УДК 511.174

НЕКРИПТОГРАФИЧЕСКАЯ ХЭШ-ФУНКЦИЯ И СУММА ЦИФР СЛУЧАЙНОГО НАТУРАЛЬНОГО ЧИСЛА

А. Большакова[1], Д. Степанян[2], А.В. Рожков[3]

1 *anastaicha94@mail.ru*; Кубанский государственный университет
2 *diana14.02.94@mail.ru*; Кубанский государственный университет
3 *ros.seminar@bk.ru*; Кубанский государственный университет

Изучаются задачи теории чисел, которые могут быть модельными для других разделов математики.

Ключевые слова: теория чисел, пакеты компьютерной алгебры, криптография, простые числа.

Построение хэш-функции

Определение. *Функция χ, ставящая в соответствие сообщению произвольной длины сообщение фиксированной длины, называется хэш-функцией. Эквивалентно, отображение $\chi : \mathbb{N} \to \mathbb{N}$, имеющее конечный образ называется хэш-функцией. Хэш называется некриптографическим, если в процессе его создания не используется шифрование.*

Отметим, что весь мир использует некриптографический хэш. Российский ГОСТ Р 34.11–2012 хэш-функции с 2012 г. тоже стал некриптографическим.

Определение. *Функция $\psi : \mathbb{N} \to \mathbb{N}$ называется однонаправленной, если для любого $n \in \mathbb{N}$ образ $\psi(n) = m$ вычисляется за полиномиальное время, но не существует полиномиального алгоритма, вычисляющего прообраз n образа m.*

Проблема построения хэш-функций является одной из основных в криптографии. Нет математически строгих доказательств, что хоть одна из хэш-функций криптостойка. Именно поэтому весь мир пользуется одними и теми же алгоритмами — погибать так вместе!

Два наиважнейших свойства хэш-функции.

По хэшу должно быть очень трудно найти прообраз, т.е. хэш должен быть однонаправленной функций.

Должно быть очень трудно одновременно создать два разных сообщения с одним и тем же хэшем.

Чрезвычайная важность хэша в криптографии определяется тем, что во всех государственных системах электронной подписи шифруется не само сообщение, а его хэш.

Поэтому криптографы, математики и просто любители высоких технологий и трудных задач создают свои хэш-функции в надежде создать математически безупречный инструмент.

В нашей работе предложен хэш на основе простых арифметических понятий.

Пусть n – натуральное число, взятое в десятичной записи и $S(n)$ – сумма цифр этого числа.

Если к получаемым суммам последовательно применять функцию S, то в итоге получится некоторая цифра, принадлежащая множеству $J = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Функцию, которая ставит исходному натуральному числу эту итоговою цифру обозначим $\overline{S}:\mathbb{N}\to J$.

Лемма 1. *Пусть $n=j+9k$, $j\in J, k\in\mathbb{N}$ натуральное число, тогда, $\overline{S}(n)=j$.*

Лемма 2. *Следующие множества совпадают:*

$$J_3=\{\overline{S}(n^3), n\in\mathbb{N}\}=\{1,8,9\}.$$

Определение некриптографической хэш-функции. *Пусть некоторое сообщение закодировано натуральным числом M, тогда в качестве его хэша возьмем число $S(M^3)$.*

Для того чтобы подобрать сообщение M с заданным хэшем, например, 2017, нам необходимо найти такое натуральное число M, что $S(M^3)=2017$.

Учитывая то, как прихотливо ведет себя функция суммы цифр числа, решение подобной задачи весьма затруднительно.

Теорема 1. *Необходимым условием существования натурального числа M, такого, что $S(M^3)=n$, является включение $\overline{S}(n)\in J_3$.*

С другой стороны, если $n\in\{1+9k,8+9k,18k,9(6k-1)|k\in\mathbb{N}\}$, то искомое решение M существует.

Для чисел вида $n\in\{9(6k-5),9(6k-3)|k\in\mathbb{N}\}$ решение неизвестно.

О сумме цифр случайного натурального числа

Случайные числа играют в криптографии огромную роль – они являются основным инструментом при выборе ключа шифрования. Неверно, что математическое ожидание выбранной наугад цифры равно 9/2, а сумма цифр случайного n-значного числа равна $9n/2$.

Лемма 3. *Средневзвешенная цифра n-значного натурального числа равна* $9/2+1/2n$

Сумма цифр случайного n-значного натурального числа равна $9n/2+1/2$.

Теорема 2. *Средневзвешенная цифра числа, имеющего не более n знаков, равна*

$$\frac{9}{2}+\frac{9}{20}\cdot\frac{10^n}{10^n-1}\cdot\left(\frac{1}{1\cdot10^{n-1}}+\frac{1}{2\cdot10^{n-2}}+\ldots+\frac{1}{n\cdot10^9}\right).$$

Положим

$$S_n=\frac{9}{20}\cdot\left(\frac{1}{1\cdot10^{n-1}}+\frac{1}{2\cdot10^{n-2}}+\ldots+\frac{1}{n\cdot10^9}\right).$$

Теорема 3. *Для любого $n>1$ имеют место неравенства*

$$\frac{1}{2n}+\frac{1}{(2n)^2}>S_n>\frac{1}{2n}+\frac{1}{(2n)^3}.$$

Для $n>11$ верны неравенства

$$\frac{1}{2n}+\frac{1}{16n^2}>S_n>\frac{1}{2n}+\frac{1}{18n^2}.$$

Следствие 1.

$$\lim_{n\to\infty}\frac{S_n}{\frac{1}{2n}+\frac{1}{18n^2}}=1.$$

Следствие 2. *Для $n>11$ сумма цифр случайного не более чем n-значного числа принадлежит интервалу*

$$\left(\frac{9n+1}{2}+\frac{1}{18n},\frac{9n+1}{2}+\frac{1}{16n}\right).$$

Литература

1. Рожков А.В. *Стратегия DPS - Debian-Python-Sage: Проблемно-ориентированные вычислительные среды на открытом коде* // Труды V междунар. науч.-практич. Конф. «Информационные технологии в образовании и науке» (ИТОН – 2016). – Казань: КФУ, 2016. – С. 172–179.

2. Рожков А.В., Рожкова М.В. *Экспериментальная (вычислительная) теория чисел* // Новые информационные технологии в образовании и науке: Материалы X межд. науч.-практ. конф., Екатеринбург, 27 февраля – 3 марта 2017 г. ФГАОУ ВО «Рос. гос. проф.-пед. ун-т». – Екатеринбург, 2017. – С. 413–417.

3. Рожков А.В., Ниссельбаум О.В. *Теоретико-числовые методы в криптографии*. – Тюмень: ТюмГУ, 2007. – 160 с.

NOT CRYPTOGRAPHIC THE HASH FUNCTION AND SUM OF DIGITS OF RANDOM NATURAL NUMBER

A. Bolchakova, D. Stepanyan, A.V. Rozhkov

Number theory tasks which can be model for many sections of mathematics are studied.

Keywords: number theory, packages of computer algebra, cryptography, prime numbers.

УДК 511.174

ЗАМЕТКА О ПРОБЛЕМЕ КОЛЛАТЦА

А. Большакова[1], Д. Степанян[2], А.В. Рожков[3]

1 *anastaicha94@mail.ru*; Кубанский государственный университет
2 *diana14.02.94@mail.ru*; Кубанский государственный университет
3 *ros.seminar@bk.ru*; Кубанский государственный университет

Изучаются задачи теории чисел, которые могут быть модельными для других разделов математики.

Ключевые слова: теория чисел, пакеты компьютерной алгебры, криптография, простые числа.

Введение

Гипотеза Коллатца (гипотеза 3n+1, сиракузская проблема) — одна из нерешённых проблем математики.
Названа по имени немецкого математика Лотара Коллатца, сформулировавшего эту задачу 1 июля 1932 года.