УДК 512.624.95:378.147.091.3

ТРЕХРАЗРЯДНЫЙ ВАРИАНТ АЛГОРИТМА «BABY-STEP GIANT-STEP» В ПРОБЛЕМЕ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

В.А. ЛИПНИЦКИЙ, Т.Г. КРУПЕНКОВА

Военная академия Республики Беларусь
Минск-57, 220057, Беларусь

Поступила в редакцию 2 октября 2015

Наряду с методом дискретного логарифмирования Д. Шенкса «шаг ребенка – шаг гиганта», авторы предлагают трехразрядный вариант «шага гиганта» для расшифровки сообщений в криптосистеме Эль Гамаля.

Ключевые слова: криптографическая система Эль Гамаля, проблема дискретного логарифмирования, Шенкс Д., алгоритм «шаг ребенка – шаг гиганта».

Введение и цель работы

Современная криптография имеет точную дату своего рождения – выход в свет в 1976 г. статьи [1] Уитни Диффи и Мартина Хелмана. Здесь авторы предложили три революционные идеи: идею применения открытых ключей, методику выработки общего секретного ключа в открытых каналах связи, идею односторонних функций. Это функции, вычисление значений которых не представляет особых трудностей, но вычисление значений обратных к ним функций практически невозможно без дополнительных, секретных данных. Диффи У. и Хелман М. предложили две кандидатуры на роль таких функций:

1) произведение двух больших натуральных чисел (обращение которого упирается в проблему факторизации больших натуральных чисел);

2) вычисление большой степени элементов в кольце классов вычетов по большому простому модулю (обращение которой сталкивается с проблемой дискретного логарифмирования).

Первая из названных функций сразу же оказалась в основе криптосистемы RSA [2], наверное, самой известной из современных криптографических систем, хотя и весьма вязкой даже для легальных пользователей [3, 4]. Вторая обеспечивает криптографическую стойкость криптосистемы Эль Гамаля [5], появившейся в 1985 г. как реакция на излишнюю сложность криптосистемы RSA. Легкая и элегантная в применении, она стала прототипом стандартов шифрования во многих странах мира, в том числе в России, а также в Республике Беларусь [6].

Строго математически существование односторонних функций не доказано [7]. Тем не менее, следует отметить, что ведутся исследования по разработке и применению в криптографии и других кандидатов на односторонние функции. Из наиболее экстравагантных направлений, пожалуй, следует назвать криптосистемы на помехоустойчивых кодах [8, 9].

В 1971 г. Даниэл Шэнкс на симпозиуме по чистой математике американского математического общества прочитал доклад [10], содержавший названный выше метод «baby-step giant-step». И этот метод и доклад знали и цитировали ученые во всем мире.

В 1978 г. Стивен Полиг и Мартин Хелман в работе [11], опираясь на факторизацию мультипликативной группы кольца классов вычетов в произведение циклических подгрупп, построили дальнейшее развитие метода «baby-step giant-step». Вскоре выяснилось, что этот же метод независимо и ранее изобрел и развил (но не опубликовал вовремя) американский математик Роланд Силвер.

В 1994 г. появилась работа [12] московского математика В.И. Нечаева. В работе утверждались следующие факты:

а) метод малых и больших шагов, именуемый на Западе как «baby-step giant-step», в Советском Союзе известен с 1962 г. и был открыт советским математиком А.О. Гельфондом;

б) метод Силвера-Полига-Хелмана был открыт еще в 1965 г. самим В.И. Нечаевым;

в) публикуемый в статье результат получен им еще в 1972 г.;

г) результат этот утверждает, что методы «baby-step giant-step» и Силвера-Полига-Хелмана в определенном смысле являются наилучшими среди детерминированных алгоритмов решения проблемы дискретного логарифмирования. В своей последней книге [13], с. 67, В.И. Нечаев полностью и категорично подтверждает свои слова.

Уважая труд ученых-первооткрывателей, авторы считают, что обсуждаемый метод должен носить название: «метод Нечаева-Силвера-Полига-Хелмана», или сокращенно: «метод НСПХ».

Алгоритм «baby-step giant-step» базируется на искусном использовании двузначного представления искомого логарифма. В данной работе рассматриваются многозначное, а точнее, трехзначное представление искомой степени, достоинства и недостатки такого подхода.

Проблема дискретного логарифмирования

Пусть $p-$ простое число, $p>2$. Мультипликативная группа Z/pZ^* кольца Z/pZ классов вычетов по модулю p является циклической порядка $p-1$ [13, 14]. Каждый элемент a этой группы имеет свой мультипликативный порядок $l(a)-$натуральное число, удовлетворяющее следующим четырем условиям:

1) $1\le l(a)\le p-1$;

2) $l(a)-$делитель числа $p-1$;

3) $a^{l(a)}=1$;

4) среди степеней $a, a^2,...,\ a^{l(a)}=1$ не имеется одинаковых (они и образуют циклическую подгруппу $<a>$ в группе Z/pZ^*, порожденную элементом a).

Если два класса вычетов $a,b\in Z/pZ^*$ связаны соотношением $a^x=b$ для некоторого целого x, и если $r-$остаток от деления x на $l(a)$, то $a^x=a^r=b$; при этом число r называют (дискретным) $\log_a b$ по модулю p.

Самый быстрый способ вычисления конкретной m-й степени элемента $a\in Z/pZ^*,\ a\ne 1,\ 1<m<l(a)$ известен со времен Лейбница и заключается в последовательном вычислении квадратов $a, a^2, (a^2)^2=a^4,...$ с последующим составлением из них степени a^m в соответствии с представлением числа m в двоичной системе счисления. Сложность такого возведения в m-ю степень оценивается в $O(\log_2 m)$ умножений [14, 15].

Обратная задача нахождения степени x из соотношения $a^x=b$ по известным $a,b\in Z/pZ^*$ несравнимо сложнее. На сегодняшний день не известно детерминированного алгоритма ее решения, исключающего перебор. Прямой перебор степеней a или метод малых шагов требует $O(p)$ умножений. Алгоритм малых и больших шагов уменьшает эту величину до $O(\sqrt{p})$.

Суть алгоритма «baby-step giant-step»

В задаче дискретного логарифмирования порядок $l(a)$ элемента a не всегда известен. Поэтому предполагаем, что $l(a)$ имеет максимальное значение $p-1$. Тем более, что в группе Z/pZ^* имеется достаточно много таких элементов (точное их число определяет функция Эйлера: $\varphi(p-1)$).

Пусть d – наименьшее натуральное число, такое, что $\sqrt{l(a)} \le d$. По теореме о делении с остатком $x = d \cdot Q + r$ для некоторых целых Q и r, таких, что $0 \le r < d,\ \ 0 \le Q < d.$ Тогда соотношение $b \equiv a^x (\mathrm{mod}\, p) = a^{Qd} a^r (\mathrm{mod}\, p)$ эквивалентно сравнению

$$b \cdot (\mathrm{a}^{-d})^Q \equiv a^r (\mathrm{mod}\, p)\,. \qquad (1)$$

«Baby step giant step algorithm» заключается в поиске пары целых чисел $Q, r,$ удовлетворяющих условиям $0 \le r < d,\ \ 0 \le Q < d$ и соотношению (1). Поиск реализуется в два этапа. Первый этап – «baby-step» – состоит в составлении таблицы степеней $a^i,\ 2 \le i \le d.$ Если в процессе ее составления не встретится значение $a^i,$ равное b, то следует перейти ко второму этапу – «giant-step». Для этого необходимо с помощью расширенного алгоритма Евклида вычислить $a^{-d} (\mathrm{mod}\, p)$. Второй этап состоит в последовательном вычислении величин $b \cdot (a^{-d})^j (\mathrm{mod}\, p),\ 1 \le j < d,$ и в сравнении их с данными таблицы степеней $a^i,\ 2 \le i \le d.$ Если на каком-то шаге найдутся $Q_0, r_0,$ удовлетворяющие сравнению $b \cdot (\mathrm{a}^{-d})^{Q_0} \equiv a^{r_0} (\mathrm{mod}\, p),$ тогда однозначно опрелеляем искомое $x = d \cdot Q_0 + r_0$. Ясно, что количество вычислений в таком алгоритме оценивается величиной $O(d) = O(\sqrt{p})$.

Трехразрядный вариант метода малых и больших шагов

Пусть δ – наименьшее натуральное число, такое, что $\sqrt[3]{\gamma} \le \delta$. Искомую величину x в задаче дискретного логарифмирования можно представить в виде: $x = \alpha\delta^2 + \beta\delta + \gamma$ для некоторых целых $\alpha, \beta, \gamma,$ удовлетворяющих неравенствам $0 \le \alpha < \delta,\ \ 0 \le \beta < \delta,\ \ 0 \le \gamma < \delta.$ Тогда соотношение $b \equiv a^x (\mathrm{mod}\, p) = a^{\alpha\delta^2} a^{\beta\delta+\gamma} (\mathrm{mod}\, p)$ эквивалентно сравнению

$$b \cdot a^{-\alpha\delta^2} \equiv a^x (\mathrm{mod}\, p) = a^{\beta\delta+\gamma} (\mathrm{mod}\, p)\,. \qquad (2)$$

Первый этап предлагаемого алгоритма – «baby-step» – состоит в составлении таблицы степеней $b \cdot (a^{-\delta^2})^i (\mathrm{mod}\, p)$, $1 \le i < \delta.$ Второй этап – «giant-step» – состоит в последовательном вычислении величин $a^{\delta j + k} (\mathrm{mod}\, p),\ \ 0 \le j < \delta,\ \ 0 \le k < \delta,$ и в сравнении их с данными таблицы степеней $b \cdot (a^{-\delta^2})^i (\mathrm{mod}\, p)$, $1 \le i < \delta.$ Если на каком-то шаге найдутся $\alpha_0, \beta_0, \gamma_0$, удовлетворяющие сравнению $b \cdot (a^{-\delta^2})^{\alpha_0} \equiv a^{\delta\beta_0 + \gamma_0} (\mathrm{mod}\, p)$, то тогда однозначно опрелеляем искомое $x = \alpha_0\delta^2 + \beta_0\delta + \gamma_0$.

Пример 1. Найдем с помощью рассмотренных алгоритмов наименьшее натуральное число x, удовлетворяющее условию $3^x = 691$ в группе $Z/1327Z^*$.

Решение. Непосредственно или же пользуясь данными из книги [14] можно убедиться, что в группе $Z/1327Z^*$ элемент $a = 3$ имеет показатель $l(a) = 1326$. В таком случае $\delta = 37$.

Прямой путь малых шагов приводит к результату: $x = 731$. При решении задачи методом малых и больших шагов придется составить таблицу степеней 3^i из 37 данных. Зная ответ, можно выяснить, что $x = 731 = 37 \cdot 19 + 28$. Это означает, что после вычисления $3^{-37} (\mathrm{mod} 1327)$ расширенным алгоритмом Евклида мы на 19-м шаге составления таблицы значений $691 \cdot (3^{-37})^j (\mathrm{mod}\, 1327)$ получим требуемое решение задачи дискретного логарифмирования. В целом мы затратим 56 умножений по модулю числа $p = 1327$, не считая обращения числа по модулю p.

Найдем решение этой же задачи с помощью трехразрядного «baby step giant step algorithm». В данном случае величина $\delta = 11$. Несложно устанавливается, что в поле $Z/1327Z$

$a^{-1} = \left(\overline{3}\right)^{-1} = \overline{885}$ и $a^{-\delta^2} = \overline{885}^{121} = \overline{927}$. Теперь составляем таблицу значений $b \cdot (a^{-\delta^2})^i (\bmod p) = 691 \cdot 927^i (\bmod 1327)$, $0 \le i < d = 11$.

Таблица 1. **Значения $691 \cdot 927^i (\bmod 1327)$, $0 \le i < 11$**

i	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
	691	943	995	100	1137	361	243	998	227	763	10

Для выполнения второго этапа алгоритма составляем таблицу значений $a^{\beta j+k} (\bmod p)$, $0 \le j < \delta$, и сравниваем их с данными табл. 1. Дальнейшие вычисления сведем в табл. 2.

Таблица 2. **Значения $3^{11j+k} (\bmod 1327)$, $0 \le j < 11$, $0 \le k < 11$**

j/k	**0**	**1**	**2**	**3**	**4**	**5**
0	1	3	9	27	81	243

Вычисленное $3^{11\cdot 0+5} (\bmod 1327) = 243$ находится в табл. 1 при $i = 6$. Таким образом, найдены: $\alpha_0 = 6, \beta_0 = 0, \gamma_0 = 5$. Следовательно, $x = \alpha_0 \delta^2 + \beta_0 \delta + \gamma_0 = 6 \cdot 121 + 731$.

Для вычисления дискретного логарифма новый алгоритм потребовал вычисления в поле $Z/1327Z$ 17 умножений вместо 730 и 56 соответственно без учета нахождения величины $a^{-\delta^2} = \overline{927}$. Конечно, в общем случае трехразрядный метод малых и больших шагов для своей реализации может потребовать $O(\delta^2)$ вычислений. Однако же приведенный пример наглядно демонстрирует несомненную эффективность трехразрядного метода «baby step giant step algorithm».

Заключение

Трехразрядный метод больших и малых шагов является прямым развитием двухшагового метода «baby step giant step algorithm». Данный метод демонстрирует свою реальную эффективность на многих и достаточно разнообразных примерах. Он должен занять достойное место в арсенале тех, кто занят практическим решение проблемы дискретного логарифмирования.

THREE-STEP VARIANT OF «BABY-STEP GIANT STEP» ALGORITHM IN THE DISCRETE LOGARITHM PROBLEM

V.A. LIPNITSKI, T.G. KRUPENKOVA

Abstract

In addition to Shanks' «baby-step giant step» algorithm of finding discrete logarithms the authors suggest a three-step variant of «giant step» to decrypt the message in the Elgamal cryptosystem.

Список литературы

1. *Diffie W. and Helman M.E.* // IEEE Trans. Inf. Theory. 1976. Vol. 22. P. 644-654.
2. *Rivest R., Shamir A., Adleman L.* // Commun. ACM. 1978. Vol. 21. №2. P. 120-126.
3. *Мао В*. Современная криптография: теория и практика. М., 2005.
4. *Фергюсон Н., Шнайдер Б.* Практическая криптография. М., 2005.
5. *Elgamal T.* // IEEE Trans. Inf. Theory. 1985. Vol. 31. P. 469-472.
6. *Харин Ю.С., Берник В.И., Матвеев Г.В. и др.* Математические и компьютерные основы криптологии. Мн., 2003.
7. *Левин Л.А.* // Проблемы передачи информации. 2003. Том 39. Вып. 1. С. 103-117.
8. *Сидельников В.М.* Теория кодирования. М., 2008.
9. *Костелецкий А.В., Липницкий В.А.* // Проблемы защиты информации. 2011. Вып. 10. С. 57-64.
10. *Shanks D.* // Proc. Symp. Pure Math. 1971. Vol. 20. 415-440.
11. *Pohlig S.C. and Helman M.E.* // IEEE Trans. Inf. Theory. 1978. Vol. 1. №24. P. 106-110.
12. *Нечаев В.И.* // Математические заметки. 1994. Том 55. Вып. 2. С. 91-101.
13. *Нечаев В.И.* Элементы криптографии. Основы теории защиты информации. М., 1999.
14. *Виноградов И.М*. Основы теории чисел. М., 1982.
15. *Липницкий В.А*. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. Мн., 2006.