

DAFTAR ISI

HALAMAN PENGESAHAN	ii
PERNYATAAN	iii
HALAMAN MOTTO DAN PERSEMBAHAN	iv
PRAKATA	v
DAFTAR ISI	vii
DAFTAR GAMBAR	x
INTISARI.....	xii
ABSTRACT	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Metode Penelitian	4
1.7 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA	7
BAB III LANDASAN TEORI	11
3.1 Kriptografi.....	11
3.2 Kriptografi Simetris	13
3.3 Algoritme Advanced Encryption Standard (AES)	14
3.3.1 SubBytes	18
3.3.2 ShiftRows.....	18
3.3.3 MixColumn	19
3.3.4 AddRoundKey.....	20
3.4 Kriptografi Asimetris.....	20
3.5 Algoritme Rivest, Shamir, Adleman (RSA).....	22

3.6	Fungsi Hash.....	23
3.7	Algoritme SHA1	24
3.8	Digital Signature.....	28
BAB IV ANALISIS DAN PERANCANGAN SISTEM.....		30
4.1	Deskripsi Sistem.....	30
4.2	Perancangan Proses.....	31
4.2.1	Pembuatan Kunci Pengguna.....	31
4.2.2	Pembangkitan <i>Digital Signature</i>	33
4.2.3	Verifikasi <i>Digital Signature</i>	35
4.3	Perancangan Sistem <i>E-Procurement</i>	37
4.3.1	Alur Proses	38
4.3.2	Rancangan Basis Data	40
4.3.3	Rancangan Antar Muka	41
BAB V IMPLEMENTASI.....		50
5.1	Batasan Implementasi	50
5.2	Implementasi Perangkat Lunak	50
5.3	Implementasi Perangkat Keras	51
5.4	Implementasi Skema Pembangkitan <i>Digital Signature</i>	51
5.5	Implementasi Verifikasi <i>Digital Signature</i>	53
BAB VI HASIL DAN PEMBAHASAN		56
6.1	Skenario Pengujian	56
6.1.1	Pengujian Sistem dengan metode <i>Blackbox Testing</i>	56
6.1.2	Pengujian Layanan Kriptografi	62
6.2	Hasil Uji Kerahasiaan	63
6.3	Hasil Uji Otentikasi	64
6.4	Hasil Uji Integritas.....	64
6.5	Uji Non-repudiation (anti penyangkalan)	65
6.6	Pembahasan.....	66
BAB VII KESIMPULAN DAN SARAN		68
7.1	Kesimpulan.....	68

7.2	Saran	68
DAFTAR PUSTAKA		70