УДК 512.624.95:378.147.091.3

Метод Нечаева–Сильвера–Полига–Хелмана (НСПХ)

Крупенкова Т.Г., Липницкий В.А.
Белорусский национальный технический университет
Военная академия Республики Беларусь

Американский учёный-исследователь Дэниэл Шенкс в 1971 году прочитал доклад, содержавший, в частности, метод больших и малых шагов (baby step giant step). И метод этот и доклад знали и цитировали учёные, как на Западе, так и в Социалистическом лагере.

В 1978 году Стивен Полиг и Мартин Хелман, опираясь на факторизацию мульпликативной группы кольца классов вычетов в произведение циклических подгрупп, построили дальнейшее развитие этого метода. Вскоре выяснилось, что этот же метод независимо и ранее изобрёл и развил американский математик Роланд Сильвер.

В 1994 году появилась работа московского математика Василия Ильича Нечаева. В ней утверждались следующие факты : а) метод малых и больших шагов известен в Советском Союзе с 1962 года и был открыт советским математиком Гельфондом А.О., б) метод Сильвера–Полига–Хелмана был открыт самим Нечаевым в 1965 году, в) метод больших и малых шагов и Сильвера–Полига–Хелмана являются наилучшими среди детерминированных алгоритмов решения проблемы дискретного логарифмирования – результата этот получен им в 1972 году.

Поэтому, обсуждаемый метод должен носить название Нечаева–Сильвера–Полига–Хелмана.

Поиск секретного ключа y в криптосистеме Эль-Гамаля для решения задачи $g^y = b$ в кольце Z/PZ существенно упрощается благодаря тому, что конечная циклическая группа Z/PZ^* раскладывается в прямое произведение $Z/PZ^* = C(p_1^{t_1}) \times C(p_2^{t_2}) \times ... \times C(p_k^{t_k})$ своих циклических подгрупп $C(p_i^{t_i})$ в соответствии с каноническим разложением $p-1 = p_1^{t_1} \cdot ... \cdot p_k^{t_k}$.

Суть алгоритма заключается в том, что достаточно найти y по модулям $p_i^{t_i}$ для всех i, а затем решение сравнения - с помощью китайской теоремы об остатках. Чтобы найти y по каждому из таких модулей, нужно решить сравнение $(g^y)^{(p-1)/p_i^{t_i}} \equiv b^{(p-1)/p_i^{t_i}} \bmod p$.