ПОДХОДЫ К РЕШЕНИЮ ПРОБЛЕМЫ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ В ЛАБОРАТОРНОМ КОМПЛЕКСЕ ВОЕННОГО ВУЗА

Военная академия Республики Беларусь
Жалобкевич Е.В., Липницкий В.А.

В современном мире все стремительно развивается и изменяется, объемы передаваемой информации растут экспоненциально. Точная и достоверная информация может оказать решающее влияние на судьбы людей и целых стран, а значит, вопрос защиты информации стоит сегодня наиболее остро. Современные методы криптографической защиты информации основаны на методах современной математики в сочетании с мощными компьютерными средствами.

В основе используемых асимметричных алгоритмов шифрования лежат односторонние функции. В роли таких функций могут выступать умножение и факторизация целых чисел, возведение в квадрат и извлечение квадратного корня по заданному модулю, а также экспоненцирование и логарифмирование в кольцах классов вычетов по большому модулю.

Классическими криптографическими схемами на основе дискретного логарифмирования являются схема выработки общего ключа Диффи-Хеллмана, схема электронной подписи Эль-Гамаля, криптосистема Мэсси-Омуры для передачи сообщений, криптосистема Эль-Гамаля. Их криптостойкость основывается на высокой вычислительной сложности обращения показательной функции. Последняя вычисляется достаточно эффективно еще со времен Лейбница, в то время как даже самые современные алгоритмы вычисления дискретного логарифма имеют очень высокую сложность, которая сравнима со сложностью наиболее быстрых алгоритмов разложения чисел на множители [1].

Рассмотрим проблему дискретного логарифмирования в контексте криптосистемы Эль-Гамаля, модификации которой долгое время были в основе российского и белорусского стандартов шифрования.

Априорное решение уравнения $\overline{g}^x = \overline{h}$ в кольце Z / pZ с простым p на сегодняшний день осуществляется единственным способом – последовательным перебором степеней $\overline{g}$ до получения требуемого класса вычетов $\overline{h}$. К примеру, в учебном варианте криптосистемы с исходными данными $(P, g, h, C, O_{sk}) = (1327, 3, 691, 1016, 48)$ искомый секретный ключ $x = 731$ можно получить за 731 шаг. Если параллельно проводить вычисления для $\overline{g}^{-1}$, то результат будет получен за 595. Конечно, хорошие студенты справляются с подбором x в этой задаче, пользуясь своими знаниями в программировании – используя возможности Excel.

Для криптограмм с шестью и более десятичными знаками применение Excel становится затруднительным. Требуется применение иных, менее переборных методов определения степени x в уравнении $\bar{g}^x = \bar{h}$. Такие алгоритмы есть, хотя известность они приобрели лишь в конце XX века. Так, использование алгоритма «Baby step giant step» Дэвида Шэнкса (1971 г., советский математик Нечаев В.И. утверждает, что этот метод известен в СССР в 1962 года и принадлежит Гельфонду А.О.) существенно сокращает время вычисления секретного ключа. Уравнение дискретного логарифма $\bar{g}^x = \bar{h}$ преобразуется к виду $\bar{h} \equiv \bar{g}^x (\mathrm{mod}\, p) = \bar{g}^{Qd} \bar{g}^r (\mathrm{mod}\, p)$, где и эквивалентно $\bar{h}\left(\bar{g}^{-d}\right)^Q \equiv \bar{g}^r (\mathrm{mod}\, p)$. Задача сводится к поиску пары целых чисел $Q, r\ (0 \le r < d, 0 \le r < d)$. Если на каком-то шаге найдутся Q_0, r_0 удовлетворяющие сравнению, то тогда однозначно опрелеляем искомое $x = d \cdot Q_0 + r_0$.

Для вычисления дискретного логарифма новый алгоритм потребовал вычисления в поле $Z/1327Z$ 55 умножений вместо 730 или 595, вычисления одного обратного расширенным алгоритмом Евклида и 19 сравнений с данными небольшой таблицы [2,3]. Данный метод доступен студентам, хотя и требует от них определенных интеллектуальных усилий.

Следующий метод нахождения дискретного логарифма, который вызывает интерес и практическое применение у специалистов, но требует у обучаемых дальнейшего погружения в глубины теории групп – это метод Полига-Хеллмана (1978 г. [4], открыт Нечаевым В.И в 1965 году (см. [5]), а позднее и независимо Силвером Р.). Идея метода НСПХ заключается в том, чтобы представить $p-1$ в каноническом виде: $p-1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$. Соответственно, циклическая мультипликативная группа $Z/\mathrm{p}Z^*$ раскладывается в прямое произведение своих циклических подгрупп $C(p_i^{\alpha_i}), 1 \le i \le n,$ порядка $p_i^{\alpha_i}$ каждая. При этом $\bar{g} = \bar{g}_1 \cdot \bar{g}_2 \cdot \ldots \cdot g_n$ и $\bar{g} = \bar{g}_1 \cdot \bar{g}_2 \cdot \ldots \cdot g_n$ для $\bar{g}_i, \bar{h}_i \in C(p_i^{\alpha_i})$. Уравнения $\bar{g}^x = \bar{h}$ распадается на n уравнений $\bar{g}_i^{x_i} = \bar{h}_i$ в группах $C(p_i^{\alpha_i}), 1 \le i \le n.$ Последовательно вычисляются значения $x_1, x_2, \ldots, x_n$ по модулям $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_n^{\alpha_n}$ соответственно. Используя китайскую теорему об остатках, искомый x (секретный ключ) восстанавливается по формулам Гарнера. Если же поиск одного или нескольких значений $x_1, x_2, \ldots, x_n$

затруднителен, то можно прибегнуть к алгоритму «Baby step giant step», описанному выше, но имеющему существенно меньший диапазон поиска. Данный метод весьма эффективен в случаях, когда p является большим числом, а множители $p-1$ – малыми числами.

Использование алгоритма Полига-Хеллмана в реальных криптосистемах сокращает время решения задачи дискретного логарифмирования примерно в 6 раз. Это возможно благодаря тому, что в данном алгоритме используются, преимущественно, операции умножения, выполнение которых происходит значительно быстрее, и как следствие, возрастает скорость выполнения всей операции дискретного логарифмирования.

Литература:

1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.
2. Липницкий В. А., Михайловская Л. В., Валаханович Е. В. Защита информации: практикум. – Минск: ВА РБ, 2012. – 87с.
3. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа: учеб. метод. пособие. – Минск, 2006. – 88 с.
4. S. C. Pohlig and M. E. Hellman An Improved Algorithm for Computing Logarithms Over GF(p) and its Cryptographic Significance (англ.) // IEEE Transactions on Information Theory. — 1978. — Т. 1. — № 24. — С. 106-110.
5. Нечаев В.И. Элементы криптографии (Основы защиты информации). – М.: Высшая школа, 1999. – 108 с.

ОСОБЕННОСТИ ПРЕПОДАВАНИЯ КУРСАНТАМ ВОИНСКОЙ ЭТИКИ И ЕЕ МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРИ САМОСТОЯТЕЛЬНОЙ РАБОТЕ

Военная академия Республики Беларусь

Грибкова С.И.

Эффективность образовательного процесса и познания определяется качеством преподавания и самостоятельной познавательной деятельностью курсантов. Эти два процесса тесно взаимосвязаны.

Самостоятельная работа курсантов является ведущей и активизирующей формой обучения по ряду обстоятельств:

- сегодня невозможно получить запас знаний на всю жизнь. Естественно, важен переход от информационного метода к эвристическому, к умению учиться самостоятельно не только в высшем