UNIVERSITAS
GADJAH MADA
**Sistem Kriptografi ElGamal atas Bilangan Bulat Gauss dan Aplikasinya pada Tanda Tangan Digital**
Raka Bukhari, Uha Isnaini, S.Si., M.Sc., Ph.D.
**Universitas Gadjah Mada, 2026 | 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 LAMBANG** . . . . . **x**
**INTISARI** . . . . . **xiii**
**ABSTRACT** . . . . . **xiv**
**I PENDAHULUAN** . . . . . **1**
1.1. Latar Belakang . . . . . 1
1.2. Tujuan dan Manfaat Penelitian . . . . . 3
1.3. Tinjauan Pustaka . . . . . 4
1.4. Metodologi Penelitian . . . . . 7
1.5. Sistematika Penulisan . . . . . 8
**II Dasar Teori** . . . . . **10**
2.0.1. Grup . . . . . 10
2.0.2. Ring dan Subring . . . . . 18
2.0.3. Daerah Integral . . . . . 28
2.0.4. Daerah Faktorisasi Tunggal . . . . . 29
**III Bilangan Bulat Gauss** . . . . . **33**
3.1. Bilangan Bulat Gauss . . . . . 33
3.1.1. Norm . . . . . 33
3.1.2. Bilangan Prima Gauss . . . . . 41
3.1.3. Aritmatika Modulus . . . . . 45
**IV Kriptografi** . . . . . **51**
4.1. Kriptografi . . . . . 51
4.1.1. Kriptosistem . . . . . 51
4.1.2. Kriptosistem Simetris . . . . . 52
4.1.3. Kriptosistem Asimetris . . . . . 53
4.2. Kriptosistem ElGamal di $Z_n$ . . . . . 55
4.2.1. Algoritma Kriptosistem ElGamal pada $Z_n^*$ . . . . . 56

UNIVERSITAS
GADJAH MADA
**Sistem Kriptografi ElGamal atas Bilangan Bulat Gauss dan Aplikasinya pada Tanda Tangan Digital**
Raka Bukhari, Uha Isnaini, S.Si., M.Sc., Ph.D.
**Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/**



4.2.2. Keberhasilan Dekripsi . . . . . 58
4.3. Kriptosistem ElGamal atas Bilangan Bulat Gauss . . . . . 60
4.3.1. Domain Bilangan Bulat Gauss . . . . . 60
4.3.2. Algoritma Kriptosistem ElGamal pada $Z_n^*$ . . . . . 64
**V Skema Tanda Tangan Digital . . . . . 68**
5.1. Skema Tanda Tangan Digital . . . . . 68
5.2. Skema Tanda Tangan Digital ElGamal atas Bilangan Bulat $\mathbb{Z}_n$ . . . 71
5.3. Skema Tanda Tangan Digital ElGamal pada Grup Residu Gauss . . 73
5.4. Hasil dan Analisisnya . . . . . 77
**VI Kesimpulan . . . . . 82**
**A LAMPIRAN SKRIP PROGRAM . . . . . 86**