



LAPORAN SKRIPSI

PENERAPAN ALGORITMA RSA DAN AES 256 BIT PADA PENGAMANAN DATA TRANSAKSI (STUDI KASUS : FOODMOCHI SUKOHARJO)

Disusun Oleh :

Nama : Dziky Ridhwanullah

NIM : 12.5.00202

Program Studi : Teknik Informatika

Jenjang Pendidikan : Strata 1

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

SINAR NUSANTARA

SURAKARTA

2017



LAPORAN SKRIPSI
PENERAPAN ALGORITMA RSA DAN AES 256 BIT PADA PENGAMANAN
DATA TRANSAKSI
(STUDI KASUS : FOODMOCHI SUKOHARJO)

Laporan ini disusun guna memenuhi salah satu syarat
untuk menyelesaikan program pendidikan strata 1
pada

STMIK Sinar Nusantara Surakarta

Disusun oleh :

Nama : Dziky Ridhwanullah

NIM : 12.5.00202

Jurusan : Teknik Informatika

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

SINAR NUSANTARA

SURAKARTA

2017



SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

STMIK SINAR NUSANTARA SURAKARTA

SURAT PERNYATAAN PENULIS

JUDUL : Penerapan Algoritma RSA dan AES 256 bit pada Pengamanan Data
Transaksi Studi Kasus : Foodmochi Sukoharjo

NAMA : Dziky Ridhwanullah

NIM : 12.5.00202

“Saya menyatakan dan bertanggung jawab dengan sebenarnya bahwa Skripsi ini adalah hasil karya sendiri kecuali cuplikan dan ringkasan yang masing-masing telah saya jelaskan sumbernya. Jika pada waktu selanjutnya ada pihak lain mengklaim bahwa Skripsi ini sebagai karyanya disertai dengan bukti-bukti yang cukup, maka saya bersedia untuk dibatalkan gelar Sarjana Komputer saya beserta hak dan kewajiban yang melekat pada gelar tersebut”.

Surakarta, September 2017



Dziky Ridhwanullah

PERSETUJUAN LAPORAN SKRIPSI

Nama Pelaksana Skripsi : Dziky Ridhwanullah
Nomor Induk Mahasiswa : 12.5.00202
Prodi / Jenjang Pendidikan : Teknik Informatika / Strata 1
Judul Skripsi : PENERAPAN ALGORITMA RSA DAN AES
256 BIT PADA PENGAMANAN DATA
TRANSAKSI STUDI KASUS : FOODMOCHI
SUKOHARJO
Dosen Pembimbing 1 : Wawan Laksito S.Si, M.Kom
Dosen Pembimbing 2 : Teguh Susyanto S.Kom, M.Cs

Surakarta,.....

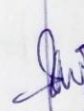
Menyetujui,

Pembimbing 1

Pembimbing 2



Wawan Laksito S.Si, M.Kom



Teguh Susyanto S.Kom, M.Cs

Mengetahui,

Ketua STMIK Sinar Nusantara



Kumaratih Sandradewi, SP., M.Kom



YAYASAN SINAR NUSANTARA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
SINAR NUSANTARA

Jl. KH. Samanhudi 84-86 Surakarta 57142 Telp./Fax. (0271) 716500
Http : //www.sinus.ac.id E-mail : sekretariat@sinus.ac.id

**PENGESAHAN TIM PENGUJI
PELAKSANAAN UJIAN SKRIPSI**

Nama : **Dziky Ridhwanullah**
NIM : 12.5.00202
Prodi : Teknik Informatika / S1
Judul Skripsi : Penerapan Algoritma RSA Dan AES 256 bit Pada Pengamanan Data Transaksi (Studi kasus : Foodmochi Sukoharjo)

Penguji I : Kustanto, ST., M.Eng
Penguji II : Dwi Remawati, S.Kom., M.Kom

Surakarta, 28 Agustus 2017

Mengesahkan

Penguji I

Kustanto, ST., M.Eng

Penguji II

Dwi Remawati, S.Kom., M.Kom

Kepala Program Studi

Iwan Ady Prabowo, M.Kom
NIK : 111000098

RINGKASAN

Foodmochi merupakan salah satu layanan jasa yang bergerak dalam pesan antar makan *online* yang berada di Kabupaten Sukoharjo. Transaksi pemesanan dilakukan secara *online*. Akan tetapi data-data penting tidak memiliki perlindungan keamanannya. Mengingat dampak negatif dari kemajuan teknologi terhadap pertukaran informasi seperti penyadapan, pencurian dan pemalsuan data, keamanan data sangat diperlukan. Tujuan skripsi ini untuk mengamankan data transaksi pada Foodmochi Sukoharjo. Objek penelitian dalam hal ini adalah data user, data temptransaksi dan data order.

Metode pengumpulan data yang digunakan peneliti adalah observasi, wawancara dan studi pustaka. Studi lapangan meliputi observasi dan wawancara. Sedangkan studi pustaka dilakukan dengan penelitian kepustakaan yang relevan dengan masalah tersebut.

Sistem keamanan data menggunakan algoritma RSA dan AES 256 bit ini diuji dengan pengujian validitas dan performa enkripsi-dekripsi. Pengujian validitas dengan membandingkan hasil dekripsi dengan *plaintext* setelah adanya proses enkripsi data. Sedangkan pengujian performa enkripsi-dekripsi dimana pengujian ini membandingkan durasi waktu yang dibutuhkan untuk enkripsi-dekripsi data. Hasil yang diperoleh pada pengujian validitas adalah hasil dekripsi sesuai dengan *plaintext* dan pada pengujian performa adalah algoritma RSA lebih unggul dalam melakukan enkripsi data daripada AES 256 bit dengan kecepatan enkripsi rata-rata 0.001605 detik dan algoritma AES 256 bit lebih unggul dalam dekripsi data dibandingkan dengan algoritma RSA dengan kecepatan dekripsi rata-rata 0.093832 detik.

SUMMARY

Foodmochi is one of service that providing online food delivery which is located in Sukoharjo. Booking transactions are done by online. However, the important data does not have security protection. Given the negative impact of technological advances on the exchange of information such as tapping, theft and data forgery, data security is indispensable. The purpose of this thesis is to secure transaction data on Foodmochi Sukoharjo. The object of research in this case is the user data, transaction data and order data.

Data collection methods used by researcher are observation, interview and literature study. Field studies include observation and interview. While the literature study is done by library research which relevant to the problem.

Data security systems using RSA and AES 256 bit algorithms are tested with validity testing and performance of decryption-encryption. Testing the validity by comparing the results of decryption with plaintext after the data encryption process. While testing the encryption-decryption performance where the test compares the duration of time required for encryption-decryption. The results obtained on the validity testing is the result decryption in accordance with plaintext and on the performance test RSA algorithm is better in encryption data than AES 256 bit with the average encryption speed of 0.001605 seconds and the AES 256 bit algorithm is better in data decryption compared to the RSA algorithm with an average decryption speed of 0.093832 seconds.

PERSEMBAHAN

1. Alhamdulillah, segala puji bagi Allah SWT yang telah memberikan keselamatan, kemudahan dan kelancaran dalam pengerjaan Skripsi ini.
2. Terima kasih kepada Abi dan Umi tercinta yang tak henti-hentinya menyemangati, mendoakan serta memotivasi yang terbaik.
3. Terima kasih kepada Keluargaku yang selalu memberikan semangat untuk menyelesaikan Skripsi ini.
4. Terima kasih kepada Dosen Pembimbing Bapak Wawan Laksito S.Si, M.Kom dan Bapak Teguh Susyanto S.Kom, M.Cs yang telah membimbing, memberi motivasi serta memberikan arahan terbaiknya dalam pengerjaan Skripsi ini.
5. Terimakasih kepada IT-E REVOLUTION yang selalu menemani dan menyemangati Penulis dalam mengerjakan skripsi ini.
6. Terimakasih kepada Saiful H, Sanggraha Adi Wicaksana L, M. Hanafi yang telah menjadi teman seperjuangan.
7. Terimakasih kepada rekan-rekan STMIK Sinar Nusantara yang telah memberi semangat kepada Penulis dalam mengerjakan skripsi ini.
8. Terimakasih pula kepada pihak-pihak terkait yang tidak dapat disebutkan satu persatu.

HALAMAN MOTTO

- ❖ *Hate no one, no matter how much they have wronged you. Live humbly, no matter how wealthy you become. Think positively, no matter how hard life is. Give much, even if you've been given little. Keep in touch with the ones who have forgotten you, and forgive who has wronged you, and don't stop praying for the best for those you love. – Ali Ibn Abi Talib.*

KATA PENGANTAR

Puji syukur kepada Allah SWT atas berkat, rahmat dan karunia-Nya, hingga penulisan laporan skripsi ini dapat diselesaikan dengan judul “Penerapan Algoritma RSA dan AES 256 pada Pengamanan Data Transaksi (Studi Kasus : Foodmochi Sukoharjo)” dengan baik.

Dalam pembuatan laporan skripsi ini dari awal hingga akhir, telah banyak bantuan dan dukungan dari berbagai pihak. Pada kesempatan ini penulis mengucapkan terimakasih kepada:

1. Ibu Kumaratih Sandradewi SP., M.Kom selaku ketua STMIK Sinar Nusantara Surakarta yang telah memberikan izin dan fasilitasnya kepada penulis dalam menyelesaikan laporan skripsi.
2. Bapak Wawan Laksito S.Si, M.Kom selaku dosen pembimbing utama skripsi atas masukan saran, arahan dan semangat selama menyusun skripsi ini.
3. Bapak Teguh Susyanto S.Kom, M.Cs selaku dosen pembimbing pendamping skripsi atas masukan saran, arahan dan semangat selama menyusun skripsi ini.
4. Erik Triawan S.Kom selaku pimpinan dan segenap staff Foodmochi Sukoharjo atas bantuan, kritikan dan semangat kepada penulis selama penelitian.

Surakarta, September 2017

Dziky Ridhwanullah

DAFTAR ISI

LAPORAN SKRIPSI.....	i
LAPORAN SKRIPSI.....	iii
PERSETUJUAN LAPORAN SKRIPSI.....	iv
RINGKASAN.....	v
SUMMARY.....	vi
PERSEMBAHAN.....	vii
HALAMAN MOTTO.....	viii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	x
DAFTAR GAMBAR.....	xiii
DAFTAR TABEL.....	xvi
BAB I.....	1
PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	2
1.3 Pembatasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.5.1 Manfaat Bagi Perusahaan.....	4
1.6 Kerangka Pikir.....	4
1.7 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI.....	7
2.1 Jaringan Komputer.....	7
2.1.1 Klasifikasi Jaringan Komputer.....	7
2.2 Keamanan Data pada Jaringan Komputer.....	8
2.2.1 Layanan keamanan jaringan.....	8
2.2.2 Mekanisme Keamanan Jaringan.....	9

2.3	Kriptografi	13
2.3.1	Sejarah.....	13
2.3.2	Algoritma Kriptografi	13
2.3.3	Sistem Kriptografi.....	14
2.3.4	Mekanisme Algoritma Kriptografi.....	15
2.4	RSA (<i>Rivest Shamir Adleman</i>).....	16
2.4.1	Pembangkitan Kunci RSA	17
2.4.2	Proses Enkripsi RSA.....	18
2.4.3	Proses Dekripsi RSA.....	19
2.4.4	Bukti Sistem Kriptografi RSA	19
2.5	AES (<i>Advanced Encryption Standard</i>).....	20
2.5.1	Proses Enkripsi AES	21
2.5.2	Proses Dekripsi AES	21
2.6	PHP (<i>PHP Hypertext Preprocessor</i>)	21
2.7	Basis Data.....	22
2.7.1	Sistem Basis Data.....	23
2.7.2	Bahasa Basis Data	23
2.8	MYSQL	24
BAB III METODE PENELITIAN.....		26
3.1	Sumber Data	26
3.1.1	Data Primer	26
3.1.2	Data Sekunder	26
3.2	Metode Pengumpulan Data	27
3.2.1	Teknik Wawancara.....	27
3.2.2	Teknik Observasi	27
3.2.3	Studi Pustaka.....	27
3.3	Langkah Penelitian	28
3.3.1	Tahap Analisa Data.....	28
3.3.2	Tahap Analisa Kebutuhan Sistem	28
3.3.3	Tahap Perancangan Sistem	29

3.3.4	Tahap Implementasi Sistem	32
3.3.5	Tahap Pengujian Sistem	32
BAB IV GAMBARAN PENELITIAN.....		34
4.1	Tinjauan Pustaka	34
4.2	Data Penelitian	37
4.3	Keamanan Data	43
4.3.1	Proses Enkripsi.....	44
4.3.2	Proses Dekripsi	64
BAB V PEMBAHASAN		77
5.1	Analisa Sistem	77
5.2	Desain Sistem	77
5.2.1	Diagram konteks	78
5.2.2	<i>Hierarchy Input Process Output (HIPO)</i>	79
5.2.3	<i>Data Flow Diagram (DFD Level 0)</i>	80
5.2.4	<i>Data Flow Diagram (DFD Level 1)</i>	81
5.2.5	<i>Flowchart</i>	84
5.3	Implementasi Sistem	101
5.3.1	Analisa Kebutuhan Sistem	101
5.3.2	Hasil Implementasi Sistem.....	102
5.4	Pengujian Sistem	110
5.4.1	Pengujian Validitas	110
5.4.2	Pengujian Performa Enkripsi dan Dekripsi.....	111
BAB VI PENUTUP		114
6.1	Kesimpulan.....	114
6.2	Saran.....	115
DAFTAR PUSTAKA		116
LAMPIRAN		

DAFTAR GAMBAR

Gambar 1.1 Kerangka Pikir.....	4
Gambar 2.1 Hubungan antara mekanisme layanan dan keamanan jaringan (ITU, 1991)	12
Gambar 2.2 Tulisan yang Menggunakan <i>Hieroglyph</i> (Ariyus, 2008)	13
Gambar 2.3 Sistem RSA (Sadikin, 2012)	17
Gambar 4.1 Proses Enkripsi Menggunakan Algoritma RSA dan AES 256	43
Gambar 4.2 Proses Dekripsi Menggunakan Algoritma RSA dan AES 256	44
Gambar 4.3 Sistem Enkripsi RSA (Sadikin, 2012).....	45
Gambar 4.4 Gambar tabel ASCII.....	47
Gambar 4.5 Struktur Enkripsi (Sadikin, 2012)	49
Gambar 4.6 Memasukkan Kunci Kedalam State	50
Gambar 4.7 Memecah Kunci Kedalam 2 State	50
Gambar 4.8 Transformasi AddRoundKey pada Enkripsi AES.....	51
Gambar 4.9 Hasil Perhitungan Transformasi AddRoundKey pada Enkripsi AES	51
Gambar 4.10 <i>State</i> Awal Perhitungan Transformasi SubBytes	52
Gambar 4.11 Hasil Perhitungan Transformasi SubBytes	52
Gambar 4.12 Transformasi Shiftrows	53
Gambar 4.13 Hasil Perhitungan Transformasi MixColumns.....	54
Gambar 4.14 Langkah Awal Pembangkitan Kunci.....	55
Gambar 4.15 Operasi RotWord.....	55
Gambar 4.16 Operasi SubWord	55
Gambar 4.17 Perhitungan Xor dan Tabel Rcon 0	56
Gambar 4.18 Perhitungan dan Hasil Kolom 1, 2 dan 3	56
Gambar 4.19 Lanjutan Perhitungan dan Hasil Kolom 1, 2 dan 3	57
Gambar 4.20 Hasil Perhitungan Kunci Ronde 2.....	57
Gambar 4.21 Pembangkitan Kunci AES 256.....	58
Gambar 4.22 Proses dan Hasil Enkripsi AES 256	59

Gambar 4.23 Lanjutan Proses dan Hasil Enkripsi AES 256.....	60
Gambar 4.24 Lanjutan Proses dan Hasil Enkripsi AES 256.....	61
Gambar 4.25 Lanjutan Proses dan Hasil Enkripsi AES 256.....	62
Gambar 4.26 Lanjutan Proses dan Hasil Enkripsi AES 256.....	63
Gambar 4.27 Struktur Dekripsi AES (Sadikin, 2012)	64
Gambar 4.28 Transformasi AddRoundkey pada Dekripsi AES	65
Gambar 4.29 Hasil Perhitungan Transformasi AddRoundKey pada Dekripsi AES...	65
Gambar 4.30 Perhitungan Transformasi InvShiftRows	65
Gambar 4.31 Perhitungan Transformasi InvSubBytes.....	66
Gambar 4.32 Hasil Perhitungan Transformasi InvSubBytes	67
Gambar 4.33 Hasil Perhitungan Transformasi InvMixColumns	70
Gambar 4.34 Proses dan Hasil Dekripsi AES 256.....	71
Gambar 4.35 Lanjutan Proses dan Hasil Dekripsi AES 256.....	72
Gambar 4.36 Lanjutan Proses dan Hasil Dekripsi AES 256.....	73
Gambar 4.37 Lanjutan Proses dan Hasil Dekripsi AES 256.....	74
Gambar 5.1 Diagram Konteks Sistem.....	78
Gambar 5.2 HIPO Sistem Keamanan Data Transaksi	79
Gambar 5.3 DFD Level 0 Sistem Keamanan Data Transaksi.....	80
Gambar 5.4 DFD Level 1 Data Pelanggan.....	81
Gambar 5.5 DFD Level 1 Kelola Data Restoran	82
Gambar 5.6 DFD Level 1 Kelola Data Pemesanan.....	83
Gambar 5.7 DFD Level 1 Kelola Data Keranjang Belanja.....	83
Gambar 5.8 DFD Level 1 Kelola Admin	84
Gambar 5.9 <i>Flowchart</i> Pendaftaran Pelanggan	85
Gambar 5.10 <i>Flowchart</i> Pemesanan	86
Gambar 5.11 <i>Flowchart</i> Konfirmasi Pesanan	87
Gambar 5.12 <i>Flowchart</i> Pembangkitan Kunci RSA.....	88
Gambar 5.13 <i>Flowchart</i> Enkripsi RSA.....	90
Gambar 5.14 <i>Flowchart</i> Kerangka AES	92
Gambar 5.15 <i>Flowchart</i> Transformasi <i>AddRoundKey</i>	93

Gambar 5.16 <i>Flowchart</i> Transformasi <i>SubBytes</i>	94
Gambar 5.17 <i>Flowchart</i> Transformasi <i>ShiftRows</i>	95
Gambar 5.18 <i>Flowchart</i> Transformasi <i>MixColumns</i>	96
Gambar 5.19 <i>Flowchart</i> Ekspansi Kunci	97
Gambar 5.20 <i>Flowchart</i> Enkripsi AES	98
Gambar 5.21 <i>Flowchart</i> Dekripsi AES	99
Gambar 5.22 <i>Flowchart</i> Dekripsi RSA.....	100
Gambar 5.23 Pendaftaran Pelanggan	103
Gambar 5.24 Proses Enkripsi RSA dan AES 256 Pendaftaran Pelanggan	103
Gambar 5.25 Halaman Login Pelanggan	104
Gambar 5.26 Pemilihan Kategori Menu	104
Gambar 5.27 Pemilihan Menu	105
Gambar 5.28 Keranjang Belanja	105
Gambar 5.29 Proses Enkripsi RSA dan AES 256 pada Pemesanan	106
Gambar 5.30 Konfirmasi Pesanan	106
Gambar 5.31 Data <i>Invoice</i> Pelanggan	107
Gambar 5.32 Halaman List Data.....	108
Gambar 5.33 Detail Data Pesanan	108
Gambar 5.34 Konfirmasi Pesanan	109
Gambar 5.35 Data <i>Invoice</i> Pesanan	110
Gambar 5.36 Pengujian Validitas	111
Gambar 5.37 Data waktu Enkripsi-Dekripsi	112
Gambar 5.38 <i>Chart</i> Kecepatan Proses Enkripsi.....	112
Gambar 5.39 <i>Chart</i> Kecepatan Proses Dekripsi	113

DAFTAR TABEL

Tabel 2.1 Jumlah Ronde dan Panjang Kunci (Sadikin, 2012)	20
Tabel 4.1 Persamaan dan Perbedaan dengan Penelitian Terdahulu	35
Tabel 4.2 Data User.....	37
Tabel 4.3 Data Temptransaksi.....	40
Tabel 4.4 Data Order.....	41
Tabel 4.5 Tabel Substitusi untuk Transformasi SubBytes (NIST, 2001)	52
Tabel 4.6 Tabel Substitusi untuk Transformasi InvSubBytes (NIST, 2001)	66