Дмитриев Егор Андреевич

студент

ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева»

г. Самара, Самарская область

КРИТЕРИЙ ПОКЛИНГТОНА

Аннотация: *в данной работе анализируется один из основных алгоритмов определения простоты числа – Критерий Поклингтона. Автор рассматривает реализацию алгоритма, определяет его практическую ценность, представляет блок-схему алгоритма.*

Ключевые слова: *криптография, простое число, вычислительная сложность, тест простоты, наибольший общий делитель.*

Основные понятия

Введем некоторые определения, которые будут использованы в работе.

Определение 1. Криптография – наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, а также невозможности отказа от авторства.

Определение 2. Простое число – натуральное (целое положительное) число $\mathbb{N}$, которое имеет ровно два различных натуральных делителя – единицу и самого себя.

Определение 3. Вычислительная сложность – функция, показывающая взаимосвязь между объемом работы, выполняемой алгоритмом, от размера входных данных.

Определение 4. Тест простоты – алгоритм, который по заданному натуральному числу $\mathbb{N}$ позволяет точно или с некоторой долей вероятности определить, является ли это число простым.

Определение 5. *НОД (a, b) = d, d* – наибольший общий делитель, если:

1) $a \vdots d \wedge b \vdots d$;

2) $a \vdots d_1 \wedge b \vdots d_1 \Rightarrow d \vdots d_1$.

Введение

Тест простоты – алгоритм, который является достаточно критичным в криптографии в системе с открытым ключом.

Тесты простоты

Следует отметить, что существующие алгоритмы проверки простоты могут быть разделены на две больших категории: истинные (детерминированные) и вероятностные тесты. Алгоритмы первой категории позволяют точно определить простоту или составность числа. А те, что относятся ко второй категории, позволяют это выяснить, но с некоторой вероятностью ошибки. Многократное их повторение для одного числа, но с разными параметрами, обычно позволяет сделать вероятность ошибки сколь угодно малой величиной.

Критерий Поклингтона

Тип теста: детерминированный.

Вычислительная сложность алгоритма: $La^n[\alpha,c]$, где c – положительная константа, $0 \le \alpha \le 1$, зависящие от выбора алгоритма факторизации.

Описание: пусть *n* – натуральное число и *n-1* имеет простой делитель *q*, причем $q > \sqrt{n} - 1$. Если найдется целое число *a*, для которого выполняются условия:

1) $a^{n-1} \equiv 1 (mod\ n)$;

2) $НОД(a^{(n-1)/q} - 1, n) = 1$.

Тогда *n* является простым числом.

Алгоритм: представлен на рисунке 1 в виде блок-схемы.

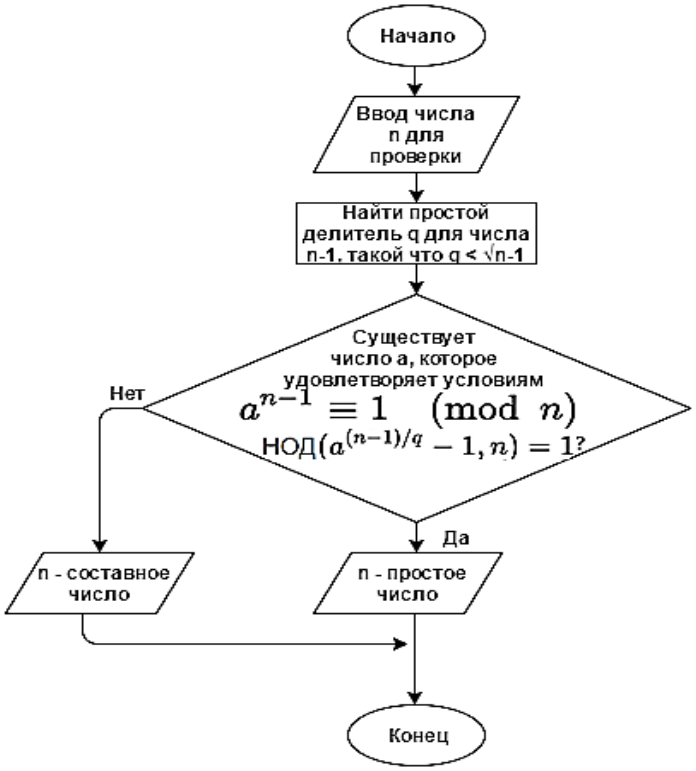

Рис. 1. Алгоритм проверки числа на простоту
при помощи критерия Поклингтона

Практическое применение: для получения больших простых чисел с частично известной факторизацией *n – 1*.

Заключение

Подводя итоги, можно констатировать, что был рассмотрен алгоритм определения простоты числа. Проведённые исследования позволяют сделать вывод о том, алгоритм достаточно трудоемок в вычислительном плане, несмотря на то, что он лучше, чем алгоритм простого перебора.

Список литературы

1. Шнайер Б.М. Прикладная криптография / Б.М.Шнайер. – Триумф 2002. – 816 с.

2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.

3. Дональд Кнут. Глава 4.5.4. Разложение на простые множители // Искусство программирования. Т. 2. Получисленные алгоритмы. – 3-е изд. – М.: Вильямс, 2007. – С. 832.

4. Нестеренко Ю В. Введение в криптографию / Под ред. В.В. Ященко. – Питер, 2001. – 288 с.