

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI
ELGAMAL PADA DATA TEXT**

TUGAS AKHIR
sebagai salah satu syarat untuk memperoleh
gelar Sarjana Komputer
pada program studi **TEKNIK INFORMATIKA**

Disusun Oleh :
Binantara Parmadi
091110172



**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI INFORMATIKA & KOMPUTER INDONESIA
MALANG
2016**

Tugas Akhir berjudul
**IMPLEMENTASI ALGORITMA KRIPTOGRAFI
ELGAMAL PADA DATA TEXT**

Disusun Oleh :
Binantara Parmadi
091110172

Telah dipertahankan dalam sidang Tugas Akhir
pada Tanggal 1 Desember 2016
Dan dinyatakan telah memenuhi syarat untuk diterima

Komisi Sidang,

Komisi Penguji,

Daniel Rudiaman, ST., M.Kom
Ketua Sidang, Pembimbing Utama

Evy Poerbaningtyas, S.Si., MT
Penguji I

Johan Ericka W. P., M.Kom
Co Pembimbing

Sugeng Widodo M. Kom
Penguji II

Go Frendi Gunawan, M.Kom
Penguji III

Malang, 1 Desember 2016

SEKOLAH TINGGI INFORMATIKA & KOMPUTER INDONESIA

KETUA

(**Dr. Eva Handriyantini, S.Kom, M.MT**)

Lembar Persembahan

Teruntuk :

1. Tuhanku, karena KASIH, ANUGRAH dan JANJI-NYA diberi kesehatan untuk menyelesaikan tugas akhir ini.
2. Papa, mama, om, yang selalu menjadi motivasi bagi saya.
3. Kepada seluruh Dosen, Staf STIKI dan seluruh asisten dosen tak lupa saya ucapkan terima kasih terutama kepada Bapak Daniel Rudiaman S., ST, M.Kom dan Bapak Johan Ericka W.P, M.Kom yang senantiasa membantu dan memberikan waktunya sebagai dosen pembimbing dan co pembimbing.
4. Elliza Dianita, terima kasih telah menghiasi hariku dengan senyum gigi kelincimu.
5. Teman seperjuangan dikampus, terlebih David, Ulung, Likke, Danik

ABSTRAK

Parmadi, Binantara. (2016). IMPLEMENTASI ALGORITMA KRIPTOGRAFI ELGAMAL PADA DATA TEXT. Tugas Akhir, Program Studi Strata -1 Teknik Informatika STIKI – Malang.
Pembimbing : Daniel Rudiaman S., ST, M.Kom.

Kata kunci : Elgamal , keamanan, data, delphi.

Keamanan data merupakan syarat wajib yang harus diterapkan seseorang ataupun kelompok dalam menjaga privasinya. Karena tidak sedikit pihak yang tidak berwenang mencuri data tersebut yang seharusnya menjadi privasi digunakan untuk kepentingan pribadi maupun kepentingan tertentu. Implementasi keamanan data adalah salah satu cara efektif dalam mengamankan data demi menjaga privasi tersebut. Dengan melakukan implementasi algoritma Elgamal sebagai keamanan pada data, pihak yang tidak berwenang diharapkan tidak dapat dengan mudah mengetahui isi data yang telah diamankan.

KATA PENGANTAR

Dengan mengucapkan puji syukur kehadirat Tuhan Yang Maha Esa yang telah memberikan Berkah dan Rahmannya Nya kepada penulis dapat menyelesaikan Tugas Akhir dengan baik dan tepat waktunya untuk memenuhi sebagai salah satu syarat dalam menyelesaikan pogram studi strata 1 di Sekolah Tinggi Informatika dan Komputer Indonesia .

Melalui kesempatan ini, penulis menyampaikan rasa hormat dan terima kasih penulis yang sebesar-besarnya kepada pihak yang telah memberikan bantuan lahir maupun batin selama penulisan tugas akhir ini. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan rasa hormat dan terima kasih penulis kepada :

1. Ibu Dr. Eva Handriyantini,S.Kom., M.MT., selaku ketua Sekolah Tinggi informatika dan Komputer Indonesia.
2. Bapak Daniel Rudiaman S., ST, M.Kom dan Bapak Johan Ericka W.P, M.Kom.,selaku dosen pembimbing tugas akhir penulis.
3. Seluruh dosen STIKI Program Studi Informatika atas kesediaan membaginya ilmunya kepada penulis.

Penulis menyadari bahwa tugas akhir ini masih banyak kekurangan dan masih jauh dari sempurna. Untuk itu, saran dan kritik yang membangun, sangat penulis harapkan. Semoga tugas akhir ini membawa manfaat bagi penyusun maupun pihak lain yang menggunakannya.

Malang, November 2016

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
LEMBAR PERSEMBAHAN	iii
ABSTRAKSI	iv
KATA PENGANTAR	v
DAFTAR ISI	vi
DAFTAR GAMBAR	vii
DAFTAR TABEL	ix
DAFTAR SEGMENT PROGRAM	x
BAB I PENDAHULUAN	
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	1
1.3 Tujuan Penelitian	2
1.4 Batasan Masalah	2
1.5 Manfaat Penelitian	2
1.6 Metodologi Penelitian	2
1.7 Sistematika Penulisan	4
BAB II LANDASAN TEORI	
2.1 Kriptografi	6
2.1.1 Pengertian Kriptografi	6
2.1.2 Sejarah Kriptografi	7
2.1.3 Konsep Kriptografi.....	10
2.2 Algoritma Kriptografi Elgamal.....	11
2.2.1 Pembentukan Kunci	12
2.2.1.1 Tes Bilangan Aman	13
2.2.1.2 Tes Elemen Primitif	13
2.2.1.3 Algoritma Pembentukan Kunci	14
2.2.2 Enkripsi	15
2.2.2.1 Algoritma Enkripsi	16
2.2.3 Dekripsi	16

2.2.3.1	Algoritma Dekripsi	16
BAB III	ANALISA DAN PERANCANGAN	
3.1	Analisa Masalah	18
3.1.1	Permasalahan.....	18
3.1.2	Solusi Pemecahan	18
3.1.3	Analisa Kebutuhan Input	19
3.2	Perancangan Sistem	19
3.2.1	Proses Enkripsi	19
3.2.2	Proses Dekripsi	21
3.3	Flowchart Aplikasi.....	23
3.3.1	Flowchart Enkripsi	23
3.3.2	Flowchart Dekripsi.....	24
3.4	Desain Interface Sistem.....	25
BAB IV	IMPLEMENTASI DAN PEMBAHASAN	
4.1	Spesifikasi Hardware dan Software	27
4.1.1	Spesifikasi Pada Proses Pengembangan.....	27
4.1.1.1	Hardware	27
4.1.1.2	Software	27
4.2	Langkah-langkah Pembuatan Program	28
4.2.1	Penulisan Kode Program	28
4.2.1.1	Form Utama.....	28
4.2.1.2	Pembangkit Bilangan Prima.....	31
4.2.1.3	Pembuat Kunci	32
4.2.1.4	Enkripsi	33
4.2.1.5	Dekripsi	40
4.2.1.6	Buka File TXT	44
4.2.1.7	Buka File Enkripsi.....	45
4.2.1.8	Simpan.....	46
BAB V	PENUTUP	
5.1.	Kesimpulan	47
5.2.	Saran	48
DAFTAR PUSTAKA	49

DAFTAR GAMBAR

Gambar 3.1	Flowchart Proses Enkripsi	20
Gambar 3.2	Flowchart Proses Dekripsi	22
Gambar 3.3	Flowchart Enkripsi Pada Aplikasi	23
Gambar 3.4	Flowchart Dekripsi Pada Aplikasi	24
Gambar 3.5	Desain Interface Aplikasi.....	25
Gambar 4.1	Form Utama Aplikasi.....	28
Gambar 4.2	Pembangkit Bilangan Prima.....	31
Gambar 4.3	Pembuat Kunci	32
Gambar 4.4	Enkripsi	33
Gambar 4.5	Dekripsi	40
Gambar 4.6	Buka File TXT	44
Gambar 4.7	Buka File Enkripsi	45
Gambar 4.8	Simpan	46

DAFTAR TABEL

Tabel 4.1	Tabel Konversi ASCII	36
Tabel 4.2	Tabel Hasil Perhitungan Gamma	37
Tabel 4.3	Tabel Hasil Perhitungan Delta	38
Tabel 4.4	Tabel Hasil Perhitungan Chiperteks.....	39

DAFTAR SEGMENT PROGRAM

Segmen Program 4.1	Pembangkit Bilangan Prima.....	31
Segmen Program 4.2	Pembuat Kunci	32
Segmen Program 4.3	Enkripsi	33
Segmen Program 4.4	Dekripsi	40
Segmen Program 4.5	Buka File TXT.....	44
Segmen Program 4.6	Buka File Enkripsi	45
Segmen Program 4.7	Simpan.....	46