INTISARI

SISTEM KRIPTOGRAFI DAN TANDA TANGAN DIGITAL RSA POLINOMIAL ATAS LAPANGAN BERHINGGA

Oleh

NUR FIKRIYAH ALKAMILA

19/439202/PA/19025

Kriptografi bertujuan untuk melindungi kerahasiaan informasi yang dikirim dari pengirim kepada penerima pesan. Sistem kriptografi kunci publik telah menjadi landasan bagi sebagian besar transmisi data di internet. Salah satu algoritma kriptografi kunci publik yang terkenal adalah RSA, yang diperkenalkan oleh Rivest, Shamir, dan Adleman. Kemudian, El-Kassar dan rekan-rekannya mengambil pendekatan dengan menggunakan ring polinomial atas lapangan berhingga untuk memodifikasi RSA ini, yang dikenal sebagai RSA polinomial. Dalam tulisan ini, akan diuraikan mengenai sistem RSA yang telah dimodifikasi dengan menggunakan ring polinomial atas lapangan berhingga, dan akan menerapkannya dalam konteks tanda tangan digital. Melalui penelitian ini, akan dibandingkan efisiensi dan kecepatan berbagai proses algoritma yang terlibat dalam sistem ini.

ABSTRACT

RSA CRYPTOGRAPHY AND DIGITAL SIGNATURE IN THE DOMAIN OF POLYNOMIALS OVER FINITE FIELDS

By

NUR FIKRIYAH ALKAMILA

19/439202/PA/19025

The purpose of cryptography is to protect the confidentiality of information transmitted from sender to receiver. The public key cryptography system has become the cornerstone for the most data transmissions on the internet. One of the well-known public key cryptography algorithms is RSA, introduced by Rivest, Shamir, and Adleman. Subsequently, El-Kassar and their colleagues took an approach by using a polynomial ring over a finite field to modify RSA, known as RSA polynomial. In this final project, it will be described about RSA system that has been modified using polynomial rings over finite fields and apply it in the context of digital signatures. Through this research, it will compare the efficiency and speed of various algorithm processes involved in this system.