Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

Отчёт по лабораторной работе №7

По дисциплине «Методы защиты информации»
По теме «Криптография с использованием эллиптических кривых»

Выполнил:
студент гр. 653501
М.Л.Спасёнов
Проверил:
В.С.Артемьев

Минск 2019

Введение

Эллиптическая кривая — это набор точек, описывающихся уравнением Вейерштрассе:

$$y^2 = x^3 + ax + b$$

Точки эллиптической кривой над конечным полем представляют собой группу. И как мы отмечали выше для этой группы определена операция сложения.

Соответственно мы можем представить умножение числа k на точку G как G+G+..+G с k слагаемыми.

Теперь представим, что у нас имеется сообщение M представленное в виде целого числа. Мы можем зашифровать его используя выражение

C=M*G.

Вопрос в том, насколько сложно восстановить M зная параметры кривой E(a,b), шифротекст C и точку G.

Данная задача называется дискретным логарифмом на эллиптической кривой и не имеет быстрого решения. Более того, считается, что задача дискретного логарифма на эллиптической кривой является более трудной для решения, чем задача дискретного логарифмирования в конечных полях.

Алгоритм

Пусть существуют два абонента: Алиса и Боб. Предположим, Алиса хочет создать общий секретный ключ с Бобом, но единственный доступный между ними канал может быть подслушан третьей стороной. Изначально должен быть согласован набор параметров (*p, a, b, G, n, h)*, Так же у каждой стороны должна иметься пара ключей состоящая из закрытого ключа *d* и открытого ключа *Q*, где *Q = d * G* - это результат проделывания *d* раз операции суммирования элемента G. Перед использованием стороны обмениваются открытыми ключами.

Первая сторона вычисляет $(x_k, y_k) = d_A * Q_B$

Вторая сторона вычисляет $(x_k, y_k) = d_B * Q_A$

Общий секрет = x_k , координата получившейся точки

Результат работы программы