TINJAUAN MATEMATIS PENGGUNAAN FUNGSI ELLIPTIC CURVES DALAM PENGUJIAN BILANGAN PRIMA YANG DIGUNAKAN DALAM ALGORITMA PUBLIC KEY

Susila Windarta, Dr. Ing. Adang Suhendra, SSi,

Penulisan Ilmiah, Fakultas Ilmu Komputer, 2005

Universitas Gunadarma

http://www.gunadarma.ac.id

kata kunci : matematika

Abstraksi :

Penemuan konsep Public Key merupakan awal era baru kriptografi modern. Sistem sandi kunci publik secara umum memerlukan bilangan prima digit besar dalam pembangkitan kunci. Masalah utama yang dihadapi adalah kesulitan membangkitkan dan menguji bilangan prima yang akan digunakan dalam sistem sandi kunci publik. Pengujian prima dapat dilakukan dengan menggunakan teorema dan fungsi matematika yang ada. Salah satu fungsi matematika yang dapat digunakan adalah fungsi elliptic curves. Tulisan ini akan mencoba menelaah aspek-aspek matematis yang mendasari pengujian bilangan prima dengan menggunakan fungsi elliptic curves. Fungsi ini dapat digunakan dalam pengujian bilangan prima karena titik-titik pada fungsi tersebut membentuk group terhadap operasi penjumlahan yang didefinisikan dalam fungsi tersebut. Fakta tersebut mengakibatkan proposisi pengujian bilangan prima yang terdefinisi dalam group dapat diaplikasikan pada fungsi ini. Algoritma yang digunakan untuk memperjelas tinjauan menggunakan algoritma Goldwasser-Killian.