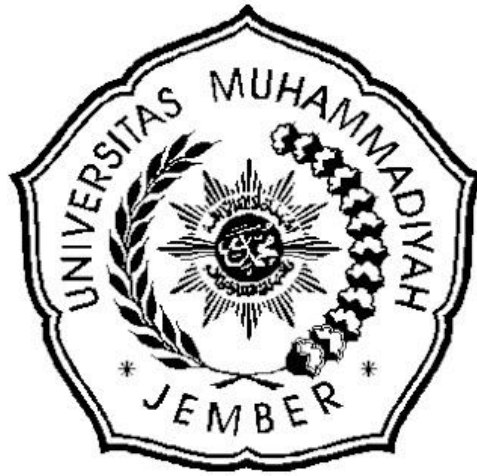


TUGAS AKHIR

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 :

Penguji I

Daryanto, S. Kom., M.Kom

NPK. 11 03 589

Penguji II

Hardian Oktavianto, S. Si

NPK. 12 03 715

Mengesahkan,

Dekan Fakultas Teknik

Ir. Suhartinah, MT.

NPK. 95 05 246

Dosen Pembimbing :

Pembimbing I

Mudafiq Riyan Pratama, S. Kom., M.Kom

NPK. 12 03 720

Pembimbing II

Triawan Adi Cahyanto, M. Kom

NPK 12 03 719

Mengetahui,

Ketua Program Studi Teknik Informatika

Yeni Dwi Rahayu, S. ST., M. Kom

NIDN. 0716108602

KATA PENGANTAR

Puji syukur kehadiran 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

Halaman Judul.....	i
Halaman Pengesahan	ii
Halaman Pernyataan.....	iii
Abstrak	iv
Abstract	v
Halaman Persembahan dan Terimakasih	vi
Kata Pengantar	viii
Daftar Isi	ix
Daftar Gambar.....	xii
Daftar Tabel	xiv
BAB I. PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Perumusan Masalah	2
1.3. Batasan Masalah	2
1.4. Tujuan	3
1.5. Manfaat	3
BAB II. TINJAUAN PUSTAKA	4
2.1. Penelitian Terdahulu	4
2.2. Surat	5
2.3. Tanda Tangan Digital	5
2.4. Metode <i>Rivest Shamir Adleman</i>	7
2.4.1. Perumusan Algoritma Rivest Shamir Adleman.....	7
2.4.2. Algoritma Membangkitkan Pasangan Kunci	8
2.4.3. Algoritma Enkripsi dan Dekripsi	9
2.4.4. Keamanan Rivest Shamir Adleman	9
2.5. Metode <i>Advance Encryption Standard</i>	10
2.5.1. Enkripsi	10
2.5.1.1. SubBytes.....	11
2.5.1.2. ShiftRows	12
2.5.1.3. MixColumns	12
2.5.1.4. AddRoundKey	13
2.5.2. Dekripsi.....	13
2.5.2.1. InvShiftRows.....	13
2.5.2.2. InvSubBytes	14
2.5.2.3. InvMixColumns.....	14
2.5.2.4. InvRoundKey.	15

2.5.3. Ekspansi Kunci	15
2.6. QR Code.....	17
2.7. PHP	18
2.8. Database	18
2.9. Sniffing	19
BAB III. METODOLOGI PENELITIAN	21
3.1. Studi Literatur	21
3.2. Pengambilan Data	21
3.3. Perancangan Sistem	22
3.3.1. Perancangan Basis Data.....	22
3.3.2. Digram Arus Tanda Tangan Surat	22
3.4. Implementasi	23
3.4.1. Spesifikasi Kebutuhan	23
3.4.2. Flowchart Sistem Pembuatan Surat Dan Enkripsi	24
3.4.3. Flowchart Sistem Cek Validasi Dan Dekripsi	26
3.4.4. Perancangan Halaman Antar Muka	27
BAB IV. PEMBAHASAN DAN IMPLEMENTASI	30
4.1. Implementasi	30
4.1.1. Implementasi Basis Data	30
4.1.2. Implementasi Fungsionalitas	31
4.1.2.1. Fungsionalitas Membuat Surat Undangan Dan Surat 3Keterangan Aktif Organisasi	31
4.1.2.2. Fungsionalitas Permintaan Persetujuan Surat.....	33
4.1.2.3. Fungsionalitas Persetujuan Surat Dengan Enkripsi AES Dan RSA	34
4.1.2.4. Fungsionalitas Cetak Surat	37
4.1.2.5. Fungsionalitas Scan QRCode Dengan Dekripsi AES Dan RSA	38
4.1.2.6. Fungsionalitas Persetujuan Surat Tanpa Enkripsi AES Dan RSA	40
4.2. Pengujian	41
4.2.1. Keaslian Surat	41
4.2.1.1. QRCode Tanpa Enkripsi AES Dan RSA.....	41
4.2.1.2. QRCode Dengan Enkripsi AES Dan RSA	44
4.2.2. Keamanan Jaringan	47
4.2.2.1. Keamanan Jaringan Tidak Menggunakan SSL ..	48
4.2.2.2. Keamanan Jaringan Menggunakan SSL.....	50

BAB V. KESIMPULAN DAN SARAN	54
5.1. Kesimpulan.....	54
5.2. Saran	54
Daftar Pustaka	55
Lampiran	57
Identitas Penulis	61

DAFTAR PUSTAKA

- Albert, Rizal, Ike., *Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email*, 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 Cryptography*, 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., *Kearsipn I*, Kanisius (Anggota IKAPI), 1991.

- Waskito., *Sistem Navigasi Di Dalam Ruang 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 from <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.