

DAFTAR ISI

HALAMAN PENGESAHAN	iv
PERNYATAAN BEBAS PLAGIARISME	v
HALAMAN PERNYATAAN PUBLIKASI PROYEK AKHIR	vi
Abstrak	vii
Kata Pengantar	ix
BAB I	1
PENDAHULUAN	1
1.1. Latar Belakang Masalah	1
1.2. Rumusan Masalah	3
1.3. Batasan Masalah	4
1.4. Tujuan Penelitian	4
1.5. Manfaat Penelitian	4
BAB II	5
LANDASAN TEORI	5
2.1. Keamanan Data	5
2.2. Algoritma	7
2.3. Enkripsi dan dekripsi	8
2.4. Kriptografi	8
2.5. Serangan pada kriptografi	10
2.6. AES (Advanced Encryption Standart)	11
2.7. RSA (Rivest Shamir Adleman)	12
BAB III	14
PERANCANGAN DAN ANALISA	14
3.1. Tinjauan Umum	14
3.2. Perancangan	16
3.2.1. Proses pembangkitan kunci dalam algoritma RSA	18
3.2.2. Proses pengirim enkripsi dan kompresi dalam algoritma RSA ..	19
3.2.3. proses penerima dekompresi dan proses dekripsi dalam algoritma RSA	20
BAB IV	23

HASIL DAN PEMBAHASAN	23
4.1. Data uji coba	23
4.1.1. uji coba dengan pesan “kampus universitas telkom jakarta”	23
4.1.2. Uji coba dengan menggunakan masukan data pesan dengan format .txt.....	24
4.1.3. Uji coba dengan panjang pesan melebihi 20 kata	27
4.2. Perbandingan Perhitungan manual pada enkripsi RSA	30
4.3. Perhitungan RSA.....	32
BAB V	35
PENUTUP.....	35
5.1. Kesimpulan	35
5.2. Saran.....	35
Daftar pustaka.....	36
LAMPIRAN.....	38