Министерство образования Республики Беларусь
Учреждение образования “Белорусский государственный университет информатики и радиоэлектроники”

Факультет компьютерных систем и сетей
Кафедра информатики
Дисциплина «Методы защиты информации»

Отчет
к лабораторной работе №7
По дисциплине «Методы защиты информации»
По теме «Криптография с использованием эллиптических кривых»

Выполнил:
студент гр.653501
Хамицевич Ф. С.

Проверил:
Артемьев В.С.

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), шифр текст 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.

Пример работы программы

Генерируем закрытые и открытые ключи, зашифровываем текст, потом дешифруем и сравниваем с исходным в результате получаем совпадение (см. Рис.1).

```
PS C:\Users\Philip\Desktop\Study\Study-7\MZI\mzilabs5-8> & C:/Users/Philip/AppData/Local/Programs/Python/Python37-32/python.exe
Is Valid?  True
```

Рисунок 1. Пример работы программы.

Вывод

Я сделал для себя вывод, что повсеместный переход на «эллиптику» не является необходимостью. В конце концов, пока мирно сосуществуют обычные RSA, DSA с одной стороны, и ГОСТ 34.10, ECDSA с другой, есть пусть и ложное, но успокаивающее чувство альтернативы, которого мы можем лишиться, погнавшись за самыми современными криптографическими методами.