

DAFTAR ISI

PERNYATAAN.....	i
KATA PENGANTAR	ii
UCAPAN TERIMA KASIH.....	iii
ABSTRAK	v
ABSTRACT.....	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	x
DAFTAR GAMBAR	xi
BAB I PENDAHULUAN	1
1.1. Latar Belakang Masalah.....	1
1.2. Rumusan Masalah	3
1.3. Batasan Masalah.....	3
1.4. Tujuan Penelitian.....	4
1.5. Sistematika Penulisan.....	4
BAB II KAJIAN PUSTAKA.....	6
2.1. Disposisi Surat.....	6
2.2. Kriptografi	6
2.3. <i>Digital Signature</i> (Tanda Tangan Digital)	7
2.4. Algoritma RSA.....	9
2.4.1. Pembuatan kunci algoritma RSA.....	10

2.5.	Algoritma AES	12
2.5.1.	Operasi XOR.....	16
2.5.2.	Fungsi Transformasi dalam AES	17
2.5.3.	Ekspansi Kunci	24
2.5.4.	Contoh Enkripsi Algoritma AES	25
BAB III METODE PENELITIAN.....		39
3.1.	Desain Penelitian	39
3.2.	Metode Penelitian.....	41
3.2.1.	Metode pengumpulan Data	41
3.2.2.	Proses Pengembangan Perangkat Lunak.....	41
3.3.	Alat dan Bahan Penelitian	42
BAB IV HASIL PENELITIAN DAN PEMBAHASAN		43
4.1.	Hasil Penelitian.....	43
4.2.	Modifikasi Skema <i>Digital Signature</i>	44
4.2.1.	Pembangkitan Kunci	46
4.2.2.	Penyandian Pesan dengan Menggunakan Algoritma AES-128	48
4.2.3.	Penyandian Kunci AES dengan Menggunakan Algoritma RSA	50
4.3.	Pengembangan Perangkat Lunak	51
4.3. 1.	Deskripsi Sistem.....	52
4.3.2.	Batasan Perangkat Lunak	52
4.3.3.	Perancangan	53
4.3.4.	Implementasi	54
4.3.5.	Pengujian.....	60

4.4.	Pengujian	61
4.4.1.	Penambahan Satu Karakter pada <i>Cipherkey</i> atau <i>Signature</i>	61
4.4.2.	Pengurangan Satu Karakter pada <i>Cipherkey</i> atau <i>Signature</i>	64
4.4.3.	Pengubahan Satu Karakter pada <i>Cipherkey</i> atau <i>Signature</i>	66
4.4.4.	Menggunakan Kunci Privat dan Kunci Publik yang Berbeda	68
4.4.5.	<i>Turn Around Time</i>	70
4.5.	Pembahasan Hasil Uji	72
4.5.1.	Analisis Pengaruh Penerapan <i>Digital Signature</i> , Algoritma AES dan Algoritma RSA pada sistem disposisi surat.....	72
4.5.2.	Pengaruh <i>Digital Signature</i> , Algoritma AES dan Algoritma RSA terhadap Empat Tujuan Kriptografi.....	73
BAB V KESIMPULAN DAN SARAN.....		75
5.1	Kesimpulan.....	75
5.2.	Saran.....	76
DAFTAR PUSTAKA		77

DAFTAR TABEL

Tabel 2. 1 Proses Mencari Kunci Privat (d)	11
Tabel 2. 2 Tabel Versi-versi AES.....	12
Tabel 2. 3 Tabel Operasi XOR.....	16
Tabel 2. 4 Tabel S-box	17
Tabel 2. 5 Tabel Inverse S-box.....	18
Tabel 2. 6 Contoh Plainteks dan Key	25
Tabel 2. 7 Ekspansi Kunci untuk Contoh Algoritma AES.....	27
Tabel 2. 8 Contoh Hasil Enkripsi AES.....	32
Tabel 2. 9 Contoh Hasil Dekripsi dengan Algoritma AES	36
Tabel 4. 1 Proses Mencari Kunci Privat (d).....	47
Tabel 4. 2 Contoh Tabel Plainteks dan Kunci Asimetri algoritma RSA.....	50
Tabel 4. 3 Tabel Model	54
Tabel 4. 4 Tabel View	55
Tabel 4. 5 Tabel Controller	56
Tabel 4. 6 Pengujian Black Box.....	60
Tabel 4. 7 Hasil Pengujian Turn Around Time	70

DAFTAR GAMBAR

Gambar 2. 1 Proses Tanda Tangan Digital (Munir, 2006).....	8
Gambar 2. 2 Diagram Proses Enkripsi dan Dekripsi Algoritma AES	14
Gambar 2. 3 Perubahan Plainteks Menjadi <i>Array State</i>	15
Gambar 2. 4 Struktur Data AES.....	15
Gambar 2. 5 Contoh <i>Array State</i> dan Kunci dalam Notasi Hex	16
Gambar 2. 6 Proses Transformasi <i>SubBytes()</i>	19
Gambar 2. 7 Matriks Perhitungan S-box	20
Gambar 2. 8 Diagram Pembuatan S-box.....	20
Gambar 2. 9 Matriks Perhitungan Inverse S-box.....	21
Gambar 2. 10 Diagram Pembuatan Inverse S-box.....	21
Gambar 2. 11 Transformasi <i>ShiftRows()</i>	22
Gambar 2. 12 Contoh Transformasi <i>ShiftRows()</i>	22
Gambar 2. 13 Matriks Transformasi <i>MixColumn()</i>	23
Gambar 2. 14 Contoh Transformasi <i>MixColumn()</i>	23
Gambar 2. 15 Matriks Transformasi Inverse <i>MixColumn()</i>	23
Gambar 2. 16 Contoh Transformasi <i>AddRoundKey()</i>	23
Gambar 3. 1 Skema Desain Penelitian.....	39
Gambar 3. 2 Model Sekuensial Linier	41
Gambar 4. 1 Proses Tanda Tangan Digital Menggunakan Fungsi Hash (Munir, 2006).....	45
Gambar 4. 2 Modifikasi Skema Tanda Tangan Digital	45
Gambar 4. 3 (a). Plainteks (sumber: http://roishare.blogspot.com/2013/11/memahami-perintah-kerja-tertulis.html) (b). Gambar Cipherteks.....	48
Gambar 4. 4 Plainteks	49
Gambar 4. 5 Cipherteks.....	50

Gambar 4. 6 <i>Usecase</i> Perangkat Lunak Disposisi Surat	53
Gambar 4. 7 Halaman Login	58
Gambar 4. 8 Halaman Tulis Surat	58
Gambar 4. 9 Halaman Surat Masuk	59
Gambar 4. 10 Halaman Detail Surat	59
Gambar 4. 11 Halaman Surat Keluar	60
Gambar 4. 12 Hasil dekripsi gambar dengan penambahan satu karakter pada signature (dalam heksadesimal)	62
Gambar 4. 13 Hasil dekripsi gambar dengan penambahan satu karakter pada signature	62
Gambar 4. 14 Hasil dekripsi gambar dengan kunci yang asli (dalam heksadesimal)	63
Gambar 4. 15 Hasil dekripsi gambar dengan kunci yang asli	63
Gambar 4. 16 Hasil dekripsi gambar dengan pengurangan satu karakter pada signature (dalam heksadesimal)	65
Gambar 4. 17 Hasil dekripsi gambar dengan pengurangan satu karakter pada signature	65
Gambar 4. 18 Hasil dekripsi gambar dengan pengubahan satu karakter pada signature (dalam heksadesimal)	67
Gambar 4. 19 Hasil dekripsi gambar dengan pengubahan satu karakter pada signature	67
Gambar 4. 20 Hasil dekripsi gambar dengan kunci privat yang berbeda (dalam heksadesimal)	69
Gambar 4. 21 Hasil dekripsi gambar dengan kunci privat yang berbeda	69