

KATA PENGANTAR



Assalamu'alaikum Warahmatullahi Wabarak aatuh

Alhamdulillah Rabbil 'alamiin segala puji dan syukur atas kehadiran Allah SWT, yang telah memberi rahmat, tuntunan dan kemurahan -Nya hikmat dalam pengerjaan Proyek Akhir ini. Proyek Akhir yang berjudul **“Implementasi Algoritma RSA untuk Perlindungan Data pada Server FTP”** dengan segala kekurangan dan kelebihan dan merupakan salah satu syarat untuk memperoleh gelar Diploma Teknik Jurusan Teknik Komputer Politeknik Telkom.

Penulis berharap dengan pembuatan proyek akhir ini dapat membantu dan semoga kedepannya hal ini dapat dilakukan pengembangan melalui *ide-ide* kreatif dari para pembaca.

Penulis menyadari bahwa dalam penyusunan proyek akhir ini masih terdapat kekurangan karena keterbatasan penulis. Penulis memerlukan kritik dan saran dari para pembaca yang bersifat membangun demi penyempurnaan pada penulisan berikutnya. Semoga laporan penelitian ini dapat memberikan manfaat bagi kita semua.

DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR PERNYATAAN	ii
UCAPAN TERIMA KASIH	iii
KATA PENGANTAR	iv
ABSTRAK	v
ABSTRACT	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL	xi
BAB I PENDAHULUAN	12
1.1 Latar Belakang	12
1.2 Rumusan Masalah	13
1.3 Tujuan	13
1.4 Batasan Masalah	13
1.5 Metodologi Penelitian	14
BAB II TINJAUAN PUSTAKA	16
2.1 Pengenalan Kriptografi	16
2.2 Algoritma Kriptografi	17
2.2.1 Algoritma Simetris	17
2.2.2 Algoritma Asimetris	18
2.3 Algoritma <i>Rivest-Shamir-Adleman</i> (RSA).....	18
2.3.1 Serangan-Serangan di RSA	22
2.3.2 Keamanan Algoritma RSA	23
2.4 Jenis-Jenis Pola Penyerangan	24
2.5 Konsep <i>Client-Server</i>	26
2.5.1 <i>Socket Programming</i>	26
2.6 <i>File Transport Protocol</i>	27
BAB III ANALISIS KEBUTUHAN DAN PERANCANGAN	28
3.1 Kebutuhan Perangkat Keras	28

3.2	Kebutuhan Perangkat Lunak	28
3.3	Perancangan Sistem	28
3.3.1	<i>Usecase</i>	30
3.3.2	Skenario <i>Usecase</i> Diagram	31
3.3.3	Class Diagram	33
3.3.4	Diagram Sequence	34
3.3.5	Proses-proses di dalam Perangkat Lunak	36
3.4	Perancangan Antarmuka	43
BAB IV IMPLEMENTASI DAN PENGUJIAN		46
4.1	Implementasi	46
4.2	Pengujian.....	49
BAB V PENUTUP		55
5.1	Kesimpulan	55
5.2	Saran	55
DAFTAR PUSTAKA		56

DAFTAR GAMBAR

Gambar 2.1 Enkripsi dan Dekripsi	17
Gambar 2.2 Prosedur Kerja Algoritma Simetris	17
Gambar 2.3 Prosedur Kerja Algoritma Simetris	18
Gambar 2.3 Taxonomy of potential attack on RSA	22
Gambar 2.4 <i>Interruption</i>	24
Gambar 2.4 <i>Interception</i>	25
Gambar 2.4 <i>Modification</i>	25
Gambar 2.4 <i>Fabrication</i>	25
Gambar 2.5 Arsitektur jaringan <i>Client-Server</i>	26
Gambar 2.6 Hubungan <i>Client</i> dan <i>Server</i>	27
Gambar 3.3 Potongan program utama <i>server</i>	29
Gambar 3.3 Potongan program utama <i>client</i>	29
Gambar 3.3 <i>Skenario</i> pengujian	30
Gambar 3.3 <i>Usecase Server</i>	30
Gambar 3.3 Hubungan <i>Usecase Client</i>	31
Gambar 3.3 Class diagram <i>server</i>	34
Gambar 3.3 Diagram <i>sequence</i> menambah <i>user</i>	34
Gambar 3.3 Diagram <i>sequence</i> menghapus <i>user</i>	35
Gambar 3.3 Diagram <i>sequence</i> menjalankan <i>server</i>	35
Gambar 3.3 Diagram <i>sequence</i> mematikan <i>server</i>	36
Gambar 3.3 Proses pada <i>server</i>	37
Gambar 3.3 Proses pada <i>server</i>	38
Gambar 3.3 Proses pertukaran kunci publik	39
Gambar 3.3 Method run	39
Gambar 3.3 Mekanisme <i>login</i>	40
Gambar 3.3 Mekanisme pengiriman data	41
Gambar 3.3 Enkripsi data	41
Gambar 3.3 Dekripsi data	42
Gambar 3.4 Tampilan utama <i>server</i>	43

Gambar 3.4 Tampilan Tambah <i>User</i>	44
Gambar 3.4 Tampilan Hapus <i>User</i>	44
Gambar 3.4 Tampilan Login <i>User</i>	45
Gambar 3.4 Tampilan Hapus <i>User</i>	45
Gambar 4.1 Tampilan utama <i>server</i>	46
Gambar 4.1 Tampilan <i>login</i>	46
Gambar 4.1 Notifikasi login	47
Gambar 4.1 Daftar <i>file</i> yang dapat diambil	47
Gambar 4.1 Proses <i>Download</i>	48
Gambar 4.1 Notifikasi bahwa <i>file</i> selesai diambil	48
Gambar 4.1 <i>Button close</i>	48
Gambar 4.1 Tampilan utama <i>server</i>	48
Gambar 4.2 Tampilan awal Cain and Abel	49
Gambar 4.2 Tampilan <i>scann</i> Cain and Abel	50
Gambar 4.2 Tampilan <i>ARP Poison</i>	50
Gambar 4.2 <i>Host</i> yang telah <i>dipoisoning</i>	51
Gambar 4.2 Aktivitas yang terlihat oleh Wireshark	51
Gambar 4.2 Melihat aktivitas keseluruhan TCP	51
Gambar 4.2 Aktivitas TCP tanpa RSA	52
Gambar 4.2 Aktivitas TCP dengan RSA	53

DAFTAR TABEL

Tabel 2.3 Algoritma RSA	20
Tabel 3.1 Spesifikasi Komponen Jaringan	28
Tabel 3.2 Spesifikasi <i>Software</i>	28
Tabel 3.3 Skenario <i>usecase login</i>	31
Tabel 3.3 Skenario <i>usecase</i> mengelola user	32
Tabel 3.3 Skenario <i>usecase</i> menjalankan <i>server</i>	32
Tabel 3.3 Skenario <i>usecase</i> mematikan <i>server</i>	33
Tabel 3.3 Skenario <i>usecase</i> mengambil <i>file</i>	33
Tabel 4.2 Pengujian aplikasi menggunakan algoritma RSA	53
Tabel 4.2 Pengujian aplikasi tanpa menggunakan algoritma RSA	54