

**IMPLEMENTASI TANDA TANGAN DIGITAL DENGAN ALGORITMA
RSA DAN VIGENERE CIPHER PADA RAPOR DIGITAL
DI SMK MUHAMMADIYAH 3 KLATEN UTARA**

SKRIPSI



disusun oleh

Aditya Benny Wicaksana

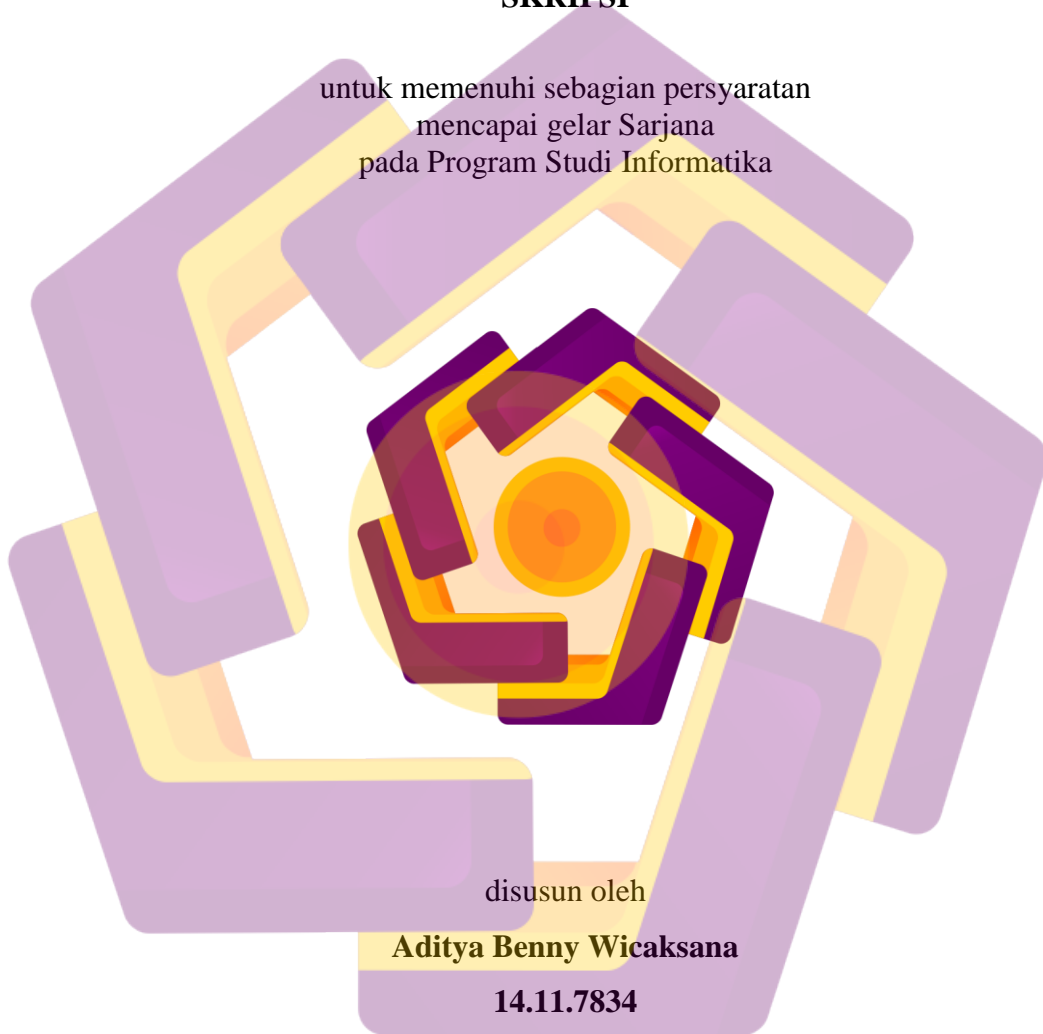
14.11.7834

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017**

**IMPLEMENTASI TANDA TANGAN DIGITAL DENGAN ALGORITMA
RSA DAN VIGENERE CIPHER PADA RAPOR DIGITAL
DI SMK MUHAMMADIYAH 3 KLATEN UTARA**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Aditya Benny Wicaksana

14.11.7834

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017**

PERSETUJUAN

SKRIPSI

**IMPLEMENTASI TANDA TANGAN DIGITAL DENGAN ALGORITMA
RSA DAN VIGENERE CIPHER PADA RAPOR DIGITAL
DI SMK MUHAMMADIYAH 3 KLATEN UTARA**

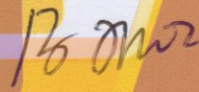
yang dipersiapkan dan disusun oleh

Aditya Benny Wicaksana

14.11.7834

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal

Dosen Pembimbing,



Barka Satya, M.Kom

NIK. 190302105

PENGESAHAN

SKRIPSI

**IMPLEMENTASI TANDA TANGAN DIGITAL DENGAN ALGORITMA
RSA DAN VIGENERE CIPHER PADA RAPOR DIGITAL
DI SMK MUHAMMADIYAH 3 KLATEN UTARA**

yang dipersiapkan dan disusun oleh

Aditya Benny Wicaksana

14.11.7834

telah dipertahankan di depan Dewan Penguji
pada tanggal 15 Desember 2017

Susunan Dewan Penguji

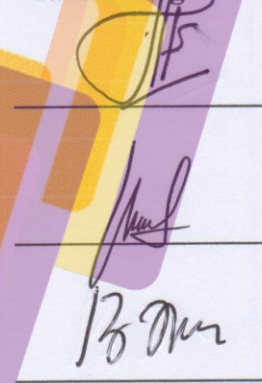
Nama Penguji

Anggit Dwi Hartanto, M.Kom
NIK. 190302163

Ike Verawati, M.Kom
NIK.190302237

Barka Satya, M.Kom
NIK. 190302105

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
tanggal 18 Desember 2017

DEKAN FAKULTAS ILMU KOMPUTER



Krisnawati, S.Si, M.T
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 20 Desember 2017

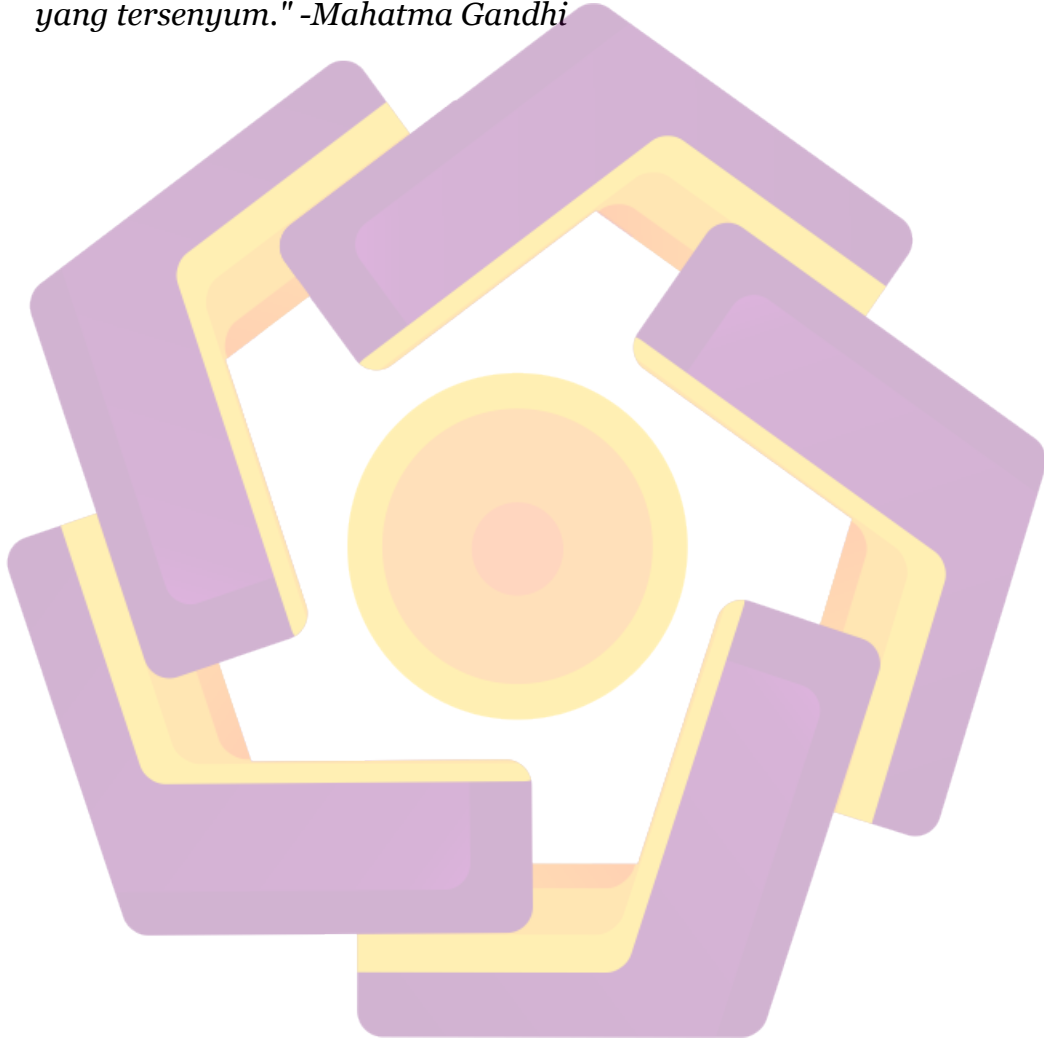


Aditya Benny Wicaksana

NIM. 14.11.7834

MOTTO

"Jadilah kamu manusia yang pada kelahiranmu semua orang tertawa bahagia, tetapi hanya kamu sendiri yang menangis; dan pada kematianmu semua orang menangis sedih, tetapi hanya kamu sendiri yang tersenyum." -Mahatma Gandhi



PERSEMBAHAN

Alhamdulillahirobbil‘alamiin, segala puji bagi Allah SWT yang telah mencurahkan rahmat dan karunia-Nya, sehingga Penulis mampu menyelesaikan Skripsi dengan judul “**Implementasi Tanda Tangan Digital Dengan Algoritma RSA dan Vigenere Cipher Pada Rapor Digital di SMK Muhammadiyah 3 Klaten Utara**” ini dengan baik.

Karya ini saya persembahkan untuk :

1. Allah SWT, yang telah memberikan pertolongan, kemudahan dan kelancaran selama perjuangan dalam menyelesaikan skripsi ini hingga akhirnya skripsi ini bisa tersusun dan selesai dengan baik.
2. Kedua Orang Tua tercinta Bapak Mukorobin dan Ibuk Sri Purwaningsih serta kakak saya satu – satunya Ika Vitasari Wahyuningtyas yang selalu menjadi motivasi saya untuk sukses dan tidak pernah lelah memberikan do'a , dukungan baik moral ataupun materil dan kasih sayang juga semangat selama ini.
3. Kepada Eyang Uti , Abang Imam , Abang Agung yang juga telah membantu dan memberikan dukungan selama saya menjalani studi di kampus ini.
4. Bapak Barka Satya, M.Kom yang telah memberikan bimbingan dalam skripsi ini.
5. Kepada objek penelitian saya SMK Muhammadiyah 3 Klaten Utara yang telah mengizinkan melakukan penelitian dan ikut membantu menyelesaikan skripsi ini.
6. Kepada Diyah Ayu Puspito Sari yang selalu menemani dan memberikan dukungan dari awal hingga sekarang saya dapat menyelesaikan studi saya.
7. Kepada kawan – kawan seperjuangan Sinta, Yuli, Komang, Evan, Ray, Irul, Hasan, Anggun yang telah mensupport dan menghibur selama mengerjakan skripsi ini.

8. Kawan – kawan 14 S1 TI 04 terimakasih telah menjadi bagian dalam menuntut ilmu selama ini , kalian luar biasa semoga kita bisa berkumpul lagi di puncak kesuksesan nanti.
9. Semua Pihak yang telah membantu tersusunnya skripsi ini yang tidak dapat saya sebutkan satu – persatu.



KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Alhamdulillahirobbil'alamin, puji syukur kehadiran Allah SWT atas rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan laporan skripsi ini.

Laporan ini disusun sebagai salah satu syarat untuk menyelesaikan studi di Universitas AMIKOM Yogyakarta pada Fakultas Ilmu Komputer. Sejak persiapan sampai selesainya Skripsi ini penulis menerima bantuan dan dukungan dari berbagai pihak yang penulis butuhkan guna terselesaikannya laporan ini. Untuk itu dalam kesempatan ini penulis mengucapkan terimakasih kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M selaku Rektor Universitas AMIKOM Yogyakarta.
2. Bapak Sudarmawan, S.T, M.T selaku Dekan Fakultas Sains dan Teknologi, dan Ketua Program Studi S1 Informatika.
3. Bapak Barka Satya, M.Kom selaku dosen pembimbing yang selalu memberikan bimbingan, waktu dan arahan dalam pembuatan skripsi ini.
4. Seluruh Dosen Universitas AMIKOM Yogyakarta yang telah men-sharing ilmu selama perkuliahan.
5. Semua pihak yang telah membantu dalam kelancaran penulisan skripsi ini baik langsung maupun tidak langsung yang tidak dapat penulis sebutkan satu – persatu.

Penulis menyadari bahwa laporan ini masih jauh dari sempurna, meskipun demikian penulis berharap semoga laporan ini bermanfaat bagi yang membacanya dan penulis dengan senang hati menerima kritik dan saran yang membangun dari para pembaca.

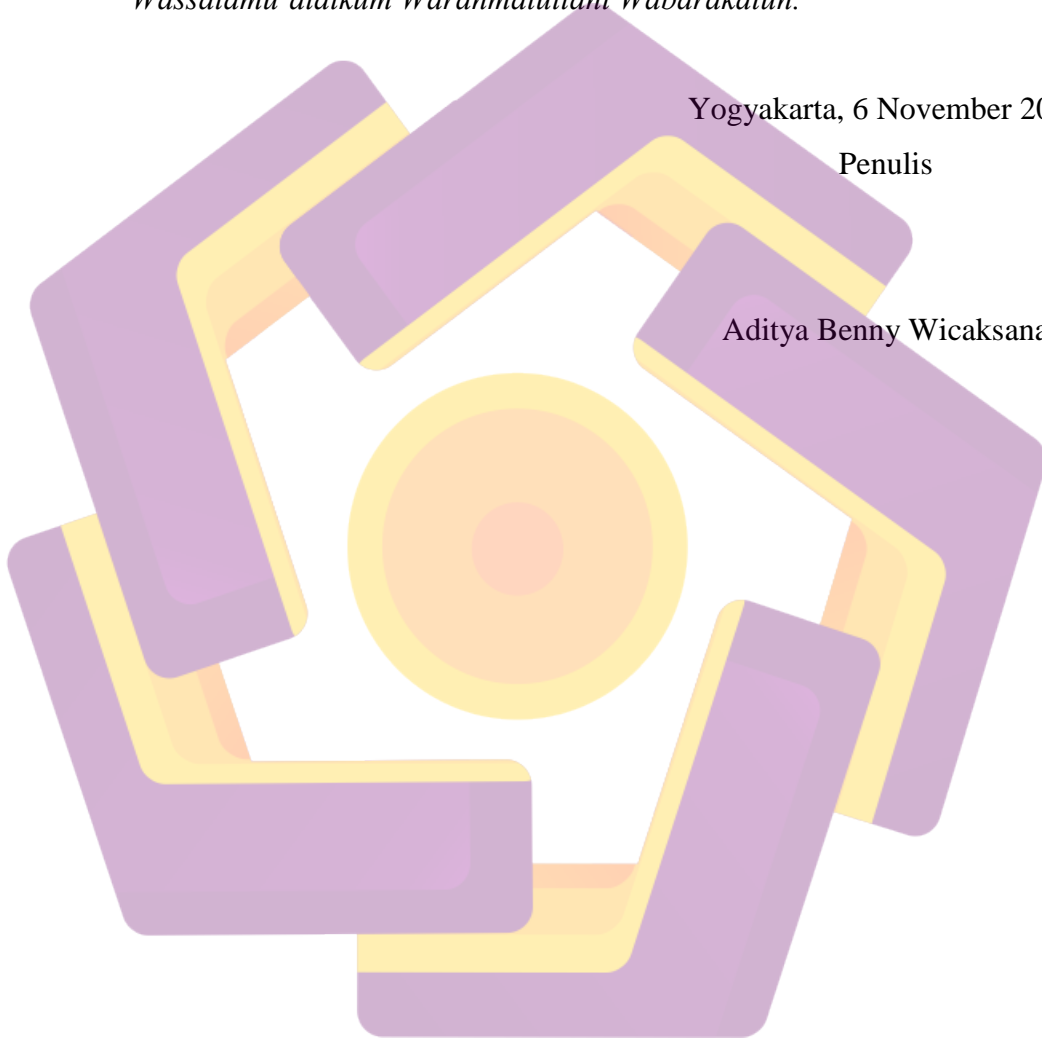
Akhir kata penulis berharap semoga hasil karya ini dapat berguna serta bermanfaat bagi perkembangan Teknologi dan Informasi pada khususnya. Serta sebagai kajian bagi mahasiswa Universitas AMIKOM Yogyakarta lainnya dalam pengambilan skripsi.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Yogyakarta, 6 November 2017

Penulis

Aditya Benny Wicaksana



DAFTAR ISI

| | |
|--|------|
| JUDUL..... | I |
| PERSETUJUAN | II |
| PENGESAHAN | III |
| PERNYATAAN..... | IV |
| MOTTO | V |
| PERSEMBAHAN..... | VI |
| KATA PENGANTAR | VIII |
| DAFTAR ISI..... | X |
| DAFTAR TABEL..... | XIII |
| DAFTAR GAMBAR | XIV |
| DAFTAR ISTILAH | XVII |
| ABSTRACT..... | XX |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 LATAR BELAKANG..... | 1 |
| 1.2 RUMUSAN MASALAH | 3 |
| 1.3 BATASAN MASALAH..... | 3 |
| 1.4 MAKSUD DAN TUJUAN PENELITIAN..... | 3 |
| 1.5 MANFAAT PENELITIAN..... | 4 |
| 1.6 METODE PENELITIAN | 4 |
| 1.6.1 METODE PENGUMPULAN DATA | 4 |
| 1.6.2 METODE ANALISIS | 5 |
| 1.6.3 METODE PERANCANGAN | 5 |
| 1.6.4 METODE PENGEMBANGAN | 5 |
| 1.7 Sistematika Penulisan | 5 |
| BAB II LANDASAN TEORI..... | 7 |
| 2.1 KAJIAN PUSTAKA..... | 8 |
| 2.2 KRIPTOGRAFI | 10 |
| 2.3 KRIPTOGRAFI MODERN..... | 14 |
| 2.4 KRIPTOGRAFI KUNCI PUBLIK | 16 |

| | | |
|---------------------------------------|--|-----------|
| 2.5 | KONSEP DASAR MATEMATIKA..... | 17 |
| 2.5.1 | Integer..... | 17 |
| 2.5.2 | <i>Group Ring</i> dan <i>Field</i> | 19 |
| 2.5.2.1 | <i>Group</i> | 19 |
| 2.5.2.2 | <i>Ring</i> | 20 |
| 2.5.2.3 | <i>Field</i> | 21 |
| 2.5.3 | <i>Finite Field</i> | 22 |
| 2.5.4 | Bilangan Prima..... | 23 |
| 2.5.5 | Aritmatika Modulo..... | 24 |
| 2.5.6 | Kekongrenan..... | 25 |
| 2.5.7 | Teorema Fermat..... | 25 |
| 2.5.8 | Teorema Euler..... | 26 |
| 2.5.9 | Algoritma Vigenere Cipher..... | 26 |
| 2.5.10 | Fungsi Hash Satu-Arah..... | 31 |
| 2.6 | <i>AUTHENTICATION</i> | 33 |
| 2.7 | TANDA TANGAN DIGITAL..... | 34 |
| 2.8 | ALGORITMA RSA (RIVEST-SHAMIR_ADLEMAN)..... | 37 |
| 2.9 | MODEL PENGEMBANGAN SISTEM DENGAN METODE WATERFALL..... | 43 |
| 2.10 | <i>DATA FLOW DIAGRAM (DFD)</i> | 46 |
| BAB III METODE PENELITIAN..... | | 48 |
| 3.1 | ALAT DAN BAHAN PENELITIAN..... | 48 |
| 3.1.1 | OBJEK PENELITIAN..... | 48 |
| 3.1.2 | METODE PENGUMPULAN DATA..... | 48 |
| 3.1.3 | ALAT PENELITIAN..... | 49 |
| 3.2 | ALUR PENELITIAN..... | 49 |
| 3.2.1 | PENGEMBANGAN SISTEM DENGAN METODE WATERFALL..... | 52 |
| 3.2.2 | ANALISIS SWOT..... | 55 |
| 3.2.2.1 | KEKUATAN (<i>STRENGTH</i>)..... | 55 |
| 3.2.2.2 | KELEMAHAN (<i>WEAKNESS</i>)..... | 56 |
| 3.2.2.3 | PELUANG(<i>OPPORTUNITY</i>)..... | 56 |

| | | |
|-----------------------------------|--|-----|
| 3.2.2.4 | ANCAMAN(<i>THREAT</i>) | 56 |
| 3.2.3 | PERANCANGAN SISTEM TANDA TANGAN DIGITAL | 57 |
| 3.2.3.1 | <i>FLOW CHART</i> | 57 |
| 3.2.3.2 | DFD (<i>DATA FLOW DIAGRAM</i>) | 60 |
| 3.2.3.3 | RANCANGAN BASIS DATA | 64 |
| 3.2.4 | PERANCANGAN ANTAR MUKA | 71 |
| BAB IV HASIL DAN PEMBAHASAN | | 74 |
| 4.1 | IMPLEMENTASI | 74 |
| 4.1.1 | IMPLEMENTASI PERANGKAT LUNAK | 74 |
| 4.1.2 | IMPLEMENTASI ANTAR MUKA | 75 |
| 4.1.3 | IMPLEMENTASI INSTALASI PROGRAM | 80 |
| 4.2 | HASIL PENELITIAN | 83 |
| 4.3 | PEMBAHASAN | 84 |
| 4.3.1 | SIMULASI TANDA TANGAN DIGITAL | 84 |
| 4.3.1.1 | PROSES PEMBUATAN KUNCI PUBLIK DAN PRIVAT | 84 |
| 4.3.1.2 | PROSES VERIFIKASI | 88 |
| 4.3.2 | ANALISA LAMA WAKTU EKSEKUSI | 108 |
| BAB V PENUTUP | | 110 |
| 5.1 | KESIMPULAN | 110 |
| 5.2 | SARAN | 110 |
| DAFTAR PUSTAKA | | 111 |
| LAMPIRAN KODE PROGRAM | | 113 |

DAFTAR TABEL

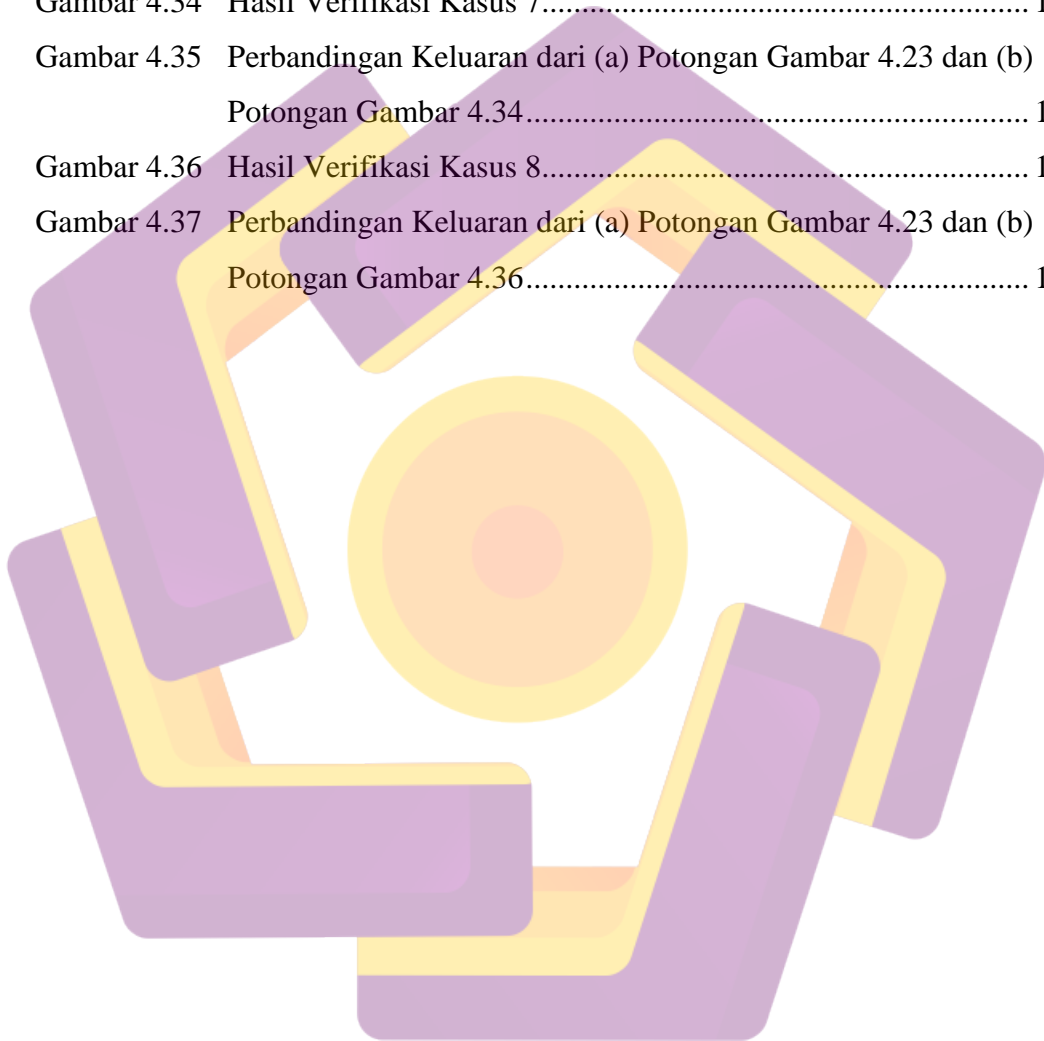
| | | |
|-----------|---|-----|
| Tabel 2.1 | Perbedaan Penelitian | 9 |
| Tabel 2.2 | Representasi Desimal, Heksadesimal dan Bit | 14 |
| Tabel 2.3 | Contoh Tabel Cayley F2 Perkalian dan Penjumlahan..... | 22 |
| Tabel 2.4 | Contoh Tabel Cayley F7 Perkalian dan Penjumlahan..... | 22 |
| Tabel 2.5 | Contoh Tabel Substitusi Algoritma Vigenere Cipher..... | 27 |
| Tabel 2.6 | Contoh Tabel Kriptografi dengan Algoritma Vigenere Cipher | 28 |
| Tabel 2.7 | Beberapa Algoritma Fungsi Hash | 33 |
| Tabel 2.8 | Tabel Korespondensi..... | 40 |
| Tabel 3.1 | Tabel Admin..... | 67 |
| Tabel 3.2 | Tabel Data_siswa | 67 |
| Tabel 3.3 | Tabel Mapel | 68 |
| Tabel 3.4 | Tabel Data_guru..... | 68 |
| Tabel 3.5 | Tabel Jurusan | 69 |
| Tabel 3.6 | Tabel Kelas..... | 69 |
| Tabel 3.7 | Tabel Ambil_kelas | 69 |
| Tabel 3.8 | Tabel Nilai..... | 70 |
| Tabel 3.9 | Tabel Data_rapot..... | 70 |
| Tabel 4.1 | Tanda Tangan (Kunci Publik & Privat) yang Digunakan..... | 83 |
| Tabel 4.2 | File E-dokumen Rapor Yang Telah Ditandatangani..... | 87 |
| Tabel 4.3 | Rekapitulasi Hasil Verifikasi dari Kasus 1 sampai 8..... | 107 |
| Tabel 4.4 | Lama Waktu Eksekusi pada Proses Tanda Tangan Digital | 108 |
| Tabel 4.5 | Lama Waktu Eksekusi pada Proses Verifikasi..... | 109 |

DAFTAR GAMBAR

| | | |
|-------------|---|----|
| Gambar 2.1 | Proses Kriptografi | 12 |
| Gambar 2.2 | Klasifikasi Kriptografi Secara Umum..... | 17 |
| Gambar 2.3 | Contoh Tabula Recta Algoritma Kriptografi Vigenere Cipher.... | 28 |
| Gambar 2.4 | Potongan Tabula Recta Baris ke-C | 29 |
| Gambar 2.5 | Contoh Potongan Tabula Recta Full Vigenere Cipher..... | 30 |
| Gambar 2.6 | Proses Hash | 32 |
| Gambar 2.7 | Proses Tanda Tangan Digital dan Verifikasi | 36 |
| Gambar 2.8 | Tahapan Pengembangan Sistem dengan Metode Waterfall..... | 43 |
| Gambar 2.9 | Simbol pada DFD..... | 47 |
| Gambar 3.1 | Alur Penelitian | 49 |
| Gambar 3.2 | Alur Proses Tanda Tangan Digital dengan Algoritma RSA | 51 |
| Gambar 3.3 | <i>Signing Flowchart</i> | 58 |
| Gambar 3.4 | <i>Verify Flowchart</i> | 59 |
| Gambar 3.5 | DFD Level 0..... | 60 |
| Gambar 3.6 | <i>DFD Level 1</i> | 62 |
| Gambar 3.7 | <i>Entity Relationship Diagram</i> | 65 |
| Gambar 3.8 | Relasi Antar Tabel..... | 66 |
| Gambar 3.9 | Perancangan Antar Muka Halaman Utama..... | 71 |
| Gambar 3.10 | Perancangan Antar Muka Halaman Tanda Tangan | 72 |
| Gambar 3.11 | Perancangan Antar Muka Halaman Verifikasi | 73 |
| Gambar 4.1 | Halaman Daftar Tanda Tangan Digital | 75 |
| Gambar 4.2 | Halaman Utama (Beranda)..... | 76 |
| Gambar 4.3 | Halaman Tanda Tangan (Pilih Kelas) | 76 |
| Gambar 4.4 | Halaman Tanda Tangan (Pilih NIS)..... | 77 |
| Gambar 4.5 | Halaman Tanda Tangan (Pilih File Rapor & ID Tanda Tangan). 77 | |
| Gambar 4.6 | Halaman Tanda Tangan (Hasil Akhir)..... | 78 |
| Gambar 4.7 | Halaman Verifikasi(Pilih Kelas Siswa) | 79 |
| Gambar 4.8 | Halaman Verifikasi(Pilih NIS Siswa) | 79 |

| | | |
|-------------|---|----|
| Gambar 4.9 | Halaman Verifikasi(Pilih File Rapor dan ID Tanda Tangan Digital) | 79 |
| Gambar 4.10 | Halaman Verifikasi(Hasil Akhir)..... | 80 |
| Gambar 4.11 | Gambar File Instalasi Sistem TTD..... | 80 |
| Gambar 4.12 | Gambar Langkah Pertama Instalasi XAMPP..... | 81 |
| Gambar 4.13 | Gambar Proses Instalasi XAMPP | 81 |
| Gambar 4.14 | Gambar Proses Menjalankan Web Server..... | 82 |
| Gambar 4.15 | Gambar Tampilan Sistem TTD Digital..... | 82 |
| Gambar 4.16 | Gambar Penginputan Kunci | 85 |
| Gambar 4.17 | Contoh Penandatanganan File 1703_XI_TKJ_2_Ganjil.pdf Dengan ID TTD Sri Wahyuni S.Kom..... | 86 |
| Gambar 4.18 | Contoh Penandatanganan File 1702_XI_TKJ_2_Ganjil.pdf Dengan ID TTD Sri Wahyuni S.Kom..... | 86 |
| Gambar 4.19 | File E-dokumen Rapor Yang Telah Ditandatangani _signed.pdf Dan Ukurannya | 88 |
| Gambar 4.20 | File E-dokumen Rapor yang Telah Diunduh oleh <i>Verifier</i> | 89 |
| Gambar 4.21 | Tampilan E-dokumen Rapor dengan <i>Signature</i> | 89 |
| Gambar 4.22 | Tampilan Potongan Halaman Pertama File 1704_XII_TKJ _Ganjil_sugned.pdf yang Diunduh <i>Verifier</i> | 91 |
| Gambar 4.23 | Hasil Verifikasi Terhadap File E-dokumen yang Diunduh Berdasarkan Gambar 4.22..... | 92 |
| Gambar 4.24 | Hasil Verifikasi Kasus 2..... | 93 |
| Gambar 4.25 | Perbandingan Keluaran dari (a) Potongan Gambar 4.23 dan (b) Potongan Gambar 4.24..... | 94 |
| Gambar 4.26 | Hasil Verifikasi Kasus 3..... | 95 |
| Gambar 4.27 | Perbandingan Keluaran dari (a) Potongan Gambar 4.23 dan (b) Potongan Gambar 4.26..... | 96 |
| Gambar 4.28 | Hasil Verifikasi Kasus 4..... | 97 |
| Gambar 4.29 | Perbandingan Keluaran dari (a) Potongan Gambar 4.23 dan (b) Potongan Gambar 4.28..... | 98 |
| Gambar 4.30 | Hasil Verifikasi Kasus 5..... | 99 |

| | | |
|-------------|--|-----|
| Gambar 4.31 | Perbandingan Keluaran dari (a) Potongan Gambar 4.23 dan (b) Potongan Gambar 4.30..... | 100 |
| Gambar 4.32 | Hasil Verifikasi Kasus 6..... | 101 |
| Gambar 4.33 | Perbandingan Keluaran dari (a) Potongan Gambar 4.23 dan (b) Potongan Gambar 4.32..... | 102 |
| Gambar 4.34 | Hasil Verifikasi Kasus 7..... | 103 |
| Gambar 4.35 | Perbandingan Keluaran dari (a) Potongan Gambar 4.23 dan (b) Potongan Gambar 4.34..... | 104 |
| Gambar 4.36 | Hasil Verifikasi Kasus 8..... | 105 |
| Gambar 4.37 | Perbandingan Keluaran dari (a) Potongan Gambar 4.23 dan (b) Potongan Gambar 4.36..... | 106 |



DAFTAR ISTILAH

- digital signature* : Tanda Tangan Digital, suatu mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya.
- GCD : Greatest Common Divisor, pembagi bersama terbesar.
- Kriptografi : Ilmu yang mempelajari tentang teknik-teknik matematika yang berhubungan dengan aspek-aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi
- Plaintext* : Informasi asli sebelum dienkripsi atau teks terang
- Enkripsi : Suatu proses transformasi plaintext menjadi ciphertext.
- Ciphertext* : Informasi acak yang berasal dari plaintext yang telah dimasukkan kedalam fungsi dan algoritma-algoritma matematika
- Dekripsi : Suatu proses pengubahan ciphertext menjadi plaintext
- Waterfall* : Merupakan salah satu metode pengembangan sistem yang diperkenalkan Herbert D. Benington pada tahun 1956
- Softcopy* : Merupakan file atau dokumen yang sebelumnya telah dibuat menggunakan komputer kemudian di simpan di media penyimpanan digital (CD , Hardisk, Flashdisk atau media penyimpanan lainnya)

Hardcopy : Merupakan sebuah dokumen yang sudah dalam bentuk cetak.

Message Digest : Merupakan angka yang dikalkulasi dari sistem informasi lewat fungsi kriptografi.

Hash : Hasil enkripsi dari sebuah password atau informasi yang dianggap penting.

MD5 : Message-Digest algorithm 5, merupakan fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit.

Algoritma : Kumpulan urutan perintah yang menentukan operasi-operasi tertentu yang diperlukan untuk menyelesaikan suatu masalah ataupun mengerjakan suatu tugas tertentu.

Digital : Merupakan penggambaran dari suatu keadaan bilangan yang terdiri dari angka 0 dan 1 atau *off* dan *on* (bilangan biner)

INTISARI

Tanda tangan digital adalah hasil transformasi kriptografi dari suatu pesan dengan panjang bit tertentu yang mampu menyediakan mekanisme untuk memverifikasi otentikasi asal, integritas data, dan non-repudiasi dari penanda tangan. Tujuan penelitian ini adalah mengimplementasikan tanda tangan digital pada rapor digital menggunakan algoritma RSA dan Vigenere Cipher.

Pengguna sistem terdiri dari dua entitas, yaitu pegawai, admin. Sistem yang dibangun mampu membangkitkan kunci pribadi dan kunci publik, membangkitkan tanda tangan kemudian ditulis di dalam rapor digital, serta memverifikasi tanda tangan menggunakan kunci publik dan privat.

Uji terhadap fungsionalitas sistem menunjukkan bahwa 100% fungsi berjalan dengan baik. Uji verifikasi tanda tangan dengan skenario tertentu menunjukkan bahwa file tanda tangan tidak tahan terhadap usaha ekstraksi dan kompresi ulang.

Kata Kunci: RSA, Vigenere, Rapor Digital, Tanda Tangan Digital

ABSTRACT

Digital signature is the result of a cryptographic transformation from a message with a certain length of bits that can provide a mechanism to verify the origin authentication, data integrity, and non-repudiation of the signatories. The purpose of this study is to implement digital signatures on digital rapport using the RSA and Vigenere Cipher algorithm.

Users of the system consists of two entities, namely employees, admin. The development system was able to generate the private key and public key, generate a signature then write the signature in digital rapport, and verify the signature with the public key and private key.

Functionality test of the system showed that 100% of the functions work is well. Verification test of signature with specific scenarios showed that the signature file was not resistant to the attempt of re-extraction and re-compression.

Keyword: *RSA , Vigenere, Digital Rapport, digital signature*