Abstract

In recent years, primality testing has become very important in constructing and maintaining the security of (important application) public-key cryptography, especially in RSA cryptosystem. RSA cryptosystem is very hard to be broken whenever prime number that is mainly used in RSA construction increases in size.

This thesis proposes a fast method for testing primality of a large number. The proposed method based on constructing a logic circuit for primality testing (CPT). This circuit contains the following three basic facilities:

1- Large space for a large number.

2- Circuit Components should be fast, to increase performing speed of the arithmetic operations.

3- Construction of the circuit should be made according to an efficient primality testing algorithm.

The main architecture of CPT has been implemented by SCPT (simulation of circuit performing primality testing). SCPT performs primality testing of positive integer with maximum length of 500 digits to determine whether it is prime or composite, where the simulated execution time increase with the increase of tested number length. The C++ programming language has been used to implement SCPT, which can be run on any IBM compatible personal computer.