Pengujian Integritas File Operasi Tanda Tangan Digital Menggunakan Kombinasi Hash MD5, RSA dan Skema Qr-Cod

By julian supardi

WORD COUNT 4105
TIME SUBMITTED 04-MAY-2023 12:14PM
PAPER ID 99353474

Pengujian Integritas File Operasi Tanda Tangan Digital Menggunakan Kombinasi Hash MD5, RSA dan Skema Qr-Cod

Hafiz Mursid[1*], Julian Supardi[2], M. Qurhanul Rizkie[3]
Teknik Informatika, Universitas Sriwijaya
Prodi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Sriwijaya[1,2,3]
Hafizmursiddd@gmail.com

***Abstrak*- Kebijakan WFH pada masa pandemi COVID-19 mengakibatkan berbagai dokumen yang awalnya masih menggunakan sistem manual beralih ke sistem digital termasuk pada pengesahan pada dokumen tersebut. Maka penerapan tanda tangan digital dapat dijadikan alternatif sebagai bukti autentik sebuah dokumen untuk menggantikan tanda tangan konvensional. Penelitian ini bertujuan untuk mengembangkan perangkat lunak guna melakukan pengujian integritas dokumen dengan tanda tangan digital yang dibangun menggunakan fungsi hash MD5 dan algoritma RSA yang kemudian di-*generate* menjadi Qr-Code pada dokumen yang terdiri dari 1000 kata dengan ekstensi .docx. Dokumen yang akan diuji tersebut diberikan tanda tangan digital dengan perangkat lunak yang dibangun dan selanjutnya dilakukan pengujian integritas dengan melakukan operasi modifikasi terhadap file teks tersebut. Pada penelitian ini telah dibuat perangkat lunak untuk menerapkan skema autentikasi pada sebuah dokumen. Dari hasil penelitian yang dilakukan maka dapat disimpulkan jika fungsi hash MD5 dan algoritma RSA yang digenerate menjadi Qr-Code dapat diimplementasikan dengan baik untuk operasi tanda tangan digital.**

Kata Kunci—Tanda Tangan digital, MD5, RSA, Or-Code

I. PENDAHULUAN

Wabah pandemi COVID-19 yang mulai masuk pada awal 2020 di Indonesia mengharuskan minimnya pertemuan langsung diadakan oleh masyarakat. Pemerintah mengeluarkan kebijakan agar diadakannya pekerjaan dari rumah atau Work From Home (WFH) untuk mengurangi dan mencegah penyeberan COVID-19. Dengan adanya kebijakan WFH maka berbagai dokumen yang awalnya masih menggunakan sistem manual beralih ke sistem digital termasuk pada pengesahan pada dokumen tersebut.

Kehadiran teknologi informasi dan komunikasi dapat dijadikan solusi pada permasalahan diatas dikarenakan sifatnya yang tidak terbatas ruang dan waktu [1]. Penggunaan tanda tangan yang dipakai pada dokumen elektronik ini biasa dikenal dengan tanda tangan digital. Dengan kehadiran tanda tangan digital, sebuah dokumen tidak perlu diprint out namun tetap dapat diverifikasi pengirimnya, ini dikarena keaslian isi file teks yang ditandatangani dapat dipertahankan dan dipertanggungjawabkan oleh pengirim.

Tanda tangan digital ialah prosedur yang digunakan sebagai pengganti tanda tangan konvensional yang dapat digunakan sebagai autentikasi pada dokumen digital[2] Proses pembuatan tanda tangan digital sendiri dapat dilakukan dengan dua cara yakni: melakukan enkripsi langsung pada pesan atau melakukan pembangkitan nilai *hash* pada pesan.

Pada penelitian ini akan dibangun tanda tangan digital dengan menerapkan skema Qr-Code yang didapatkan dari hasil generate fungsi hash MD5 dan Algoritma RSA. Fungsi hash MD5 dapat digunakan untuk proses autentikasi dan integritas, dimana hasilnya tidak dapat dikembalikan lagi. Proses ini akan menghasilkan keluaran dengan panjang 32 karakter yang umumnya digunakan untuk memeriksa integritas sebuah file [3]. Kemudian hasil hash dari proses sebelumnya akan dilanjutkan dengan enkripsi menggunakan Algoritma RSA. Algoritma RSA dipilih dikarenakan memiliki tingkat keamanan yang tinggi. Akan tetapi hasil dari kedua kombinasi algortima di atas akan menampilkan *chipertext* yang berupa susunan huruf atau angka acak. Maka dilakukan penyederhanaan dengan mengadopsi skema Qr-Code yang nantinya akan disisipkan pada dokumen yang hendak ditandatangani.

II. TINJAUAN PUSTAKA

A. Kriptografi

Kriptografi ialah ilmu mengenai teknik enkripsi dimana “naskah asli” (*plaintext*) diacak menggunakan kunci *enkripsi* menjadi “naskah acak yang sulit dibaca” (*ciphertext*) oleh orang lain yang tidak memiliki kunci deskripsi [4]. Kriptografi ini memecahkan masalah dengan menggunakan sebuah kunci yang digunakan saat enkripsi dan dekripsi [5].

Didalam kriptografi terdapat dua teknik pengenkripsian yakni kriptografi kunci simetris dan

[*] Presentasi terbaik kedua dalam SNASIKOM 2 yang diselenggarakan LLDIKTI wilayah 2 bekerjasama dengan Universitas Sumatera Selatan

kriptografi kunci asimetris. Teknik enkripsi kunci simetris ialah teknik yang didalam proses enkripsi dan proses dekripsi menggunakan kunci yang sama. Sedangkan teknik kriptografi kunci asimetris ialah kunci yang digunakan untuk proses enkripsi dan proses dekripsi memiliki perbedaan. Proses teknik enkripsi dalam pendistribusian kunci publik pada enkripsi asimetris lebih mudah dan tidak memerlukan saluran khusus dibandingkan dengan enkripsi simetris.

Ada beberapa aspek keamanan pada kriptografi yang harus dipenuhi, aspek tersebut yakni: Kerahasiaan (confidentiality), Autentikasi (*authentication*), Integritas (*integrity*), wewenang (*authority*), pribadi (*privacy*), hak akses (*access control*), (*availability*) dan Nir-penyangkalan (*nonrepudiation*) (Gunadhi et al., 2017).

B. Tanda Tangan Digital

Tanda tangan digital ialah suatu prosedur yang digunakan sebagai pengganti tanda tangan konvensional, hal ini digunakan sebagai autentikasi pada pesan [2]. Di Indonesia sendiri, tanda tangan digital telah diatur dan tertera dalam Undang-Undang Nomor 11 Tahun 2008 Pasal 11 ayat 1 tentang Informasi dan Transaksi Elektronik (UU ITE). Tanda tangan digital juga tertera pada Peraturan Pemerintah Nomor 82 Tahun 2012 Pasal 52 ayat 1 dan 2 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Pemberian tanda tangan digital pada sebuah dokumen dapat dilakukan dalam dua cara yakni:

1. Melakukan enkripsi pada pesan
   Pesan yang akan diberikan tanda tangan dilakukan enkripsi dengan algoritma simetri. Pesan yang telah dienkripsi sudah dapat dinyatakan bahwa pesan tersebut telah ditandatangani.
2. Tanda tangan digital dibangkitkan dari nilai *hash* dari pesan.
   Nilai *hash* merupakan kode singkat dan ringkas yang dibangkitkan dari nilai pesan. Tanda tangan digital memiliki fungsi layaknya tanda tangan pada dokumen fisik yakni disisipkan pada pesan. Cara seperti ini dapat digunakan saat pesan tidak diperlukan enkripsi secara keseluruhan, sebab yang diperlukan hanya autentikasi [7].

C. *Fungsi Hash MD5*

Fungsi *hash* adalah fungsi yang digunakan untuk mengkompresi pesan dengan ukuran panjang teks sembarang menjadi *message-digest* yang berukuran tetap. Biasanya ukuran panjang keluaran jauh lebih kecil daripada ukuran pesan awal. Fungsi *hash* MD5 *(Message Digest 5)* ialah fungsi *hash* yang menghasilkan keluaran dengan panjang 32 karakter atau 128-bit yang umumnya digunakan untuk memeriksa integritas sebuah file [3].

Pembuatan *message digest* secara garis besar terdiri dari beberapa tahapan yakni: pesan diberikan penambahan bit pengganjal, selanjutnya diberikan penambahan berdasarkan nilai panjang pesan awal, dilakukan inisialisasi penyangga MD dan yang terakhit dilakukan pengolahan pesan dalam blok berukuran 512 bit [2]

D. *Algoritma RSA*

Algoritma *RSA* pertama kali dikenalkan pada 1977 oleh tiga orang peneliti dari MIT *(Massachussets Institute of Technology)*. Algoritma RSA memiliki keunggulan pada sukarnya memfaktorkan bilangan yang besar menjadi faktor primanya. Kunci private diperoleh dari hasil komputasi kombinasi sejumlah bilangan prima dan bilangan kunci publik. Kunci publik dan kunci private yang digunakan pada proses RSA haruslah berupa bilangan bulat. Kunci private didapatkan dengan memfaktorkan bilangan non-prima menjadi faktor primanya. Memfaktorkan bilangan non-prima menjadi faktor prima ini merupakan hal yang sulit. Selain itu algoritma RSA juga memiliki tingkat keamanan yang tinggi. Hal ini karena Algoritma RSA menggunakan pemfaktoran bilangan prima yang besar dalam membangkitkan kuncinya

E. *Qr-Code*

QR-Code dikenalkan oleh Denso Corporation, sebuah perusahan Jepang yang bergerak pada bidang otomotif. Awalnya Qr-code digunakan untuk mengontrol produksi komponen otomotif di perusahaan tersebut. Namun kemudian, penerapan QR-Code meluas di *bidang* lain, penggunaannya telah banyak digunakan dalam aplikasi komersial.

Kapasitas data yang dapat disimpan didalam Qr-code cukup besar apabila dibandingkan matriks kode yang lain. Qr-code ini dapat menampung 4.296 data alphanumerik, 7.089 data numerik, serta 2.953 data biner. Qr-code juga memiliki keunggulan pada dukungan kecepatan pengkodean dan ukuran cetak yang relatif kecil dan sederhana. Selain itu Qr-Code mampu memperbaiki kesalahan sampai dengan 30% sehingga cukup tahan terhadap kerusakan [8].

F. Penelitian yang relevan

Penelitian ini terkait dengan penggunaan tanda tangan digital, beberapa penelitian yang terkait dengan dengan proses autentikasi dan integritas untuk pengamanan suatu dokumen, antara lain:

1. Pengembangan Metode Otentikasi Keaslian Ijasah dengan Memanfaatkan Gambar Qr Code [9]. Pada penelitian ini penulis menggunakan data dari alumni yang kemudian diolah sehingga menghasilkan output berupa Qr-Code. Hasil

penelitian mendapat kesimpulan bahwasanya Qr-Code dapat menampung informasi dari alumni yang memiliki ijazah serta dapat digunakan untuk memverifikasi ijazah dengan cepat dan akurat.

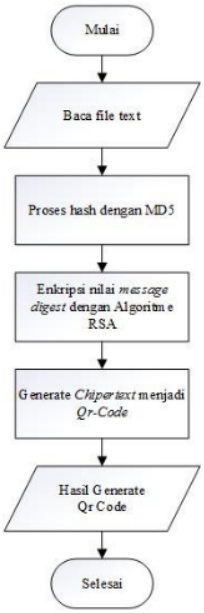
2. Implementasi Quick Response Code Dalam Deteksi Pendistribusian Dokumen Ujian Nasional [8]. Penelitian ini memanfaatkan penambahan Qr-Code pada box distribusi ujian nasional untuk mengamankan dan mencegah terjadinya kecurangan penggandaan dokumen ujian nasional. Hasil dari penelitian ini menunjukkan penyisipan QR code pada box pendistribusian ujian nasional dapat memberikan keamanan pada saat pendistribusian.
3. Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital [10]. Penelitian ini menerapkan algoritma RSA dalam menghasilkan tanda tangan digital. Hasil dari penelitian ini menunjukkan penggunaan algoritma kriptografi RSA dapat menjamin keamanan dari dokumen yang ditandatangani.
4. Aplikasi Tanda Tangan Digital (*Digital Signature*) Menggunakan Algoritma Message Digest 5 (MD5) [11]. Penelitian membangun aplikasi tanda tangan digital menggunakan algoritma MD5 dan menggunakan bahasa pemrograman visual basic studio. Pesan yang disisipkan tanda tangan ialah surat pemberitahuan dan surat penagihan. Penelitian ini memberikan kesimpulan penggunaan algoritma MD5 untuk keperluan tanda tangan digital dapat membantu memebrikan jamianan keamanan pada dokumen digital yang ditanda tangani.
5. A Comparative Analysis of SHA and MD5 Algorithm [12]. Penelitian ini melakukan perbandingan eksekusi diantara algoritma SHA dan algoritma MD5. Penelitian ini mendapat kesimpulan bahwas waktu eksekusi dari MD5 lebih cepat dibandingkan dengan algoritma SHA pada perangkat 32 bit. Meskipun disisi lain algortima SHA dibuktikan memiliki keamanan yang lebih bagus.
6. Perbandingan Kriptografi Menggunakan Algoritma Data Encryption Standart (DES) dan Algoritma Rivest Shamir Adleman (RSA) untuk Keamanan Data [13]. Penelitian ini melakukan perbandingan kriptografi pada algoritma *data encryption standart* (DES) dan algoritma *rivest shamir adleman* (RSA) untuk keamanan data. Dari penelitian ini memberikan kesimpulan bahwa kecepatan enkripsi dan dekripsi menggunakan algoritma RSA akan lebih cepat dibandingkan dengan penggunaan algoritma DES. Meskipun penelitian ini menyebutkan tingkat keamanan DES lebih baik dikarenakan perhitungan pada algoritma ini lebih rumit dan lit.
7. Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital sebagai Alternatif Pengesahan Dokumen di Masa Pandemi [1]. Penelitian ini melakukan review dan perbandingan pada beberapa *literature* yang berkaitan dengan autentikasi pada dokumen elektronik yang disisipkan tanda tangan digital. Hasil dari penelitian ini menyatakan penggunaan skema *Digital Signature Algorithm* dengan pemanfaatan sertifikat digital cocok untuk digunakan. Selain itu juga dapat dilkaukan penyematan Qr-Code dengan menggunakan skema berbasis *Software as a Service* pada dokumen.
8. Penggunaan QR Code dengan Enkripsi Vigenere Cipher dalam Pengamanan Data [14]. Pada penelitian ini menggunakan Qr-Code yang didapat dari enkripsi Vigenere Cipher untuk pengamanan pada sebuah data. Kemampuan penggunaan Qr-Code untuk mengoreksi kesalahan yang beri modifikasi dengan enkripsi Vigenere Cipher dapat membantu dan mempermudah dalam mengamankan data.
9. Sistem Validasi Keaslian Dokumen Digital Berbasis Qr-Code [15]. Penelitian ini melakukan pembuatan sistem yang menerapkan Qr-Code yang disisipkan pada dokumen digital, selanjutnya dilakukan verifikasi pada Qr-Code untuk mengetahui keaslian dari dokumen tersebut. Hasil dari penelitian menyatakan Qr-Code dapat digunakan sebagai tanda tangan digital untuk mengetahui validasi dari sebuah dokumen sehingga dapat meminimalisir potensi pemalsuan dokumen.
10. Desain dan Implementasi Mekanisme Tanda Tangan Dijital dalam Pertukaran Data dengan Hash MD5 dan Enkripsi/Dekripsi Menggunakan Algoritma RSA [16]. Penelitian ini melakukan pembangunan sistem tanda tangan digital untuk melakukan pertukaran data atau informasi dengan menggunakan kombinasi algoritma tersebut. Hasil dari penelitian ini menyatakan fungsi Hash MD5 dan Menggunakan Algoritma RSA 256 telah berhasil dibangun dan diimplementasikan sebagai tanda tangan dalam sebuah informasi dalam bentuk pesan.

III. METODE PENELITIAN

1. Jenis dan Sumber Data
   Jenis data pada penelitian ini adalah data sekunder, dimana teks file yang akan disisipkan tanda tangan

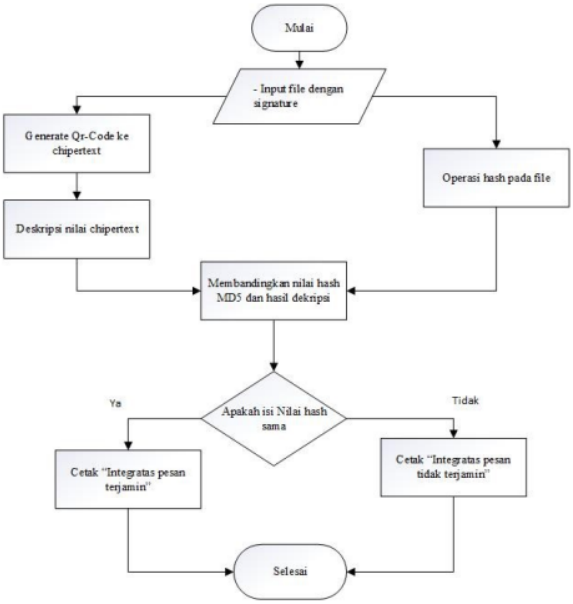
digital berupa pesan teks yang terdiri dari karakter ASCII. Teks didapatkan dari website *http://www.dummytextgenerator.com/ dengan* kata kunci "*lorem ipsum*".

2. Metode Pengumpulan Data
   Data pesan teks di generate dan diunduh dari website berdasarkan jumlah kata yang diinginkan dan menggunakan kata kunci "*Lorem Ipsum*" yang merupakan standar sebuah teks yang tidak terlalu berkonsentrasi pada arti per kalimatnya.
3. Kerangka Kerja Penelitian
   Dalam melakukan proses enkripsi dan dekripsi pada dokumen digital yang akan diberikan tanda tangan digital terdapat dua skenario. Skenario tersebut akan digambarkan dalam bentuk *flowchart.*
   a. Flowchart pembuatan dan penyisipan tanda tangan digital
      Flowchart pembuatan dan penyisipan tanda tangan digital melalui empat tahapan. Tahapan tersebut yakni: melakukan operasi *hash* pada pesan, melakukan enkripsi nilai *hash* pada pesan, dilakukannya pembangkitan Qr-Code dari hasil enkripsi proses sebelumnya, serta melakukan penggabungan file dokumen digital dan tanda tangan digital.



Gambar 1. Kerangka Kerja Pembuatan dan Penyisipan Tanda Tangan Digital

   b. Flowchart melakukan pengujian pada integritas isi file
      Flowchart dalam melakukan pengujian pada integritas isi file melalui empat proses. Proses proses tersebut yakni: melakukan pembacaan pada tanda tangan digital yang berupa Qr Code, melakukan dekripsi pada nilai pembacaan Qr Code sehingga akan didapatkan hasil hash dari tanda tangan, selanjutnya dilakukan operasi hash pada pesan, diakhiri dengan melakukan perbandingan nilai hash pada pesan dan nilai hash pada tanda tangan.



Gambar 2. Kerangka Kerja Pengujian Integritas Isi File

4. Perangkat yang Digunakan dalam Melaksanakan Penelitian
   Dalam melaksanakan penelitian ini digunakan perangkat keras dan perangkat lunak dengan spesifikasinya yakni:
   1. Perangkat Keras
      a. Processor Intel(R) Core(TM) i5-4300U CPU 1.92GHz.
      b. RAM 4 GB.
      c. SSD 256 + HDD 500 GB.
   2. Perangkat Lunak
      a. Sistem Operasi Windows 10 64 bit.
      b. Apache NetBeans 12.6.
      c. Website Dummy Text Generator.
5. Metode pengembangan perangkat lunak
   Metode pengembangan perangkat lunak yang digunakan pada penelitian ini menggunakan pemrograman berorientasi objek dan metode *Relational Unified Process* (RUP). Metode RUP melalui empat proses yakni:
   1. Fase Insepsi
      Pada fase insepsi dilakukan pendefinisian yang dibutuhkan di dalam sistem, termasuk juga user requirement, ruang lingkup serta

kebutuhan fungsional dari perangkat lunak yang akan dikembangkan.

2. Fase Elaborasi
   Fase ini menentukan perencanaan arsitektur sistem, desain komponen dan desain antar muka sesuai dengan analisis pada tahap sebelumnya. User requirement juga dapat diperbaiki dan ditambahkan apabila dinilai belum lengkap pada tahap pengumpulan kebutuhan
3. Fase Konstruksi
   Pada fase ini dilakukan koding. Tahap ini fokus pada pengembangan fitur dan komponen utama dalam sistem. Fase konstruksi ini juga telah menghasilkan produk perangkat lunak.
4. Fase Transisi
   Pada tahap akhir ini fokus pada *deployment* dan instalasi sistem. Pada tahap transisi, pengembangan perangkat lunak telah selesai dilakukan selanjutnya diikuti dengan pengujian sistem, termasuk juga pemeliharaan dan pengujian sistem apakah sudah sesuai dengan pengguna.

IV. HASIL DAN PEMBAHASAN

Berdasarkan dengan uraian dari metode penelitian diatas, maka pada bagian ini akan dijelaskan pembahasan rancangan dari sistem yang akan dibangun.

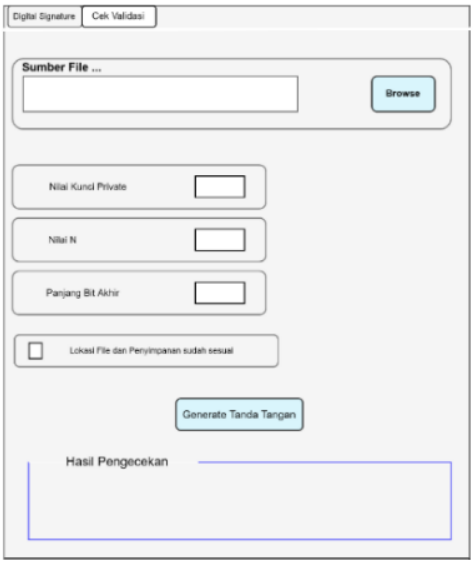
A. Implementasi Perangkat Lunak
   Dari desain yang sudah dirancang pada tahapan sebelumnya kemudian diimplementasikan kedalam bahasa pemrograman Java.

B. Rancangan antarmuka
   Desain dari antarmuka didesain dalam satu kelas utama yakni kelas 'FormUtama' yang di dalamnya terdapat dua halaman, yakni halaman 'Digital Signature' dan 'Cek Validasi'.

1. Antarmuka "Digital Signature"
   Pada halaman 'Digital Signature' terdapat dua tombol browse. Tombol browse yang pertama digunakan untuk memilih file teks yang akan diberikan atau disisipkan tanda tangan sedangkan tombol browse yang kedua digunakan untuk memilih direktori tempat penyimpanan file teks setelah dilakukan tanda tangan digital. Kemudian terdapat textfield yang memiliki fungsi diberikan masukan berupa panjang bit kunci yang akan diberikan untuk penandatanganan.
   Selanjutnya terdapat tempat checkbox yang harus user masukkan, ini digunakan sebagai validasi bahwa user telah memberikan masukan berupa lokasi direktori file yang ingin ditandatangani dan penyimpanan file pasca tanda tangan, serta panjang bit kunci yang ingin digunakan. Terdapat tombol 'Generate Tanda Tangan' yang digunakan untuk melakukan operasi tanda tangan pada file yang sebelumnya dipilih.
   Berikut ini desain dari antarmuka pada halaman Digital Signature

Gambar 3. Tampilan Antarmuka halaman Digital Signature

2. Antarmuka "Cek Validasi"
   Pada halaman 'Cek validasi' terdapat tombol 'Browse'. Tombol ini memiliki fungsi untuk memilih file dokumen yang akan divalidasi tanda tangan di dalamnya. Pada halaman ini terdapat tiga buah textfield, ketiga textfield ini digunakan sebagai tempat masukan kunci private, nilai N dan panjang bit terakhir pada plaintext. Nilai-nilai ini digunakan untuk proses dekripsi.
   Selanjutnya terdapat checkbox yang harus user masukkan, ini digunakan sebagai validasi bahwa pengguna telah memberikan masukan berupa lokasi direktori file yang ingin dicek keasliannya, serta pengguna telah memberikan masukan pada textfield kunci private, nilai N dan panjang bit terakhir pada plaintext. Checkbox ini juga berfungsi untuk mengaktifkan tombol 'Periksa Integritas isi File & Autentikasi Pengirim'. Kemudian terdapat 'Periksa Integritas isi File dan Autentikasi Pengirim' yang berfungsi untuk melakukan operasi pengujian integritas file.
   Berikut ini desain dari antarmuka pada halaman Cek Validasi.

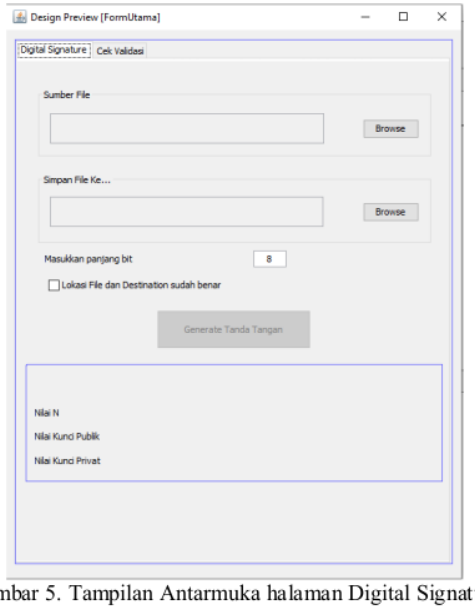


Gambar 4. Tampilan Antarmuka halaman Cek Validasi

C. Implementasi antarmuka

Implementasi antarmuka dilakukan berdasarkan rancangan antarmuka pada tahap pengembangan pada sub bab sebelumnya.

1. Berikut ini implementasi dari antarmuka pada halaman Digital Signature



Gambar 5. Tampilan Antarmuka halaman Digital Signature

2. Berikut ini desain dari antarmuka pada halaman Cek Validasi.

Gambar 5. Tampilan Antarmuka halaman Cek Validasi

D. Kriteria Pengujian

Proses pengambilan keputusan dalam pengujian integritas file teks pada operasi tanda tangan digital dilakukan dengan membandingkan hasil keluaran dari proses hash pada pesan dengan nilai message digest yang didapatkan pada proses deskripsi tanda tangan digital. Adapun kriteria pengujian yang dilakukan pada penelitian ialah keluaran akan dinyatakan integritas isi pesan terjamin dan autentikasi pengirim berhasil jika hasil hash pada pesan yang sudah bertanda tangan dan message digest yang didapatkan pada proses deskripsi tanda tangan digital bernilai sama. Apabila file teks memiliki nilai pesan yang berbeda, maka keluaran akan menyatakan integritas isi pesan dan autentikasi pengirim tidak terjamin.

E. Metode Pengujian Perangkat Lunak

Pengujian dilakukan dengan metode *blackbox*. Metode *blackbox* sendiri ialah sebuah metode yang digunakan untuk menemukan kesalahan dan mendemonstrasikan seluruh fungsionalitas dari aplikasi yang dibangun, apakah sistem dapat menerima input dengan benar dan output yang dihasilkan telah sesuai. Kebutuhan fungsional perangkat lunak sendiri terdiri dari:

1. Perangkat lunak yang dikembangkan dapat membuat file yang bertanda tangan berupa Qr-Code hasil kombinasi fungsi hash MD5 dan algoritma RSA, pada file dengan format atau ekstensi .docx yang sebelumnya telah dipilih.
2. Perangkat lunak dapat melakukan pemeriksaan integritas dan autentikasi pengirim pada dokumen yang sebelumnya ditandatangani.

F. Pengujian Perangkat Lunak

Pada penelitian ini perangkat lunak akan membangkitkan tanda tangan dengan menggabungkan fungsi hash menggunakan fungsi hash MD5 dan algoritma RSA. Hasil enkripsi dengan algoritma RSA tersebut digunakan untuk membangkitkan QR Code yang selanjutnya disisipkan pada file teks dengan ekstensi .docx. Pengujian yang dijalankan dilakukan pada dokumen yang termuat teks dengan panjang 1000 kata. Sedangkan panjang bit bilangan prima, yang digunakan pada operasi penandatanganan dokumen untuk membangkitkan kunci adalah sepanjang 8 bit.

Pengujian ini akan menerapkan pengaplikasian konsep tanda tangan dengan menggabungkan fungsi hash menggunakan fungsi hash MD5. Hasil hash dengan fungsi hash MD5 kemudian dienkripsi dengan algoritma RSA. Hasil enkripsi dengan algoritma RSA tersebut digunakan untuk membangkitkan QR code. File hasil tanda tangan akan disimpan dan dibuatkan file baru dengan format ekstensi .docx yang mana termuat nilai pesan inputan user dan di dalamnya juga termuat Qr-Code dari proses penandatanganan. Selain itu sistem juga membuatkan file berformat ekstensi .txt sebagai tempat menyimpan atribut nilai tanda tangan dengan nama file yang sama dengan file yang sudah ditandatangani.

Masukan yang diberikan pada percobaan ini ialah dokumen sebelum diberikan tanda tangan digital, dokumen setelah diberikan tanda tangan digital terdapat lima skenario percobaan pada penelitian dijelaskan pada tabel dibawah ini:

Tabel 1. Skenario Pengujian Perangkat Lunak

Skenario	Perubahan nilai pesan	Perubahan tanda tangan digital	Perubahan kombinasi kunci
Skenario 1	Tidak	Tidak	Tidak
Skenario 2	Ya	Tidak	Tidak
Skenario 3	Tidak	Ya	Tidak
Skenario 4	Tidak	Tidak	Ya
Skenario 5	Ya	Ya	Ya

G. Hasil Penelitian

Hasil konfigurasi untuk percobaan pada skema 1 yakni tidak dilakukannya perubahan pada nilai file teks, nilai tanda tangan digital, serta kombinasi kunci. Sehingga sistem memberikan pesan "Integritas Isi Pesan dan Autentikasi Pengirimnya Berhasil". Hal ini dikarenakan tidak adanya perubahan yang dilakukan terhadap nilai didalamnya. Integritas pesan dan autentikasi pengirim dinyatakan berhasil dikarenakan hasil *hash* pada pesan memiliki nilai yang sama dengan hasil dekripsi nilai dari QR Code.

Hasil konfigurasi untuk percobaan pada skema 2 sesuai pada tabel 1 yakni dilakukan perubahan pada nilai pesan, sehingga pesan asli sebelum ditandatangani dan pesan setelah diberi tanda tangan memiliki nilai yang berbeda. Sehingga sistem memberikan pesan "Integritas Isi Pesan Tidak Terjamin dan Autentikasi Pengiriman Gagal". Hal ini dikarenakan saat sistem melakukan perbandingan terdapat perbedaan pada hasil *hash* nilai pesan dengan hasil dekripsi nilai dari *QR Code.*

Pada skema ketiga dilakukan perubahan pada *QR Code* yang merupakan tanda tangan digital pada file teks. Hasil skenario ini mengakibatkan saat sistem melakukan perbandingan pada hasil *hash* pesan dengan hasil dekripsi nilai dari *QR Code* terdapat perbedaan. Sehingga sistem memberikan pesan "Integritas Isi Pesan Tidak Terjamin dan Autentikasi Pengiriman Gagal".

Pada skema keempat dilakukan perubahan pada kombinasi kunci yang digunakan untuk melakukan dekripsi pada tanda tangan. Perubahan dilakukan pada nilai kunci *private*, nilai N serta pada panjang bit terakhir. Hasil dari perubahan kombinasi kunci ini mengakibatkan terdapat perbedaan pada hasil *hash* pesan dengan hasil dekripsi nilai dari *QR Code.* Sehingga sistem juga memberikan pesan "Integritas Isi Pesan Tidak Terjamin dan Autentikasi Pengiriman Gagal".

Pada skema terakhir dilakukan perubahan pada isi pesan, nilai tanda tangan serta kombinasi kunci yang digunakan untuk melakukan dekripsi. Hasil dari skenario perubahan kombinasi kunci ini mengakibatkan terdapat perbedaan pada hasil *hash* pesan dengan hasil dekripsi nilai dari *QR Code.* Perbedaan dari kedua variabel tersebut mengakibatkan proses autentikasi gagal dilakukan.

V. KESIMPULAN

Sistem yang dibangun ini hanya dapat melakukan penyisipan pada file dengan ekstensi .docx sehingga pada penelitian selanjutnya dapat dilakukan penyisipan tanda tangan serta melakukan pengujian integritas pada file dengan berbagai jenis format file teks seperti .doc, dotm dan .pdf.

Selain itu sistem yang dibangun tidak mencakup pada pengambilan pada style di dokumen asli sehingga pada penelitian kedepannya dapat dilakukan pengembangan sistem yang dapat mengambil style file yang akan diberi tanda tangan seperti ukuran huruf, warna huruf, jenis huruf serta objek yang ada didalam teks seperti tabel dan gambar. Sehingga format style file asli dan file yang telah ditandatangani autentik.

Penelitian ini telah menghasilkan sistem yang dapat mengimplementasikan *Qr-Code* untuk pengujian integritas isi file teks pada operasi tanda tangan digital menggunakan kombinasi fungsi *hash MD5* dan

algoritma RSA diawali dengan dilakukannya penyisipan tanda tangan digital pada dokumen kemudian dilanjutkan pengujian integritas isi file text. Hasil pengujian integritas file teks yang sebelumnya disisipkan tanda tangan digital *Qr-Code* hasil kombinasi fungsi *hash* MD5 dan algoritma RSA menghasilkan bahwa: Integritas isi file teks dan autentikasi pengirim pada file teks dapat terjamin selama tidak dilakukan perubahan pada isi pesan, *Qr-Code*, ataupun kombinasi kunci untuk deskripsi. Sehingga sistem dapat digunakan untuk penandatanganan dokumen teks sebagai pengganti tanda tangan konvensional.

DAFTAR PUSTAKA

[1] T. Yuniati and M. F. Sidiq, "Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital sebagai Alternatif Pengesahan Dokumen di Masa Pandemi," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 6, 2020, doi: 10.29207/resti.v4i6.2502.

[2] R. Munir, *Kriptografi*, 2nd ed. Bandung: Penerbit Informatika, 2019.

[3] R. Damara Ardy, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5)," *Proceeding 2017 Int. Conf. Smart Cities, Autom. Intell. Comput. Syst. ICON-SONICS 2017*, vol. 2018-Janua, pp. 87–92, 2017, doi: 10.1109/ICON-SONICS.2017.8267827.

[4] D. R. Saragi, J. M. Gultom, J. A. Tampubolon, and I. Gunawan, "Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4," *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 114, 2020, doi: 10.30865/json.v1i2.1745.

[5] O. G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," *Int. J. Sci. Res. Publ.*, vol. 8, no. 7, 2018, doi: 10.29322/ijsrp.8.7.2018.p7978.

[6] E. Gunadhi and A. P. Nugraha, "Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection," *J. Algoritm.*, vol. 13, no. 2, pp. 391–398, 2017, doi: 10.33364/algoritma/v.13-2.391.

[7] O. K. Sulaiman, M. Ihwani, and S. F. Rizki, "Model Keamanan Informasi Berbasis Tanda Tangan Digital Dengan Data Encryption Standard (Des) Algorithm," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 14–19, 2016, doi: 10.30743/infotekjar.v1i1.82.

[8] B. Ramadhanis and H. Yenni, "Implementasi Quick Response Code Dalam Deteksi Pendistribusian Dokumen Ujian Nasional," *SATIN - Sains dan Teknol. Inf.*, vol. 2, no. 1, pp. 31–37, 2016.

[9] E. Ardhianto *et al.*, "Dengan Memanfaatkan Gambar Qr Code," *Pengemb. Metod. OTENTIKASI KEASLIAN IJASAH DENGAN MEMANFAATKAN GAMBAR QR CODE Eka*, vol. 13, pp. 35–41, 2016.

[10] Y. Anshori, A. Y. Erwin Dodu, and D. M. P. Wedananta, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital," *Techno.Com*, vol. 18, no. 2, pp. 110–121, 2019, doi: 10.33633/tc.v18i2.2166.

[11] D. P. Precilia and A. Izzuddin, "Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (MD5)," *Energy*, vol. 5, no. 1, pp. 14–19, 2016.

[12] P. Gupta and S. Kumar, "A Comparative Analysis of SHA and MD5 Algorithm," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 3, pp. 4492–4495, 2014.

[13] A. Hidayat and A. Faizin, "Perbandingan Kriptografi Menggunakan Algoritma Data Encryption Standart (Des) Dan Algoritma Rivest Shamir Adleman (Rsa) Untuk Keamanan Data," *JASIEK (Jurnal Apl. Sains, Informasi, Elektron. dan Komputer)*, vol. 1, no. 2, pp. 143–148, 2019, doi: 10.26905/jasiek.v1i2.3451.

[14] R. Syahdan, E. Anitasari, P. Pendidikan, M. Program Pascasarjana, and U. N. Yogyakarta, "Penggunaan QR Code dengan Enkripsi Vigenere Cipher dalam Pengamanan Data," 2017.

[15] R. K. R, R. F. Sari, and N. Azizah, "Sistem Validasi Keaslian Dokumen Digital Berbasis QR-Code," *J. Teknol. Inf.*, vol. 4, no. 2, pp. 321–327, 2020, doi: 10.36294/jurti.v4i2.1722.

[16] J. B. Sanger, "Desain dan Implementasi Mekanisme Tanda Tangan Dijital Dalam Pertukaran Data Dengan Hash MD5 dan Enkripsi/Dekripsi Menggunakan Algoritma RSA," vol. 12, no. 2, 2018.

Pengujian Integritas File Operasi Tanda Tangan Digital Menggunakan Kombinasi Hash MD5, RSA dan Skema Qr-Cod

ORIGINALITY REPORT

4%
SIMILARITY INDEX

PRIMARY SOURCES

1	jurnal.unprimdn.ac.id Internet	85 words — 2%
2	jurnal.iaii.or.id Internet	77 words — 2%

EXCLUDE QUOTES	OFF	EXCLUDE SOURCES	< 2%
EXCLUDE BIBLIOGRAPHY	ON	EXCLUDE MATCHES	OFF