1. Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. **Институт кибербезопасности и защиты информации**

**ЛАБОРАТОРНАЯ РАБОТА № 6**

1. «Решение задачи дискретного логарифмирования на эллиптической кривой»
2. по дисциплине «Криптографические методы защиты информации»
3. Выполнил
4. студент гр. 4851003/70801 Гасанов Э.А.

<*подпись*>

1. Преподаватель
2. ассистент Ярмак А.В.

<*подпись*>

1. Санкт-Петербург
2. 2021

**Цель**

Изучение методов дискретного логарифмирования на эллиптической кривой, реализация методов Полларда и Полига-Хеллмана в группе точек эллиптической кривой.

**Задание**

1. Вариант задания — 4
2. Разработать программу (**П-1**), реализующую метод Полига-Хеллмана дискретного логарифмирования на эллиптической кривой.

**Ход работы**

Была написана программа на Python, реализующая метод Полига-Хеллмана дискретного логарифмирования на эллиптической кривой.

Программа была проверена на 4 примерах, представленных на рисунке 1.

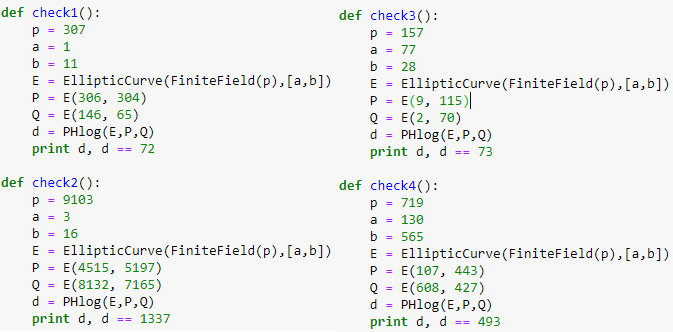


Рисунок 1. Примеры для проверки работоспособности алгоритма

Все 4 примера были успешно посчитаны за небольшое время.

**Выводы**

Был изучен алгоритм дискретного логарифмирования Полига-Хеллмана в группе точек эллиптической кривой. Алгоритм был реализован и проверен на практике.

**Контрольные вопросы**

1. **Сравните сложности задач дискретного логарифмирования на эллиптической кривой и в конечном поле.**

Решение задачи дискретного логарифмирования на эллиптической кривой является более трудоёмким, чем решение аналогичной задаче в конечном поле. Наиболее быстрые алгоритмы решения задачи дискретного логарифмирования в конечном поле не подходят или неэффективны для решения задачи в группе точек эллиптической кривой. Один из наиболее быстрых алгоритмов дискретного логарифмирования в конечном поле имеет сложность , гдe c и d — некоторые константы, а — размер конечного поля. В то же время наиболее эффективные алгоритмы на эллиптических кривых имеют сложность , где —число точек кривой. Тогда для обеспечения стойкости в операций необходимо, чтобы выполнялось условие или . Отсюда видно, что использую эллиптические кривые можно добиться схожих уровней стойкости при гораздо меньших размерах параметров.

1. **Оцените срок безопасной эксплуатации криптосистемы, основанной на задаче дискретного логарифмирования в группе точек эллиптической кривой, по отношению к методу Полларда, если характеристика поля и порядок группы имеют длину 256 бит. Оцените срок действия ключа в начале и в конце срока эксплуатации.**

Криптосистему с порядком группы длиной 109 бит удалось взломать методом Полдарса за 17 месяцев. Исходя из этих данных вычислим, сколько потребуется времени для взлома в случае длины порядка группы в 256 бит:

1. **Сформулируйте требования к параметрам эллиптической кривой для обеспечения стойкости к методу Полига-Хеллмана.**

Данный метод основывается на разложении порядка циклической группы точек. Чем больше множителей в разложении порядка, и чем они меньше, тем эффективнее алгоритм. Следовательно, циклическую группу точек следует выбирать так, чтобы её порядок имел большие простые делители.

# Приложение

Исходный код программы:

def PHlog(E,P,Q):

q = P.order()

f = factor(q)

rems = list()

mods = list()

for j in range(0,len(f)):

p, a = f[j]

S = E(0,1,0)

z\_1 = 0

P0 = (q // p) \* P

dj = 0

for k in range(0,a):

S += ZZ(z\_1 \* p ^ (k - 1)) \* P

Qk = (q // p ^ (k + 1)) \* (Q - S)

zk = P0.discrete\_log(Qk)

dj += (zk \* p ^ k) % (p ^ a)

z\_1 = zk

rems.append(dj % (p ^ a))

mods.append(p ^ a)

return crt(rems,mods)