УДК 004.021:056.55

ПРОТОКОЛЫ ДИФФИ-ХЕЛЛМАНА НА ОСНОВЕ СИНГУЛЯРНЫХ ПРОСТЫХ ЧИСЕЛ

А. Я. Белецкий, *д-р техн. наук, профессор,*
Национальный авиационный университет,
просп. Космонавта Комарова, 1, г. Киев-058, 03680, Украина,
E-mail: abelnau@ukr.net

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

Ключевые слова: *протоколы Диффи-Хеллмана, сингулярные простые числа.*

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 Галуа $GF(p)$. Как и p, примитивный элемент q рекомендуется выбирать также достаточно большим (в окрестности значений $\simeq p/2$). Алиса генерирует случайный секретный показатель x, вычисляет число $A = q^x (\mathrm{mod}\ p)$ и посылает его Бобу. Аналогичным образом Боб генерирует случайный секретный показатель y, вычисляет число $B = q^y (\mathrm{mod}\ p)$ 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

$$B^x = q^{yx} (\mathrm{mod}\ p) = A^y = q^{xy} (\mathrm{mod}\ p), \qquad (1)$$

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 разрядностью 1, 2 и даже 4 Кбит. Столь большие размеры простых чисел p являются причиной значительных сложностей, которые возникают при синтезе 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 нового предлагаемого класса так называемых *сингулярных простых чисел* (СПЧ).

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 $\bmod p$ формирует последовательность максимальной длины (m-последовательность), покрывая все подмножество ненулевых элементов поля [2]. Важнейшей характеристикой элементов ω множества Ω служит их порядок. *Порядком,* обозначаемым $ord\ \omega$, элемента $\omega \in \Omega$ поля $GF(p)$ является такое минимальное значение показателя e, при котором $\omega^e \left(\bmod p\right) = 1$. Последовательность степеней элемента ω, начиная с нулевой степени, для которой $\omega^0 = 1$, образует *циклическую группу*, обозначаемую $\langle\omega\rangle$, порядка e. Совершенно очевидно, что примитивные элементы q поля $GF(p)$ порождают мультипликативные группы $\langle q\rangle$ максимального порядка (МГМП). Это означает, в частности, что $\forall q \in Q \Rightarrow ord\ q = p-1$.

Как следует из соотношения (1), на образующие элементы q и показатели x и y протокола Диффи-Хеллмана должны быть наложены, по крайней мере, такие ограничения. Во-первых, элемент q, как уже было отмечено выше, следует выбирать из подмножества Q примитивных элементов поля $GF(p)$. И, во-вторых, показатели x и y не должны превышать максимальное значение $ord\ q - 1$, равное $p-2$.

Кратко, опираясь на числовые примеры, поясним причины, обуславливающие необходимость приведенных ограничений. Итак, пусть p=19 и, следовательно, $ord\ q$ =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 (мультипликативной группы) 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. Поле $GF^*(p)$, т. е. поле $GF(p)$, за исключением его нулевого элемента, называют также *мультипликативной группой максимального порядка* (МГМП), или просто мультипликативной группой поля $GF(p)$.

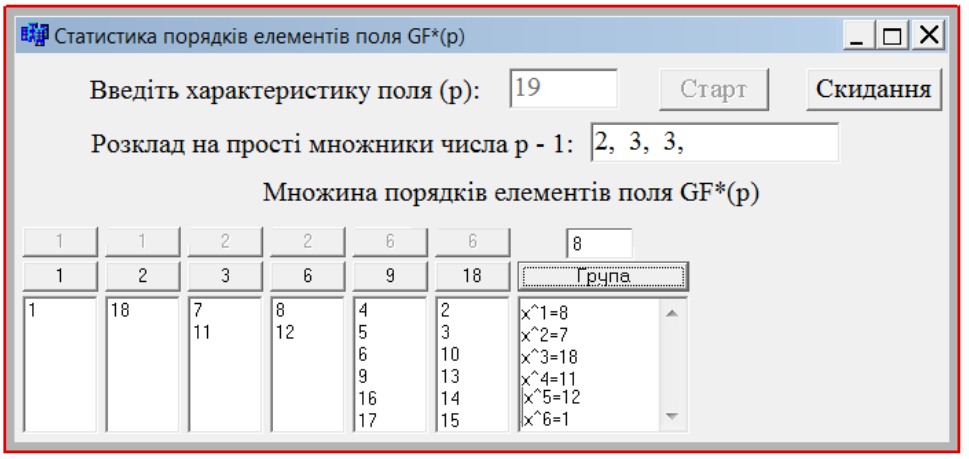

Рисунок 1 - Интерфейс программы «Статистика порядков элементов поля $GF(19)$ *»*

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 $q^x = q^{18} = q^{ord\ q} = 1$. 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 $K = B^x = B^{18} = B$. Если же $x > ord\, q$, то представив x соотношением $x = m \cdot ord\, q + \tilde{x}$, где m - натуральное число, а $\tilde{x}$ – остаток числа x по модулю p, меньший чем $ord\ q$, получим, что $q^x = q^{\tilde{x}}$, поскольку $q^{m \cdot ord\, q} \equiv 1$. Следовательно, выбирать значение x, превышающее $ord\, q - 1$, 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 θ = 8 в поле $GF(19)$ равен шести, т. е. $ord\, q = 6$. Следовательно, показатель x можно представить в виде $x = 2 \cdot ord\, \theta = 5$, что приводит к соотношению $\theta^x = \theta^{17} = \theta^5$, поскольку $\theta^{2 \cdot ord\, \theta} \equiv 1 (\mathrm{mod}\ p)$. Тем самым мы подтвердили целесообразность ограничений, которые должны накладываться на образующие элементы q протокола Диффи-Хеллмана.

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. Вычисленные с помощью приводившейся выше программы «Статистика» множество порядков ненулевых элементов поля $GF^*(p)$ и соответствующие им (порядкам) частоты сведены в табл. 1.

Таблица 1 - Статистические характеристики элементов поля $GF^*(64081)$

№	Порядок / Частота	№	Порядок / Частота	№	Порядок / Частота	№	Порядок / Частота	№	Порядок / Частота	№	Порядок / Частота
1	1 / 1	11	15 / 8	21	60 / 16	31	267 / 176	41	1335 / 704	51	5340 / 1408
2	2 / 1	12	16 / 8	22	72 / 24	32	356 / 176	42	1424 / 704	52	6408 / 2112
3	3 / 2	13	18 / 6	23	80 / 32	33	360 / 96	43	1602 / 528	53	7120 / 2816
4	4 / 2	14	20 / 8	24	89 / 88	34	445 / 352	44	1780 / 704	54	8010 / 2112
5	5 / 4	15	24 / 8	25	90 / 24	35	534 / 176	45	2136 / 704	55	10680 / 2816
6	6 / 2	16	30 / 8	26	120 / 32	36	712 / 352	46	2670 / 704	56	12816 / 4224
7	8 / 4	17	36 / 12	27	144 / 48	37	720 / 192	47	3204 / 1056	57	16020 / 4224
8	9 / 6	18	40 / 16	28	178 / 88	38	801 / 528	48	3560 / 1408	58	21360 / 5630
9	10 / 4	19	45 / 24	29	180 / 48	39	890 / 352	49	4005 / 2112	59	32040 / 8448
10	12 / 4	20	48 / 16	30	240 / 64	40	1068 / 352	50	4272 / 4272	60	64080 / 16896

Как следует из табл. 1 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^* должны быть простыми числами.

В табл. 2 приведены значения первых 120 сингулярных простых чисел. Порядковый номер k СПЧ в таблице определяется соотношением $k = 10 \cdot (i-1) + j$.

Таблица 2 – Сингулярные простые числа

$i \setminus j$	1	2	3	4	5	6	7	8	9	10
1	7	11	23	47	59	83	107	167	179	227
2	263	347	358	383	467	479	503	563	587	719
3	839	863	887	983	1039	1187	1283	1307	1319	1367
4	1439	1487	1523	1619	1823	1907	2027	2039	2063	2099
6	2207	2447	2459	2579	2819	2879	2903	2963	2999	3023
7	3119	3167	3203	3467	3623	3779	3803	3863	3947	4007
8	4079	4127	4139	4259	4283	4547	4679	4703	4787	4799
9	4919	5087	5099	5387	5399	5483	5507	5639	5807	5879
10	5927	5939	6047	6599	6659	6719	6779	6827	6899	6983
11	7079	7187	7247	7523	7559	7607	7643	7703	7727	7823
12	8039	8147	8423	8543	8699	8747	8783	8819	8963	9467

Обратим внимание на следующий момент. Простое число $p = 5$ не включено в таблицу 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 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 включено в состав СПЧ.

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

$$a^2 = (p-1)\cdot(p-1) = (p^2 - 2p + 1) \pmod{p} = 1.$$

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 $q = 2$.

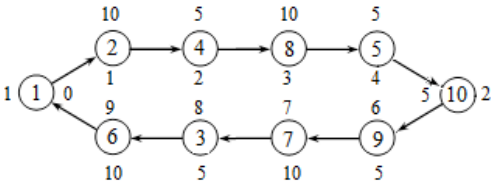

Рисунок 2 - Граф МГМП поля GF(11) над ОЭ $q = 2$

Принципиальными здесь (на графе) являются такие два момента. Во-первых, левая вершина графа по определению всегда равна 1, а правая – значению $p-1$.

Пусть p – сингулярное простое число. Тогда для любого элемента $a \in [2,\ p-2]$, обозначив $\hat{a} = a^{(p-1)/2} \pmod p$, имеем: если a – не примитивный элемент, то $\hat{a} = 1$, но если a – примитивный элемент, то $\hat{a} = p-1$, т.е.

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

Результаты работы программы «Статистика» для СПЧ $p = 64019$, ближайшего к характеристике поля 64081, показаны на рис. 3.

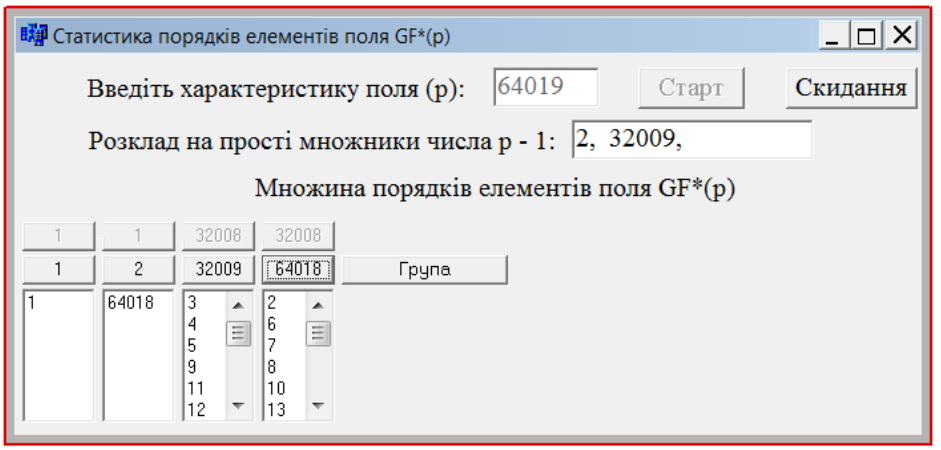

Рисунок 3 - Множество порядков элементов поля $GF^*(p)$ *над СПЧ* $p = 64019$

Как следует из данного рисунка, 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 СПЧ p. Последовательно перебирая числа $a = 2, 3, \ldots$ найдем такое его минимальное значение $a = \theta$, для которого выполняется условие $\theta^{(p-1)/2} \pmod{p} = 1$. Это, 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 $\overline{\{2, p-2\}}$ элементы группы, порождаемой образующим элементом θ, получим подмножество Q примитивных элементов q поля $GF(p)$. Тем самым задача, связанная с выбором образующего элемента (ОЭ) q для протоколов Диффи-Хеллмана, становится достаточно легко разрешимой.

СИНТЕЗ СИНГУЛЯРНЫХ ПРОСТЫХ ЧИСЕЛ

Ниже предлагаются рекомендации относительно выбора сингулярных простых чисел p, которые, как отмечено во введении, должны быть большими числами, чтобы исключить возможность взлома противником протокола Диффи-Хеллмана. Формирование приемлемых значений p осуществляется в следующей последовательности. На первом этапе следует выбрать нечетное число p^* и функционально связанное с ним число $p = 2p^* + 1$, 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 p является простым, если оно удовлетворяет сравнению

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

Соотношение (3) является необходимым, но далеко не достаточным признаком простоты числа p. Дело в том, что существуют такие целые p, 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 – 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 p^* и p, то подбирают очередную пару нечетных чисел. После того, как найдена пара p^* и p, 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 p^* или p 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.

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 $\overline{Q}$ и 1, получаем подмножество Q примитивных элементов q поля $GF(p)$. Отмеченные свойства сингулярных простых чисел дают возможность существенно сократить затраты машинного времени, связанные с подбором примитивных элементов q в протоколах Диффи-Хеллмана.

DIFFIE-HELLMAN KEY EXCHANGE PROTOCOLS BASED ON SINGULAR PRIME NUMBERS

A. J. Bielecki,
National Aviation University,
Ave. Komarova, 1, Kiev-058, 03680, Ukraine
E-mail: *abelnau@ukr.net*

A class of singular primes, based on an algorithm which significantly reduce computing time needed to select the appropriate values in the form of primitive elements of the Diffie-Hellman key exchange.

Key words: *Diffie-Hellman key exchange, singular primes.*

ПРОТОКОЛИ ДІФФІ-ХЕЛЛМАНА НА ОСНОВІ СИНГУЛЯРНИХ ПРОСТИХ ЧИСЕЛ

А. Я. Білецький,
Національний авіаційний університет,
Просп. Космонавта Комарова, 1, м. Київ-058, 03680, Україна,
E-mail: *abelnau@ukr.net*

Введено клас сингулярних простих чисел, на основі яких запропоновано алгоритм істотного скорочення витрат машинного часу, необхідного для вибору прийнятних значень утворюючих примітивних елементів у протоколах Діффі-Хеллмана.

Ключові слова: *протоколи Діффі-Хеллмана, сингулярні прості числа.*

СПИСОК ЛИТЕРАТУРЫ

1. Diffe W. New Directions in Cryptography / W. Diffe, V. E. Hellman // IEEE Transact. On Information Theory. - 1976, Nov.. - V. IT-22, No. 6. - P. 644-654.
2. Лидл Р. Конечные поля / Р. Лидл, Г. Нидеррайтер. – М. : Мир, 1988. – Т. 1. – 432 с.
3. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М.: МЦНМО, 2003. – 328 с.

Поступила в редакцию 18 декабря 2013 г.