УДК 004.056.55

А.В. Соколов, магистр,
В.Д. Буряк, магистр,
Одес. нац. политехн. ун-т

АЛГОРИТМ ИСЧИСЛЕНИЯ ПОРЯДКА ДЛЯ РАСЧЕТА ДИСКРЕТНЫХ ЛОГАРИФМОВ НА ОСНОВЕ ТАБЛИЦ ИНДЕКСОВ

Введение. Задача дискретного логарифмирования является основной из задач, на которых базируется криптография с открытым ключом [1]. На основе данного подхода базируется безопасность таких современных криптографические алгоритмов как Диффи-Хеллмана, Эль-Гамаля, Мэсси-Омуры и др. В основе криптостойкости упомянутых систем лежит вычислительная сложность обращения показательной функции: последняя вычисляется сравнительно быстро, в то время как задача вычисления дискретных логарифмов даже при применении самых современных алгоритмов имеет сложность, сравнимую со сложностью разложения чисел на множители [2].

Одна из возможностей существенного упрощения задачи дискретного логарифмирования связана с применением квантовых вычислений, тем не менее их эффективность доказана только теоретически. Практическая реализация квантовых алгоритмов будет означать непригодность практического применения всех криптосистем, основанных на вычислительной сложности задачи дискретного логарифмирования [3].

Все эти факторы послужили причиной для поиска нового метода решения сравнений, содержащих дискретные логарифмы, — более быстрого и практичного.

Пусть в некоторой конечной мультипликативной абелевой группе [4] задано сравнение вида

$$y \equiv a^x (\mathrm{mod}\, p), \qquad (1)$$

где y, a — элементы поля Галуа $GF(p)$;

$x \in GF(p-1)$.

Задача состоит в нахождении такого x, который удовлетворяет (1), и может быть представлен в виде дискретного логарифма

$$x = \log_a y (\mathrm{mod}\, p-1),$$

при этом число x называют дискретным логарифмом или индексом числа y по основанию a.

Анализ последних исследований и публикаций. Известно множество алгоритмов для решения данной задачи. Среди них: алгоритмы Шенкса, и Полига-Хеллмана, *p*-метод Полларда, алгоритм COS, алгоритм Адлемана, решето числового поля [5].

Если задача рассматривается в расширенном конечном поле $GF(q)$, где $q = p^n$, p — простое, то для нахождения дискретного логарифма применяются алгоритмы Эль-Гамаля и исчисления порядка. Но данные алгоритмы довольно трудоемкие и сложные с вычислительной точки зрения (сложность каждого из указанных алгоритмов — $O(\exp c(\log p \log\log p)^{2^{-1}})$ арифметических операций) [6].

Ввиду высокой практической ценности операции дискретного логарифмирования для каждого используемого на практике простого модуля p составлены так называемые таблицы индексов. Таблица индексов состоит из двух: первая — для нахождения индекса по числу (ин-

DOI: 10.15276/opu.1.43.2014.30

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

дексный код), вторая — для нахождения числа по индексу. Таблицы содержат наименьшие отсчеты чисел (приведенная система) и их наименьших индексов (полная система) соответственно по модулям p и $c = \varphi(p) = p - 1$ [6]. Например, для простого модуля $p = 41$ может быть построена таблица индексов (табл. 1) в соответствии с первообразным элементом $\theta = 6$.

Таблица 1

Таблицы индексов для простого числа 41

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Целью работы является усовершенствование алгоритма исчисления порядка, основанного на применении таблиц индексов.

Изложение основного материала. Таблицы индексов находят применение в следующих задачах науки и техники:

— Построение индексных кодов. Проведенные исследования показали, что синтез кодирующих последовательностей, обладающих хорошими корреляционными свойствами, для задач формирования дискретных частотных сигналов [7] может быть проведен с использованием индексных кодов. Исходя из известных таблиц индексов для простых чисел, две последовательности (прямая и обратная) могут быть использованы в качестве времякодирующей последовательности (ВКП) или частотно-кодирующей последовательности (ЧКП). Причем полное множество кодирующих слов может быть получено за счет всех циклических сдвигов по времени и по частоте [7, 8];

— Решение уравнений вида (1) при условии, что α является минимальным первообразным корнем простого числа p. Например, пусть задано сравнение

$$10 = 6^x \pmod{41}.$$

Используя табл. 1, находим, что $x = 8$. Выполняя проверку, нетрудно установить, что это соответствует действительности.

— Алгоритм шифрования Эль-Гамаля, процедуру шифрования в соответствии с которым можно представить в виде нескольких шагов.

Пусть необходимо зашифровать открытый текст, который представляет собой сообщение $M = 5$.

Произведем генерацию ключей. Пусть $p = 11$, $g = 2$.

Выберем $x = 8$ — случайное целое число x, такое, что $1 < x < p$. Вычислим $y = g^x \bmod p = 2^8 \bmod 11 = 3$. Открытой является тройка $(p, g, y) = (11, 2, 3)$, а закрытым ключом является число $x = 8$.

Выбираем случайное целое число k такое, что $1 < k < (p - 1)$. Пусть, например, $k = 9$.

Вычисляем число $a = g^k \bmod p = 2^9 \bmod 11 = 6$.

Вычисляем число $b = y^k M \bmod p = 3^9 \cdot 5 \bmod 11 = 9$.

Полученная пара $(a, b) = (6, 9)$ является шифртекстом.

Расшифровка. Необходимо получить сообщение $M = 5$ по известному шифртексту $(a, b) = (6, 9)$ и закрытому ключу $x = 8$.

Вычисляем M по формуле

$$M = b(a^x)^{-1} \bmod p = 9(6^8)^{-1} \bmod 11 = 5.$$

Получаем исходное сообщение $M = 5$.

В данном алгоритме все вычисления основаны на операции возведения в степень, реализация которой может быть значительно ускорена путем применения таблиц индексов.

— Алгоритм исчисления порядка. Основная идея данного алгоритма заключается в использовании *p*-гладких чисел. В соответствии с основной теоремой арифметики любое число может быть представлено в виде произведения простых чисел $n=\prod_{i=1}^{k} p_i^{\alpha_i}$, где $p_1 < p_2 < ... < p_k$, p_i — простые числа, α_i — натуральные числа. Число n называют p_t-гладким, если в его разложении $n=\prod_{i=1}^{t} p_i^{C_i}$, p_t — наибольший сомножитель. Кратко рассмотрим сущность алгоритма исчисления порядка, представив его в виде конкретных шагов, проиллюстрированных примером решения сравнения вида

$$17 \equiv 10^x \pmod{47}.$$

Шаг 1. Выбираем набор базовых множителей (факторная база)

$$S = \{p_1, p_2, p_3 ... p_t\},$$

для нашего примера выберем факторную база $S = [p_1, p_2, p_3] = [2,3,5]$, т.е. 5-гладкие числа.

Шаг 2. Находим множество из $(t+\varepsilon)$ p_t-гладких чисел, по правилу

$$a^k \pmod{p} = \prod_{i=1}^{t} p_i^{C_i}, \text{ для } k = 1,2,3..., \tag{2}$$

что соответствует множеству из $t+\varepsilon = 3+1 = 4$ 5-гладких чисел

$$10^1 \bmod 47 = 10 = 2 \cdot 5;$$

$$10^2 \bmod 47 \equiv 6 = 2 \cdot 3;$$

$$10^3 \bmod 47 \equiv 13;$$

$$10^4 \bmod 47 \equiv 36 = 2 \cdot 2 \cdot 3 \cdot 3;$$

$$10^5 \bmod 47 \equiv 31;$$

$$10^6 \bmod 47 \equiv 28 = 2 \cdot 2 \cdot 7;$$

$$10^7 \bmod 47 \equiv 45 = 3 \cdot 3 \cdot 5,$$

Шаг 3. Логарифмируем (2):

$$k = \sum_{i=1}^{t} C_i \log_a p_i, \; k = 1,2,3....$$

Тогда

$$U_i = \log_a p_i;$$

$$U_1 = \log_a p_1, U_2 = \log_a p_2, ..., U_t = \log_a p_t.$$

Составляем систему уравнений для неизвестных U_i. Решая такие уравнения методами линейной алгебры, находим решение U_i, $i = \overline{1,t}$

$$\begin{cases} U_1 + U_3 = 1; \\ U_1 + U_2 = 2; \\ 2U_1 + 2U_2 = 4; \\ 2U_2 + U_3 = 7; \end{cases}$$

$$\begin{cases} (2)-(1) \Rightarrow 1 = U_2 - U_3; \\ (4)+(5) \Rightarrow 8 = 3U_2; \end{cases} \tag{3}$$

$$U_2 = \frac{8}{3} \pmod{46} = 8 \cdot 3^{-1} \pmod{46} = [\varphi(46) =$$

$$= \varphi(2 \cdot 23) = 22] = 8 \cdot 3^{22} \pmod{46} \equiv 18.$$

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Действительно, $10^{18} \bmod 47 \equiv 3$, а значит $U_1 = 30$, $U_2 = 18$, $U_3 = 17$.

Шаг 4. Находим такое случайное число r, для которого величина $y \cdot a^r = \prod_{i=1}^{t} p_i^{C_i}$ — p_t-гладкое, что для примера соответствует такому r, что $y \cdot a^r (\bmod 47) = \prod_{i=1}^{t} p_i^{C_i}$, которое можно выразить как

$$17 \cdot 10^1 (\bmod 47) = 29;$$

$$17 \cdot 10^2 (\bmod 47) = 8 = 2 \cdot 2 \cdot 2 \Rightarrow r = 2.$$

Шаг 5. Логарифмируем полученное на Шаге 4 выражение и находим решение

$$x = \log_a y = \left[\left(\sum_{i=1}^{t} C_i \log_a p_i \right) - r \right] (\bmod p - 1),$$

для примера

$$\log_a 17 = \left[\sum (\log_a 2 + \log_a 2 + \log_a 2) - 2 \right] \bmod 46 = (3 \cdot 30 - 2) \bmod 46 \equiv 42.$$

Алгоритм исчисления порядка является одним из наиболее эффективных и быстродействующих алгоритмов решения задачи дискретного логарифмирования. Тем не менее, его вычислительная сложность является достаточно высокой.

Показано, что вычислительная сложность алгоритма исчисления порядка измеряется величиной не более чем $O(c_1 \cdot 2^{(c_2 + o(1))\sqrt{\log p \log\log p}})$ [1], где c_1, c_2 — некоторые константы, зависящие от хода промежуточных вычислений алгоритма, в частности, от выбора факторной базы.

Результаты. Алгоритм исчисления порядка позволяет разделить задачу нахождения дискретного логарифма на несколько менее вычислительно сложных задач нахождения парциальных дискретных логарифмов. Соответственно имеется возможность существенно увеличить скорость вычислений применив таблицы индексов.

Предлагается ускоренный алгоритм исчисления порядка (УАИП), суть которого состоит в том, что любое число n из таблицы индексов простого числа p, удовлетворяющее условию $n \le p - 1$, можно представить в виде z_p^m, где z_p — минимальный первообразный корень модуля p; индекс $m = \overline{ij}$, где i — номер строки (указывает число десятков), j — номер столбца (указывает число единиц), на пересечении которых расположено число n, "$\overline{\ .\ }$" — означает, что число m находится на пересечении i-й строки и j-го столбца в таблице индексов.

Пусть, например, необходимо решить сравнение вида $10 \equiv 34^x (\bmod 41)$. Воспользуемся таблицей индексов числа 41 [6].

Минимальным первообразным корнем числа 41 является 6, в соответствии с которым составлена таблица индексов. Используя табл. 2, находим, что 10 может быть представлено как 6^8, а 34 — как 6^{19}, в результате чего переходим к новым уравнениям

$$6^8 = 6^{19x} (\bmod 41);$$

$$8 = 19x (\bmod 40);$$

$$x = \frac{8}{19} (\bmod 40) = 8 \cdot 19^{-1} (\bmod 40).$$

При этом важно отметить, что при переходе к работе с показателями степеней значение модуля изменяется на ($p - 1$), т.е. на 40. Для оптимизации вычислений таблицы индексов могут быть предварительно отсортированы в целях использования дихотомического поиска, вычислительная сложность которого $O(\log_2(p))$.

Для нахождения обратного элемента к 19 по модулю 40 можно воспользоваться теоремой Ферма, которая является частным случаем теоремы Эйлера

$$\varphi(40) = \varphi(2^3 \cdot 5) = \varphi(2^3) \cdot \varphi(5) = (2^3 - 2^2) \cdot 4 = 16,$$

в результате чего

$$x = 8 \cdot 19^{-1} \cdot 19^{16} (\mathrm{mod}\, 40) = 8 \cdot 19^{15} (\mathrm{mod}\, 40) = 32,$$

что является окончательным решением, т.к. $34^{32} (\mathrm{mod}\, 40) \equiv 10$. Известно, что приведенный метод решения сравнений имеет вычислительную сложность порядка $O(\log_2(p))$ [6].

Таким образом, общая вычислительная сложность УАИП будет измеряться величиной $O(2\log_2(p))$ как сумма вычислительных сложностей двух его основных действий.

Рассмотрим еще один пример. Пусть необходимо решить сравнение $17 \equiv 10^x (\mathrm{mod}\, 47)$. Для этого воспользуемся таблицей индексов для числа 47 [6].

Таблица 2

Таблица индексов простого числа 41

	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Таблица 3

Таблица индексов простого числа 47

	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	**17**	38	2	**10**
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

Минимальным первообразным корнем числа 47 является 5. Используя таблицу, число 17 можно представить как 5^{16}, а 10 — как 5^{19}. В результате

$$\begin{gathered} 5^{16} = 5^{19x} (\mathrm{mod}\, 47); \\ 16 = 19x (\mathrm{mod}\, 46); \\ x = \frac{16}{19} (\mathrm{mod}\, 46) = 16 \cdot 19^{-1} (\mathrm{mod}\, 46); \\ \phi(46) = \phi(2 \cdot 23) = \phi(2) \cdot \phi(23) = 22; \\ x = 16 \cdot 19^{-1} \cdot 19^{22} (\mathrm{mod}\, 46) = 16 \cdot 19^{21} (\mathrm{mod}\, 46) = 42. \end{gathered} \qquad (3)$$

Верность решения (3) подтверждается тождеством $10^{42} (\mathrm{mod}\, 46) \equiv 17$.

Для наглядной оценки сложности практической реализации приведена схема работы двух алгоритмов: алгоритма исчисления порядка (рис. 1) и УАИС (рис. 2), что наглядно показывает, насколько был усовершенствован стандартный алгоритм исчисления порядка и как повлияла модернизация на сложность вычисления сравнений по УАИП.

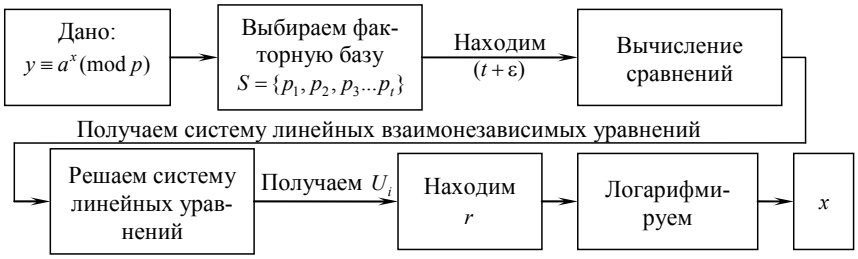

Рис. 1. Схема работы алгоритма исчисления порядка

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

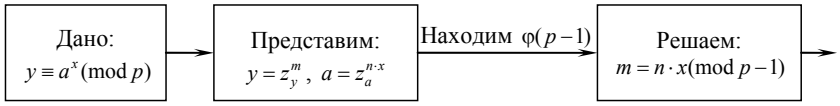

Рис. 2. Схема работы УАИП

Таким образом, удалось снизить вычислительную сложность алгоритма УАИП до величины $O(2\log_2(p))$, по сравнению с оригинальным алгоритмом исчисления порядка, вычислительная сложность которого $O(c_1 \cdot 2^{(c_2+o(1))\sqrt{\log p \log\log p}})$.

Отметим также, что УАИП в случае больших модулей p может работать в составе оригинального алгоритма исчисления порядка для упрощения промежуточных вычислений.

Выводы. Получил дальнейшее развитие алгоритм исчисления порядка, в рамках чего был создан УАИП — более простой и быстрый алгоритм. Предложены блок-схемы работы алгоритма исчисления порядка и УАИП, иллюстрирующие сложность первого и проведенной работы по его модернизации. Установлено, что разработанный алгоритм имеет меньшую вычислительную сложность, что позволяет быстрее решать поставленную задачу, а также не требует длительных и громоздких вычислений.

Литература

1. Рябко, Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. — М.: Горячая линия — Телеком, 2010. — 232 с.
2. Ишмухаметов, Ш.Т. Методы факторизации натуральных чисел / Ш.Т. Ишмухаметов. — Казань: Казан. ун. КФУ, 2011. — 190 с.
3. Вялый, М. Квантовые компьютеры и квантовые вычисления [Электронный ресурс] / М. Вялый // Кафедра информатики МФТИ. — Режим доступа: http://cs.mipt.ru/docs/comp/rus/develop/other/quantum_comp (Дата обращения: 26.11.2013).
4. Buchmann, J. On some computational problems in finite abelian groups / J. Buchmann, M.J. Jacobson, Jr., E. Teske. — Mathematics of Computation. — 1997. — Vol. 66, No. 220. — PP. 1663 — 1687.
5. Studholme, C. The Discrete Log Problem [Электронный ресурс] / C. Studholme // Department of Computer Science, University of Toronto. — 2002. — 57 p. — Режим доступа: http://www.cs.toronto.edu/~cvs/dlog/research_paper.pdf (Дата обращения: 26.11.2013).
6. Виноградов, И.М. Основы теории чисел / И.М. Виноградов. — М.: Регулярная и хаотическая динамика, 2003. — 176 с.
7. Мазурков, М.И. Системы широкополосной радиосвязи / М.И. Мазурков. — Одесса.: Наука и техника, 2010. — 340 с.
8. Варакин, Л.Е. Системы связи с шумоподобными сигналами: монография / Л.Е. Варакин. — М.: Радио и связь, 1985. — 384 с.

References

1. Ryabko, B.Ya. Osnovy sovremennoy kriptografii i stenografii [Foundations of modern cryptography and steganogrphy] / B.Ya. Ryabko, A.N. Fionov. — Moscow, 2010. — 232 p.
2. Ishmukhametov, Sh.T. Metody faktorizatsii natural'nykh chisel [Factorization methods of natural numbers] / Sh.T. Ishmukhametov. — Kazan', 2011. — 190 p.
3. Vyalyy, M. Kvantovye komp'yutery i kvantovye vychisleniya [Quantum computers and quantum computing [Electronic resource] / M. Vyalyy // Kafedra informatiki MFTI [Department of Informatics MIPT]. — Available at: http://cs.mipt.ru/docs/comp/rus/develop/ other/quantum_comp (Access date: 26.11.2013).
4. Buchmann, J. On some computational problems in finite abelian groups / J. Buchmann, M.J. Jacobson, Jr., E. Teske. — Mathematics of Computation. — 1997. — Vol. 66, No. 220. — pp. 1663 — 1687.

5. Studholme, C. The Discrete Log Problem [Electronic resource] / C. Studholme // Department of Computer Science, University of Toronto. — 2002. — 57 p. – Available at: http://www.cs.toronto.edu/~cvs/dlog/research_paper.pdf (Access date: 26.11.2013).
6. Vinogradov, I.M. Osnovy teorii chisel [Basics of number theory] / I.M. Vinogradov. — Moscow, 2003. — 176 p.
7. Mazurkov, M.I. Sistemy shirokopolosnoy radiosvyazi [Wideband radio communication systems] / M.I. Mazurkov. — Odessa, 2010. — 340 p.
8. Varakin, L.E. Sistemy svyazi s shumopodobnymi signalami [Communication systems with noise-like signals: monograph] / L. E. Varakin. — Moscow, 1985. — 384 p.

АНОТАЦІЯ / АННОТАЦИЯ / ABSTRACT

А.В. Соколов, В.Д. Буряк. **Алгоритм зчислення порядку для розрахунку дискретних логарифмів на основі таблиць індексів.** Трудомісткість завдання дискретного логарифмування покладена в основу криптографічної стійкості багатьох алгоритмів асиметричного шифрування, наприклад, широко використовуваного криптоалгоритму RSA. Одним з найбільш ефективних алгоритмів обчислення дискретних логарифмів є алгоритм обчислення порядку, основним недоліком якого є висока обчислювальна складність. Метою є удосконалення алгоритму зчислення порядку, заснованого на застосуванні таблиць індексів, які використовуються в багатьох галузях сучасної теорії передачі інформації та криптографії. Встановлено, що використання таблиць індексів дозволяє значно спростити завдання обчислення дискретних логарифмів, широко використовується у задачах криптографії, що робить можливою розробку нових практично привабливих алгоритмів шифрування, а також представляє цінність з позиції криптоаналізу існуючих криптоалгоритмів, заснованих на обчислювальній складності завдання дискретного логарифмування.

Ключові слова: шифрування, зчислення порядку, дискретний логарифм, *p*-гладке число.

А.В. Соколов, В.Д. Буряк. **Алгоритм исчисления порядка для расчета дискретных логарифмов на основе таблиц индексов.** Трудоемкость задачи дискретного логарифмирования положена в основу криптографической устойчивости многих алгоритмов ассиметричного шифрования, например, широко используемого криптоалгоритма RSA. Одним из наиболее эффективных алгоритмов вычисления дискретных логарифмов является алгоритм исчисления порядка, основным недостатком которого является высокая вычислительная сложность. Целью является усовершенствование алгоритма исчисления порядка, основанного на применении таблиц индексов, применяемых во многих областях современной теории передачи информации и криптографии. Установлено, что использование таблиц индексов позволяет значительно упростить задачу вычисления дискретных логарифмов, широко применяемых в задачах криптографии, что делает возможной разработку новых практически привлекательных алгоритмов шифрования, а также представляет ценность с позиции криптоанализа существующих криптоалгоритмов, основанных на вычислительной сложности задачи дискретного логарифмирования.

Ключевые слова: шифрование, исчисление порядка, дискретный логарифм, *p*-гладкое число.

A.V. Sokolov, V.D. Buryak. **Index-calculus algorithm for calculating the discrete logarithms based on index tables.** The complexity of the discrete logarithm problem is the basis of many asymmetric encryption algorithms cryptographic stability, such as the widely used cryptographic algorithm RSA. One of the most effective algorithm to compute discrete logarithms is the index-calculus algorithm, however, its computational complexity is high. The purpose is to improve the algorithm for calculation of discrete logarithms based on the use of index tables, which are used in many areas of modern communication theory and cryptography. It is found that the use of index tables can greatly simplify the problem of discrete logarithms computing, which makes possible the development of new encryption algorithms with practically attractive properties. It is also valuable from the standpoint of cryptanalysis of the existing cryptographic algorithms based on the computational complexity of the discrete logarithm problem.

Keywords: encryption, index-calculus, discrete logarithm, *p*-smooth number.

Рецензент д-р. техн. наук, проф. Одес. нац. политехн. ун-та Мазурков М.И.

Поступила в редакцию 21 февраля 2014 г.