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

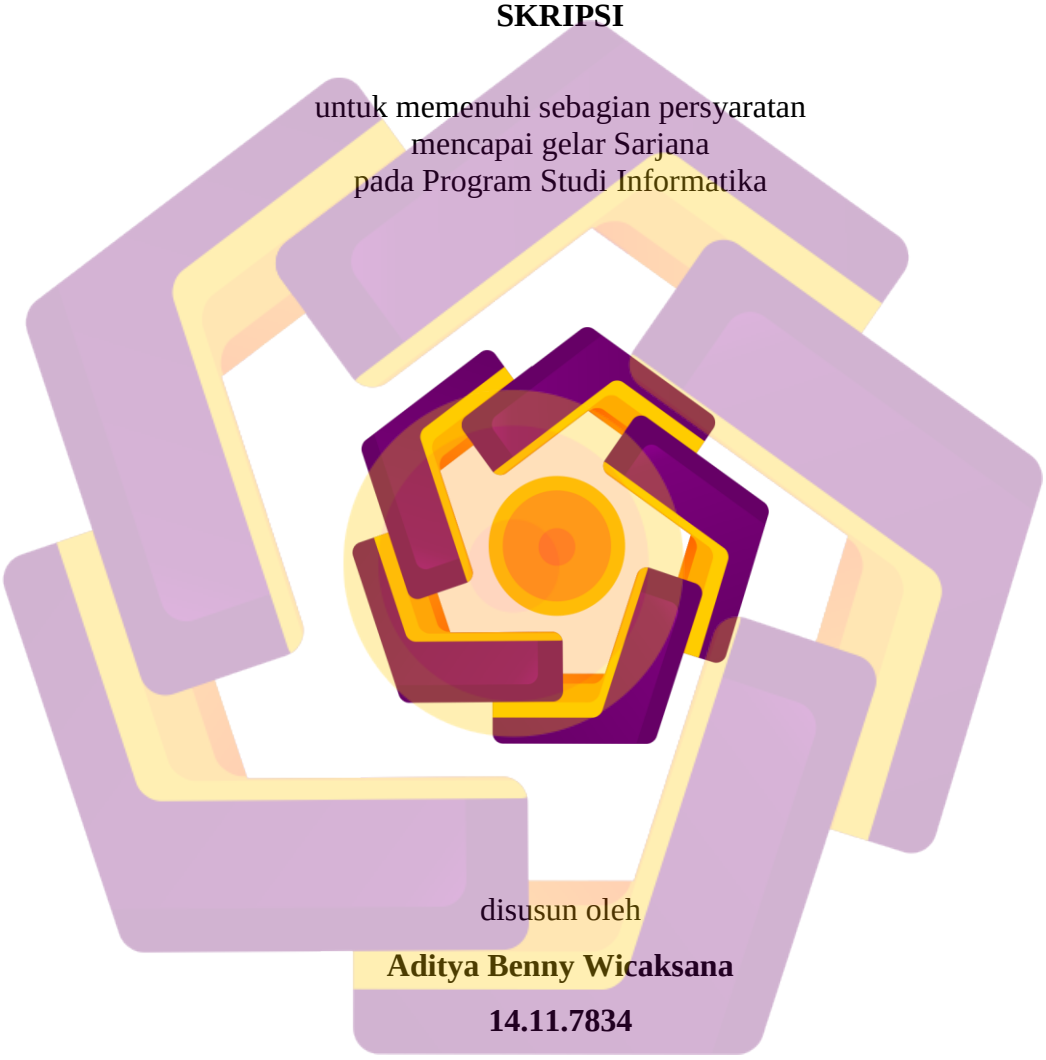
14.11.7834

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	Tanda Tangan
Anggit Dwi Hartanto, M.Kom **NIK. 190302163**	
Ike Verawati, M.Kom **NIK.190302237**	
Barka Satya, M.Kom **NIK. 190302105**	

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.

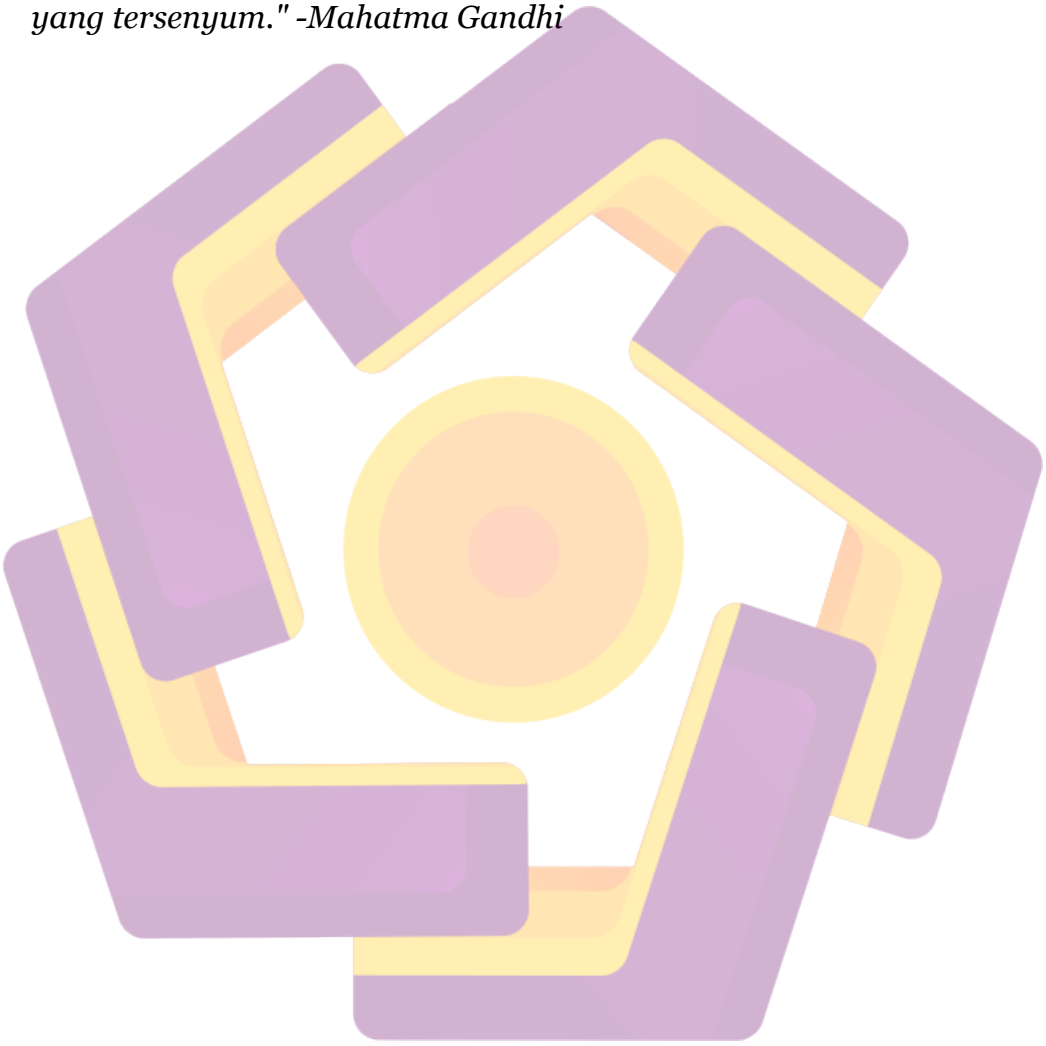
Yogyakarta, 20 Desember 2017

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



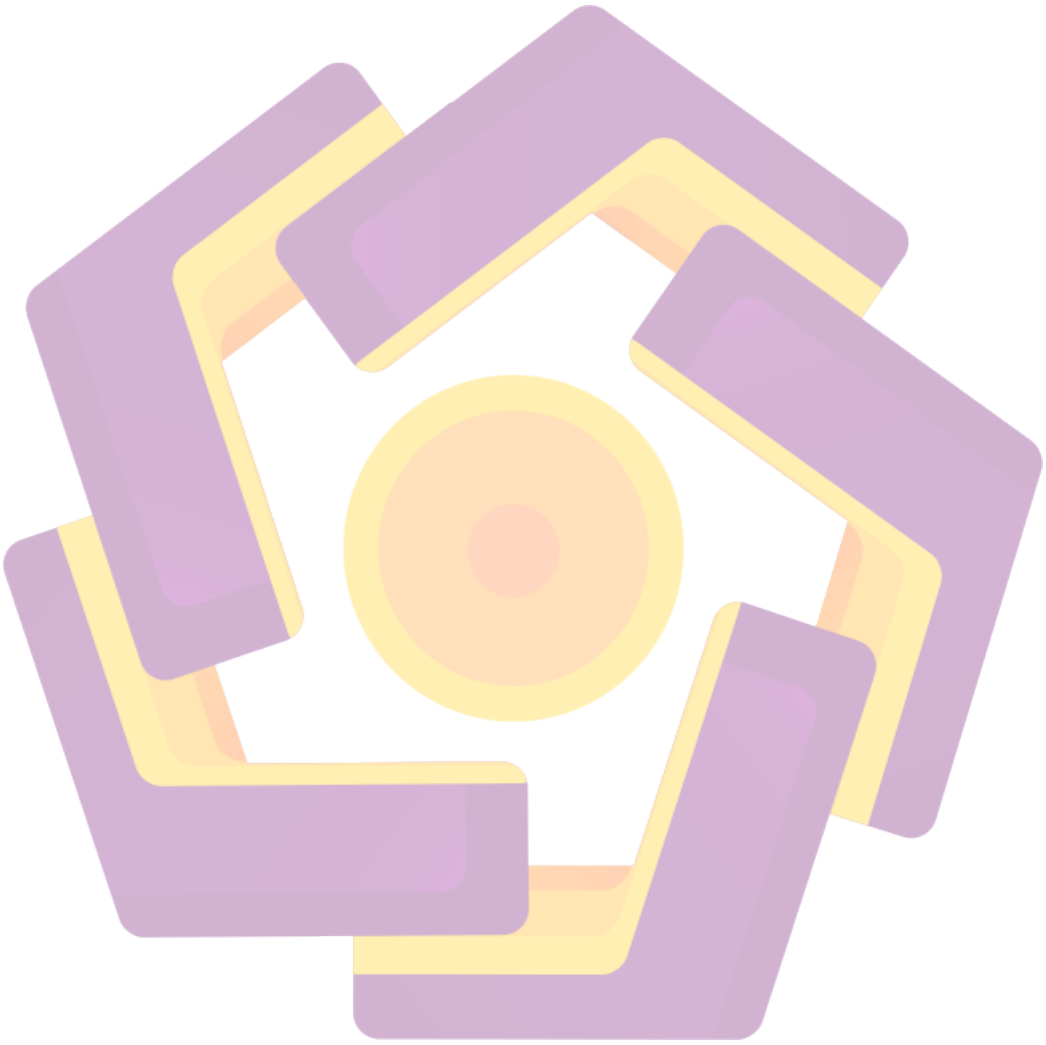
PERSEMBAHAN

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.

Alhamdulliahirobbil'alamin, puji syukur kehadirat 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

DAFTAR TABEL

DAFTAR GAMBAR

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.

Massage 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*