

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR.....	iii
UCAPAN TERIMA KASIH	iv
DAFTAR ISI	v
DAFTAR TABEL.....	vii
DAFTAR GAMBAR	viii
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Batasan Masalah.....	4
1.4. Tujuan Penelitian.....	4
1.5. Sistematika Penulisan.....	5
BAB II KAJIAN PUSTAKA	7
2.1. <i>E-Voting</i>	7
2.2. <i>Central Legitimization Agency (CLA)</i>	9
2.3. <i>Central Tabulating Facilities (CTF)</i>	9
2.4. Kriptografi	10
2.5. Algoritma RSA	10
2.6. Algoritma AES-Rindjael	15
2.6.1. Fungsi Transformasi dalam AES.....	19
2.6.2. Ekspansi Kunci	26
2.6.3. Contoh Enkripsi Algoritma AES.....	27
2.7. SHA2 (SHA-512)	31
2.8. Protokol <i>Two Central Facilities</i>	32

BAB III METODE PENELITIAN.....	37
3.1. Desain Penelitian.....	37
3.2 Metode Penelitian.....	40
3.2.1. Metode Pengumpulan Data.....	40
3.2.2. Proses Pengembangan Perangkat Lunak.....	40
3.3 Alat dan Bahan.....	42
BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....	44
4.1. Modifikasi Protokol <i>Two Central Facilities</i>	44
4.2. Pengembangan Perangkat Lunak.....	60
4.2.1. Deskripsi Sistem.....	60
4.2.2. Batasan Sistem.....	60
4.2.3. Pemodelan.....	61
4.2.4. Desain Sistem.....	63
4.2.5. Implementasi.....	65
4.2.6. Pengujian.....	74
4.3. Pembahasan Implementasi Protokol <i>Two Central Facilities</i>	75
4.3.1. Hasil Implementasi Protokol <i>Two Central Facilities</i>	75
4.3.2. Analisis Terhadap Hasil Implementasi Protokol <i>Two Central Facilities</i>	81
4.4. Pembahasan Implementasi Algoritma AES dan RSA.....	83
4.4.1. Implementasi Algoritma AES dan RSA.....	83
4.4.2. Analisis Hasil Implementasi Algoritma AES dan RSA.....	105
BAB V KESIMPULAN DAN SARAN.....	110
5.1. Kesimpulan.....	110
5.2. Saran.....	111
DAFTAR PUSTAKA.....	x
LAMPIRAN.....	xii

DAFTAR TABEL

Tabel 2. 1. Tabel Proses Mencari Kunci Privat (d)	13
Tabel 2. 2. Tabel Versi-Versi AES	16
Tabel 2. 3. <i>S-box</i>	19
Tabel 2. 4. <i>Inverse S-box</i>	20
Tabel 2. 5. Contoh Plainteks dan Key	27
Tabel 2. 6. Ekspansi Kunci untuk Contoh AES	28
Tabel 2. 7. Contoh Hasil Enkripsi AES	30
Tabel 4. 1. Implementasi Modul Program.....	65
Tabel 4. 2. Pelaksanaan Pengujian <i>BlackBox</i>	74
Tabel 4. 3. Tabel Hasil Percobaan Perbandingan Turn Around Time	79
Tabel 4. 4. Contoh Proses Enkripsi Algoritma AES.....	91
Tabel 4. 5. Contoh Proses Dekripsi Algoritma AES	97
Tabel 4. 6. Contoh Pembangkitan Kunci AES	97
Tabel 4. 7. Contoh Proses Enkripsi Algoritma RSA	98
Tabel 4. 8. Contoh Proses Dekripsi Algoritma RSA	99
Tabel 4. 9. Contoh Proses Pembuatan Sertifikat	99
Tabel 4. 10. Contoh Proses Pengecekan Sertifikat.....	101
Tabel 4. 11. Tabel Proses Mencari Kunci Privat CLA	103
Tabel 4. 12. Tabel Proses Mencari Kunci Privat CTF	103
Tabel 4. 13. Tabel Proses Mencari Kunci Privat CA	104
Tabel 4. 14. Pengiriman Kunci Rahasia AES yang Dienkripsi RSA ke CLA.....	105
Tabel 4. 15. Pengiriman Data Pemilih yang dienkripsi AES ke CLA.....	105
Tabel 4. 16. Pengiriman ValidationID Terenkripsi ke CTF	106
Tabel 4. 17. Penerimaan ValidationID dari <i>Voter Client</i>	107
Tabel 4. 18. Detail Hasil Percobaan Proses Autentikasi	107
Tabel 4. 19. Proses Pengecekan Sertifikat	108

DAFTAR GAMBAR

Gambar 2. 1. Diagram Proses Enkripsi dan Dekripsi Algoritma AES	17
Gambar 2. 2. Perubahan Plainteks Menjadi Array State	18
Gambar 2. 3. Struktur Data AES	18
Gambar 2. 4. Contoh array State dan kunci dalam notasi HEX.....	19
Gambar 2. 5. Proses Transformasi <i>SubBytes()</i>	21
Gambar 2. 6. Contoh Transformasi <i>SubBytes()</i>	21
Gambar 2. 7. Matriks Perhitungan <i>Sbox</i>	22
Gambar 2. 8. Diagram Pembuatan <i>Sbox</i>	22
Gambar 2. 9. Matriks Perhitungan <i>Inverse Sbox</i>	23
Gambar 2. 10. Diagram Pembuatan <i>Sbox</i>	23
Gambar 2. 11. Transformasi <i>ShiftRows</i>	24
Gambar 2. 12. Contoh Transformasi <i>ShiftRows</i>	24
Gambar 2. 13. Matriks Transformasi <i>MixCollums</i>	25
Gambar 2. 14. Contoh Transformasi <i>MixCollums</i>	25
Gambar 2. 15. Matriks <i>InvMixCollums</i>	25
Gambar 2. 16. Contoh Transformasi <i>AddRoundKey</i>	26
Gambar 2. 17. Skema Protokol <i>Two Central Facilities</i>	33
Gambar 3. 1. Skema Desain Penelitian.....	37
Gambar 3. 2. Model Sekuensial Linier	40
Gambar 4. 1. Skema Protokol untuk Pemilih.....	46
Gambar 4. 2. Skema Protokol untuk AdminCTF	47
Gambar 4. 3. <i>Flowchart</i> Protokol <i>Two Central Facilities</i> untuk Pemilih.....	54
Gambar 4. 4. <i>Flowchart</i> Protokol <i>Two Central Facilities</i> untuk Pemilih (Lanjutan)	55
Gambar 4. 5. <i>Flowchart</i> Protokol <i>Two Central Facilities</i> untuk AdminCTF	59
Gambar 4. 6. <i>Context Diagram Voter Client</i>	61
Gambar 4. 7. <i>Context Diagram CLA</i>	62
Gambar 4. 8. <i>Context Diagram CTF</i>	62
Gambar 4. 9. Antarmuka Halaman Login Pemilih.....	69

Gambar 4. 10. Antarmuka Halaman Utama Pemilih Sebelum Pemilihan	69
Gambar 4. 11. Antarmuka Halaman Utama Pemilih Setelah Pemilihan.....	70
Gambar 4. 12. Antarmuka Halaman Pemilihan	70
Gambar 4. 13. Antarmuka Halaman Verifikasi	71
Gambar 4. 14. Antarmuka Halaman Pemberitahuan.....	71
Gambar 4. 15. Antarmuka Halaman Login Admin	72
Gambar 4. 16. Antarmuka Halaman Utama Admin	73
Gambar 4. 17. Antarmuka Halaman Hasil Pemilihan	73
Gambar 4. 18. Diagram Three Ways Handshake	75
Gambar 4. 19. Proses Three Ways Handshake.....	76
Gambar 4. 20. Proses Komunikasi Data	76
Gambar 4. 21. Diagram Komunikasi Data.....	77
Gambar 4. 22. Diagram Akhir Transmisi.....	77
Gambar 4. 23. Akhir Transmisi.....	78
Gambar 4. 24. Grafik Hasil Percobaan Perbandingan Turn Around Time.....	80

