УДК 004.021:056.55

СИНГУЛЯРНЫЕ ПРОСТЫЕ ЧИСЛА В ПРОТОКОЛАХ ДИФФИ-ХЕЛЛМАНА

Белецкий А.Я.

Национальный авиационный университет, Киев, Украина

Введен класс сингулярных простых чисел, на основе которых предлагается алгоритм существенного сокращения затрат машинного времени, необходимого для выбора значения образующих примитивных элементов в протоколах Диффи-Хеллмана.

КЛЮЧЕВЫЕ СЛОВА: сингулярные простые числа, машинное время, примитивные элементы, протокол Диффи-Хеллмана.

СИНГУЛЯРНІ ПРОСТІ ЧИСЛА У ПРОТОКОЛАХ ДІФФІ-ХЕЛЛМАНА

Белецький А.Я.

Введено клас сингулярних простих чисел, на основі яких пропонується алгоритм істотного скорочення витрат машинного часу, яке необхідне для вибору значення утворюючих примітивних елементів в протоколах Діффі-Хеллмана.

КЛЮЧОВІ СЛОВА: сингулярні прості числа, машинний час, примітивні елементи, протокол Діффі-Хеллмана.

SINGULAR PRIME NUMBER IN THE DIFFIE-HELLMAN PROTOCOL

Beletsky A.Ya.

A class of singular primes, based on which an algorithm which significantly reduces the cost of computer time required for selection the values of primitive elements in the Diffie-Hellman protocol is introduced.

KEY WORDS: singular primes, machine time, primitive elements, the Diffie-Hellman protocol.

1. Введение и постановка задачи. Опубликование Уитфилдом Диффи и Мартином Хеллманом в 1976 году статьи [1] знаменовало собою начало эры несимметричной (двухключевой) криптографии. Предложенный авторами протокол обмена данными в каналах связи (сетях), получивший название *протокол Диффи-Хеллмана* (сокращенно DH-протокол), обеспечивает формирование секретного ключа K, общего для двух легализованных абонентов сети (Алисы и Боба) и предназначенного для использования в алгоритмах симметричного шифрования. Генерация секретного ключа K осуществляется в открытых каналах связи, незащищенных от прослушивания противником (Евой), но защищённых от подмены передаваемой информации.

Суть DH-протокола состоит в следующем. Абонентам сети Алисе и Бобу предполагаются известными открытые ключи протокола, в качестве которых используются большое простое число p и примитивный элемент q поля $GF(p)$. Примитивный элемент q, как и p, рекомендуется выбирать также достаточно большим. Алиса генерирует случайный секретный показатель x, вычисляет число $A = q^x \pmod p$ и посылает его Бобу. Аналогичным образом Боб генерирует случайный секретный показатель y, вычисляет число $B = q^y \pmod p$ и посылает его Алисе. После этого абоненты сети возводят полученные от партнера числа в свои секретные степени и приводят их к остатку по модулю p. В результате выполнения описанных операций у Алисы и Боба образуется одинаковый секретный ключ K, в силу того что

$$B^x \pmod p = q^{yx} \pmod p = A^y \pmod p = q^{xy} \pmod p, \quad (1)$$

так как $yx \equiv xy$.

Противник Ева, перехватив сообщения A и B, которыми обмениваются легализованные абоненты сети, не в состоянии вычислить ключ K, поскольку сталкивается с практически неразрешимой в настоящее время проблемой дискретного логарифмирования, если только открытые ключи p и q выбраны достаточно большими. Рекомендованными значениями p и q являются двоичные числа, разрядность которых составляет $1, 2$ и даже 4 Кбит. Столь большие

размеры простых чисел p являются причиной значительных сложностей, которые возникают при вычислении примитивных элементов q DH-протокола.

В данной работе ставится задача разработки достаточно эффективного алгоритма сокращения затрат машинного времени, связанного с выбором образующих элементов q для протоколов Диффи-Хеллмана. Алгоритм основан на применении так называемых *сингулярных простых чисел* (СПЧ).

2. Статистика порядков элементов поля GF(p)**.** Множество Ω ненулевых элементов поля GF(p) мощности $p-1$ состоит из подмножества Q примитивных элементов q и подмножества $\overline{Q}$ элементов $\overline{q}$, не принадлежащих Q. *Примитивными* являются такие элементы (числа) q поля GF(p), последовательность степеней которых по mod p формирует последовательность максимальной длины (m - последовательность), покрывая все подмножество ненулевых элементов поля [2]. Важнейшей характеристикой элементов ω множества Ω служит их порядок. *Порядком,* обозначаемым $\operatorname{ord}\omega$, элемента $\omega \in \Omega$ поля GF(p) является такое минимальное натуральное значение показателя e, при котором $\omega^{e} \pmod p = 1$. Последовательность степеней элемента ω, начиная с нулевой степени, для которой $\omega^{0} = 1$, образует *циклическую группу*, обозначаемую $\langle\omega\rangle$, порядка e. Примитивные элементы q поля GF(p) порождают мультипликативные группы $\langle q\rangle$ максимального порядка (МГМП). Это означает, в частности, что $\forall q \in Q \Rightarrow \operatorname{ord} q = p-1$.

Как следует из соотношения (1), на показатели x и y протокола Диффи-Хеллмана должно быть наложено ограничение, состоящее в том, что они не должны превышать значения $\operatorname{ord} q - 1$, равное $p-2$. Опираясь на числовые примеры, поясним причины, обуславливающие необходимость указанного ограничения. Итак, пусть $p = 19$ и, следовательно, $\operatorname{ord} q = 18$. Поле GF(19) включает 18 ненулевых элементов, из которых шесть являются примитивными. Таковыми являются числа 2, 3, 10, 13, 14 и 15, вычисленные с помощью программы, интерфейс которой показан на рис. 1.

На средних клавишах интерфейса приведены значения порядков ненулевых элементов поля GF(19), над ними – число элементов данного порядка, а в нижних окнах – список этих элементов. Мультипликативная группа, для примера, рассчитана относительно образующего элемента $\omega = 8$, который вставлен в окно над клавишей «Группа» интерфейса. Порядок этого элемента, как видно из данных, выписанных в окне «Группа», равен шести.

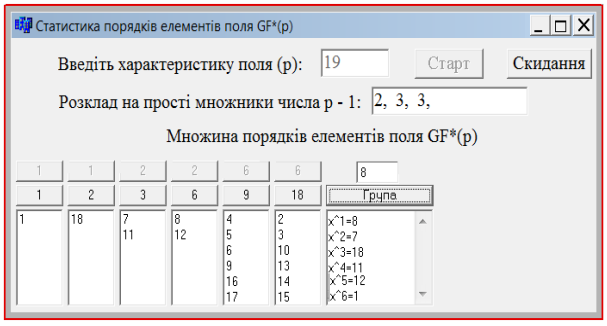

Рис. 1. К вычислению порядков элементов поля $GF^{*}(p)$.

Выберем в качестве образующего элемента (ОЭ) DH-протокола любой примитивный элемент q поля GF(19). А теперь предположим, что значение одного из показателей, например, x совпадает с порядком примитивных элементов, т.е. $x = 18$ (либо кратен 18). Это приводит к тому, что вне зависимости от величины q получим $q^{x} \pmod p =$ $= q^{18} \pmod p = q^{\operatorname{ord} q} \pmod p = 1$. В таком случае Ева, перехватив сообщение $A = 1$, придет к однозначному выводу о том, что показатель $x = 18$. Следствием данного заключения является то, что Еве становится известным секретный ключ K протокола Диффи-Хеллмана, поскольку $K = B^{x} \pmod p = B^{18} \pmod p = B$. Если же $x > \operatorname{ord} q$, то представив x соотношением $x = m \cdot \operatorname{ord} q + \tilde{x}$, где m – натуральное число, а $\tilde{x}$ – остаток числа x по модулю p, меньший чем $\operatorname{ord} q$, получим $q^{x} = q^{\tilde{x}}$ поскольку $q^{m \cdot \operatorname{ord} q} \equiv 1 \pmod p$. Следовательно, выбирать значение x, превышающее $\operatorname{ord} q - 1$, не имеет смысла. Это, во-первых, и, во-вторых, также теряет смысл в качестве образующего элемента DH-протокола выбирать элемент, не являющийся примитивным элементом поля GF(p)**.** В самом деле, предположим, что образующим выбран элемент $\theta = 8$, не принадлежащий подмножеству Q, а показатель $x = 17$. Порядок элемента $\theta = 8$ в поле GF(19) равен шести, т.е. $\operatorname{ord}\theta = 6$. Следовательно, показатель x можно представить в виде $x = 2 \cdot \operatorname{ord}\theta + 5$, что приводит к соотношению $\theta^{x} \pmod p = \theta^{17} \pmod p = \theta^{5} \pmod p$, поскольку $\theta^{2 \cdot \operatorname{ord}\theta} \equiv 1 \pmod p$. Тем самым мы подтвердили целесообразность ограничений, которые должны накладываться на образующие элементы q DH-протокола.

3. Сингулярные простые числа. Как отмечено в первом разделе статьи, рекомендуемые размеры простых чисел p в DH-протоколах достигают больших величин, составляя несколько Кбит. В связи с этим могут возникнуть определенные затруднения, связанные с выбором примитивных

образующих элементов q. Покажем суть данной проблемы на примере простого числа $p = 64081$.

Как следует из результатов компьютерных вычислений с помощью упоминавшийся выше программы «Статистика», относительная частота (*частость*) примитивных элементов анализируемого поля $GF(p)$, в котором $p = 64081$, составляет порядка 0,26. Для больших значений p частость примитивных элементов может достигать существенно меньших величин, что и является причиной проблем, возникающих при поиске образующих элементов в DH-протоколе. Ниже будет предложен способ выбора характеристик p поля $GF(p)$, гарантирующий достижение частости примитивных элементов на уровне 0,5. Этот способ основан на использовании так называемых сингулярных (особенных) простых чисел.

Сингулярными будем называть такие простые числа p, для которых нетривиальными делителями числа $p-1$ являются лишь числа 2 и $(p-1)/2$. Согласно определению, делитель $(p-1)/2$ также должен быть простым числом (обозначим его p^*) т.е. должно выполняться условие $p = 2p^* + 1$, причем как p, так и p^* – простые числа.

Обратим внимание на следующий момент. Простое число $p = 5$ не входит в состав СПЧ, несмотря на то, что $(p-1)/2$ является простым числом, равным 2. Такое решение имеет простое обоснование. В самом деле, для любого СПЧ число $p-1$ должно иметь четыре делителя, два из которых равны 2 и $(p-1)/2$, а оставшиеся два – тривиальные делители 1 и $p-1$. В то же время простому числу $p = 5$ отвечают только три делителя числа $p-1$; а именно, делители 1, 2 и 4, поскольку делитель 2 совпал с делителем $(p-1)/2$, что нарушило полноту приведенного выше определения СПЧ. На этом основании число 5, как и 3, не является сингулярным.

Простое поле $GF(p)$ включает $p-1$ ненулевых элементов от 1 до $p-1$. Порядок элемента 1 равен 1, т.е. $\operatorname{ord} 1 = 1$, тогда как $\operatorname{ord}(p-1) = 2$. В самом деле, пусть элемент a поля $GF(p)$ равен $p-1$. Имеем $a^0 = 1$, $a^1 = p-1$ и, наконец,

$$a^2 = ((p-1)\cdot(p-1))(\bmod p) = (p^2 - 2p + 1)(\bmod p) = 1,$$

Следовательно, порядок элемента $a = p-1$ равен двум.

Мультипликативную группу максимального порядка, порождаемую тем или иным примитивным элементом q поля $GF(p)$, для небольших значений p удобно отображать в виде направленного графа. На рис. 2 представлен такой граф для характеристики поля $p = 11$. Внутри кружочков размещены элементы группы, по внешнему контуру расположены порядки соответствующих элементов графа, а внутри – степени примитивного образующего элемента МГМП $q = 2$.

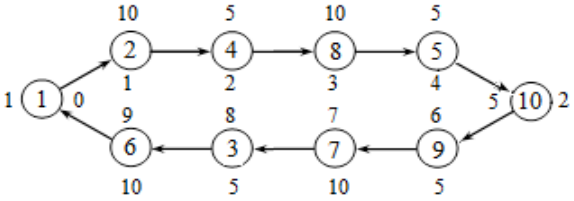

Рис. 2. Граф МГМП поля $GF(11)$ над ОЭ $q = 2$

Принципиальными на графе (рис.2) являются следующие два момента. Во-первых, левая вершина графа по определению всегда равна 1 и, во-вторых, правая вершина графа равна $p-1$.

Пусть p – СПЧ. Тогда для любого элемента $a \in [2, p-2]$, введя обозначение $\hat{a} = a^{(p-1)/2} \pmod p$, имеем

$$\operatorname{ord} a = \begin{cases} (p-1)/2, & \text{если } \hat{a} = 1, \\ p-1, & \text{если } \hat{a} = p-1. \end{cases} \qquad (2)$$

Соотношения (2) легко могут быть доказаны, если воспользоваться графом группы, приведенным на рис. 2.

Выберем в качестве сингулярного числа ближайшее (снизу) к простому числу $p = 64081$. Таковым является СПЧ $p = 64019$. Множество элементов поля $GF^*(64019)$ включает четыре группы подмножеств, порядок которых равен 1, 2, 32009 и 64018 соответственно. Особенность элементов простого поля Галуа, характеристика которого p есть СПЧ, состоит в том, что произвольный элемент порядка $(p-1)/2$ порождает группу того же самого порядка. При этом число элементов порядка $(p-1)/2$, как и число элементов порядка $p-1$, равно $(p-3)/2$.

Опираясь на приведенные свойства поля $GF(p)$ над СПЧ p и систему равенств (2), можно предложить достаточно простой алгоритм формирования подмножеств элементов поля, порядки которых определяются значениями $(p-1)/2$ и $p-1$ соответственно.

Суть алгоритма состоит в следующем. Пусть выбрано некоторое сингулярное простое число p. Последовательно перебирая числа $a = 2, 3, \ldots$, найдем такое его минимальное значение $a = \theta$, для которого выполняется условие $\theta^{(p-1)/2} \pmod p = 1$. Выполнение этого условия, согласно соотношениям (2), будет означать, что θ является минимальным образующим элементом группы порядка $(p-1)/2$. Порядок всех элементов данной группы, кроме тривиального элемента 1, также равен $(p-1)/2$. Исключая из множества чисел

$\{\overline{1, p-2}\}$ элементы группы, порождаемой образующим элементом θ, получим подмножество Q примитивных элементов q поля GF(p). Тем самым задача, связанная с выбором ОЭ q для протоколов Диффи-Хеллмана, становится легко разрешимой.

4. Синтез сингулярных простых чисел. Ниже предлагается алгоритм выбора сингулярных простых чисел p, которые, как отмечено во введении, должны быть большими числами, чтобы исключить возможность взлома противником DH-протокола.

Формирование приемлемых значений p осуществляется в следующей последовательности. На первом этапе следует выбрать нечетное число ρ^* и функционально связанное с ним число $\rho = 2\rho^* + 1$, также являющееся нечетным. После этого можно переходить к проверке простоты этой пары чисел. Известно большое число тестов простоты. Наиболее простым из них является *тест Ферма*, основанный на малой теореме Ферма [3], согласно которому число ρ является простым, если оно удовлетворяет сравнению

$$a^{\rho-1} \equiv 1 \pmod{\rho}, \quad a \in \overline{2, \rho-1}. \qquad (3)$$

Соотношение (3) является необходимым, но далеко не достаточным признаком простоты числа ρ. Дело в том, что существуют такие целые ρ, называемые *псевдопростыми числами* [3], которые обладают некоторыми свойствами простых чисел, являясь, тем не менее, составными числами. Псевдопростыми, например, являются *числа Кармайкла* [3] по основанию $a = 2$, образующие последовательность 341, 561, 645, 1105, 1387, 1729, …, по основанию $a = 3$ – числа 91, 121, 286, 671, 703, 849 и т.д.

Если сравнение (3), которое проводится, как правило, по основанию $a = 2$, не подтверждается хотя бы для одного числа из пары ρ^* и ρ, то подбирают очередную пару нечетных чисел. После того, как найдена пара ρ^* и ρ, удовлетворяющая сравнению (3), переходят к дополнительному тестированию простоты этих чисел. Гарантированно надежным тестом является *перебор делителей*, который сводится к полному перебору всех возможных потенциальных делителей. Обычно перебор делителей заключается в переборе всех простых чисел от 2 до корня квадратного из тестируемого числа. Если окажется, что ρ^* или ρ будет кратно переборному делителю, то тестируемая пара бракуется, и процесс подбора СПЧ продолжается над новой парой нечетных чисел.

Следует отметить, что в практических задачах данный алгоритм (перебор делителей) тестирования простоты применяется не так уж и часто ввиду его большой асимптотической сложности, но его применение оправдано в случае, если проверяемые числа относительно невелики, так как данный алгоритм довольно легко реализуем.

5. Выводы. Сингулярные простые числа p характеризуются тем свойством, что мультипликативные группы $GF^*(p)$, порождаемые СПЧ p, обладают минимальным набором нетривиальных делителей. Такими делителями являются числа 2 и $p^* = (p-1)/2$. Если исключить из совокупности элементов группы $GF^*(p)$ их крайние значения 1 и $p-1$, то оставшееся элементы образуют два равномощных подмножества Q и $\overline{Q}$. Подмножество Q включает полный набор примитивных элементов q поля GF(p). Подмножество $\overline{Q}$ состоит из элементов, порядок которых равен $(p-1)/2$, причем любой элемент этого подмножества порождает мультипликативную группу, которая кроме единицы содержит все элементы подмножества $\overline{Q}$. Исключая из множества элементов поля $GF^*(p)$ элементы подмножества $\overline{Q}$, получаем подмножество Q примитивных элементов q поля GF(p).

Отмеченные свойства сингулярных простых чисел p дают возможность существенно сократить затраты машинного времени, связанные с подбором примитивных элементов q в DH-протоколах. В самом деле, пусть выбрано некоторое число a такое, что $1 < a < p-1$, где p – СПЧ. Относительно a необходимо вынести решение, является ли оно примитивным элементом поля $GF^*(p)$. С этой целью следует вычислить значение $\hat{a} = a^{p^*} \pmod{p}$. Если окажется, что $\hat{a} = 1$, то это будет означать, что элемент a не является примитивным. В таком случае переходят к тестированию очередного элемента $a := a+1$. Примитивным будет являться такой элемент a, для которого $\hat{a} = p-1$. Поскольку для сингулярных простых чисел p частость примитивных элементом поля $GF^*(p)$ практически равна 0.5, то процесс поиска таких элементов завершается за минимальное число итераций.

ЛИТЕРАТУРА

1. Diffe W., Hellman V.E. New Directions in Cryptography. *IEEE Transactions on Information Theory*. – 1976. – v. IT-22, N6. – P. 644–654.
2. Лидл Р., Нидеррайтер Г. *Конечные поля.* М.: Мир. – 1988. – 432 с.
3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО. – 2003. – 328с.