

ABSTRAK

Salah satu teknik pengamanan data adalah dengan menggunakan kriptografi. Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Suatu pesan teks dapat dienkripsi menggunakan algoritma kriptografi tertentu sehingga menghasilkan teks lain yang dinamakan ciphertext yaitu suatu teks yang berisi karakter-karakter yang akan sulit dimengerti atau tidak bermakna apabila dibaca oleh pihak yang tidak berkepentingan. Tugas akhir ini akan memperlihatkan contoh penerapan algoritma kriptografi Elgamal pada suatu teks. Teks akan dienkripsi sehingga menghasilkan suatu ciphertext, ciphertext ini kemudian dapat didekripsi kembali menjadi file teks seperti semula. Penggunaan tanda tangan digital (Digital Signature) bertujuan untuk memastikan integritas dan keaslian berita/data berikut pengirimnya.

ABSTRACT

One technique to secure data is cryptography. Cryptography is a science and an art to maintain the confidentiality of news. A text message can be encrypted using a particular cryptographic algorithm to produce another text called ciphertext. It is a text containing characters that would be difficult to understand or are not meaningful when read by unauthorized parties. This final project will show the application of ElGamal cryptography algorithms on a text. The text was encrypted so as to produce a ciphertext, then the ciphertext can be decrypted back into its original text file. The use of digital signatures aims to ensure the integrity and authenticity of the news / following data sender.

DAFTAR ISI

ABSTRAK.....	i
ABSTRACT.....	ii
KATA PENGANTAR	iii
DAFTAR ISI.....	v
DAFTAR TABEL.....	vii
DAFTAR GAMBAR	viii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	1
1.3 Tujuan	2
1.4 Pembatasan Masalah	2
1.5 Sistematika Pembahasan	2
BAB II DASAR TEORI.....	3
2.1 Kriptografi	3
2.1.1 Terminologi.....	4
2.1.2 Sejarah Kriptografi.....	6
2.1.3 Jenis-jenis Kriptografi.....	7
2.1.4 Public Key.....	10
2.2 Tanda Tangan Digital (Digital Signature)	11
2.2.1 Terminologi.....	11
2.2.2 Sejarah Tanda Tangan Digital	13
2.2.3 Cara Kerja Tanda Tangan Digital.....	13
2.3 NetBeans IDE	15
2.4 Algoritma ElGamal	15
BAB III PERANCANGAN	19
3.1 Perancangan Proses Generate Key	19
3.2 Perancangan Proses Enkripsi.....	21
3.3 Perancangan Proses Generate Digital Signature	23
3.4 Perancangan Proses Verifikasi Digital Signature	25
3.5 Perancangan Proses Dekripsi	27
3.6 Perancangan Antarmuka Pengguna	29

3.6.1 Perancangan Antarmuka menu utama	29
3.6.2 Perancangan Antarmuka Generate Key	29
3.6.3 Perancangan Antarmuka Enkripsi	30
3.6.4 Perancangan Antarmuka Buat Digital Signature	31
3.6.5 Perancangan Antarmuka Verifikasi Digital Signature	32
3.6.6 Perancangan Antarmuka Dekripsi	33
BAB IV DATA HASIL IMPLEMENTASI	34
4.1 Implementasi Menu Utama	34
4.2 Implementasi Generate Key	35
4.3 Implementasi proses enkripsi	36
4.4 Implementasi proses pembuatan digital signature	37
4.5 Implementasi proses verifikasi digital signature	38
4.6 Implementasi proses dekripsi	39
4.7 Pengujian	40
4.7.1 Pengujian Enkripsi	40
4.7.2 Pengujian Generate Digital Signature	41
4.7.3 Pengujian Verifikasi Digital Signature	42
4.7.4 Pengujian Dekripsi	43
4.7.5 Pengujian Jika terdapat perubahan pada pesan terenkripsi atau digital signature ..	44
BAB V KESIMPULAN DAN SARAN	50
5.1 Kesimpulan	50
5.2 Saran	50
DAFTAR PUSTAKA	51
LAMPIRAN A PROGRAM	A-1

DAFTAR TABEL

Tabel 4.1 Pengujian Enkripsi	41
Tabel 4.2 Pengujian Pembuatan Digital Signature	42
Tabel 4.3 Pengujian Verifikasi Digital Signature	443
Tabel 4.4 Pengujian Dekripsi	44

DAFTAR GAMBAR

Gambar 2.1 Enkripsi dan dekripsi	5
Gambar 2.2 Proses kriptografi simetris	8
Gambar 2.3 Proses Kriptografi Asimetris	9
Gambar 3.1 Flowchart Generate Key	19
Gambar 3.2 Flowchart Enkripsi	21
Gambar 3.3 Flowchart Generate Digital Signature	23
Gambar 3.4 Flowchart Verifikasi Digital Signature	25
Gambar 3.5 Flowchart Verifikasi Digital Signature	27
Gambar 3.6 Perancangan Antarmuka Form Menu Utama.....	29
Gambar 3.7 Perancangan Antarmuka Form Generate Key.....	29
Gambar 3.8 Perancangan Antarmuka Form Enkripsi	30
Gambar 3.9 Perancangan Antarmuka Form Buat Digital Signature	31
Gambar 3.10 Perancangan Antarmuka Form Verifikasi Digital Signature.....	32
Gambar 3.11 Perancangan Antarmuka Form Dekripsi.....	33
Gambar 4.1 Tampilan Antarmuka Menu Utama	34
Gambar 4.2 Tampilan Antarmuka Generate Key	35
Gambar 4.3 Tampilan Antarmuka Enkripsi.....	36
Gambar 4.4 Tampilan Antarmuka Generate Digital Signature.....	37
Gambar 4.5 Tampilan Antarmuka Verifikasi Digital Signature	38
Gambar 4.6 Tampilan Antarmuka Proses Dekripsi	39
Gambar 4.7 Pengujian Enkripsi.....	40
Gambar 4.8 Pengujian Pembuatan Digital Signature	41
Gambar 4.9 Pengujian Verifikasi Digital Signature	42
Gambar 4.10 Pengujian Dekripsi	43
Gambar 4.11 Enkripsi pesan asli	45
Gambar 4.12 Pembuatan Digital Signature	46
Gambar 4.13 Pesan gagal verifikasi perubahan pada file pesan hasil enkripsi	47
Gambar 4.14 Pesan gagal verifikasi perubahan pada file digital signature.....	48
Gambar 4.15 Pesan berhasil verifikasi	49
Gambar 4.16 Pesan berhasil didekripsi	49