ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 3
2012

С. Ю. К а т ы ш е в (Москва, ТВП)**. Задача дискретного логарифмирования в конечномерной алгебре над полем.**

Хорошо известна процедура открытого распределения ключей — алгоритм У. Диффи и М. Э. Хеллмана [1], основанный на том, что в качестве общего ключа используется степень g^{mn} некоторого элемента g (обычно циклического образующего) группы G. При этом числа m и n секретны, передаются же только степени g^m и g^n. Установление общего ключа происходит благодаря соотношению:

$$\forall m,n\in \mathbf{N}\ \ (g^m)^n=(g^n)^m.$$

Если определить в произвольном (возможно неассоциативного) группоиде $(\Omega,*)$, *правую степень* элемента g как умножение справа нужное число раз:

$$g^{[m]}=(\ldots((g*g)*g)\ldots m\text{ раз}\ldots),$$

то единственным требованием для возможности реализации процедуры открытого распределения ключа будет выполнение системы тождеств

$$\forall m,n\in\mathbf{N}:\ \ g^{[m][n]}=g^{[n][m]}, \tag{1}$$

где g — фиксированный элемент из Ω.

Если группоид обладает свойством ассоциативности, то система тождеств (1) выполнена для любого элемента g. Однако, данная система тождеств выполнена и в некоторых неассоциативных группоидах, именно они и представляют для нас интерес.

Среди конечномерных алгебр над полем удалось найти такие, в которых система тождеств (1) выполнена.

Пусть P — конечное поле. Рассмотрим произвольную алгебру A размерности n над полем P (P-алгебру размерности n).

Для анализа процедур, являющихся обобщением алгоритма Диффи-Хеллмана на алгебру A, была рассмотрена задача дискретного логарифмирования на данной структуре, которая формулируется, как решение уравнения

$$u^{[x]}=v, \tag{2}$$

для некоторых элементов $u,\ v$, принадлежащих P-алгебре A.

Получен следующий результат.

Теорема. *Задача дискретного логарифмирования на P-алгебре A, с полиномиальной сложностью сводится к задаче дискретного логарифмирования в поле Q, являющегося расширением степени n поля P.*

СПИСОК ЛИТЕРАТУРЫ

1. *Алферов А. П.*, *Зубов А. Ю.*, *Кузьмин А. С.*, *Черемушкин А. В.* Основы криптографии. Москва, 2001.