Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических алгоритмов  
на основе эллиптических кривых

Студент: Шедько Е. А.

ФИТ 3 курс 3 группа

Преподаватель: Копыток Д. В.

Минск 2022

Задание 1. Найти точки ЭК для значений х, указанных в табл. 11.6.

Xmin = 0; Xmax = 35;

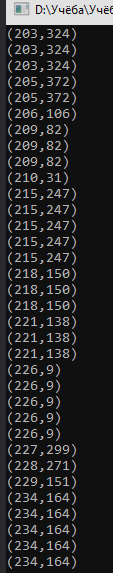


Рисунок 1 – Все точки ЭК

Разработать приложение для выполнения операций над  
точками кривой: 

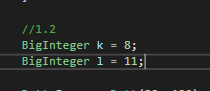


Рисунок 2 – Коэффициенты для вычисления

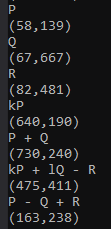


Рисунок 3 – Вычисленные значения

Создать приложение для зашифрования/расшиф-  
рования собственной фамилии (или имени – по выбору) на основе  
ЭК, указанной в задании 1, для генерирующей точки G = (0, 1).

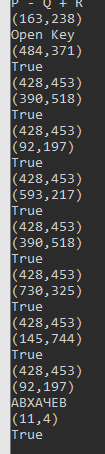


Рисунок 4 – Результат шифрования и верификации верификации  
ЭЦП

Вывод: В ходе лабораторной работы было разработано приложение для реализации сложения точек эллиптической кривой, умножения данных точек н число, нахождения обратной точки и комбинирования упомянутых алгебраических операций при решении задач.