



LAPORAN SKRIPSI

**APLIKASI KEAMANAN DOKUMEN PADA LKP BHASKORO
TRAINING EDUCATION CENTRE MENGGUNAKAN ALGORITMA
KRIPTOGRAFI ELGAMAL DENGAN BAHASA PEMROGRAMAN
JAVA BERBASIS DESKTOP**

Disusun Oleh:

Nama : Sri Widodo
NIM : 09.5.00099
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata 1

**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
SINAR NUSANTARA
SURAKARTA**

2015



LAPORAN SKRIPSI

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

Pada

STMIK Sinar Nusantara Surakarta

Disusun Oleh:

Nama : Sri Widodo

NIM : 09.5.00099

Program Studi : Teknik Informatika

Jenjang Pendidikan : Strata 1

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

SINAR NUSANTARA

SURAKARTA

2015

PERSETUJUAN LAPORAN SKRIPSI

Nama Pelaksana Skripsi : Sri Widodo
Nomor Induk Mahasiswa : 09.5.00099
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata 1
Judul Laporan Skripsi : Aplikasi Keamanan Dokumen pada LKP Bhaskoro
Training Education Centre menggunakan Algoritma
Kriptografi Elgamal dengan Bahasa Pemrograman
Java Berbasis Desktop
Dosen Pembimbing 1 : Wawan Laksito YS, S.Si, M.Kom
Dosen Pembimbing 2 : Sri Tomo, S.T, M.Kom

Surakarta, Februari 2015

Menyetujui,

Dosen Pembimbing 1

Dosen Pembimbing 2

(Wawan Laksito YS, S.Si, M.Kom)

(Sri Tomo, S.T, M.Kom)

Mengetahui

Ketua STMIK Sinar Nusantara

(Kumaratih Sandradewi, S.P, M.Kom)



**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
SINAR NUSANTARA**

Surat Pernyataan Penulis

Judul : Aplikasi Keamanan Dokumen pada LKP Bhaskoro Training Education Centre menggunakan Algoritma Kriptografi Elgamal dengan Bahasa Pemrograman Java Berbasis Desktop

Nama : Sri Widodo

NIM : 09.5.00099

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

Surakarta, Februari 2015

Sri Widodo

MOTTO

1. “Wahai orang-orang yang beriman jadikanlah sabar dan sholat sebagai penolongmu. Sesungguhnya Allah beserta orang-orang yang sabar.”

(Q.S Al Baqarah : 153)

2. Dimana ada kemauan, disitu pasti ada jalan.
3. *A Big Journey Begins with Little Step.*
4. Kalau dia bisa, saya juga bisa
5. *Every Action has an Equal and Opposite Reaction.*

PERSEMBAHAN

Laporan skripsi ini penulis persembahkan kepada

1. Ayah dan Ibu yang selalu mendukung dan mendoakan kesuksesan anak-anaknya.
2. Istriku yang selalu mendukung dan memberikan semangat.
3. Bapak Wawan Laksito YS, S.Si, M.Kom dan bapak Sri Tomo, S.T, M.Kom yang dengan sabar telah membimbing dan memberikan pengarahan dalam pengerjaan laporan skripsi.
4. Teman-teman STMIK Sinar Nusantara terutama angkatan 2009 yang tidak dapat saya sebutkan satu-persatu.
5. Bapak Ritwan Ervianto B.O yang telah memberikan kesempatan untuk melakukan penelitian di LKP Bhaskoro *Training Education Centre*.

RINGKASAN

Laporan skripsi dengan judul “Aplikasi Keamanan Dokumen pada LKP Bhaskoro Training Education Centre menggunakan Algoritma Kriptografi Elgamal dengan Bahasa Pemrograman Java Berbasis Desktop” telah dilaksanakan pada tanggal 1 September 2014 sampai dengan 31 Januari 2015.

Tujuan penyusunan skripsi yaitu terbentuknya aplikasi keamanan dokumen menggunakan algoritma kriptografi Elgamal dengan bahasa pemrograman java berbasis desktop yang siap diterapkan di LKP Bhaskoro *Training Education Centre*. Aplikasi ini diharapkan dapat menjadi alternatif pengamanan dokumen yang mudah digunakan dengan keamanan yang dapat dipertanggungjawabkan.

Metode yang digunakan dalam penelitian adalah metode interview, observasi, dan studi pustaka. Implementasi algoritma elgamal dalam bahasa pemrograman java terdiri dari pembuatan flowchart, pemilihan panjang kunci, pembuatan pseudocode, dan penulisan kode program dalam java dengan Netbeans.

Pengujian aplikasi dilakukan dengan melakukan pengujian fungsionalitas dan pengujian validitas. Pengujian fungsionalitas dilakukan dengan metode *black box*. Pengujian fungsionalitas dilakukan untuk mengetahui kesesuaian antara output aplikasi dengan tombol yang dipilih. Pengujian validitas dilakukan untuk mengetahui kesesuaian perhitungan aplikasi dengan perhitungan manual.

SUMMARY

The final project report entitled “Aplikasi Keamanan Dokumen pada LKP Bhaskoro Training Education Centre menggunakan Algoritma Kriptografi Elgamal dengan Bahasa Pemrograman Java Berbasis Desktop” has been fulfilled on September, 1st 2014 until Januari, 31st 2015.

The aim of this final project is the document security program is formed using Elgamal algorithm with desktop based Java which is ready to be applied at LKP Bhaskoro Training Education Centre. This program is expected to be the alternative of document security which is easy to use and security trusted.

The methods used in this research are interview, observation, and literature study. The implementation of Elgamal algorithm on Java consist of flowchart making, key length choosing, pseudocode making, and code program writing in Java with Netbeans.

The program is tested using fungsionality test and validity test. Fungsionality test is performed using black box method. The fungsionality test is done to find out the appropriation between output program and choosen button. Validity test is done to find out the appropriation between program quantification and manual quantification.

KATA PENGANTAR

Dengan memanjatkan puji syukur ke hadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan laporan Skripsi ini dengan judul “Aplikasi Keamanan Dokumen pada LKP Bhaskoro Training Education Centre menggunakan Algoritma Kriptografi Elgamal dengan Bahasa Pemrograman Java Berbasis Desktop”.

Laporan skripsi ini disusun sebagai salah satu kewajiban untuk melengkapi syarat dalam menyelesaikan program pendidikan Strata 1 pada STMIK Sinar Nusantara Surakarta.

Penyusunan laporan skripsi ini tidak lepas dari bimbingan dan bantuan berbagai pihak. Oleh karena itu dalam kesempatan ini penulis mengucapkan terima kasih kepada:

1. Ibu Kumaratih Sandradewi, SP, M.Kom selaku Ketua STMIK Sinar Nusantara.
2. Bapak Wawan Laksito YS, S.Si, M.Kom selaku Dosen Pembimbing I.
3. Bapak Sri Tomo, ST, M.Kom selaku Dosen Pembimbing II.
4. Segenap dosen STMIK Sinar Nusantara Surakarta.
5. Staf karyawan dan karyawan kampus STMIK Sinar Nusantara Surakarta.
6. Bapak Ritwan Ervianto BO, selaku Pimpinan LKP Bhaskoro *Training Education Centre*.
7. Kedua orang tua yang selalu memberikan dukungan, semangat dan doa.
8. Istri yang selalu mendukung dan memberikan semangat.
9. Semua sahabat yang telah banyak membantu memberikan sumbangan pemikiran dan saran dalam penyusunan laporan skripsi.

Semoga karya yang sederhana ini dapat memberikan manfaat kepada para pembaca.

Surakarta, Februari 2015

Penulis

DAFTAR ISI

HALAMAN JUDUL.....	i
PERSETUJUAN LAPORAN SKRIPSI	iii
SURAT PERNYATAAN PENULIS	v
MOTTO	vi
PERSEMBAHAN.....	vii
RINGKASAN.....	viii
SUMMARY	ix
KATA PENGANTAR	x
DAFTAR ISI.....	xi
DAFTAR GAMBAR	xv
DAFTAR TABEL.....	xvii
BAB I : PENDAHULUAN.....	1
1.1. Latar Belakang Masalah	1
1.2. Perumusan Masalah.....	2
1.3. Pembatasan Masalah.....	2
1.4. Tujuan Skripsi.....	3
1.5. Manfaat Skripsi.....	3
1.5.1. Bagi Akademik	3
1.5.2. Bagi Penulis	3
1.5.3. Bagi Instansi.....	3
1.6. Kerangka Pikir.....	3
1.7. Sistematika Penulisan.....	4

BAB II	: LANDASAN TEORI	7
2.1.	Dokumen	7
2.2.	Dokumen Digital	7
2.3.	Kriptografi	8
2.4.	Algoritma Kriptografi Simetris dan Asimetris	9
2.5.	Algoritma Kriptografi Elgamal	10
2.6.	Java	11
2.7.	Netbeans	11
2.8.	Studi Pustaka	11
BAB III	: METODE PENELITIAN	15
3.1.	Sumber Data	15
3.2.	Metode Pengumpulan Data	16
3.3.	Teknik Pengolahan Data.....	17
3.4.	Desain Sistem	17
3.5.	Pembuatan Program.....	18
3.6.	Implementasi	18
3.7.	Pengujian	18
3.8.	Penarikan Kesimpulan.....	19
BAB IV	TINJAUAN UMUM OBYEK PENELITIAN	20
4.1.	Variabel yang Digunakan dalam Algoritma Elgamal.....	20
4.2.	Pembangkitan Kunci.....	21
4.3.	Perhitungan Enkripsi	21
4.4.	Perhitungan Dekripsi	25
BAB V	PEMBAHASAN.....	29
5.1.	Algoritma dan <i>Flowchart</i>	29

5.1.1.	<i>Flowchart</i> Sistem	29
5.1.2.	<i>Flowchart</i> Proses	32
5.2.	<i>Pseudocode</i>	37
5.2.1.	<i>Pseudocode</i> Pembangkitan Kunci.....	37
5.2.2.	<i>Pseudocode</i> Proses Enkripsi	38
5.2.3.	<i>Pseudocode</i> Proses Dekripsi	38
5.3.	Perancangan Antar Muka (<i>Interface</i>)	39
5.3.1.	Desain Menu Utama	39
5.3.2.	Desain Menu Kunci	40
5.3.3.	Desain Menu Enkripsi.....	41
5.3.4.	Desain Menu Dekripsi	41
5.4.	Desain Teknologi.....	42
5.5.	Implementasi Program.....	43
5.5.1.	Penentuan Panjang Kunci	43
5.5.2.	Pembangkitan Kunci	44
5.5.3.	Skema Blok Pesan.....	45
5.5.4.	Cara Penggunaan Aplikasi	46
5.6.	Pengujian Aplikasi.....	52
5.6.1.	Pengujian Fungsional.....	52
5.6.2.	Pengujian Validitas	59
BAB VI PENUTUP		67
6.1.	Kesimpulan.....	67
6.2.	Saran	67
DAFTAR PUSTAKA		68

LAMPIRAN.....	69
---------------	----

DAFTAR GAMBAR

Gambar 1. 1 Skema Pemikiran Penelitian.....	4
Gambar 2. 1 Skema Enkripsi dan Dekripsi (Munir, 2006)	8
Gambar 2. 2 Skema Algoritma Simetris (Munir, 2006).....	9
Gambar 2. 3 Skema Algoritma Asimetri (Munir, 2006).....	10
Gambar 5. 1 <i>Flowchart</i> sistem pembangkitan kunci	29
Gambar 5. 2 <i>Flowchart</i> sistem enkripsi	30
Gambar 5. 3 <i>Flowchart</i> sistem dekripsi	31
Gambar 5. 4 <i>Flowchart</i> proses pembangkitan kunci	32
Gambar 5. 5 <i>Flowchart</i> proses enkripsi	34
Gambar 5. 6 <i>Flowchart</i> proses dekripsi	36
Gambar 5. 7 Menu Utama.....	39
Gambar 5. 8 Menu Kunci.....	40
Gambar 5. 9 Menu Enkripsi	41
Gambar 5. 10 Menu Dekripsi.....	42
Gambar 5. 11 Rekomendasi panjang kunci minimal	44
Gambar 5. 12 Blok pesan dengan byte tambahan	45
Gambar 5. 13 Pembangkitan kunci dan simpan kunci.....	46
Gambar 5. 14 file kunci publik	47
Gambar 5. 15 <i>File</i> daftar riwayat hidup (plainteks).....	47
Gambar 5. 16 <i>Input file</i> kunci dan <i>file</i> plainteks ke dalam aplikasi	48
Gambar 5. 17 <i>File</i> cipherteks dibuka dengan aplikasi notepad	49
Gambar 5. 18 <i>Input file</i> kunci privat dan <i>file</i> cipherteks ke dalam aplikasi.....	50

Gambar 5. 19 <i>File</i> plainteks hasil dekripsi aplikasi	51
Gambar 5. 20 <i>Output</i> variabel-variabel kunci pada aplikasi.....	59
Gambar 5. 21 Pengujian variabel P dengan BigInteger Calculator v1.14	60
Gambar 5. 22 Pengujian panjang variabel p, g, x, p	60
Gambar 5. 23 Kunci publik 24 bit.....	61
Gambar 5. 24 Perhitungan enkripsi oleh aplikasi	62
Gambar 5. 25 Kunci privat 24 bit	64
Gambar 5. 26 Perhitungan dekripsi oleh aplikasi	64

DAFTAR TABEL

Tabel 4. 1 Blok pesan dalam <i>ASCII</i>	22
Tabel 4. 2 Perhitungan enkripsi	23
Tabel 4. 3 Perhitungan dekripsi	26
Tabel 5. 1 Pengujian Menu Utama.....	52
Tabel 5. 2 Pengujian Menu Kunci.....	53
Tabel 5. 3 Pengujian Menu Enkripsi.....	55
Tabel 5. 4 Pengujian Menu Dekripsi.....	57
Tabel 5. 5 Hasil pengujian fungsionalitas	58
Tabel 5. 6 Perbandingan output aplikasi dan pengujian BigInteger Calc v1.14	61
Tabel 5. 7 Perhitungan manual enkripsi.....	62
Tabel 5. 8 Perbandingan hasil perhitungan aplikasi dan manual	63
Tabel 5. 9 Perhitungan manual dekripsi.....	65
Tabel 5. 10 Perbandingan hasil perhitungan aplikasi dan manual	65
Tabel 5. 11 Hasil pengujian validitas	66