КРИПТОСИСТЕМЫ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кобяк Е. Ф., Королев В. В., Палатов Е. В.

Матюшков В. Е. – д-р.техн.наук, профессор

Шифрование данных методом эллиптических кривых преследует цели выработать метод быстрого и эффективного шифрования на базе эллиптической криптографии и в то же время повысить устойчивость шифрования (стойкость шифра) и целостность передаваемой информации в процессе обмена данными.

Одной из самых важных проблем современных сетей является безопасность при передаче данных. Хотя во всех системах реализованы механизмы шифрования на транспортном уровне, такие как SSL/TLS, многие облачные подключения остаются уязвимыми для атак.

Одним из решений является шифрование с использованием эллиптических кривых. Сегодня криптосистемы на эллиптических кривых используются в TLS, PGP и SSH, важнейших технологиях, на которых базируются современный веб и мир ИТ, а также Bitcoin и другие криптовалюты.[1]

Эллиптическая кривая — это набор точек, описывающихся уравнением Вейерштрассе:

$$y^2 = x^3 + ax + b, \qquad (1.1)$$

По определению, эллиптическая кривая обладает следующим свойством: если три ее точки лежат на одной прямой, то их сумма равна нулю. Это свойство позволяет описать правила сложения и умножения точек эллиптической кривой. Пример эллиптической кривой представлен на рисунке ниже (рисунок 1).

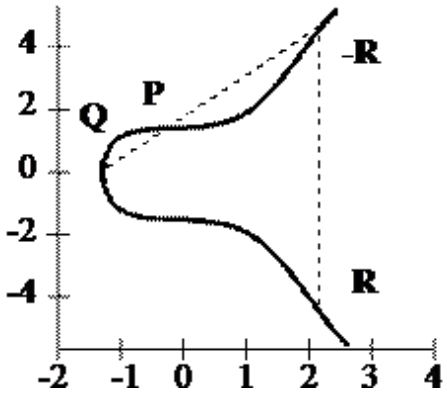

Рисунок 1 – Эллиптическая кривая

Использование эллиптических групп в криптографических целях основано на сложности решения задачи дискретного логарифмирования в эллиптической группе, которая может быть сформулирована так: для заданных точек *P* и *Q* найти такое *k,* чтобы *kP* = *Q.* Значение *k* называется логарифмом от *Q* по основанию *P.* Если взять значение *k* достаточно большим, то задача нахождения *k* становится практически неосуществимой.[2]

Особое достоинство криптосистем на эллиптических кривых состоит в том, что по сравнению с системами на основе алгоритма RSA они обеспечивают существенно более высокую стойкость при равной трудоемкости или, наоборот, существенно меньшую трудоемкость при равной стойкости. В результате тот уровень стойкости, который достигается в RSA при использовании 1024-битных модулей, в системах на эллиптических кривых реализуется при размере модуля 160 бит, что обеспечивает более простую как программную, так и аппаратную реализацию.

Список использованных источников:

1. Доступно о криптографии на эллиптических кривых [Электронный ресурс]. – Режим доступа: https://habr.com/company/gsgroup/blog/394343/ – Дата доступа: 14.03.2019.

2. Криптография с использованием эллиптических кривых [Электронный ресурс]. – Режим доступа: https://www.intuit.ru/studies/courses /28/28/lecture/20430 – Дата доступа: 15.03.2019.