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/

INTISARI

Sistem Kriptografi ElGamal atas Bilangan Bulat Gauss dan Aplikasinya pada Tanda Tangan Digital

Oleh

Raka Bukhari

21/481202/PA/20940

Keamanan informasi menjadi aspek penting dalam pertukaran data digital. Salah satu algoritma kriptografi kunci publik yang banyak digunakan adalah ElGamal, yang keamanannya bertumpu pada permasalahan logaritma diskrit. Tugas Akhir ini membahas pengembangan skema ElGamal dengan memanfaatkan bilangan prima Gauss pada domain bilangan bulat Gauss $\mathbb{Z}[i]$.

Tugas Akhir ini bertujuan merancang dan menganalisis implementasi algoritma ElGamal berbasis bilangan prima Gauss. Pesan terlebih dahulu dikonversi ke dalam kode ASCII, kemudian dipetakan secara bijektif ke bentuk bilangan Gauss. Proses pembangkitan kunci, enkripsi, dan dekripsi dilakukan dengan memanfaatkan sifat aljabar, keterbagian, dan struktur Euclidean pada $\mathbb{Z}[i]$. Analisis dilakukan terhadap ketepatan dekripsi, kompleksitas perhitungan, dan potensi keamanan sistem.

Hasil Tugas Akhir menunjukkan bahwa skema ElGamal berbasis bilangan prima Gauss dapat menjalankan proses enkripsi dan dekripsi dengan baik serta mampu mengembalikan pesan asli secara tepat. Penggunaan bilangan prima Gauss memberikan ruang representasi yang lebih luas dan struktur matematis yang lebih kompleks dibandingkan ElGamal klasik. Dengan demikian, skema ini berpotensi menjadi alternatif pengembangan kriptografi kunci publik yang aman dan efisien.

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/

ABSTRACT

ElGamal Cryptosystem over Gaussian Integers and Its Application to Digital Signatures

By

Raka Bukhari

21/481202/PA/20940

Information security is an essential aspect of digital data exchange. One widely used public-key cryptographic algorithm is ElGamal, whose security relies on the discrete logarithm problem. This study discusses the development of an ElGamal scheme using Gaussian primes in the Gaussian integer domain $\mathbb{Z}[i]$.

This study aims to design and analyze the implementation of the ElGamal algorithm based on Gaussian primes. The message is first converted into ASCII code and then bijectively mapped into Gaussian integers. The key generation, encryption, and decryption processes are carried out by utilizing algebraic properties, divisibility, and the Euclidean structure of $\mathbb{Z}[i]$. The analysis focuses on decryption accuracy, computational complexity, and the security potential of the proposed system.

The results show that the Gaussian prime-based ElGamal scheme can perform encryption and decryption properly and accurately recover the original message. The use of Gaussian primes provides a broader representation space and a more complex mathematical structure than the classical ElGamal scheme. Therefore, the proposed scheme has the potential to serve as an alternative for developing secure and efficient public-key cryptographic systems.