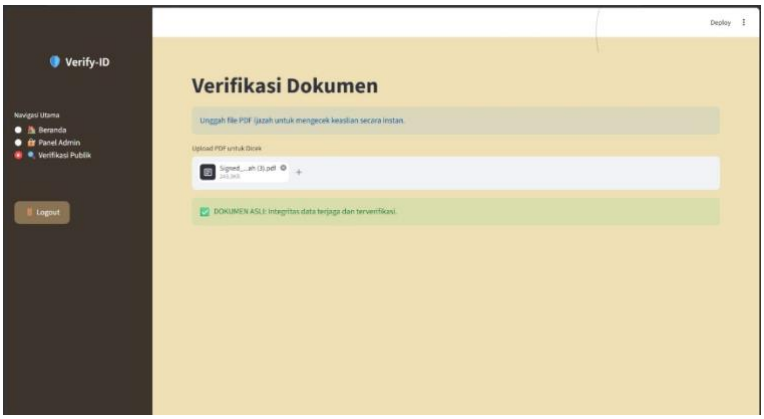
3.4 Implementasi Verifikasi Keaslian Ijazah

Implementasi verifikasi dilakukan melalui halaman verifikasi publik yang dapat diakses tanpa proses autentikasi. Pada halaman ini pengguna diminta mengunggah dokumen PDF dan file signature yang sesuai. Setelah kedua file diterima, sistem menghitung ulang nilai hash dokumen menggunakan SHA-256. Selanjutnya file signature diverifikasi menggunakan kunci publik RSA. Sistem kemudian membandingkan hasil verifikasi signature dengan nilai hash dokumen yang baru dihitung.

Apabila kedua nilai hash identik, sistem menampilkan status Valid yang menunjukkan bahwa dokumen tidak mengalami perubahan sejak proses penandatanganan dilakukan. Sebaliknya, apabila ditemukan perbedaan nilai hash, sistem menampilkan status Tidak Valid yang menandakan adanya perubahan isi dokumen atau penggunaan file signature yang tidak sesuai.



Gambar 6 Halaman Dokumen Tidak Valid



Gambar 8 Halaman Verifikasi Dokumen Valid

3.5 Implementasi Antarmuka Sistem

Implementasi sistem merupakan tahap pembuktian visual yang menunjukkan hasil transformasi dari seluruh rancangan arsitektur, diagram alir, dan formula matematika ke dalam bentuk sistem. Sistem Verify-ID diimplementasikan berbasis web menggunakan bahasa pemrograman Python dan kerangka kerja Streamlit. Bagian ini

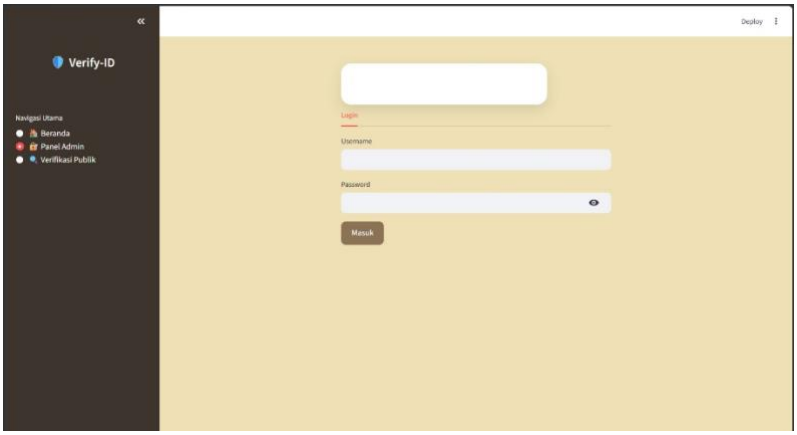
memaparkan bentuk nyata antarmuka aplikasi serta cara pengguna berinteraksi dengan fungsionalitas sistem yang terbagi ke dalam beberapa halaman operasional.

3.5.1 Halaman Utama Sistem

Gambar 9 Halaman Utama Sistem

Pada halaman ini, pengguna dapat memilih menu yang tersedia melalui side bar navigasi. Sistem membagi hak akses menjadi dua bagian utama, yaitu Panel Admin dan Verifikasi Publik. Pembagian tersebut bertujuan untuk memisahkan proses penandatanganan dokumen yang bersifat rahasia dengan proses verifikasi yang dapat diakses oleh pihak umum.

3.5.2 Halaman Login Administrator



Gambar 10 Halaman Login Admin

Digunakan sebagai mekanisme autentikasi sebelum administrator dapat mengakses fitur penandatanganan dokumen dan manajemen kunci RSA. Pengguna diwajibkan memasukkan username dan password yang valid untuk menjaga keamanan kunci privat RSA dari akses yang tidak sah.

3.6 Hasil Pengujian Fungsionalitas *(Black-Box Testing)*

Pengujian fungsionalitas dilakukan menggunakan metode *Black-Box Testing* untuk memastikan bahwa setiap fitur pada sistem verifikasi keaslian ijazah digital dapat berfungsi sesuai dengan kebutuhan yang telah ditetapkan. Pengujian dilakukan dengan memberikan berbagai masukan (input) pada sistem dan mengamati keluaran (output) yang dihasilkan tanpa memperhatikan struktur kode program yang digunakan. Fitur yang diuji meliputi proses autentikasi administrator, pembangkitan pasangan kunci RSA, pembentukan tanda tangan digital, serta verifikasi keaslian dokumen ijazah. Selain itu, pengujian juga dilakukan terhadap dokumen yang telah dimodifikasi untuk mengetahui kemampuan sistem dalam mendeteksi perubahan isi dokumen.

Hasil pengujian fungsionalitas ditunjukkan pada Tabel 1

Tabel 1. Pengujian Black-Box Testing

No	Komponen / menu	Skenario Pengujian	Masukan (input)	Harapan Hasil	Hasil Aktual Sistem	Status
1	Gerbang Autentikasi	Menguji respons sistem terhadap masukan kredensial admin yang salah	Username: salah Password: 123	Sistem menolak akses dan menampilkan pesan peringatan merah	Muncul notifikasi kesalahan "Username atau Password salah"	Sesuai /Lolos
2	Gerbang Autentikasi	Menguji respons sistem terhadap masukan kredensial admin yang benar	Username: admin Password: admin123	Sistem meloloskan autentikasi dan mengalihkan halaman ke dashboard admin	Mengalihkan halaman ke menu internal otoritas admin	Sesuai /Lolos
3	Manajemen Kunci RSA	Menguji fungsi regenerasi pasangan kunci kriptografi baru pada peladen.	Penekanan tombol "Generate Kunci Baru"	Sistem membuat berkas private.pem & public.pem baru dan memberikan pesan sukses hijau.	Berkas kunci diperbarui di direktori root peladen dan muncul bar hijau sukses.	Sesuai /Lolos
4	Penandatanganan Dokumen	Menguji proses penyegelan berkas ijazah asli kelulusan mahasiswa.	Mengunggah file ijazah_asli.pdf dan mengeklik tombol penandatanganan.	Sistem memproses hash SHA-256, enkripsi privat RSA, dan mengaktifkan tombol unduh berkas.	Struktur objek metadata /Subject terisi string Base64 dan tombol unduh aktif.	Sesuai /Lolos
5	Verifikasi Publik	Menguji pembuktian validitas terhadap berkas dokumen ijazah yang asli.	Mengunggah file PDF ijazah yang telah dibubuhi tanda tangan digital.	Sistem mengekstrak metadata, mendekripsi hash, dan menampilkan status valid berlatar hijau.	Layar menampilkan kotak indikator hijau bertuliskan "Dokumen Valid"	Sesuai /Lolos
6	Verifikasi Publik	Menguji deteksi manipulasi komponen isi data teks pada berkas ijazah	Mengunggah file PDF ijazah yang disunting melalui aplikasi editor eksternal	Sistem mendeteksi ketidakcocokan nilai hash dan memunculkan status gagal berlatar merah	Layar menampilkan indikator merah bertuliskan "Dokumen Tidak Valid"	Sesuai /Lolos

Berdasarkan hasil pengujian yang telah dilakukan, seluruh skenario pengujian memperoleh status sesuai/lolos. Sistem berhasil menolak akses ketika pengguna memasukkan kredensial yang tidak valid dan memberikan akses ketika kredensial yang digunakan sesuai. Fitur pembangkitan kunci RSA mampu menghasilkan pasangan kunci baru sesuai dengan kebutuhan sistem, sedangkan fitur penandatanganan dokumen berhasil menghasilkan tanda tangan digital yang dapat digunakan pada proses verifikasi. Pada proses verifikasi dokumen, sistem mampu mengidentifikasi dokumen asli sebagai dokumen yang valid dan menolak dokumen yang telah mengalami perubahan setelah proses penandatanganan dilakukan. Hasil tersebut menunjukkan bahwa seluruh fungsi utama sistem telah berjalan sesuai dengan spesifikasi yang dirancang.

4. KESIMPULAN

Penelitian ini berhasil mengimplementasikan sistem verifikasi keaslian ijazah digital berbasis tanda tangan digital menggunakan algoritma RSA dan SHA-256. Algoritma SHA-256 digunakan untuk menghasilkan nilai hash yang merepresentasikan identitas unik dokumen, sedangkan algoritma RSA digunakan dalam proses pembentukan dan verifikasi tanda tangan digital. Integrasi kedua algoritma tersebut memungkinkan sistem untuk menjamin integritas dokumen sekaligus memvalidasi keaslian dokumen yang diverifikasi.

Berdasarkan hasil pengujian fungsionalitas menggunakan metode Black-Box Testing, seluruh fitur sistem dapat berjalan sesuai dengan kebutuhan yang telah ditetapkan. Sistem mampu melakukan autentikasi administrator, menghasilkan pasangan kunci RSA, membentuk tanda tangan digital, serta melakukan verifikasi dokumen dengan

baik. Selain itu, sistem juga mampu mendeteksi perubahan pada dokumen maupun ketidaksesuaian antara dokumen dan file tanda tangan digital yang digunakan dalam proses verifikasi.

Kontribusi penelitian ini terletak pada penerapan mekanisme verifikasi ijazah digital berbasis web yang memanfaatkan kombinasi algoritma RSA dan SHA-256 untuk meningkatkan keamanan dokumen akademik. Sistem yang dibangun dapat menjadi alternatif solusi dalam mendukung proses validasi keaslian ijazah secara lebih cepat, mudah, dan terpercaya dibandingkan metode pemeriksaan manual.

Meskipun demikian, penelitian ini masih memiliki keterbatasan karena pengujian yang dilakukan hanya berfokus pada aspek fungsionalitas sistem dan belum mencakup analisis performa, skalabilitas, maupun pengujian keamanan terhadap berbagai jenis serangan kriptografi. Oleh karena itu, penelitian selanjutnya dapat mengembangkan sistem dengan menambahkan fitur manajemen sertifikat digital, integrasi kode QR untuk verifikasi publik, serta melakukan pengujian performa dan keamanan yang lebih komprehensif guna meningkatkan keandalan sistem dalam lingkungan penggunaan yang lebih luas.

REFERENSI

[1] G. R. Mulyawan and Asmunin, “Penerapan Tanda Tangan Digital Menggunakan Algoritma RSA Dan SHA 256 Dengan QR Code Pada Sertifikat Elektronik,” pp. 1–11, 2024.

[2] R. K. Hondro, “Modifikasi Platform Kunci Algoritma Playfair Untuk Meningkatkan Nilai Confusion Pada Ciphertext,” *J. Comput. Syst. Inform. JoSYC*, vol. 1, no. 2, pp. 76–82, Feb. 2020.

[3] A. Aryasanti, M. Hardjianto, and ..., “Implementasi Tanda Tangan Digital Menggunakan Algoritme RSA dan SHA-512 Berbasis Web,” *... Inf. ...*, vol. 10, pp. 181–186, 2022.

[4] J. Hutagalung, P. S. Ramadhan, and S. J. Sihombing, “Keamanan Data Menggunakan Secure Hashing Algorithm (SHA)-256 dan Rivest Shamir Adleman (RSA) pada Digital Signature,” *J. Teknol. Inf. Dan Ilmu Komput.*, vol. 10, no. 6, pp. 1213–1222, 2023, doi: 10.25126/jtiik.2023107319.

[5] S. F. R. Syahfira Chairunnisa Lubis, Khairi Ibnutama, “Implementasi Digital Signature Pada Faktur Dengan,” vol. 5, pp. 112–124, 2022.

[6] F. M. Rangkuti, N. Budi Nugroho, and 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),” *J. CyberTech*, vol. x. No.x, no. x, 2019.

[7] F. Nuraeni, S. Tinggi, T. Garut, and D. Kurniadi, “Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik Academic Information System View project Educational Data Mining View project,” pp. 43–52, 2020.

[8] Rada Petrata Barus, Mhd. Gilang Suryanata, Deski Helsa Pane, and A. Alhaifz, “Penerapan Tanda Tangan Digital Mengunakan Algoritma SHA - 256 Dan RSA Untuk Pengamanan Surat Perintah Perjalanan Dinas Di Desa Namo Rambe,” *J. Sist. Inf. Triguna Dharma JURSI TGD*, vol. 4, no. 4, pp. 881–892, 2025, doi: 10.53513/jursi.v4i4.10313.

[9] A. M. Ajif, F. Nuraeni, D. Kurniadi, and R. Elsen, “Implementasi Modul Tanda Tangan Digital dengan Superenkripsi RSA-ECDSA dan SHA-512 Pada Sistem Informasi Akademik Sekolah,” *J. Algoritma*, vol. 22, no. 2, 2025, doi: 10.33364/algoritma/v.22-2.2353.

[10] A. E. Okeyinka, O. Alao, B. Gbadamosi, R. O. Ogundokun, and R. Oluwaseun, “Application of SHA-256 in formulation of digital signatures of RSA and Elgamal cryptosystems,” *Oper. Res. Inf. Eng.*, vol. 1, no. 2, pp. 61–66, 2018.

[11] J. Dermawan Ikhsan, “Implementasi Algoritma RSA dan Hash SHA-256 untuk Tanda Tangan Digital dalam Membangkitkan Kode QR Akses Masuk Kampus,” pp. 2–3, 2021.

[12] M. T. Adithia, N. Elianora, and M. Veronica, “Document Verification And Authentication By Using Password Based Qr Code Signature With Rsa 2048 , Aes Encryption , And Sha-256,” vol. 7, no. 2, pp. 1981–1996, 2026.

[13] A. G. Prawiyogi, R. Rahman, A. Sastromiharjo, S. Sulistiawati, and Q. Aini, “Ontologi Blockchain Pada Karya Tulis Puisi Di Pendidikan Sekolah Dasar : Metode Merkle Root,” *CSRID Comput. Sci. Res. Its Dev. J.*, vol. 13, no. 1, p. 23, 2021, doi: 10.22303/csrid.13.1.2021.24-34.

[14] O. Yosefyius, P. Naibaho, N. Budi Nugroho, N. Yanti, and L. Gaol, “Penerapan Digital Signature Menggunakan Metode DSA Untuk Verifikasi Surat Keterangan Keaslian Ijazah Di SMA RK Swasta Lubuk Pakam,” *J. CyberTech*, vol. 4, no. 5, 2021.

[15] T. Abdurrachman and B. R. Suteja, “Pengembangan Sistem Informasi Asosiasi Jasa Konstruksi dengan Menerapkan Tanda Tangan Digital,” *J. Tek. Inform. Dan Sist. Inf.*, vol. 7, no. 1, pp. 261–273, 2021, doi: 10.28932/jutisi.v7i1.3431.

[16] D. Safira and R. K. Hondro, “Pemeringkatan Algoritma Kriptografi Ringan untuk Keamanan Perangkat IoT Menggunakan Simple Additive Weighting,” *Bimantara J. Artif. Intell.*, vol. 1, no. 01, pp. 01–10, Jan. 2026, doi: 10.70404/1g4k6w77.

[17] I. I. J. Rifka Alkhilyatul Ma’rifat, I Made Suraharta, “No Title 済無No Title No Title No Title,” vol. 2, pp. 306–312, 2024.