TANDA TANGAN DIGITAL MENGGUNAKAN ALGORITMA SHA-256 DAN RSA PADA FILE PDF

Diajukan Sebagai Syarat Untuk Menyelesaikan

Pendidikan Program Strata-1 pada

Jurusan Teknik Informatika

Oleh :

Aditiya Ramadhan Saputra

NIM : 09021181924003

Jurusan Teknik Informatika

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN TUGAS AKHIR

TANDA TANGAN DIGITAL MENGGUNAKAN ALGORITMA SHA-256 DAN RSA PADA FILE PDF

Oleh :

ADITIYA RAMADHAN SAPUTRA

NIM. 09021181924003

Palembang, 20 Juli 2023

Pembimbing I

Al Farissi, M.Comp., Sc.
NIP. 198512152014041001

Pembimbing II

Osvari Arsalan, M.T.
NIP. 198806282018031001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN SIDANG SKRIPSI

Pada hari Jum'at, 07 Juli 2023 telah dilaksanakan ujian sidang skripsi oleh Jurusan Teknik informatika Fakultas Ilmu Komputer Universitas Sriwijaya

Nama : Aditiya Ramadhan Saputra
NIM : 09021181924003
Judul : Tanda Tangan Digital Menggunakan Algoritma SHA-256 dan RSA pada File PDF

dan dinyatakan **LULUS**

1. Ketua Penguji

Novi Yusliani, M.T
NIP. 198211082012122001 .....

2. Pembimbing I

Al Farissi, M.Comp., Sc.
NIP. 198512152014041001 .....

3. Pembimbing II

Osvari Arsalan, M.T.
NIP. 198806282018031001 .....

4. Penguji

Matura Diana Marieska, M.T.
NIP. 198603212018032001 .....

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

Halaman Pernyataan bebas plagiat

Yang bertanda tangan dibawah ini :

Nama	: Aditiya Ramadhan Saputra
NIM	: 09021181924003
Program Studi	: Teknik Informatika
Judul	: TANDA TANGAN DIGITAL MENGGUNAKAN ALGORITMA SHA-256 DAN RSA PADA FILE PDF

Hasil Pengecakan Software iThenticate/Turnitin : 13%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

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

Palembang, 21 Juli 2023

Aditiya Ramadhan Saputra
NIM. 09021181924003

Motto dan Persembahan

“We are who we choose to be”

-Green Goblin-

“Always remember that a bad day is just 24 hours. Not a bad life”

- Thomas Shelby”

Kupersembahkan karya tulis ini kepada :

- Kedua Orang Tua dan Saudaraku
- Teman-Teman Seperjuangan
- Fakultas Ilmu Komputer
- Universitas Sriwijaya

ABSTRACT

The Rapid advancement of technology has led to crimes committed using information technology, one of which is digital document forgery. This has resulted in issues concerning the misuse of such digital documents by irresponsible individuals. To maintain the authenticity of distributed messages, a method is required to serve as an assurance that the documents are not manipulated. Digital signatures are one of the methods that can be used to ensure the authenticity of distributed messages. This research utilizes the SHA-256 and RSA algorithms in its implementation. The data used in this study is obtained from the website https://repository.unsri.ac.id/. The testing of the avalanche effect on modified documents concludes that encryption in digital signatures does not affect the value of the avalanche effect. Furthermore, the testing of the values P and Q used to form key pairs in the RSA algorithm demonstrates that these values affect the duration of the encryption process in digital signatures.

Keywords : Digital Signature, SHA-256, RSA ,PDF File.

ABSTRAK

Kemajuan teknologi yang semakin pesat menimbulkan kejahatan-kejahatan dengan menggunakan teknologi informasi, salah satunya adalah pemalsuan dokumen digital. Hal tersebut menimbulkan masalah berupa penyalahgunaan dokumen digital tersebut oleh orang yang tidak bertanggung jawab. Untuk menjaga keaslian pesan yang didistribusikan diperlukan suatu metode yang dapat digunakan sebagai jaminan bahwa dokumen tersebut tidak dipalsukan. Tanda tangan digital merupakan salah satu metode yang dapat digunakan untuk menjaga keaslian dari pesan yang didistribusikan. Penelitian ini menggunakan algoritma SHA-256 dan juga RSA pada implementasinya. Data yang digunakan pada penelitian ini diperoleh dari website https://repository.unsri.ac.id/. Pada pengujian avalanche effect terhadap dokumen yang dimodifikasi diperoleh kesimpulan bahwa enkripsi pada tangan digital tidak mempengaruhi nilai dari avalanche effect. Selanjutnya pengujian besaran nilai P dan Q yang digunakan untuk membentuk pasangan kunci pada algoritma RSA menunjukkan bahwa nilai P dan Q mempengaruhi durasi proses enkripsi pada tanda tangan digital.

Kata Kunci : tanda tangan digital, SHA-256, RSA, file PDF.

KATA PENGANTAR

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

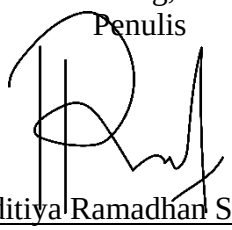
Dalam menyelesaikan Tugas Akhir ini, banyak pihak yang telah memberikan bantuan dan dukungan baik secara langsung maupun tidak langsung. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih kepada :

1. Orang tua saya, Bapak M. Yani, S.Pd., M.Si dan Ibu Jumiatin, S.Pd yang terus memberikan dukungan baik secara moril dan materil.
2. Alm. Bapak Jaidan Jauhari, S.Pd.., M.T., selaku Dekan Fakultas Ilmu Komputer
3. Bapak Al Farissi, M.Comp.Sc. selaku Pembimbing I dan Bapak Osvari Arsalan, M.T. selaku Pembimbing II, yang telah banyak memberikan masukan, arahan, serta membimbing Penulis dalam menyusun Tugas Akhir.
4. Ibu Novi Yusliani, M.T. selaku ketua penguji dan Ibu Mastura Diana Marieska M.T. selaku penguji
5. Bapak Qurhanul Rizkie, S.Kom., M.T., Pd.D. selaku dosen pembimbing akademik.
6. Seluruh dosen Program Studi Teknik informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Kak Ricy selaku staff administrasi Teknik Informatika Reguler, dan seluruh staff Fakultas Ilmu Komputer Universitas Sriwijaya yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan.

8. Teman-teman TI Reg B 2019, khususnya kepada Adit (totok), Andri, Dimas, Giga, Indra, Irvan, Kurniawan (babang), Ricky, Theja, Vinito, Zananda, Yuyun, Rahel, Friska, dan Debo yang telah menemani Penulis dari awal hingga akhir perkuliahan.
9. Anggota grup Primum Coertus M. Rizky Azizi dan Muhammad Naufal yang memberikan pengalaman-pengalaman yang menyenangkan kepada Penulis dari bolos bersama hingga ke proyek bersama.
10. Teman-teman iphone no toxic yang telah memberikan motivasi-motivasi kehidupan.
11. Teman-temanku penghuni "ini group" Anam, Ardi, Ilham (senen), Ilham(irwanto), dan fadhil yang telah memberikan banyak motivasi kepada Penulis dan menjadi penghibur ketika Penulis kehilangan motivasi.
12. Pemilik NIM 1308618028 yang telah meluangkan waktu, tenaga, serta pikiran. Terima kasih atas kesediannya menjadi tempat berkeluh kesah Penulis dan telah menjadi bagian dari perjalanan Penulis dalam menyusun Tugas Akhir.
13. Seluruh pihak yang telah membantu dalam penyusunan dan penyempurnaan tugas akhir ini yang tidak dapat disebutkan satu persatu.

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan disebabkan keterbatasan pengetahuan dan pengalaman, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya. Akhir kata semoga Tugas Akhir ini dapat berguna dan bermanfaat bagi kita semua.

Palembang, 21 Juli 2023
Penulis



Aditiya Ramadhan Saputra
NIM. 09021181924003

DAFTAR ISI

Halaman

ABSTRACT vi
ABSTRAK vii
KATA PENGANTAR viii
DAFTAR ISI x
DAFTAR TABEL xiii
DAFTAR GAMBAR xv
BAB I 1
PENDAHULUAN 1
1.1 Pendahuluan 1
1.2 Latar Belakang 1
1.3 Rumusan Masalah 3
1.4 Tujuan Penelitian 4
1.5 Manfaat Penelitian 5
1.6 Batasan Masalah 5
1.7 Sistematika Penulisan 5
1.8 Kesimpulan 7
BAB II 1
KAJIAN LITERATUR 1
2.1 Pendahuluan 1
2.2 Landasan Teori 1
2.2.1 Tanda Tangan Digital 1
2.2.1.1 Sifat Tanda Tangan digital 3
2.2.1.2 Manfaat Tanda Tangan digital 3
2.2.1.3 Tanda tangan digital dengan menggunakan fungsi *hash* dan enkripsi 5
2.2.2 Fungsi Hash 6
2.2.2.1 Algoritma SHA-256 8
2.2.3 Kriptografi Asimetris 12

2.2.3.1 Algoritma RSA 13
2.2.4 Avalanche Effect 15
2.3 Penelitian Lain yang Relevan 15
2.4 Kesimpulan 17
BAB III 1
METODOLOGI PENELITIAN 1
3.1 Pendahuluan 1
3.2 Pengumpulan Data 1
3.3 Tahapan Penelitian 1
3.3.1 Kerangka Kerja 3
3.3.2 Kriteria Pengujian 6
3.3.3 Format Data Pengujian 7
3.3.4 Alat yang Digunakan dalam Pelaksanaan Penelitian 7
3.3.5 Pengujian Penelitian 8
3.3.6 Analisis Hasil Pengujian dan Kesimpulan 9
3.4 Metode Pengembangan Perangkat Lunak 10
3.4.1 Fase Insepsi 10
3.4.2 Fase Elaborasi 11
3.4.3 Fase Konstruksi 11
3.4.4 Fase Transisi 11
3. 5 Kesimpulan 11
BAB IV 1
PENGEMBANGAN PERANGKAT LUNAK 1
4.1 Pendahuluan 1
4.2 *Rational Unified Process* 1
4.2.1 Fase Insepsi 1
4.2.1.1 Pemodelan Bisnis 1
4.2.1.2 Analisis Kebutuhan 2
4.2.1.2.1 Kebutuhan Sistem 2
4.2.1.2.2 Kebutuhan Fungsional dan Non-Fungsional Perangkat Lunak 3
4.2.1.3 *Use Case Diagram* 4
4.2.2 Fase Elaborasi 12
4.2.2.1 Rancangan Tampilan Antarmuka Perangkat Lunak 13

4.2.2.*2 Activity Diagram* 14
4.2.2.3 *Sequence Diagram* 15
4.2.3 Fase Konstruksi 19
4.2.3.1 *Class Diagram* 19
4.2.3.2 Implementasi Perangkat Lunak 20
4.2.4 Fase Transisi 21
4.2.4.1 Rencana Pengujian dan Kasus Uji 21
4.2.4.1.1 Rencana pengujian 22
4.2.4.1.2 Kasus Uji 23
4.3 Kesimpulan 25
BAB V .....
HASIL DAN ANALISIS PENELITIAN 1
5.1 Pendahuluan 1
5.2 Data Hasil Percobaan/Penelitian 1
5.2.1 Konfigurasi Percobaan 1
5.2.2 Hasil Pengujian 2
5.2.2.1 Hasil Pengujian Aspek Avalanche Effect 2
5.2.2.2 Hasil Pengujian Kecepatan Waktu Eksekusi 3
5.3 Analisis Hasil Penelitian 5
5.4 Kesimpulan 7
BAB VI 1
KESIMPULAN DAN SARAN 1
6.1 Pendahuluan 1
6.2 Kesimpulan 1
6.3 Saran 2
DAFTAR PUSTAKA vii

DAFTAR TABEL

Halaman

Tabel II-1. Algoritma Hash II-7
Tabel II-2. Nilai Initial Hash SHA-256 ..... II-9
Tabel III-1. Rancangan Tabel Analisa Hasil Pengujian *Avalanche Effect* III-9
Tabel III-2. Rancangan Tabel Analisa Hasil Pengujian Lamanya Proses Eksekusi III-10
Tabel IV-1. Deskripsi Aktor IV-5
Tabel IV-2. Deskripsi Use Case IV-5
Tabel IV-3. Skenario Use Case Membuat Tanda Tangan Digital IV-6
Tabel IV-4. Skenario Use Case Verifikasi File PDF IV-9
Tabel IV-5 Skenario Use Case Membuat Tanda Tangan Digital dengan Membangkitkan Nilai Prima P dan Q. IV-11
Tabel IV-6. Implementasi Kelas IV-21
Tabel IV-7. Rencana Pengujian Use Case Membuat File Tanda Tangan Digital IV-22
Tabel IV-8. Rencana Pengujian Use Case Verifikasi File PDF IV-22
Tabel IV-9. Rencana Pengujian *Use Case* Mmebuat File Tanda Tangan Digital dengan Membangkitkan Nilai Prima P dan Q IV-22
Tabel IV-10. Pengujian Use Case Membuat File Tanda Tangan Digital IV-23
Tabel IV-11. Pengujian Use Case Verifikasi File PDF IV-21
Tabel IV-12 Pengujian Use Case Membuat File Tanda Tangan Digital Dengan Membangkitkan Nilai Prima P dan Q IV-25
Tabel V-1. Perhitungan Nilai Avalanche Effect Message Digest Tanda Tangan Digital V-2
Tabel V-2. Perhitungan Nilai Avalanche Effect Enkripsi Tanda Tangan Digital V-3

Tabel V-3. Hasil Kecepatan Proses Tanda Tangan Digital Berdasarkan Besaran Nilai P dan Q..... V-4

DAFTAR GAMBAR

Halaman

Gambar III-1. Diagram Tahapan Penelitian III-2
Gambar III-2. Kerangka Kerja Pembangkitan Tanda Tangan Digital III-4
Gambar III-3. Kerangka Kerja Verifikasi Tanda Tangan Digital III-5
Gambar IV-1. Use Case Diagram IV-4
Gambar IV-2. Rancangan Tampilan Antarmuka Halaman Tanda Tangan Digital IV-13
Gambar IV-3. Rancangan Tampilan Antarmuka Halaman Verifikasi IV-14
Gambar IV-4. Activity Diagram Membuat Tanda Tangan Digital IV-14
Gambar IV-5. Acitivity Diagram Verifikasi File PDF dengan Tanda Tangan Digital IV-15
Gambar IV-6. Sequence Diagram Buat Tanda Tangan Digital IV-16
Gambar IV-7. Sequence Diagram Verifikasi Tanda Tangan Digital IV-17
Gambar IV-8. Membuat Tanda Tangan Digital Dengan Membangkitkan Nilai Prima Pada Kolom P dan Q IV-18
Gambar IV-9. Class Diagram Perangkat Lunak Tanda Tangan Digital IV-19
Gambar IV-10. Implementasi Rancangan Tampilan Antarmuka Halaman Tanda Tangan Digital IV-20
Gambar IV-11. Implementasi Rancangan Tampilan Antarmuka Halaman Verifikasi IV-20
Gambar V-1. Diagram Avalanche Effect pada Operasi Hash V-5
Gambar V-2 Diagram Avalanche Effect Enkripsi Tanda Tangan Digital V-6
Gambar V-3 Diagram Waktu Proses Tanda Tangan Berdasarkan Nilai P dan Q V-6

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab I pendahuluan membahas latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan, serta kesimpulan mengenai pengangkatan topik mengenai "Tanda Tangan Digital Menggunakan Algoritma SHA-256 dan RSA pada *File* PDF" sebagai bahan penelitian yang dilaksanakan.

1.2 Latar Belakang

Kemajuan teknologi yang semakin pesat menimbulkan kejahatan-kejahatan dengan menggunakan sarana teknologi informasi, salah satunya adalah pemalsuan dokumen digital. Pemalsuan dokumen ini dapat berupa pemalsuan dokumen pribadi, dokumen niaga, serta dokumen-dokumen lainnya yang dapat dipalsukan (Kanter, 2022). Menurut Setiawan & Syahputra (2020) hal tersebut kemudian memicu timbulnya masalah berupa penyalahgunaan dokumen digital tersebut oleh orang yang tidak bertanggung jawab dengan cara memanipulasi informasi digital seperti memanipulasi lampiran kelengkapan dokumen. Berdasarkan Undang-Undang No. 11 Tahun 2008 tentang informasi dan transaksi elektronik manipulasi dokumen elektronik dapat berupa penciptaan, perubahan, dan pengrusakan informasi elektronik dan/atau dokumen elektronik yang bertujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

Untuk mengatasi masalah yang ditimbulkan diperlukan upaya untuk menjamin keamanan pada dokumen digital tersebut, salah satu cara yang dapat dilakukan yaitu dengan mengautentikasi dokumen digital untuk menjamin keamanannya. Autentikasi dokumen digital dapat dilakukan dengan cara menandatangani dokumen digital tersebut dengan menggunakan tanda tangan digital (*digital signature*). Tanda tangan digital menjamin kerahasiaan, autentitikasi, *non-repudiation*, dan integritas pada dokumen digital yang sesuai dengan tujuan dari kriptografi (Azzahra, 2022). Tanda tangan digital digunakan sebagai identifikasi keabsahan seseorang dari dokumen digital yang ditandatangani. Tanda tangan digital digunakan sebagai tanda bahwa informasi atau isi dari dokumen digital tersebut disetujui oleh penandatangan (Azdy, 2016).

Penandatanganan dokumen digital dengan cara enkripsi pesan memberikan kerahasiaan pesan dan otentifikasi pada dokumen digital tersebut. Namun, pada beberapa kasus seringkali kerahasiaan pesan tidak dibutuhkan. Menggunakan algoritma kriptografi simetris tidak dapat mengatasi masalah penyangkalan terhadap pesan yang telah dikirim atau membantah isi pesan tersebut (Jamaludin et al., 2022). Berdasarkan kasus tersebut digunakan kombinasi algoritma hash dan kriptografi kunci publik (asimetris), algoritma fungsi hash digunakan untuk membentuk *message digest* dari sebuah dokumen digital, dan algoritma kunci publik digunakan untuk mengenkripsi *message digest* tersebut. Algoritma kunci publik tersebut mengatasi masalah autentikasi dan non-repudiation dengan cara menggunakan kunci yang berbeda antara pembuat tanda tangan dan penerima dokumen (Azdy, 2016).

Fungsi hash pada tanda tangan digital memungkinkan terjadinya *collision* pada dokumen digital yang ditandatangani sehingga dokumen tersebut memiliki nilai hash yang sama dengan dokumen lainnya. Google security pada tanggal 23 februari 2017 mengumumkan bahwa CWI Institue in Amsterdam dan Google menemukan collision pada fungsi hash dengan menggunakan algoritma SHA-1 (Sutopo et al., 2020). Berdasarkan masalah tersebut algoritma SHA-256 digunakan sebagai algoritma pembangkitan tanda tangan digital. Untuk keamanan yang lebih kuat maka fungsi hash SHA-256 tersebut dikombinasikan dengan algoritma kriptografi Asimetris. Menurut Abood & Guirguis (2018), kriptografi asimetris memiliki keamanan yang lebih kuat dibandingkan dengan algoritma simetris. Algoritma kriptografi asimetris yang sering digunakan yaitu algoritma RSA dan juga Algoritma El-Gamal. Menurut Himawan et al. (2016), Algoritma RSA memiliki keunggulan dalam proses enkripsi dan dekripsi yang memiliki waktu proses jauh lebih cepat serta menghasilkan jumlah karakter ciphertext yang lebih sedikit dibandingkan algoritma El-Gamal.

Berdasarkan latar belakang tersebut diperlukan penelitian terhadap implementasi tanda tangan digital dengan kombinasikan fungsi hash dan kriptografi kunci asimetris. Adapun algoritma *hash* yang digunakan yaitu SHA-256 dan juga algoritma kriptografi kunci publik yang digunakan yaitu RSA yang digunakan dalam membuat tanda tangan digital.

1.3 Rumusan Masalah

Dengan latar belakang yang telah diuraikan, maka rumusan masalah yang dibahas adalah sebagai berikut :

1. Bagaimana mengembangkan perangkat lunak tanda tangan digital menggunakan algoritma SHA-256 dan RSA?
2. Bagaimana membandingkan *message digest* untuk menguji integritas file pada dokumen digital yang telah ditandatangani?
3. Bagaimana tingkat perubahan nilai *ciphertext* algoritma SHA-256 dan RSA pada tanda tangan digital dengan menggunakan metode *Avalanche Effect*?
4. Bagaimana pengaruh besarnya nilai kunci yang digunakan untuk membentuk kunci RSA terhadap lamanya proses penandatangan dokumen digital berekstensi PDF?

1.4 Tujuan Penelitian

Tujuan penelitian ini dilakukan adalah :

1. Mengembangkan perangkat lunak tanda tangan digital menggunakan algoritma SHA-256 dan RSA.
2. Membandingkan *message digest* untuk menguji integritas file pada dokumen digital yang telah ditandatangani.
3. Melakukan pengukuran perubahan nilai *ciphertext* algoritma SHA-256 dan RSA pada tanda tangan digital menggunakan *Avalanche Effect*.
4. Melakukan pengukuran waktu proses tanda tangan digital berdasarkan besarnya besarnya nilai kunci.

1.5 Manfaat Penelitian

Adapun manfaat penelitian ini adalah sebagai berikut :

1. Memberikan informasi, menambah wawasan dan ilmu pengetahuan, serta sumbangan literatur untuk pembaca khususnya yang berkaitan dengan tanda tangan digital pada dokumen digital dengan ekstensi pdf
2. Membantu perkembangan teknologi terutama dalam hal keamanan khususnya pada autentikasi suatu dokumen digital.

1.6 Batasan Masalah

Adapun batasan-batasan masalah pada penelitian ini adalah sebagai berikut :

1. Dokumen digital yang digunakan untuk tanda tangan digital berupa *file* berekstensi pdf.
2. Pengamanan dokumen digital hanya sebatas pada autentikasi keaslian *file* dokumen digital.
3. Tidak melihat proses pertukaran informasi pada *file* dokumen digital.

1.7 Sistematika Penulisan

Sistematika penulisan penelitian ini adalah :

BAB I. PENDAHULUAN

Bab I membahas latar belakang masalah, perumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Bab II membahas konsep dasar teori yang terkait dengan permasalahan penelitian yang juga digunakan dalam penelitian, seperti algoritma SHA-256 dan algoritma RSA. Bab II membahas hasil penelitian relevan terdahulu.

BAB III. METODOLOGI PENELITIAN

Bab III membahas tahapan-tahapan yang dilakukan pada penelitian. Rencana-rencana pada tahapan penelitian ini juga dideskripsikan secara rinci dengan mengacu pada suatu kerangka kerja. Pada bab ini juga berisi perancangan manajemen proyek pada pelaksanaan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Bab IV membahas pengembangan perangkat lunak yang digunakan sebagai sarana penelitian yang telah direncanakan pada Bab III.

BAB V. HASIL DAN ANALISIS PENELITIAN

Bab V membahas hasil dan analisis penelitian yang diperoleh dari pengujian yang telah dilakukan pada perangkat lunak yang dibangun berdasarkan rancangan penelitian yang direncanakan.

BAB VI. KESIMPULAN DAN SARAN

Bab VI menyimpulkan penelitian yang dilakukan berdasarkan hasil dan analisis penelitian. Bab ini menjelaskan saran-saran yang diharapkan dapat membantu penelitian terkait untuk kedepannya.

1.8 Kesimpulan

Berdasarkan uraian dari latar belakang masalah dengan mengautentikasi keaslian dokumen digital yang berupa file pdf dengan tanda tangan digital. Penelitian ini mengimplementasikan algoritma SHA-256 dan juga algoritma RSA.

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

Andi Rsiki Alvianto dan Darmaji. (2015). Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android. *Jurnal Sains Dan Seni ITS*, *4*(1).

Andika, R. A., Putradana, A. G., & Pahlevi, R. R. (2021). Aplikasi Enterprise Document Digital Signature menggunakan RSA dan SHA256 untuk WFH di Era Pandemi COVID-19. *E-Proceeding of Engineering*, *8*(5), 10179–10186.

Azdy, R. A. (2016). Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi (JNTETI)*, *5*(3), 184–191. https://doi.org/10.22146/jnteti.v5i3.255

Azzahra, N. J. (2022). Implementasi Tanda Tangan Digital untuk Pengamananan Dokumen Digital pada Pelaksanaan Smart Governance. *Informatika.Stei.Itb.Ac.Id*, *18219065*. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/Makalah2022/Makalah-II4031-Kripto-2022 (11).pdf

Himawan, C., Wibowo, T., Sulityo, B., Roestam, R., Wahyu, Y., & Wahyu, R. B. (2016). Studi Perbandingan Algoritma RSA dan Algoritma El-Gamal. *Seminar Nasional APTIKOM (SEMNASTIKOM)*, *6*(1), 28–29.

Ikhsan, J. D. (2022). *Implementasi Algoritma RSA dan Hash SHA-256 untuk Tanda*

Tangan Digital dalam Membangkitkan Kode QR Akses Masuk Kampus.

Jamaludin, J., Sulaiman, O. K., Tandungan, S., Putra, L. M., Yuswardi, Y., Yulianti, N., Sidabutar, J., Aisa, S., Tantriawan, H., Arizal, A., Mardalius, M., & Pakpahan, A. F. (2022). *Kriptografi: Teknik Keamanan Data*. Yayasan Kita Menulis. https://www.google.co.id/books/edition/Kriptografi_Teknik_Keamanan_Data/1W1tEAAAQBAJ?hl=en&gbpv=1&dq=metode+AES&pg=PA53&printsec=frontcover

Kanter, V. J. (2022). PENERAPAN SANKSI PIDANA PELAKU PEMALSUAN DOKUMEN YANG DILAKUKAN MELALUI MEDIA SOSIAL. *LEX CRIMEN*, *11*(2).

Kaur, R., & Kaur, A. (2012). Digital signature. *Proceedings: Turing 100 - International Conference on Computing Sciences, ICCS 2012*, 295–301. https://doi.org/10.1109/ICCS.2012.25

Munir, R. (2005). *Penggunaan Tanda-Tangan Digital untuk Menjaga Integritas Berkas Perangkat Lunak*. *2005*(Snati), 6–9.

Munir, R. (2018). Fungsi Hash. *Institut Teknologi Bandung*. *Dipetik Agustus*, *1*(2021), 2017–2018.

Muslih Muslih, & Lekso Budi Handoko. (2022). Pengujian Avalanche Effect Pada Kriptografi Teks Menggunakan Autokey Cipher. *Seminar Nasional Teknologi Dan Multidisiplin Ilmu (SEMNASTEKMU)*, *2*(1), 127–134. https://doi.org/10.51903/semnastekmu.v2i1.162

Setiawan, A., & Syahputra, T. (2020). *Implementasi Digital Signature Pada Lampiran Kelengkapan Dokumen Pengeluaran Menggunakan Algoritma Rivest Shamir Adleman Di Klinik Kecantikan London Beauty Center Medan*. *x*.

Suharya, Y., & Widia, H. (2020). Implementasi Digital Signature Menggunakan Algoritma Kriftografi RSA Untuk Pengamanan Data Di Smk Wirakarya 1 Ciparay. *Jurnal Informatika (Computing)*, *07*(01), 20–29.

Sulastri, S. (2019). *... Data Message Digest Algorithm 5 (Md5) Dan Secure Hash Algorithm (Sha-256) Pada Sistem Penjadwalan Karyawan Agrowisata Setya ….* *5*. https://lib.unnes.ac.id/35717/

Sulastri, S., & Putri, R. D. M. (2018). Implementasi Enkripsi Data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan. *Jurnal Teknik Elektro*, *10*(2), 70–74. https://doi.org/10.15294/jte.v10i2.18628

Sutopo, S. F., Marwati, R., & Kustiawan, C. (2020). Implementasi Digital Signature Algorithm (DSA) Menggunakan Secure Hash Algorithm-256 (SHA-256) pada Media Gambar. *Jurnal EurekaMatika*, *9*(2), 94–106.