

**Implementasi Skema *Qr-Code* untuk Pengujian Integritas Isi File
Teks pada Operasi Tanda Tangan Digital Menggunakan
Kombinasi Fungsi *Hash MD5* dan *Algoritma RSA***

Diajukan Sebagai Syarat Untuk Menyelesaikan

Pendidikan Program Strata-1

di Jurusan Teknik Informatika



Oleh:

Hafiz Mursid

09021281722066

Jurusan Teknik Informatika

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2022

LEMBAR PENGESAHAN SKRIPSI

Implementasi Skema *QR-Code* untuk Pengujian Integritas Isi File
Teks pada Operasi Tanda Tangan Digital Menggunakan
Kombinasi Fungsi Hash MD5 dan Algoritma RSA

Oleh:

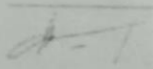
Hafiz Mursid

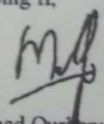
09021281722066

Indralaya, 21 Juli 2022

Pembimbing I

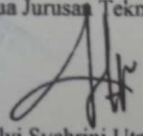
Pembimbing II,


Julian Supardi, M.T.
NIP. 197207102010121001


Muhammad Qurhanul Rizqie, M.T., Ph.D.
NIP. 1671060312870008

Mengetahui,

Ketua Jurusan Teknik Informatika


Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003



TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Rabu tanggal 06 Juli 2022 telah dilaksanakan ujian sidang skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Hafiz Mursid
NIM : 09021281722066
Judul : Implementasi Skema Qr-Code untuk Pengujian Integritas Isi File Teks pada Operasi Tanda Tangan Digital Menggunakan Kombinasi Fungsi Hash MD5 dan Algoritma RSA

dan dinyatakan **LULUS**

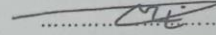
1. Ketua Penguji

Yunita, M.Cs
NIP. 198306062015042002



2. Penguji 1

Osvari Arsalan, M.T.
NIP. 198806282018031001



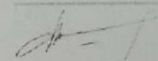
3. Penguji 2

Kanda Januar Miraswan, M.T
NIP. 199001092019031012



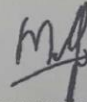
4. Pembimbing 1

Julian Supardi, M.T.
NIP. 197207102010121001



5. Pembimbing 2

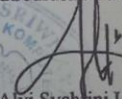
Muhammad Qurhanul Rizqie, M.T.,
Ph.D
NIP. 1671060312870008



Mengetahui,
Ketua Jurusan Teknik Informatika



Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003



HALAMAN PERNYATAAN BEBAS PLAGIAT

Yang bertanda tangan dibawah ini:

Nama : Hafiz Mursid
NIM : 09021281722066
Program Studi : Teknik Informatika Reguler
Judul Skripsi : Implementasi Skema QR-Code untuk Pengujian
Integritas Isi File Teks pada Operasi Tanda Tangan
Digital Menggunakan Kombinasi
Fungsi Hash MD5 dan Algoritma RSA

Hasil Pengecekan Software *iThenticate/Turnitin*: 16%

Menyatakan bahwa laporan proyek saya merupakan hasil karya sendiri dan bukan hasil plagiat. Apabila ditemukan unsur plagiat dalam laporan proyek ini, maka saya bersedia menerima sanksi akademik dari Univeristas Sriwijaya sesuai dengan ketentuan yang berlaku

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun



Palembang, 21 Juli 2022



Hafiz Mursid
NIM. 09021281722066

MOTTO DAN PERSEMBAHAN

MOTTO:

“Aku adalah sebagaimana prasangka hamba-Ku kepada-Ku, Aku bersamanya ketika dia mengingat-Ku”

(Hadist Qudsi: 15)

“Manusia diciptakan bukan untuk meraih kesempurnaan tapi untuk berguna. Maka, lakukanlah kebaikan walaupun tak sempurna dan biarkanlah Allah yang menyempurnakan langkah-langkahmu”

--Anonim--

“There are many aspects of life that we cannot control.”

--Haemin Sunim--

Kupersembahkan Karya Tulis ini kepada:

- Keluargaku Tercinta
- Teman dan Sahabatku
- Fakultas dan Almamater
Kebangganku
- Ilmu Pengetahuan, Agama, Bangsa
dan Negara

ABSTRACT

Digital signature is an authentication mechanism that allows the message maker to add a code that can act as a signature. The value of a digital signature is highly dependent on the original document and the message maker, so it will have a unique value for each existing signature. In this research, software development is carried out to test the integrity of documents with digital signatures built using the MD5 hash function and the RSA algorithm which is then generated into a Qr-Code on a document consisting of 1000 words with the .docx extension. The document to be tested is given a digital signature with the software built and then integrity testing is carried out by modifying the text file. This research also calculates the processing time by the system using 10 documents, with 8 bit and 13 bit key-forming values during encryption and the validation process of signed documents. The average time required for the encryption process will be longer when a high key-forming value is used. However, in the decryption process, the processing time between the high and low key-forming values did not have a significant difference. In this research, software has been created to apply the authentication scheme to a document. From the results of the research, it can be concluded that the MD5 hash function and the RSA algorithm which is generated into a Qr-Code can be implemented to be used as digital signatures. In addition, a large key-forming value will affect to the signing process.

Keywords: Digital Signature, Hash MD5, RSA, Qr-Code

ABSTRAK

Tanda tangan digital ialah suatu mekanisme autentikasi yang memungkinkan pengirim pesan dapat menambahkan kode yang dapat bertindak sebagai tanda tangannya. Nilai dari tanda tangan digital sangat bergantung pada dokumen asli dan pengirim pesan, sehingga akan memiliki nilai yang unik untuk setiap tanda tangan yang ada. Didalam penelitian ini dilakukan pengembangan perangkat lunak guna melakukan pengujian integritas dokumen dengan tanda tangan digital yang dibangun menggunakan fungsi hash MD5 dan algoritma RSA yang kemudian digenerate 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 proses modifikasi terhadap file teks tersebut. Penelitian ini juga dilakukan perhitungan waktu proses oleh sistem menggunakan data sebanyak 10 dokumen, dengan nilai pembentuk kunci sepanjang 8 dan 13 bit saat enkripsi serta proses validasi dari dokumen yang telah ditanda tangani. Rata-rata waktu yang dibutuhkan untuk proses enkripsi akan lebih lama saat digunakan nilai pembentuk kunci yang tinggi. Namun, pada proses dekripsi waktu proses diantara nilai pembentuk kunci yang tinggi dan rendah tidak memiliki perbedaan yang signifikan. Pada penelitian ini telah dibuat perangkat lunak untuk menerapkan skema autentikasi pada sebuah dokumen. Dari hasil penelitian yang dilakukan maka dapat disimpulkan fungsi hash MD5 dan algoritma RSA yang digenerate menjadi Qr-Code dapat diimplementasikan untuk digunakan sebagai tanda tangan digital. Selain itu, nilai pembentuk kunci yang besar akan berpengaruh pada proses penanda tanganan.

Kata Kunci: Tanda Tangan Digital, Hash MD5, RSA, Qr-Code

KATA PENGANTAR

Puji syukur kepada Allah SWT atas berkat dan rahmat-Nya yang telah melimpahkan rahmat dan karunianya kepada Penulis sehingga mampu menyelesaikan Tugas Akhir ini dengan baik. Tugas akhir ini disusun untuk memenuhi salah satu syarat untuk menyelesaikan Pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Dalam menyelesaikan Tugas Akhir ini, banyak pihak yang telah memberikan bantuan dan dukungan baik secara langsung maupun tidak langsung. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih kepada:

1. Orang tua saya, Bapak Yohar.S dan Ibu Midah yang terus memberikan baik secara moril dan materiil. Keluarga besar “Pasukan Matau” yakni: Keluarga Dang Indarmawan, S.Hut., Keluarga Dunga Supintri, S.Hut., Keluarga Wah Iramalija, Keluarga Cik Besak Dady Artony, Keluarga Cik Tuga (Ary Yoga Purnama, S.Pd) dan Keluarga Inga Leny Sofyah, S.Pd.
2. Keluarga besar Kak Rizal Dediarto yang selalu mendoakan, memberikan bantuan dan dukungan.
3. Civitas Akademika Fakultas Ilmu Komputer Universitas Sriwijaya, khususnya seluruh Dosen Teknik Informatika yang telah memberikan ilmu pengetahuan serta membimbing penulis baik dalam kegiatan akademik dan non akademik.
4. Pembimbing Tugas Akhir, Bapak Julian Supardi, M.T. dan Bapak Muhammad Qurhanul Rizqie, M.T., Ph.D. yang telah membimbing penulis dengan sabar dan semangat.
5. Ketua Penguji Ibu Yunita, M.Cs serta penguji tugas akhir, Bapak Osvari Arsalan, M.T., dan Bapak Kanda Januar Miraswan, M.T. yang telah

memberikan masukan kepada penulis mengenai tugas akhir dan pengalaman kerja.

6. Pembimbing Akademik, Muhammad Fachrurrozi, S.Si., M.T. yang telah banyak memberikan masukan kepada penulis sejak mulai perkuliahan.
7. Pasukan perjuangan Tugas Akhir Ahmad, Faiz, Abi, Johancan, Suci, Adinda dan Grup Skype “Belajar” serta seluruh keluarga Informatika Reguler B 17 yang tak kenal lelah dalam menyelesaikan pertugas akhiran.
8. Semua teman organisasi saat menjalani kepengurusan di WIFI dan KEMMAS Ghazali yang telah memberikan masukan, pelajaran hidup serta telah menjadi keluarga baru bagi penulis.
9. Teman-teman; Yuni, Ani, Dewi, Asih, Lesi, Tektong, Etek Ling, Jik, David, Eja, Put, Via, Zah dan semuanya yang tidak dapat disebutkan satu persatu, yang telah kebersamai dalam proses perkuliahan, pertugas akhiran.

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya. Akhir kata semoga Tugas Akhir ini dapat digunakan sebaik-baiknya serta bermanfaat bagi kita semua.

Indralaya, 21 Juli 2022

Penulis

Hafiz Mursid

DAFTAR ISI

Halaman

LEMBAR PENGESAHAN SKRIPSI	ii
TANDA LULUS UJIAN SIDANG TUGAS AKHIR	iii
HALAMAN PERNYATAAN.....	iv
MOTTO DAN PERSEMBAHAN.....	v
ABSTRACT	vi
ABSTRAK	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR.....	xiv
BAB I PENDAHULUAN.....	I-1
1.1 Pendahuluan.....	I-1
1.2 Latar Belakang.....	I-1
1.3 Rumusan Masalah.....	I-4
1.4 Tujuan Penelitian	I-5
1.5 Manfaat Penelitian	I-5
1.6 Batasan Masalah	I-5
1.7 Sistematika Penulisan	I-6
1.8 Rangkuman	I-7
BAB II KAJIAN LITERATUR	II-1
2.1 Pendahuluan.....	II-1
2.2 Landasan Teori	II-1
2.2.1. Kriptografi	II-1
2.2.2. Fungsi <i>Hash</i> MD5.....	II-3
2.2.3. Algoritma RSA	II-6
2.2.4. Tanda Tangan Digital	II-9
2.2.5. <i>Qr-Code (Quick Response Code)</i>	II-11
2.2.6. <i>Rational Unified Process (RUP)</i>	II-12

2.3 Penelitian yang Relevan	II-14
2.4 Rangkuman	II-16
BAB III METODOLOGI PENELITIAN	III-1
3.1 Pendahuluan.....	III-1
3.2 Pengumpulan Data.....	III-1
3.3 Tahapan Penelitian.....	III-2
3.4 Metode Pengembangan Perangkat Lunak	III-9
3.5 Rangkuman	III-11
BAB IV PENGEMBANGAN PERANGKAT LUNAK	IV-1
4.1 Pendahuluan.....	IV-1
4.2 Rational Unified Process	IV-1
4.2.1 Analisis Kebutuhan.....	IV-1
4.2.2 Perancangan Perangkat Lunak.....	IV-2
4.2.2.1 Use-Case Diagram	IV-2
4.2.2.2 Activity Diagram.....	IV-10
4.2.2.3 Sequence Diagram	IV-13
4.2.2.4 Class Diagram.....	IV-15
4.2.2.5 Interface Desain	IV-15
4.2.3 Implementasi Perangkat Lunak.....	IV-20
4.2.4 Pengujian Perangkat Lunak.....	IV-23
4.3 Rangkuman	IV-29
BAB V HASIL DAN ANALISIS PENELITIAN.....	V-1
5.1 Pendahuluan.....	V-1
5.2 Data Hasil Percobaan/Penelitian.....	V-1
5.2.1 Konfigurasi Percobaan	V-1
5.2.2 Hasil Konfigurasi Skema 1	V-2
5.2.3 Hasil Konfigurasi Skema 2	V-5
5.2.4 Hasil Konfigurasi skema 3	V-7
5.2.5 Hasil Konfigurasi skema 4	V-9
5.2.6 Hasil Konfigurasi skema 5	V-11
5.2.7 Hasil Pengujian Aspek Kecepatan Waktu Eksekusi	V-13
5.2.7.1 Waktu Eksekusi Proses Tanda Tangan	V-13

5.2.7.2 Waktu Eksekusi Proses Validasi	V-14
5.3 Analisis Hasil Penelitian.....	V-15
5.4 Rangkuman	V-20
BAB VI KESIMPULAN DAN SARAN.....	VI-1
6.1 Kesimpulan	VI-1
6.2 Saran	VI-2
DAFTAR PUSTAKA	xv

DAFTAR TABEL

Tabel II- 1. Properti RSA	II-9
Tabel III- 1. Rancangan Hasil Pengujian	III-8
Tabel IV- 1. Definisi Aktor.....	IV-4
Tabel IV- 2. Definisi Use-Case.....	IV-5
Tabel IV- 3. Skenario Use-Case Membuat File Bertanda Tangan Digital.....	IV-5
Tabel IV- 4. Skenario Use Case Melakukan Pengujian Terhadap Integritas File.....	IV-8
Tabel IV- 5. Daftar Implementasi Kelas.....	IV-20
Tabel IV- 6. Rencana Pengujian Use Case Membuat File dengan Tangan Digital	IV-24
Tabel IV- 7. Rencana Pengujian Use Case untuk Pengujian Integritas File dan Autentikasi File.....	IV-24
Tabel IV- 8. Pengujian Use Case Membuat File dengan Tangan Digital	IV-25
Tabel IV- 9. Pengujian <i>Use-case</i> untuk Pengujian Integritas dan Autentikasi File	IV-27
Tabel V-1. Pengujian Data Skema 1	V-4
Tabel V-2. Pengujian Data Skema 2	V-6
Tabel V-3. Pengujian Data Skema 3	V-8
Tabel V-4. Pengujian Data Skema 4	V-10
Tabel V-5. Pengujian Data Skema 5	V-12
Tabel V-6. Kecepatan Proses Tanda Tangan	V-13
Tabel V-7. Kecepatan Proses validasi Tanda Tangan.....	V-14

DAFTAR GAMBAR

Gambar II- 1. Proses HMD5	II-6
Gambar II- 2. Qr-Code	II-12
Gambar II- 3. Arsitektur RUP	II-13
Gambar III-1. Diagram Tahap Penelitian	III-2
Gambar III-2. Kerangka Kerja Pembuatan dan Penyisipan Tanda Tangan Digital	III-4
Gambar III-3. Kerangka Kerja Pengujian Integritas Isi File.....	III-5
Gambar IV-1. Diagram Use-Case	IV-4
Gambar IV-2. Activity Diagram Membuat File dengan Tanda Tangan Digital	IV-11
Gambar IV-3. Activity Diagram Melakukan Pengujian Terhadap Integritas Isi File ...	IV-12
Gambar IV-4. Sequence Diagram Membuat File dengan Tanda Tangan Digital	IV-13
Gambar IV-5. Sequence Diagram Pengujian Terhadap Integritas File.....	IV-14
Gambar IV-6. Diagram Kelas Pada Sistem	IV-15
Gambar IV-7. Tampilan Antarmuka Halaman Digital Signature	IV-17
Gambar IV-8. Tampilan Antarmuka Halaman Cek Validasi.....	IV-19
Gambar IV-9. Tampilan Antarmuka Halaman Digital Signature	IV-22
Gambar IV-10. Tampilan Antarmuka Halaman Cek Validasi.....	IV-23
Gambar V-1. Kecepatan Eksekusi Enkripsi.....	V-19
Gambar V-2. Kecepatan Eksekusi Dekripsi	V-20

BAB I

PENDAHULUAN

1.1 Pendahuluan

Bab I Pendahuluan ini membahas latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, dan batasan masalah serta sistematika penulisan pada penelitian ini. Pada Latar belakang, akan dijelaskan mengenai permasalahan-permasalahan yang menjadi alasan untuk dilakukannya penelitian ini. Pada tujuan penelitian, dijelaskan tujuan yang ingin dicapai dalam melakukan penelitian. Pada manfaat penelitian, dijelaskan manfaat dari hasil penelitian ini. Sedangkan pada batasan masalah, akan dijelaskan ruang lingkup penelitian agar penelitian tidak melebar dan lebih fokus pada judul penelitian yang diangkat.

1.2 Latar Belakang

Perkembangan teknologi menuntut hampir segala sesuatu dilakukan dengan cara digital. Pesatnya perkembangan teknologi informasi juga merambah ke berbagai bidang, tidak terkecuali dalam sebuah dokumen. Sebuah dokumen dalam bentuk digital ini biasa disebut dokumen elektronik atau dokumen digital. Dokumen elektronik merupakan pengganti dokumen kertas yang memiliki banyak kelebihan. Dokumen ini memiliki karakteristik lebih fleksibel, menghemat ruang penyimpanan, pencarian akan lebih mudah, kemungkinan kecil data akan hilang, serta akan mudah saat ingin mentransfer dokumen ke orang lain.

Seperti layaknya dokumen cetak, sebuah dokumen elektronik juga membutuhkan sebuah tanda tangan. Tanda tangan ini untuk menjamin keasliannya. Tanda tangan dapat digunakan sebagai penanda yang autentik bahwa seseorang telah memahami, membaca, serta menyetujui isi dokumen tersebut (Munir, 2019)

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 karena keaslian isi file teks yang ditanda tangani dapat dipertahankan dan dipertanggung jawabkan oleh pengirim.

Maka pada penelitian ini dalam menciptakan tanda tangan elektronik diterapkan fungsi *hash* MD5 yang dikombinasikan dengan algoritma *RSA*. Algoritma MD5 sebagai fungsi *hash* serta algoritma *RSA* digunakan untuk proses enkripsi pada skema tanda tangan digital. Algoritma MD5 dapat digunakan untuk proses autentikasi, dimana hasilnya tidak dapat dikembalikan lagi. Output MD5 berupa 128-bit message (Handoko et al., 2018)

Fungsi *Hash* MD5 merupakan bentuk penyempurnaan dari *hash* MD4. Fungsi *hash* MD5 memiliki waktu proses yang cepat. Fungsi *hash* MD5 juga memiliki tingkat keamanan yang tinggi. Hal ini dikarenakan banyaknya jumlah putaran di dalam algoritma MD5 (Gupta & Kumar, 2014)

Algoritma *RSA* merupakan salah satu algoritma kriptografi asimetri atau algoritma kunci publik yang paling banyak pengaplikasiannya. Algoritma *RSA* memiliki kelebihan pada kombinasi kunci publik serta kunci privat yang tidak perlu dilakukan perubahan meskipun pada jangka waktu lama. Selain itu algoritma *RSA*

juga memiliki tingkat keamanan yang tinggi. Hal ini karena Algoritma *RSA* menggunakan pemfaktoran bilangan prima yang besar dalam membangkitkan kuncinya (Suhandinata et al., 2019).

Akan tetapi, tanda tangan digital hasil enkripsi dari algoritma *RSA* ini akan menampilkan *chipertext* yang berupa susunan huruf dan atau angka dalam jumlah relatif banyak. Sehingga, jika digunakan sebagai tanda tangan digital pada sebuah dokumen, dipandang terlalu terlalu panjang dan akan memakan tempat saat disisipkan pada dokumen tersebut. Maka, pada penelitian ini akan dilakukan penyederhanaan terhadap tampilan tanda tangan digital (Soon, 2008)

QR-Code adalah jenis *barcode* dua dimensi, ditemukan dan dikembangkan oleh Perusahaan *Denso Corporation*, salah satu perusahaan bidang Otomotif di Jepang. Awalnya, simbol dua dimensi ini hanya digunakan untuk mengontrol produksi komponen otomotif. Namun seiring berkembangnya teknologi, penggunaan *QR-Code* meluas di berbagai bidang lain

QR-Code mampu menampung 7.089 data *numerik*, 4.296 data *alphanumeric*, 2.953 data biner, serta 1.817 karakter huruf kanji dengan proses pengkodean yang cepat dan ukuran cetak yang kecil. Kapasitas data yang dapat ditampung oleh *QR-Code* lebih besar apabila dibandingkan dengan matriks kode lain. (Ramadhanis dan Yenni, 2016)

Dari permasalahan-permasalahan di atas, maka pada penelitian ini akan dilakukan Implementasi Skema *QR-Code* untuk Pengujian Integritas dari Isi File Teks pada Operasi Tanda Tangan Digital Menggunakan Kombinasi Fungsi *Hash MD5* dan *Algoritma RSA*. Dalam tahap penelitian, akan dilakukan penyisipan tanda

tangan digital dalam bentuk *Qr-Code* pada sebuah dokumen digital. *Qr-Code* ini merupakan hasil generate dari enkripsi algoritma RSA yang sebelumnya dilakukan fungsi *hash MD5*. Selanjutnya, tanda tangan digital dalam bentuk *Qr-Code* ini akan digunakan untuk menguji integritas file yang sebelumnya disisipkan tanda tangan digital. Pengujian ini dilaksanakan dengan membandingkan nilai *hash* yang didapatkan dari teks yang sudah ditanda tangani dengan nilai *hash* dari hasil dekripsi tanda tangan dalam bentuk *Qr-Code*.

1.3 Rumusan Masalah

Berdasarkan dari latar belakang diatas, maka pada penelitian ini akan mengimplementasikan skema *Qr-Code* untuk pengujian integritas pada isi file teks pada operasi tanda tangan digital menggunakan kombinasi fungsi *hash MD5* dan *RSA*. Sehingga, dirumuskan pertanyaan penelitian sebagai berikut:

1. Bagaimana membangun perangkat lunak untuk mengimplementasikan skema *Qr-Code* untuk pengujian integritas isi file teks pada operasi tanda tangan digital menggunakan kombinasi fungsi *hash MD5* dan *algoritma RSA*?
2. Bagaimana hasil dari pengujian integritas file setelah disisipkan tanda tangan digital *Qr-Code* hasil kombinasi fungsi *hash MD5* dan *algoritma RSA*?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini ialah:

1. Membuat perangkat lunak untuk mengimplementasikan skema *Qr-Code* untuk pengujian integritas isi file teks pada operasi tanda tangan digital menggunakan kombinasi fungsi *hash MD5* dan *algoritma RSA*?
2. Menguji integritas file teks yang sebelumnya telah disisipkan tanda tangan digital *Qr-Code* hasil kombinasi fungsi *hash MD5* dan *algoritma RSA*?

1.5 Manfaat Penelitian

Manfaat yang dapat diperoleh dari penelitian ini ialah:

1. Menghasilkan sebuah perangkat lunak yang menerapkan skema *Qr-Code* untuk pengujian integritas isi file teks pada operasi tanda tangan digital menggunakan kombinasi fungsi *hash MD5* dan *algoritma RSA*.
2. Mengetahui hasil uji integritas file teks yang sebelumnya disisipkan tanda tangan digital *Qr-Code* hasil kombinasi fungsi *hash MD5* dan *algoritma RSA*.
3. Menambah referensi untuk penelitian lainnya, khususnya mengenai tanda tangan digital.

1.6 Batasan Masalah

Batasan masalah dari penelitian ini ialah:

1. Algoritma yang digunakan ialah fungsi *hash MD5* serta *Algoritma RSA*.
2. Dokumen yang disisipkan tanda tangan ialah file teks dengan ekstensi (*.docx*).

3. Pengamanan file teks hanya meliputi autentikasi pengirim dan keutuhan isi file teks.
4. Aplikasi yang dibangun merupakan aplikasi berbasis dekstop.
5. *Barcode* yang digunakan adalah barcode dua dimensi jenis *Qr-Code*.

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini mengikuti standar penulisan skripsi pada Fakultas Ilmu Komputer Universitas Sriwijaya yaitu:

BAB I. PENDAHULUAN

Bab I menguraikan mengenai latar belakang, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah/ruang lingkup, metodologi penelitian dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini akan membahas dasar-dasar teori yang digunakan dalam penelitian ini. Dasar-dasar teori ini melingkupi: tanda tangan digital, pengenalan kriptografi, *Qr-Code*, fungsi *hash MD5*, *Algoritma RSA* serta beberapa penelitian sebelumnya yang relevan.

BAB III. METODOLOGI PENELITIAN

Bab III berisi tentang tahapan yang dilakukan pada penelitian ini. Setiap rancangan tahapan-tahapan pada penelitian diuraikan dengan rinci dengan berpedoman pada suatu kerangka kerja dan kemudian pada akhir bab berisi perancangan manajemen proyek pada pelaksanaan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini, dibahas proses yang dilakukan dalam upaya pengembangan perangkat lunak. Digunakan metode RUP dalam pengembangan perangkat lunak. Terdapat 3 fase dalam pengembangannya yaitu Insepsi, Elaborasi, Konstruksi dan Transisi.

BAB V. HASIL DAN ANALISIS PENELITIAN

Bab ini akan dijelaskan mengenai hasil dari percobaan penelitian dan analisisnya. Pengujian dilakukan dengan data yang sebelumnya telah ditentukan sebelumnya

BAB VI. KESIMPULAN DAN SARAN

Bab ini akan diberikan poin-poin kesimpulan dan saran yang didapatkan berdasarkan hasil dari penelitian ini.

1.8 Rangkuman

Bab ini telah menjelaskan secara umum tentang masalah – masalah yang menjadi latar belakang didalam penelitian ini. Pada bab ini pula telah diuraikan rumusan masalah, tujuan penelitian, manfaat penelitian, batasan-batasan masalah pada penelitian, dan sistematika penulisan yang digunakan.

DAFTAR PUSTAKA

- Abood, O. G., Guirguis, S. K. (2018). A Survey on Cryptography Algorithms. *International Journal of Scientific and Research Publications (IJSRP)*, 8(7). <https://doi.org/10.29322/ijsrp.8.7.2018.p7978>
- Ardy, R. D., Indriani, O. R., Sari, C. A., Setiadi, D. R. I. M., Rachmawanto, E. H. (2017). Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5). *Proceeding of 2017 International Conference on Smart Cities, Automation and Intelligent Computing Systems, ICON-SONICS 2017, 2018-Janua*, 87–92. <https://doi.org/10.1109/ICON-SONICS.2017.8267827>.
- Ariyus, D. (2008). *Pengantar ilmu kriptografi: teori analisis & implementasi* (1st ed.). Penerbit Andi.
- Gupta, P., Kumar, S. (2014). A Comparative Analysis of SHA and MD5 Algorithm. *International Journal of Computer Science and Information Technologies*, 5(3), 4492–4495.
- Kromodimoeljo, S. (2009). *Teori dan Aplikasi Kriptografi*. Penerbit SPK IT Consulting. SPK IT Consulting.
- Handoko, L. B., Umam, C., Sari, C. A. (2018). Autentikasi Citra Rgb Menggunakan Kombinasi Fungsi Hash MD5 Dan RSA. *Prosiding SNST Fakultas Teknik*, 1(1).
- Munir, R. (2019). *Kriptografi* (2nd ed.). Penerbit Informatika.
- Pangaribuan, L. J., Simbolon, F. H. (2017). Kriptografi Hybrida Menggunakan Algoritma Hill Cipher dan Algoritma RSA untuk Keamanan Pengiriman Informasi pada Email. *KOMIK (Konferensi Nasional Teknologi Informasi Dan Komputer)*, 1, 1–11.
- Péraire, C., Edwards, M., Fernandes, A., Mancin, E., Carroll, K. (2007). *The IBM Rational Unified Process for System z*. 252.
- Precilia, D. P., Izzuddin, A. (2016). Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (MD5). *Energy*, 5(1), 14–19.
- Ramadhanis, B., Yenni, H. (2016). Implementasi Quick Response Code Dalam Deteksi Pendistribusian Dokumen Ujian Nasional. *SATIN - Sains Dan Teknologi Informasi*, 2(1), 31–37. <http://jurnal.sar.ac.id/index.php/satin/article/view/120>
- Soon, T. J. (2008). QR code. *Synthesis Journal*, 2008, 59-78.

- Suhandinata, S., Rizal, R. A., Wijaya, D. O., Warren, P., Srinjiwi, S. (2019). Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, 6(1), 1–10. <https://doi.org/10.33330/jurteksi.v6i1.395>
- Sulaiman, O. K., Ihwani, M., Rizki, S. F. (2016). Model Keamanan Informasi Berbasis Tanda Tangan Digital Dengan Data Encryption Standard (Des) Algorithm. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, 1(1), 14–19. <https://doi.org/10.30743/infotekjar.v1i1.82>
- Widayati, Y. T. (2017). Aplikasi Teknologi Qr (Quick Response) Code Implementasi Yang Universal. *KOMPUTAKI*, 3(1), 6–18.