UNIVERSITAS
GADJAH MADA
SISTEM KRIPTOGRAFI DAN TANDA TANGAN DIGITAL RSA POLINOMIAL ATAS LAPANGAN BERHINGGA
Nur Fikriyah Alkamila, Prof. Dr.rer.nat. Indah Emilia Wijayanti, S.Si., M.Si.
Universitas Gadjah Mada, 2023 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR ISI

HALAMAN JUDUL . . . . . **i**
HALAMAN PENGESAHAN . . . . . **ii**
HALAMAN PERNYATAAN . . . . . **iii**
HALAMAN PERSEMBAHAN . . . . . **iv**
HALAMAN MOTTO . . . . . **v**
PRAKATA . . . . . **vi**
DAFTAR ISI . . . . . **viii**
DAFTAR TABEL . . . . . **xi**
DAFTAR GAMBAR . . . . . **xii**
DAFTAR LAMBANG . . . . . **xiv**
INTISARI . . . . . **xv**
ABSTRACT . . . . . **xvi**
I PENDAHULUAN **1**
1.1. Latar Belakang Masalah 1
1.2. Tujuan dan Manfaat Penelitian 2
1.3. Tinjauan Pustaka 3
1.4. Metodologi Penelitian 4
1.5. Sistematika Penulisan 5
II DASAR TEORI **6**
2.1. Konsep Dasar Ring 6
2.2. Daerah Euclid 16
2.3. Ring Polinomial sebagai Daerah Euclid 32
III MODIFIKASI SISTEM KRIPTOGRAFI DAN TANDA TANGAN DIGITAL RSA **39**
3.1. Kriptografi 39
3.2. Kriptografi Kunci-Publik RSA 44
3.2.1. Sistem Kriptografi RSA 44
3.2.2. Algoritma RSA 47
3.3. Kriptografi Kunci-Publik RSA Polinomial atas Lapangan Berhingga 53
3.4. Tanda Tangan Digital 61
3.5. Tanda Tangan Digital RSA 62
3.5.1. Sistem Tanda Tangan Digital RSA 63
3.5.2. Algoritma Tanda Tangan Digital RSA 65

UNIVERSITAS
GADJAH MADA
SISTEM KRIPTOGRAFI DAN TANDA TANGAN DIGITAL RSA POLINOMIAL ATAS LAPANGAN BERHINGGA
Nur Fikriyah Alkamila, Prof. Dr.rer.nat. Indah Emilia Wijayanti, S.Si., M.Si.
Universitas Gadjah Mada, 2023 | Diunduh dari http://etd.repository.ugm.ac.id/

3.6. Tanda Tangan Digital RSA Polinomial 69
IV SIMULASI SISTEM KRIPTOGRAFI DAN TANDA TANGAN DIGITAL RSA 73
4.1. Simulasi Sistem Kriptografi RSA 73
4.2. Simulasi Sistem Kriptografi RSA Polinomial 81
4.3. Simulasi Digital Signature RSA 89
4.4. Simulasi Tanda Tangan RSA Polinomial atas Lapangan Berhingga . 97
V PENUTUP 106
5.1. Kesimpulan 106
5.2. Saran 108
DAFTAR PUSTAKA 109
A SKRIP PROGRAM RSA KLASIK 110
1.1. Pembangkitan Kunci 110
1.2. Enkripsi 111
1.3. Dekripsi 112
B SKRIP PROGRAM RSA POLINOMIAL ATAS LAPANGAN BERHINGGA 113
2.1. Pembangkitan Kunci 113
2.2. Enkripsi 115
2.3. Dekripsi 119
C SKRIP PROGRAM PERBANDINGAN 124
3.1. Sistem Kriptografi RSA 124
3.1.1. Kasus 1 124
3.1.2. Kasus 2 126
3.1.3. Kasus 3 128
3.2. Sistem Kriptografi RSA Polinomial 130
3.2.1. Kasus 1 130
3.2.2. Kasus 2 132
3.2.3. Kasus 3 134
3.3. Tanda Tangan Digital RSA 136
3.3.1. Kasus 1 136
3.3.2. Kasus 2 138
3.3.3. Kasus 3 140
3.4. Tanda Tangan Digital RSA Polinomial 142
3.4.1. Kasus 1 142
3.4.2. Kasus 2 144

UNIVERSITAS
GADJAH MADA
SISTEM KRIPTOGRAFI DAN TANDA TANGAN DIGITAL RSA POLINOMIAL ATAS LAPANGAN BERHINGGA
Nur Fikriyah Alkamila, Prof. Dr.rer.nat. Indah Emilia Wijayanti, S.Si., M.Si.
Universitas Gadjah Mada, 2023 | Diunduh dari http://etd.repository.ugm.ac.id/

3.4.3. Kasus 3 146