INTISARI

SISTEM KRIPTOGRAFI RSA ATAS BILANGAN BULAT GAUSS DAN APLIKASINYA PADA SKEMA TANDA TANGAN DIGITAL

Oleh

LAILIL MUTHOHAROH

19/442573/PA/19322

Sistem kriptografi RSA merupakan salah satu contoh dari kriptografi kunci publik yang juga dapat diterapkan pada skema tanda tangan digital. Sistem kriptografi ini bekerja pada domain bilangan bulat modulo n. Pada tahun 2002, diperkenalkan modifikasi baru dari RSA dengan memanfaatkan domain bilangan bulat Gauss beserta penerapannya pada skema tanda tangan digital. Pada tulisan ini, akan ditunjukkan klasifikasi sistem kriptografi RSA atas bilangan bulat Gauss berdasarkan pemilihan tipe bilangan prima Gauss. Dalam klasifikasi ini, diberikan dua kasus baru dengan memanfaatkan norm bilangan prima Gauss sebagai pengganti dari bilangan prima Gauss. Kemudian, dilakukan analisis perbandingan antara RSA dengan RSA atas bilangan bulat Gauss. Selain itu, akan ditunjukkan juga penerapan skema tanda tangan digital RSA atas bilangan bulat Gauss beserta simulasi contohnya.

ABSTRACT

RSA CRYPTOSYSTEM OVER GAUSSIAN INTEGER AND ITS APPLICATION ON DIGITAL SIGNATURE SCHEMES

By

LAILIL MUTHOHAROH

19/442573/PA/19322

RSA cryptosystem is an example of public key cryptography which can also be applied to digital signature schemes. This cryptosystem works in the domain of integers modulo n. In 2002, a new modification of RSA was introduced using the Gaussian integer domain and its application to digital signature schemes. In this paper, we will show the classification of the RSA cryptographic system for Gaussian integers based on the selection of Gaussian prime number types. In this classification, two new cases are given using the norm of Gaussian prime number as a substitute for the Gaussian prime number. Then, it continues with a comparative analysis between RSA and RSA over Gaussian integers. In addition, we will also show the application of the RSA digital signature scheme for Gaussian integers along with simulation examples.