ISSN 2181-3187

АЛГОРИТМ МИЛЛЕРА-РАБИНА ДЛЯ ПРОВЕРКИ ЧИСЕЛ НА ПРОСТОТУ

Бердимуратов М.К.[1], Ибрагимов К.[2]
[1]Каракалпакский государственный университет
[2]Нукусский филиал Самаркандского государственного университета ветеринарной медицины, животноводства и биотехнологии
ibragimov.kuanishbay@gmail.com

Немногие криптографические алгоритмы являются и безопасными и практичными. Обычно эти алгоритмы основаны на одном из трудных разрешимых проблем математики. Некоторые из этих безопасных и практичных алгоритмов подходят только для распределения ключей. Другие подходят только для шифрования данных и для цифровых подписей. Первый полноценный алгоритм с открытым ключом, который можно использовать для шифрования и цифровых подписей является алгоритм RSA.

Безопасность алгоритма RSA основана на трудности разложения на множители больших чисел. Открытый и закрытый ключи являются функциями двух больших (не менее 200 десятичных разрядов) простых чисел. Предполагается, что восстановление открытого текста по шифротексту и открытому ключу эквивалентно разложение на множители двух простых чисел. В теории чисел не смотря на многолетнюю историю и на очень интенсивные поиски в течение последних несколько лет, эффективный алгоритм разложения натуральных чисел на множители так и не найден.

В алгоритме RSA для генерации двух ключей используются два (p и q) больших случайно выбранных простых числа равной длины. Проверка чисел на простоту является составной частью алгоритмов генерации простых чисел, используемых в криптографии с открытым ключом. Существует вероятностные и детерминированные алгоритмы. Детерминированный алгоритм гарантированно решает поставленную задачу, однако на сегодняшний день они считаются непрактичными, а вероятностный алгоритм использует генератор случайных чисел и дает не гарантированно точный ответ. На сегодняшней день для проверки чисел на простоту чаще всего используется тест Миллера-Рабина, который является вероятностным алгоритмом. Алгоритм был разработан Гари Миллером в 1976 году и модифицирован Майклом Рабином 1980 году. Он позволяет находить вероятно простые числа, которые могут оказаться составными. Основное преимущество алгоритма заключается в том, что на обычном компьютере он выполняется всего за несколько секунд.

ISSN 2181-3187

В алгоритме n нечетное число и $n-1=2^s r$ простое число, где r -нечетное. Если n простое, то $\forall n \geq 2$, где $НОД(a,n)=1$, выполняется $a^{p-1}=1(\mathrm{mod}\, p)$, где p - простое число.

Алгоритм может быть записан следующим образом:

Ввод: $n \geq 5$ нечётное натуральное число, которое необходимо проверить на простоту; k, параметр, определяющий точность теста.

Вывод: *составное*, означает, что n точно составное; *вероятно простое*, означает, что n с высокой вероятностью является простым

Представить $n-1$ в виде $2^s r$, где число r нечётно

цикл A: повторить k раз:

Выбрать случайное a в диапазоне $[2, n-2]$

$y \leftarrow a^r (\mathrm{mod}\, n)$

если $y=1$ или $y=n-1$ то перейти на следующую итерацию цикла A

цикл B: повторить *s-1* раз:

$y \leftarrow y^2 (\mathrm{mod}\, n)$

если $y=1$ то вернуть *составное*

если $y=n-1$ то перейти на следующую итерацию цикла A

вернуть *составное*

вернуть *вероятно простое*

Трудоемкость теста Миллера-Рабина для одного числа a оценивается величиной $O(\log^3 n)$. М.Рабин доказал что в случае составного n вероятность правильного ответа в тесте не менее 3/4.

Для изучения поставленной задачи был использован язык Python, который широко используется в интернет-приложениях, разработке программного обеспечения, науке о данных и машинном обучении. Он эффективен, прост в изучении и работает на разных платформах. В Python также есть несколько библиотек для работы с асимметричным шифрованием, например, *cryptography*.

В статье описываются тест Миллера-Рабина, позволяющий определить является ли число простым на основании сложных математических проверок. А также создана программа на языке Python способный работать с числами, содержащим сотни цифр.

Литература:

1. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С //Москва. Изд.Триумф. 2002. – 816 с.
2. Н. Коблиц. Курс теории чисел и криптографии.//Москва. Изд. ТВП.2001. – 269 с.

ISSN 2181-3187

3. Маховенко Е.Б. Теоретико-числовые методы в криптографии. //Учебное пособие. М.: Гелиос АРВ, 2006. – 320 с.
4. Коутинхо С. Введение в теорию чисел, Алгоритм RSA. //М.: Постмаркет, 2001. – 328 с.
5. Свейгарт Э. Криптография и взлом шифров на Phyton. //Пер.с анг. -СПб.: ООО “Диалектика”, 2020. – 512 с.
6. Бердимуратов М.К, Ибрагимов К.И, Балтабаев Ж.Е. "Изучение проблемы факторизации параметра n в алгоритме RSA с помощью системы «Mathematica»."*Вестник науки и образования”* 23-2 (77) (2019): 4-7.