УДК 004.942

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РАБОТ «ЭФФЕКТИВНОСТЬ ВЕРОЯТНОСТНЫХ И ДЕТЕРМИНИРОВАННЫХ АЛГОРИТМОВ ПОИСКА БОЛЬШИХ ПРОСТЫХ ЧИСЕЛ ДЛЯ ЗАДАЧ КРИПТОГРАФИИ»

И.А. РОГУЛИН [1*] ***,И.М. ЯЧИКОВ*** [2]

[1] *магистрант кафедры вычислительной техники и программирования, ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», Магнитогорск, РОССИЯ*

[2] *профессор кафедры вычислительной техники и программирования, д-р. техн. наук, ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», Магнитогорск, РОССИЯ*

[*] *email: rogggg93@mail.ru*

Все алгоритмы проверки простоты делятся на две больших подгруппы: детерминированные и вероятностные проверки. Алгоритмы первой группы позволяют точно сказать, является число простым или составным. Алгоритмы второй группы позволяют это определить, но с некоторой вероятностью ошибки. Многократное их повторение для одного числа, но с разными параметрами, обычно позволяет сделать вероятность ошибки сколь угодно малой величиной.

Целью научной работы является исследование детерминированных и вероятностных алгоритмов поиска больших простых чисел для генерации простых чисел заданной разрядности, проверка их эффективности с помощью алгоритма RSA для получения открытого и закрытого ключей.

Объектом исследования являются алгоритмы, реализующие поиск больших простых чисел. Предмет исследования: алгоритмы поиска больших простых чисел, используемые генерации простых чисел разных разрядностей. Результаты, полученные в ходе проведения научного исследования могут быть использованы в алгоритме шифрования RSA для получения открытого и закрытого ключей.

В данной работе будут рассмотрены алгоритмы для получения простых чисел, их сравнительных анализ посредством временной характеристики выполнения, а так же будет произведена проверка этих алгоритмов в алгоритме шифрования RSA, чтобы сделать выводы об эффективности каждого из рассмотренных алгоритмов.

Для сравнения своей работы с другими авторами, были выбраны две работы: работа Кучина Б. и работа Дикарева С.

В своем эссе Кучин Б., из «Московского Физико-технического Института», берет для сравнения некоторые детерминированные и вероятностные алгоритмы для проверки числа на простоту.

Кучин Б. описывает принцип работы каждого, рассмотренного в эссе, алгоритма. Ищет их плюсы и минусы. А так же, для некоторых алгоритмов, приводит псевдокод, показывающий реализацию данного алгоритма.

В конце эссе приводится сводная таблица, которая показывает, какой алгоритм где используется. А так же, в заключении, сказано, что в зависимости от поставленной задачи, те или иные алгоритмы отрабатывают довольно хорошо. Другими словами, если использовать один и тот же алгоритм для одних и тех же задач, то его эффективность, а так же временные характеристики будут очень сильно отличаться, и, поэтому, нельзя будет сделать какое-либо утверждение о том, хорош ли алгоритм или нет.

В другой работе, написанной Дикаревым С., автор исследует алгоритмы генерации простых чисел. Он изучает 3 алгоритма: «Алгоритм частичного деления», «Тест Фема» и «Тест Соловея-Штрассена». Для каждого алгоритма приводится полное описание и получение некого псевдоалгоритма, который и будет использоваться в качестве генерации простых чисел. Так же автор использует эмпирические данные, для оценки скорости работы алгоритмов.

Отличительной особенностью моей работы будет исследование алгоритмов поиска больших простых чисел с помощью языка программирования, проверка полученного алгоритма в крипто-алгоритме RSA и, на основе временных характеристиках выполнения данных алгоритмов в RSA, будут сделаны выводы, какой из алгоритмов в наиболее удачно подходит для генерации простых чисел разных разрядностей.

Список литературы:

1. *Шнайер Б.* Практическая криптография / *Б. Шнайер., Н. Фергюсон.* – М.: Вильямс, 2005. – 424 с.

2. *Шнайер Б.* Секреты и ложь. Безопасность данных в цифровом мире / *Б. Шнайер.* – СПб.: Питер, 2003. – 368 с.

3. *Кучин Д.В.* Программное обеспечение для анализа тестов простоты натурального числа / *Д.В. Кучин., Ю.В. Шабля* // Доклады ТУСУРа. – 2014. – № 4 (34). – С. 95-99.

4. *Логунова О.С.* Методика исследования предметной области на основе теорико-множественного анализа / *О.С. Логунова, Е.А. Ильина* // Математическое и программное обеспечение систем в промышленной и социальной сферах. – 2012. – № 2. – С. 281-291.

5. *Дикарев С.С.* Исследование алгоритмов генерации простых чисел / *С.С. Дикарев, Е.Н. Рябухо, Т.В. Турка* // Молодой ученый. – 2015. – № 10. – С. 6-9.