Дорожкин А.С., студ. гр. 208 ФК и СКД
БГУ культуры и искусств
Научный руководитель – Гляков П.В.,
канд. физ.-мат. наук, доцент

ГЕНЕРАЦИЯ БОЛЬШИХ ПРОСТЫХ ЧИСЕЛ

Идея сделать информацию недоступной для посторонних появилась так же давно, как и сама письменность. С тех пор криптография и криптографический анализ достигли очень высокого уровня. Появилось множество алгоритмов как шифрования, так и взлома шифров. Чего стоит, например, разгадка письменностей практически всех известных древних цивилизаций.

Особенно большой прорыв в этой области был сделан после изобретения компьютера. Появились шифры, на взлом которых, по подсчетам прошлых лет, понадобились бы годы или даже столетия. Но фантастическое развитие информационных технологий сыграло злую шутку с разработчиками алгоритмов шифрования. Развитие сетевых технологий, возможность распараллеливания вычислений, а главное — развитие криптоанализа позволили взламывать шифры, которые еще недавно считались абсолютно надежными. Но наука идет впереди техники. Появляются все новые и новые методы защиты информации и, соответственно, новые методы взлома. В своём докладе я расскажу о генерации больших простых чисел, так как, в последнее время они все чаще используются в алгоритмах шифрования.

Наиболее эффективным средством построения простых чисел является несколько модифицированная малая теорема Ферма.

Теорема 1. Пусть N, S — нечётные натуральные числа, N-1 = S·R, причем для каждого простого делителя q числа S существует целое число a такое, что a^{N-1}=1(mod N), НОД($a^{N-\frac{1}{q}}$-1, N) = 1

РЕПОЗИТОРИЙ БГУКИ

Тогда каждый простой делитель p числа N удовлетворяет сравнению p=1(mod 2S).

Следствие. Если выполнены условия теоремы Ферма и R $\leq$ 4S+2, то N — простое число.

Покажем теперь, как с помощью последнего утверждения, имея большое простое число S, можно построить существенно большее простое число N. Выберем для этого случайным образом чётное число R на промежутке R $\leq$ 4S+2 и положим N=SR+1. Затем проверим число N на отсутствие малых простых делителей, разделив его на малые простые числа, испытаем N некоторое количество раз с помощью алгоритма Рабина.

Теорема 2. Свидетели простоты и теорема Рабина

Пусть m — нечётное число большее 1. Число m - 1 однозначно представляется в виде $m-1=2^s \cdot t$, где t нечётно. Целое число a, 1 < a < m, называется свидетелем простоты числа m, если выполняются два условия:

1. m не делится на a;
2. $a^t \equiv 1(mod\ m)$ или существует целое k, , такое, что $a^{2^k t} \equiv -1(mod\ m)$

Теорема Рабина утверждает, что составное нечётное число m имеет не более $\frac{\varphi(m)}{4}$ различных свидетелей простоты, где $\varphi(m)$ — функция Эйлера.

Алгоритм Миллера — Рабина параметризуется количеством раундов r. Рекомендуется брать r порядка величины $log_2(m)$, где m — проверяемое число.

Для данного m находятся такие целое число s и целое нечётное число t, что $m-1=2^s \cdot t$. Выбирается случайное число a,1 < a < m. Если a не является свидетелем простоты числа m, то выдается ответ «m составное», и алгоритм завершается. Иначе, выбирается новое случайное число a и процедура проверки повторяется. После нахождения r свидетелей простоты, выдается ответ «m, вероятно, простое», и алгоритм завершается.

Если после такой проверки выяснится, что N — составное число, следует выбрать новое значение R и опять повторить вычисления. Так

РЕПОЗИТОРИЙ БГУКИ

следует делать до тех пор, пока не будет найдено число N, выдержавшее испытания алгоритмом Рабина достаточно много раз. В этом случае появляется надежда на то, что N — простое число, и следует попытаться доказать простоту с помощью тестов теоремы 2.

Для этого можно случайным образом выбирать число a, 1 < a < N, и проверять для него выполнимость соотношений a^{N-1} =1(mod N),
НОД(a^R-1, N) =1.

Если при выбранном a эти соотношения выполняются, то, согласно следствию из теоремы Ферма, можно утверждать, что число N простое. Если же эти условия нарушаются, нужно выбрать другое значение a и повторять эти операции до тех пор, пока такое число не будет обнаружено.
Предположим, что построенное число N действительно является простым. Зададимся вопросом, сколь долго придётся перебирать числа a, пока не будет найдено такое, для которого будут выполнены условия обеих теорем. Заметим, что для простого числа N первое условие теоремы Рабина, согласно малой теореме Ферма, будет выполняться всегда. Те же числа a, для которых нарушается второе условие второй теоремы, удовлетворяют сравнению a^R =1(mod N). Как известно, уравнение $x^R = 1$ в поле вычетов F_n имеет не более R решений. Одно из них x=1. Поэтому на промежутке 1 < a < N имеется не более R-1 чисел, для которых не выполняются оба условия второй теоремы. Это означает, что, выбирая случайным образом числа a на промежутке 1 < a < N, при простом N можно с вероятностью большей, чем 1-O(S^{-1}), найти число a, для которого будут выполнены условия теоремы Ферма, и тем доказать, что N действительно является простым числом.

Обсудим теперь некоторые теоретические вопросы, возникающие в связи с нахождением числа R, удовлетворяющего следующим неравенствам S $\leq$ R $\leq$ 4S+2, и такого, что N=SR+1 — простое число. Прежде всего, согласно теореме Дирихле, доказанной ещё в 1839г., прогрессия 2Sn+1, n=1,2,3,... содержит бесконечное количество простых чисел. Соответствующая теорема утверждает, что наименьшее простое число

РЕПОЗИТОРИЙ БГУКИ

в арифметической прогрессии 2Sn+1 не превосходит S^c, где C — некоторая достаточно большая абсолютная постоянная. В предположении справедливости расширенной гипотезы Римана можно доказать, что наименьшее такое простое число не превосходит $c(e)\cdot S^{2+e}$ при любом положительном e.

В качестве итога подчеркну следующее: если принять на веру, что наименьшее простое число, а также расстояние между соседними простыми числами в прогрессии 2Sn+1 при $S \leq n \leq 4S+2$ оцениваются величиной $O(ln^2 S)$, то описанная схема построения больших простых чисел имеет полиномиальную оценку сложности. Кроме того, несмотря на отсутствие теоретических оценок времени работы алгоритмов, отыскивающих простые числа в арифметических прогрессиях со сравнительно большой разностью, на практике эти алгоритмы работают вполне удовлетворительно. На обычном персональном компьютере без особых затрат времени строятся таким способом простые числа порядка 10^{300}. Наконец, отмечу, что существуют методы построения больших простых чисел, использующие не только простые делители $N-1$, но и делители чисел $N+1$, N^2+1, $N^2 \pm N+1$ и т. д. В основе их лежит использование последовательностей целых чисел, удовлетворяющих линейным рекуррентным уравнениям различных порядков. Отметим, что последовательность a^n, члены которой присутствуют в формулировке малой теоремы Ферма, составляет решение рекуррентного уравнения первого порядка $u_{n+1}=au_n$, $u_0 = 1$.

РЕПОЗИТОРИЙ БГУКИ

Список использованных источников:

1. Гашков, С. Б. Упрощенное обоснование вероятностного теста Миллера — Рабина для проверки простоты чисел / С. Б. Гашков – М.: Феникс, 2003. – 124 с.

Нестеренко, Ю. В. Введение в криптографию // Глава 4.4. Как отличить составное число от простого / Ю. В. Нестеренко — СПб: Просвещение, 2001. — 288 с.