УДК 681.3.06, 65.012

В.Я. Певнев

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

МЕТОДИКА ПОСТРОЕНИЯ ПСЕВДОПРОСТЫХ ЧИСЕЛ

Рассматривается проблема построения простых чисел. Предлагается новый подход, который основывается на построении кандидатов на простое число. Для теоретического обоснования данной методики формулируется две теоремы, на основании которых производится поиск псевдопростых чисел. Представленные результаты экспериментов подтверждают эффективность предложенной методики.

Ключевые слова: *простые числа, псевдопростые числа, простые сомножители.*

Введение

Хотя проблема кибербезопасности возникла одновременно с возникновением компьютера, говорить о ней начали совсем недавно. Сейчас под кибербезопасностью подразумевают ту часть информационной безопасности, которая связана с инфокоммуникационными технологиями. Одной из задач информационной безопасности является обеспечение конфиденциальности, которая достигается криптографическими методами. Применение сетевых и облачных технологий позволило резко уменьшить время криптоанализа шифрованных текстов. Ответом криптографов стало создание принципиально новых систем шифрования. В настоящее время широко используются системы симметричного и асимметричного шифрования. Двухключевые системы шифрования дали огромный импульс развития теории простых чисел (ПЧ). Сложность задачи факторизации, основы системы RSA, базируется на проблеме нахождения и распределения ПЧ в натуральном ряде, которая занимает центральное место в аналитической теории чисел. Для достижения приемлемого уровня конфиденциальности пользователи асимметричных систем увеличивают размеры ключей. Если в 2000 году размер ключа в системе RSA был равен 512 бит, то сегодня поднимается вопрос об его увеличении до 4096 бит. Совершенно неожиданно возникла проблема использования ограниченного количества ПЧ в качестве ключей [1]. В связи с этим силовые структуры, получив некоторое количество ПЧ за достаточно большое время (1-2 года), будут иметь практически неограниченный доступ с конфиденциальной информации граждан.

Анализ основных достижений и литературы. Наиболее известной по представлению материалов, касающихся нахождения и распределения ПЧ, является книга К. Прахара, изданная в 1957 году в Германии [2]. В работе [3] показаны методы факторизации, которые возможно применять при отыскании ПЧ. Наиболее полными работами по современным методам нахождению ПЧ и факторизации являются [4, 5]. В работах [6, 7] рассматриваются как закономерности в строении ПЧ, так и некоторые их свойства.

В абсолютном большинстве алгоритмов нахождения ПЧ процесс начинается с вычисления числа заданной размерности. После этого построения полученное число проверяется на простоту различными тестами, и если оно проходит эти проверки, то обьявляется ПЧ.

В [8] предложен и теоретически обоснован принципиально новый подход к построению ПЧ. Он основан на выделении множества псевдопростых чисел (ППЧ), которые могут стать ПЧ. Причем с ростом размерности искомого ПЧ количество ППЧ, предлагаемых для проверки, уменьшается.

Цель работы. Целью работы является продолжение теоретических и экспериментальных исследований законов распределения ПЧ.

Постановка задачи. Усовершенствовать методику построения множества ППЧ и провести экспериментальную оценку эффективности представленной методики.

Материалы и результаты исследований

В работе [8] сформулированы и доказаны следующие теоремы.

Теорема 1 (Т1)**.** Сумма произведений двух непересекающихся множеств ПЧ есть взаимно ПЧ с каждым из элементов этих множеств.

Теорема 2 (Т2). Величина ПЧ, прибавляемого к произведению первых K чисел множества ПЧ, должна быть менее a_{K+1}^2, где a – ПЧ.

Данные теоремы являются основанием для разработки метода нахождения ПЧ.

Т2 устанавливает ограничения на количество прибавляемых ПЧ к произведению первых K чисел множества ПЧ с целью однозначного определения местоположения ППЧ. При невыполнении данного условия возможен пропуск кандидата на ПЧ. Например, если к произведению первых шести ПЧ

(2,3,5,7,11,13) не прибавить число 289 = 17*17, то пропускается ПЧ 30319. Но, следует отметить, что НОД(2*3*5*7*11*13, 289) =1, или другими словами Т1 выполняется.

Введем понятие шага определения (ШО). Под ШО будем понимать максимальную величину числа, прибавляемого к произведению ПЧ, позволяющую не допустить пропуска ППЧ. Размер ШО можно вычислить, исходя из Т2.

В табл. 1 приведены статистические данные, позволяющие оценить предлагаемую методику отыскания ПЧ. В таблице представлены следующие данные:

– количество простых сомножителей (КолПС) – количество последовательно идущих ПЧ от 2 и далее чисел в произведении;

– размер произведения ПЧ(РАЗМЕР) – количество десятичных знаков в произведении;

– старший сомножитель (Ст.сомн) – наибольшее ПЧ в произведении из КолПС;

– количество ПЧ (Кол ПЧ) – количество ПЧ на ШО, которое соответствует количеству полученных ППЧ на ШО;

– процент проверяемых чисел (% ПрЧ) – отношение количества ПЧ на ШО к общему числу чисел на ШО.

Таблица 1

Статистические данные, позволяющие оценить предлагаемую методику отыскания ПЧ

Кол ПС	10	15	20	25	30	35	40	45	50	55	60	65
РАЗМЕР	9	17	25	35	46	57	68	79	91	103	115	127
Ст.сомн	29	47	71	97	113	149	173	197	229	257	281	313
ШО	961	2809	5329	10201	16129	22801	32041	39601	54289	69169	80089	100489
Кол ПЧ	152	394	685	1227	1847	2513	3396	4119	5472	6724	7782	9566
% ПрЧ	22	14	13	12	11,5	11	10,6	10,4	10	9,7	9,7	9,5

Кол ПС	70	75	80	85	90	95	100	105	110	115	120	125
РАЗМЕР	140	153	166	179	191	205	218	232	246	260	274	288
Ст.сомн	349	379	409	439	463	499	541	571	601	631	659	691
ШО	124609	146689	175561	196249	218089	253009	299209	332929	368449	410881	436921	491401
Кол ПЧ	11631	13491	15873	17593	19361	22187	25836	28527	31310	34566	36594	40749
% ПрЧ	9,3	9,2	9	9	8,9	8,8	8,6	8,6	8,5	8,4	8,4	8,3

Как видно из табл. 1, скорость роста величины размера произведения ПЧ превышает скорость роста факториальной зависимости, что еще раз подчеркивает сложность задачи нахождения ПЧ больших размеров. Наиболее интересными данными в таблице, по мнению автора, является процент проверяемых чисел. Практически все предлагаемые алгоритмы поиска ПЧ используют простой перебор претендентов. Для больших чисел (D >200) данный показатель составляет менее 9% от общего числа чисел на проверяемом интервале. Если взять какой-либо алгоритм, который будет проверять только числа, заканчивающиеся на 1,3,7,9, то процент проверяемых чисел будет равен 40.

В качестве примера можно привести и произведение ПЧ меньших тысячи. В результате произведения 168 ПЧ получается число размером 416 десятичных знаков. При проведении проверки на простоту, используя первые сто ПЧ больших 1000 от 1009 до 1721, было обнаружено одно ПЧ. Данная проверка осуществлялась с помощью модуля is_prime языка Python [9]. Очевидно, что без использования предложенного метода, необходимо провести более 1700 проверок. Если рассматривать только числа, которые заканчиваются на 1,3,7,9, то количество проверок станет примерно равным 690. При использовании предложенного метода количество просматриваемых ППЧ составит 100. Нельзя сказать, что суммарное время нахождения ПЧ уменьшится в шесть раз, но выигрыш будет достаточно большим.

Следует отметить и тот факт, что при использовании вероятностного теста на простоту Соловея – Штрассена [10], все числа, полученные в результате наших вычислений числа, будут простыми с вероятностью $1\text{-}2^{\text{-}169}$.

Недостатком предложенного подхода является относительно малый интервал рассматриваемых чисел в ШО. Как сказано выше, размер ШО определяется квадратом первого ПЧ, которое используется для вычисления ППЧ.

Каким образом можно увеличить размер ШО?

На взгляд автора можно пойти двумя путями.

Первый путь. Модифицируем теоремы Т1 и Т2 следующим образом.

Усиленная теорема 1 (Т3). Сумма (разность) произведений двух непересекающихся множеств ПЧ есть взаимно ПЧ с каждым из элементов этих множеств.

Усиленная теорема 2 (Т4). Величина ПЧ, прибавляемого (вычитаемого) к произведению первых K чисел множества ПЧ, должна быть менее a^2_{K+1}, где a – ПЧ.

Доказательство Т3(Т4) аналогично Т1(Т2) в [8]. Использование этих теорем позволяет увеличить ШО в два раза.

Второй путь предполагает использование комбинации ПЧ больших, чем максимальное ПЧ в произведении. Под комбинацией в данном случае понимается произведение двух и более ПЧ, их степени, которые не превосходят заранее определенного числа. Рассмотрим число 2310, полученное в результате умножения первых пяти ПЧ. Следующее число, в рассматриваемом примере – 30030 (2*3*5*7*11*13). Для того, чтобы найти все ПЧ на интервале от 2310 до 30030 необходимо взять ПЧ от 13 до 28720. Таких чисел 3123. Кроме этого все возможные комбинации составят еще 2001. Итого получается 5124 число, которые необходимо проверить. Если учесть то, что на выделенном интервале находится 2905 ПЧ (включая число 2311), то КПД предлагаемого метода в данном примере – 56,7 процента. Если воспользоваться Т4, то необходимо брать простые числа от 13 до 13183. В этом случае уменьшается количество вычисляемых комбинаций.

Очевидно, что полученные результаты относятся только к данному примеру. При увеличении количества сомножителей в произведении ПЧ полученные цифры значительно изменятся. Очевидно и то, что при росте произведения, количество ПЧ на фиксированном отрезке натуральных чисел будет уменьшаться. В связи с этим будет уменьшаться и количество проверяемых ППЧ, а это приведет к дальнейшему росту эффективности предлагаемого метода.

Выводы

В статье предлагается методика поиска ППЧ. Теоретическое обоснование данной методики основывается на представленных теоремах, что позволяет резко сократить число претендентов на ПЧ. Его эффективность растет с ростом размера искомого ПЧ, что видно из представленных в статье результатов экспериментов.

Недостатком является относительно небольшой интервал однозначно определяемых чисел, достаточно большое количество генерируемых составных чисел, которые необходимо проверять для того, чтобы не пропустить ПЧ. Однако, сложность проверки больших чисел на простоту значительно уменьшает данный недостаток за счет значительного уменьшения проверяемых ППЧ.

Дальнейшим развитием данного метода может быть изменение стратегии поиска ППЧ.

Список литературы

1. Mimoso M. Prime Diffie-Hellman Weakness May Be Key to Breaking Crypto / M. Mimoso [Электронный ресурс]. – Режим доступа к ресурсу: https://threatpost. com/prime-diffie-hellman-weakness-may-be-key-to-breaking-crypto/115069 /#sthash.wnLEv2zR.dpuf.

2. Прахар К. Распределение простых чисел / К. Прахар. –М.: Мир, 1967. – 513 с.

3. Коблиц Н. Курс теории чисел и криптография / Н. Коблиц. –М.: ТВП, 2001. – 254 с.

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

5. Крэндалл Р. Простые числа: Криптографические и вычислительные аспекты / Р. Крэндалл, К. Померанс. – М.: УРСС: Кн. «ЛИБРОКОМ», 2011. – 664 с.

6. Малаховский В.С. О компьютерном моделировании некоторых числовых систем и дискретных семейств пифагоровым треугольников / В.С. Малаховский, Н.В. Малаховский // Вестник Калининградского государственного университета. – Калининград: КГУ, 2003. – № 3. – С. 39-46.

7. Малаховский В.С. Подмножества простых чисел в обобщенным арифметически прогрессиях / В.С. Малаховский // Вестник БФУ им. И. Канта. – Калининград: БФУ им. И. Канта, 2014. – Вып. 4. – С. 147-150.

8. Певнев В.Я. Генератор простых чисел / В.Я. Певнев // Кафедра систем інформації : Зб. наукових праць. – Х.: ТОВ «Щедра садиба плюс», 2014. – С. 140-146.

9. Python Software Foundation [Электронный ресурс]. – Режим доступа к ресурсу: https://www.python.org/.

10. Solovay R. A fast Monte-carlo test for primality / R. Solovay, V. Strassen // SIAM J. Comput. – 1977. – V. 6. – P. 84-85.

Поступила в редколлегию 1.02.2016

Рецензент: д-р техн. наук, проф. А.А. Серков, Национальный технический университет «ХПИ», Харьков.

МЕТОДИКА ПОБУДОВИ ПСЕВДОПРОСТИХ ЧИСЕЛ

В.Я. Пєвнєв

Розглядається проблема побудови простих чисел. Пропонується новий підхід, який ґрунтується на побудові кандидатів на просте число. Для теоретичного обґрунтування даної методики формулюється дві теореми, на підставі яких проводиться пошук псевдопростих чисел. Представлені результати експериментів підтверджують ефективність запропонованої методики.

***Ключові слова**: прості числа, псевдопростие числа, прості множники.*

THE METHOD OF CONSTRUCTING PSEUDOPRIMES

V.Ja. Pevnev

Considers the problems of constructing primes. Propose a new approach, which is based on the construction of the candidates for prime. For the theoretical foundation of this method is formulated two theorems, on the basis of which to search pseudoprimts. The results of experiments confirm the effectiveness of the proposed method.

***Keywords:** prime numbers, pseudoprime, prime factors.*