Section 1

ANALYZING ALGORITHMS FOR VERIFYING PRIMALITY OF LARGE NUMBERS

Oles Yudin
National Aerospace University «Kharkiv Aviation Institute»
Scientific advisor: Vladimir Pevnev

Relevance. In the modern world, an information and communication system without cryptographic protection is inconceivable. The Entrust report «Global Encryption Trends» highlights that client data stands as the primary encryption priority among surveyed enterprises. However, only 42% of respondents are projected to utilize encryption to safeguard their clients' data in 2021 [1]. It is worth noting that prime numbers play a pivotal role in the field of cryptography and are considered a fundamental element in many cryptographic systems. One of the primary reasons for their relevance is their unique mathematical property: they have only two divisors – 1 and themselves. This property makes them a suitable tool for generating cryptographic keys. For instance, in asymmetric encryption systems like RSA, the security of keys relies on the complexity of factoring large composite numbers into their prime factors. Due to this complexity, it becomes challenging for attackers to break cryptographic messages encrypted using such keys.

The importance of analyzing algorithms for checking the primality of large numbers lies in the fact that with the increase in computational power of modern electronic computing machines, it becomes possible to factorize increasingly larger composite numbers, thereby posing a risk to the security of cryptographic systems [2]. In 1991, the «RSA Factoring Challenge» was introduced with the aim of stimulating research in the field of computational number theory. The latest achievement in the challenge was the factorization of a number of length 829 bits into prime factors. As of 2023, the optimal key length in the RSA cryptosystem is considered to be a 2048-bit key. Considering the current pace of development in information technologies and computational systems, questions arise regarding the security of existing encryption algorithms in the near future.

The purpose of this work is to analyze existing algorithms used for primality testing of large numbers.

Principal provisions. The report examined the fundamental and most popular algorithms for determining the primality of numbers, such as: sieve of Eratosthenes; Miller-Rabin primality test; sieve of Atkin; AKS primality test.

A significant breakthrough occurred in 2004 when researchers from the Indian Institute of Technology in Kanpur proposed a primality testing method named AKS (Agrawal-Kayal-Saxena) [3]. The test was simultaneously general, polynomial, deterministic, and unconditional.

The report investigates the possibility of transforming the prime number determination problem by integrating it with the task of number factorization. It asserts that when determining two factors, which can be either prime or composite, it is possible to conclude that a number is composite. Additionally, the report provides evidence that such tasks do not belong to the class of NP-complete problems. The evidence in the report is illustrated by an example showing that these algorithms have polynomial complexity.

Conclusions. The protection of information through cryptography continues to evolve, especially during data transmission over unsecured communication channels. However, public key encryption algorithms quickly exhaust the supply of known prime numbers. Additionally, the capability of modern computing systems is growing, potentially enabling the factorization of larger prime numbers in the future. Due to these reasons, it's necessary to optimize existing and develop new primality testing algorithms to cover a broader range of potential prime numbers within a given range.

List of references

1. Ponemon Institute. Global Encryption Trends Study, 2021. – Page 5. URL: https://www.entrust.com/lp/en/global-encryption-trends-study (date of access: 05.10.2023).
2. Pevnev V. Pseudoprime Numbers: Basic Concepts and the Problem of Security. ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer : Proc. of 13th Int. Conf. Kyiv, Ukraine, May 15 18. 2017. Kyiv. 2017. P. 583–593.
3. Agrawal M., Kayal N., Saxena N. Primes is in P. Annals of Mathematics. 2004. Volume 160. Page 781–793. DOI: https://doi.org/10.4007/annals.2004.160.781.

Information about the authors

Oles Yudin, a PhD student from the Department of Computer Systems, Networks and Cybersecurity, o.yudin@csn.khai.edu
Vladimir Pevnev, Dr. Sc., professor from the Department of Computer Systems, Networks and Cybersecurity, v.pevnev@csn.khai.edu