UNIVERSITAS
GADJAH MADA
Sistem Kriptografi RSA Menggunakan Grup GL_{t}(\Z_{n})^{*} dan Aplikasinya pada Skema Tanda Tangan Digital
Rizky Nur Afifah, Prof. Dr.rer.nat. Indah Emilia Wijayanti, S.Si., M.Si.
Universitas Gadjah Mada, 2024 | 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 . . . . . **xiii**
INTISARI . . . . . **xiv**
ABSTRACT . . . . . **xv**
I PENDAHULUAN **1**
1.1. Latar Belakang Masalah 1
1.2. Tujuan dan Manfaat Penelitian 4
1.3. Tinjauan Pustaka 4
1.4. Metodologi Penelitian 6
1.5. Sistematika Penulisan 7
II DASAR TEORI **8**
2.1. Himpunan Bilangan Bulat 8
2.1.1. Sifat Keterbagian 8
2.1.2. Algoritma Pembagian 12
2.1.3. Faktor Persekutuan Terbesar 14
2.1.4. Algoritma Euclid 15
2.1.5. Algoritma Euclid yang Diperluas 17
2.1.6. Bilangan Prima 18
2.1.7. Kongruensi 21
2.2. Struktur Aljabar 23
2.2.1. Grup dan Subgrup 25
2.2.2. Grup Permutasi 30
2.2.3. Grup Hingga 37
2.2.4. Homomorfisma Grup 47
2.2.5. Ring dan Lapangan 52

UNIVERSITAS GADJAH MADA
Sistem Kriptografi RSA Menggunakan Grup GL_{t}(\Z_{n})^{*} dan Aplikasinya pada Skema Tanda Tangan Digital
Rizky Nur Afifah, Prof. Dr.rer.nat. Indah Emilia Wijayanti, S.Si., M.Si.
Universitas Gadjah Mada, 2024 | Diunduh dari http://etd.repository.ugm.ac.id/

2.2.6. Modul 55
2.3. Himpunan Bilangan Bulat Modulo n 60
2.3.1. Ring Bilangan Bulat Modulo n 61
2.3.2. Grup Perkalian Bilangan Bulat Modulo n 63
2.4. Metode *Fast Exponentiation* 68
2.5. Tes Miller-Rabin 69
III Matriks 73
3.1. Matriks atas Ring Komutatif 73
3.2. Determinan 84
3.3. Grup Linear Umum 114
IV Sistem Kriptografi RSA Menggunakan Grup $GL_t(\mathbb{Z}_n)^*$ 117
4.1. Sistem Kriptografi 117
4.2. Sistem Kriptografi RSA 120
4.2.1. Parameter dan Algoritma 121
4.2.2. Keberhasilan Dekripsi 122
4.3. Sistem Kriptografi RSA Menggunakan Grup $GL_t(\mathbb{Z}_n)^*$ 127
4.3.1. Parameter dan Algoritma 127
4.3.2. Keberhasilan Dekripsi 129
4.4. Perbandingan Sistem Kriptografi RSA dan Sistem Kriptografi RSA Menggunakan Grup $GL_t(\mathbb{Z}_n)^*$ 135
4.4.1. Ruang Pesan 136
4.4.2. Banyak Kunci dan Ruang Kunci 136
4.4.3. Tingkat Kesulitan Pemfaktoran Kunci Publik n 138
4.4.4. Waktu Total Simulasi (Penjumlahan Waktu Pengubahan Pesan, Pembangkitan Kunci, Enkripsi, dan Dekripsi) 138
V Skema Tanda Tangan Digital RSA Menggunakan Grup $GL_t(\mathbb{Z}_n)^*$ . . 143
5.1. Skema Tanda Tangan Digital 143
5.2. Skema Tanda Tangan Digital RSA 147
5.2.1. Parameter dan Algoritma 148
5.3. Skema Tanda Tangan Digital RSA menggunakan Grup $GL_t(\mathbb{Z}_n)^*$. 152
5.3.1. Parameter dan Algoritma 153
VI PENUTUP 159
6.1. Kesimpulan 159
6.2. Saran 164
DAFTAR PUSTAKA 165
A Skrip *Functions* dari Program 167

UNIVERSITAS
GADJAH MADA
Sistem Kriptografi RSA Menggunakan Grup GL_{t}(\Z_{n})^{*} dan Aplikasinya pada Skema Tanda Tangan Digital
Rizky Nur Afifah, Prof. Dr.rer.nat. Indah Emilia Wijayanti, S.Si., M.Si.
Universitas Gadjah Mada, 2024 | Diunduh dari http://etd.repository.ugm.ac.id/

1.1. Sistem Kriptografi dan Skema Tanda Tangan Digital RSA 167
1.2. Sistem Kriptografi dan Skema Tanda Tangan Digital RSA Menggunakan Grup $GL_t(\mathbb{Z}_n)^*$ 170
B Skrip Program untuk Contoh 177
2.1. Sistem Kriptografi RSA 177
2.2. Sistem Kriptografi RSA Menggunakan Grup $GL_t(\mathbb{Z}_n)^*$ 178
2.3. Skema Tanda Tangan Digital RSA 181
2.4. Skema Tanda Tangan Digital RSA Menggunakan Grup $GL_t(\mathbb{Z}_n)^*$. 183
C Skrip Program untuk Simulasi Perbandingan Waktu Total 186
3.1. Simulasi Waktu Total Sistem Kriptografi RSA 186
3.2. Simulasi Waktu Total Sistem Kriptografi RSA Menggunakan Grup $GL_t(\mathbb{Z}_n)^*$ 188
3.3. Perbandingan Waktu Total Simulasi (Grafik) 189
D Tabel ASCII 191