# INTISARI

## ALGORITMA AKS TERIMPROVISASI PADA PENGUJIAN BILANGAN PRIMA

A Hasan Mubarok
14/364164/PA/15925

Salah satu penemuan yang bermanfaat dalam teori bilangan adalah algoritma RSA. Algoritma ini membantu menjaga informasi agar aman. Dalam algoritma ini diperlukan sebuah bilangan prima bernilai besar untuk membangkitkan kunci yang akan digunakan untuk melakukan enkripsi dan dekripsi. Untuk mendapatkan bilangan prima tersebut, pendekatan yang digunakan adalah dengan membangkitkan bilangan bulat secara acak kemudian dilakukan pengujian bilangan prima. Pengujian bilangan prima adalah algoritma untuk menentukan apakah suatu bilangan merupakan bilangan prima atau bukan.

Algoritma yang digunakan adalah yang diusulkan oleh Han Wei Wu, dkk. Algoritma pengujian bilangan prima dibagi menjadi dua macam, yaitu probabilistik dan deterministik. Algoritma probabilistik dapat melakukan pengujian dengan cepat namun sangat rentan terjadi kesalahan. Sementara algoritma deterministik dapat melakukan pengujian secara tepat namun kecepatan pengujiannya sangat rendah. AKS termasuk algoritma pengujian bilangan prima deterministik yang sangat lambat sehingga tidak dapat digunakan dalam praktik. Dalam penelitian ini akan dilakukan improvisasi terhadap AKS sehingga dapat digunakan dalam praktik meskipun menjadi bersifat probabilistik.

Kata kunci: AKS, probabilistik, pengujian primalitas

# ABSTRACT

## *IMPROVED AKS ALGORITHM IN PRIMALITY TESTING*

A Hasan Mubarok
14/364164/PA/15925

One of useful finding in number theory is RSA algorithm. This algorithm is needed to keep information secure. This algorithm requires a big prime to generate a key that will be used to encrypt and decrypt. The approach used to get the prime number is to randomly generate an integer and then perform the primality test. Primality test is an algorithm to determine whether a number is a prime or not.

The algorithm used is proposed by Han Wei Wu, et al. The primality testing algorithm is divided into two types, probabilistic and deterministic. The probabilistic algorithm is fast but its misjudgment probability is high. While deterministic algorithm can perform the test precisely but its test speed is so low. AKS is a deterministic primality test algorithm that is so slow that it is not useful in practice. This research will improvise AKS so that it can be used in practice although probability-based.

Keywords: AKS, probabilistic, primality testing