ABSTRAK

Kriptosistem RSA adalah kriptosistem kunci publik yang berdasar pada Teorema Sisa Cina. Untuk mengerjakan kriptosistem ini, bilangan-bilangan prima dibutuhkan untuk mendapatkan kunci publik. Untuk menguji keprimaan suatu bilangan, algoritma yang dapat digunakan adalah algoritma Solovay-Strassen dan algoritma Miller-Rabin. Algoritma-algoritma yang dapat digunakan untuk memfaktorkan kunci publik, yaitu algoritma Pollard $p-1$, algoritma Pollard rho dan algoritma kuadrat acak Dixon.

ABSTRACT

RSA cryptosystem is a public key cryptosystem based on the Chinese Remainder Theorem. To perform the cryptosystem, prime numbers are needed to obtain public keys. Algorithms that can be used to test the primeness of a number are the Solovay-Strassen algorithm and Miller-Rabin algorithm. The algorithms that can be used to factor the public key are Pollard $p-1$ algorithm, Pollard rho algorithm, and Dixon's random squares algorithm.