УДК003.26:51:004(075.8)

Применение чисел Софи Жермен в криптографии

Королева М.Н., Липницкий В.А.
Белорусский национальный технический университет
Военная академия Республики Беларусь

В теории чисел, простое число p является ***простым числом Софи Жермен***, если $2p+1$ также является простым. Числа $2p+1$, объединённые простотой Софи Жермен, называются ***безопасными простыми***. Например, 29 – простое число Софи Жермен и $2 \cdot 29 + 1 = 59$ – связанное с ним безопасное простое число. Таким образом, поиск безопасных простых чисел и чисел Софи Жермен – задача, имеющая одинаковую вычислительную сложность. Название «безопасное» происходит из опыта эксплуатации криптографической системы Эль Гамаля [1]. Призрачные надежды её составителей на то, что хакеры будут решать используемую в ней задачу дискретного логарифма методом «baby-step» практически сразу же провалились под натиском методов «baby-step giant-step» и НСПХ [2]. Понятие безопасной простоты может быть усилено до ***сильной простоты***, для которой оба $p-1$ и $p+1$ имеют большие простые множители. Если для ца Z/pZ каноническое разложение числа $p-1=2q$ (т.к. p – простое, то $p-1$ четное), где q – безопасное или сильное простое число, взлом криптосистемы Эль Гамаля перечисленными методами становится весьма затруднительным, практически невозможным.

Аналогичный подход применим и для обмена ключами в системах Диффи Хелмана и аналогичных системах, которые зависят от безопасности задачи дискретного логарифма, а не от целочисленной факторизации[3]. По этой причине, протоколы генерации ключей для этих криптосистем часто полагаются на эффективные алгоритмы генерации сильных и безопасных простых чисел [4].

Литература

1. Конопелько В.К., Липницкий В.А. и др. Прикладная теория кодирования.Т.1-2. – Мн.: БГУИР, 2004.-688с.
2. Венбо Мао Современная криптография – М.: Издательский дом «Вильямс», 2005.-768с.
3. Cheon, Jung Hee(2000)“Security analysis of the strong Diffie-Helman problem”, 24-th Annyal International Conference of the Theory and Applications of Cryptographic Techniques (EUROCRYPT’06), St.Petersburg, Russia, May28-June1, 2006, Proceedings, Lecture Notes in Computer Science 4004, Springer-Verlag, pp. 1-11, doi:10.1007/11761679_1.