American Journal of Applied Science and Technology

VOLUME Vol.06 Issue 05 2026
PAGE NO. 166-168
DOI 10.37547/ajast/Volume06Issue05-28

# Analysis Of Primality Testing Algorithms And Their Applications In Cryptography

Mamaraimov Bekzod

Academic Lyceum of Termez State University, Uzbekistan

Boykuziev Ilkhom

Tashkent University of Information Technologies named after Muhammad ibn Musa al-Khwarizmi, Uzbekistan

**Received:** 13 March 2026; **Accepted:** 21 April 2026; **Published:** 23 May 2026

**Abstract:** This article analyzes the theoretical foundations, operating principles, and practical efficiency of primality testing algorithms. The role of prime numbers in modern cryptographic systems and the necessity of testing large integers are discussed. The mathematical foundations, advantages, and limitations of the Fermat, Solovay–Strassen, Miller–Rabin, and AKS primality tests are examined. In addition, the computational complexity of probabilistic and deterministic algorithms and their impact on the security of cryptographic systems are evaluated. The research results demonstrate that primality testing algorithms play a crucial role in public-key cryptosystems such as RSA.

**Keywords:** Prime number, primality test, Miller–Rabin algorithm, Fermat test, AKS algorithm, cryptography, RSA, number theory, probabilistic algorithms, deterministic algorithms.

## INTRODUCTION

The rapid development of information and communication technologies, along with the expansion of the digital economy, has significantly increased the demand for modern cryptographic systems. In particular, mathematical methods based on large numbers are widely used to ensure data security in electronic commerce, banking systems, cloud technologies, and governmental information infrastructures. The security of such cryptographic systems largely depends on the mathematical properties of prime numbers and the ability to efficiently and reliably determine the primality of large integers. Therefore, primality testing has become one of the most important research areas not only in theoretical mathematics but also in practical cryptography.

Prime numbers are fundamental objects in number theory and constitute the mathematical basis of many public-key cryptographic systems, including RSA, Diffie–Hellman, and ElGamal algorithms. In these systems, generating large prime numbers and verifying their primality require significant computational resources. Since traditional deterministic methods become inefficient for very large integers, probabilistic primality tests are widely applied in practice. Algorithms such as the Miller–Rabin, Fermat, and Solovay–Strassen tests allow large numbers to be tested for primality with high accuracy and relatively low computational complexity.

Currently, improving primality testing algorithms, reducing their computational complexity, and evaluating their cryptographic robustness in the era of quantum computing are among the most relevant scientific challenges. In particular, with the emergence of post-quantum cryptography, comprehensive analysis of the efficiency and security of prime-based cryptographic methods has become increasingly important. From this perspective, the main objective of this article is to investigate the theoretical foundations, operating principles, and practical efficiency of primality testing algorithms.

## Main Part

The problem of determining whether a number is prime or composite is one of the fundamental problems in number theory. A natural number n>1 is called a prime number if it is divisible only by 1 and itself. Otherwise, the number is considered composite [1]. Since prime numbers are widely used in cryptography, especially in public-key algorithms, the efficiency of primality testing algorithms for large integers is of great importance.

One of the simplest methods for determining primality is the trial division method. In this approach, divisibility of the number $n$ is checked for all integers satisfying $2 \leq d \leq \sqrt{n}$. If the following condition holds:

$$d \mid n$$

then $n$ is considered a composite number. Although this method is straightforward, its computational complexity becomes extremely high for large integers [2].

One of the efficient primality tests for large numbers is the Fermat primality test. This test is based on Fermat's Little Theorem. If $p$ is a prime number and $a$ is not divisible by $p$, then the following congruence holds [3]:

$$a^{p-1} \equiv 1(\mathrm{mod}p)$$

If the above relation is not satisfied for a chosen value of $a$, then the number is composite. However, there exist certain composite numbers for which this congruence still holds. Such numbers are known as Carmichael numbers [4].

An improved version of the Fermat test is the Solovay-Strassen primality test. This algorithm is based on Euler's criterion and uses the Jacobi symbol. The test is performed using the following expression [5]:

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)(\mathrm{mod}n)$$

where $\left(\frac{a}{n}\right)$ denotes the Jacobi symbol. Compared to ↓ Fermat test, this method provides more reliable results.

One of the most widely used primality tests in practical cryptography is the Miller-Rabin algorithm [6]. In this algorithm, the value $n-1$ is represented in the following form:

$$n-1 = 2^s \cdot d$$

where $d$ is an odd number. Then, for randomly selected values of $a$, the following quantity is computed:

$$a^d(\mathrm{mod}n)$$

If the result is neither 1 nor -1 , repeated squaring operations are performed. During this process, if the following condition is not satisfied:

$$a^{2^r d} \equiv -1(\mathrm{mod}n)$$

then $n$ is considered composite. Although the Miller-Rabin test is probabilistic, after several iterations it provides extremely high accuracy [7].

Among deterministic primality tests, the AKS algorithm occupies a special place. This algorithm was proposed in 2002 by Agrawal, Kayal, and Saxena and became the first universal primality test operating in polynomial time [8]. The main idea of the AKS algorithm is based on the following congruence:

$$(x-a)^n \equiv x^n - a(\mathrm{mod}n)$$

if and only if $n$ is a prime number. Despite its theoretical significance, in practice the Miller-Rabin test is much faster than the AKS algorithm.

Primality testing algorithms are an essential component of key generation processes in modern cryptographic systems. In the RSA algorithm, two large prime numbers $p$ and $q$ are selected to generate the following value [9]:

$$n = pq$$

The computational difficulty of factorizing this number ensures the security of the system. Therefore, the efficiency and reliability of primality testing algorithms directly affect the overall robustness of cryptographic systems.

## Conclusion

Primality testing algorithms are among the fundamental components of modern cryptography. Since simple deterministic methods become inefficient for very large integers, probabilistic primality tests are widely used in practice. The Fermat, Solovay–Strassen, and Miller–Rabin tests allow large integers to be tested rapidly with high accuracy. The AKS algorithm, on the other hand, proved that the primality testing problem can be solved in polynomial time from a theoretical perspective. In the future, the development of quantum computing technologies may require reconsideration of the security of primality tests and prime-based cryptographic systems.

## REFERENCES

1. Hardy G. H., Wright E. M. An Introduction to the Theory of Numbers. — Oxford University Press, 2008.
2. Crandall R., Pomerance C. Prime Numbers: A Computational Perspective. — Springer, 2005.
3. Rosen K. H. Elementary Number Theory and Its Applications. — Pearson, 2010.
4. Carmichael R. D. "On Composite Numbers P Which Satisfy the Fermat Congruence". American Mathematical Monthly, 1910.
5. Solovay R., Strassen V. "A Fast Monte-Carlo Test for Primality". SIAM Journal on Computing, 1977.
6. Miller G. L. "Riemann's Hypothesis and Tests for Primality". Journal of Computer and System Sciences, 1976.
7. Rabin M. O. "Probabilistic Algorithm for Testing Primality". Journal of Number Theory, 1980.
8. Agrawal M., Kayal N., Saxena N. "PRIMES is in P". Annals of Mathematics, 2004.
9. Rivest R., Shamir A., Adleman L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM, 1978.