TUGAS AKHIR

IMPLEMENTASI ALGORITMA AES (ADVANCED ENCRYPTION STANDARD) DAN RSA (RIVEST SHAMIR ADLEMAN) UNTUK PENGAMANAN SURAT DI HUMANIKA

Binar Putri Pratiwi

14 1065 1060

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2018

HALAMAN PENGESAHAN

IMPLEMENTASI ALGORITMA AES (ADVANCED ENCRYPTION STANDARD) DAN RSA (RIVEST SHAMIR ADLEMAN) UNTUK PENGAMANAN SURAT DI HUMANIKA

BINAR PUTRI PRATIWI

14 1065 1060

Telah Mempertanggung Jawabkan Laporan Tugas Akhirnya Pada Sidang Tugas Akhir Tanggal 15 Maret 2018 Sebagai Salah Satu Syarat Kelulusan Guna Meraih Gelar Sarjana Komputer Program Studi Teknik Informatika Universitas Muhammadiyah Jember

Disetujui Oleh :

Dosen Penguji :	Dosen Pembimbing :
Penguji I	Pembimbing I
Daryanto, S. Kom., M.Kom	**Mudafiq Riyan Pratama, S. Kom., M.Kom**
NPK. 11 03 589	NPK. 12 03 720
Penguji II	Pembimbing II
Hardian Oktavianto, S. Si	**Triawan Adi Cahyanto, M. Kom**
NPK. 12 03 715	NPK 12 03 719
Mengesahkan,	Mengetahui,
Dekan Fakultas Teknik	Ketua Program Studi Teknik Informatika
Ir. Suhartinah, MT.	**Yeni Dwi Rahayu, S. ST., M. Kom**
NPK. 95 05 246	NIDN. 0716108602

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang Maha Pengasih lagi Maha Penyayang, Yang hanya kepadaNya-lah segala sesuatu bergantung. Alhamdulillah tak lupa senantiasa saya panjatkan karena hanya dengan ridho, kemurahan dan kekuasaanNya-lah proyek akhir yang berjudul:

"IMPLEMENTASI ALGORITMA AES (ADVANCED ENCRYPTION STANDARD) DAN RSA (RIVEST SHAMIR ADLEMAN) UNTUK PENGAMANAN SURAT DI HUMANIKA"

dapat diselesaikan dengan segala kelebihan dan tak lepas dari kekurangan yang terdapat di dalamnya.

Proyek akhir ini menjelaskan tentang pengamanan tanda tangan digital pada sistem informasi manajemen persuratan dengan algoritma AES dan RSA.

Dengan segala kerendahan hati, penulis memohon maaf jika ternyata di kemudian hari diketahui bahwa hasil dari proyek akhir ini masih jauh dari kesempurnaan. Semoga bermanfaat bagi setiap insan yang mempergunakannya untuk kebaikan di jalan Allah SWT.

Jember, 15 Maret 2018

Penulis

DAFTAR ISI

DAFTAR PUSTAKA

Albert, Rizal, Ike., *Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Emai*, Program Studi Sistem Komputer Fakultas Teknik Universitas Diponegoro, Jurnal Teknologi dan Sistem Komputer. Vol.3, No.2, 2015.

Kholifah, Riza, Nia., *Membangun Sistem Informasi Pengelolaan Surat Menggunakan Metode Waterfall Studi Kasus Direktorat Perencanaan Dan Studi Kasus Direktorat Perencanaan Dan Pengembangan Pendanaan Pembangunan*, Program Studi Sistem Informasi Universitas Telkom, Jurnal Tugas Akhir. Vol.2, No.1, 2015.

Menezes, A.J., *Handbook of Applied Cyrptography*, CRC Press, 1997.

Munir, Rinaldi., *Kriptografi*, Bandung, Informatika, 2006.

Persadh, Pratama. (2015). *E-Signature,Otentikasi Tanda Tangan Digital Modern*. Diakses 15 November 2017, diambil kembali dari https://techno.okezone.com/read/2015/10/14/207/1231664/e-signature-otentikasi-tanda-tangan-digital-modern/feed.

Raharjo, Budi., *Pemrograman Web Dengan Php + Oracle*, Bandung, Informatika Bandung, 2011.

Rahmad, Muhammad, Yudi dkk., *Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma Advanced Encryption Standard (AES)*, Tangerang: Jurnal Sisfotek Global. Vol. 6,No.2, 2016.

Rohman, Abdul., *Mengenal Framework "Laravel"*, 2014.

Rosnawan., *Aplikasi Algoritma RSA Untuk Keamanan Data Pada Sistem Informasi Berbasis Web*, Skripsi, Program Studi Matematika, Universitas Negeri Semarang, 2011.

Sipahutar, Tetti., *Perancangan Aplikasi QR Code Generator Dan QR Code Reader Menggunakan Metode Stroke Histogram*, 2014.

Stalling, William., *Cryptography and Network Security Principles and Practices Third Edition*, New Jersey, Prentice Hall, 2003.

Warsanto., *Kearsiapn I*, Kanisius (Anggota IKAPI), 1991.

Waskito., *Sistem Navigasi Di Dalam Ruangan Berbasis QR Code Tag*, Skripsi, Program Studi Teknik Informatika, Universitas Muhammadiyah Jember, 2017.

Wibowo, Budi, Junius., *Penerapan Algoritma Kriptografi Asimetris RSA Untuk Keamanan Data Di Oracle*: Jurnal Informatika, Vol 5, No.1, 2009.

Kurniawan, A. (2012). *Network Forensic*. Yogyakarta: Andi Offset.

Parmo, I. (2008, juni 6). *Mengenal Dunia Hacking : Sniffing*. Retrieved fromisparmo.web.id:http://isparmo.web.id/2008/06/06/mengenal-dunia-hacking-sniffing/

Supriyono., *Pengujian Sistem Enkripsi-Dekripsi Dengan Metode RSA Untuk Pengamanan Dokumen*: JFN, Vol 2 No 2, 2008.