Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №13**

Студент: Бобрович Г.С.

ФИТ 3 курс 7 группа

Преподаватель: Савельева М.Г.

Минск 2023

**Разработать приложение для реализации указанных преподавателем методов криптопреобразования на основе ЭК.**

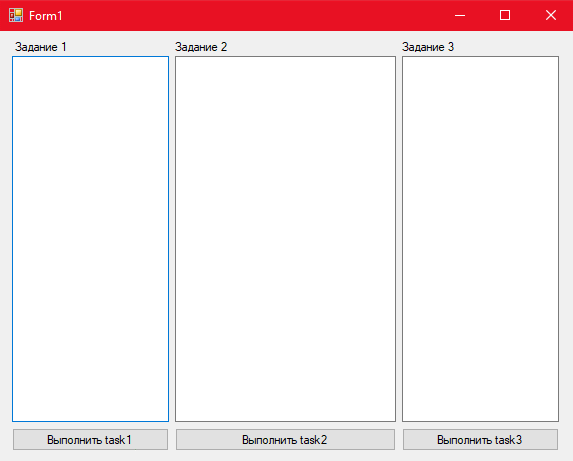
****

Рисунок 1.1 — Приложение

Условия для первого задания:

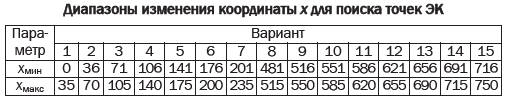




Рисунок 1.2 — Параметры для задания 1

Возьмем параметры 4 варианта. Минимальный *х* будет равен 106, максимальный 140. Параметр *к* и *l* равны 9 и 7 соответственно

Проверим работоспособность выполнения задания 1:

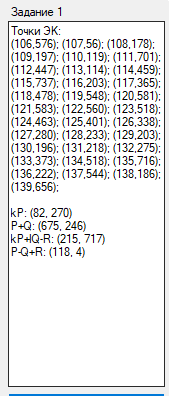


Рисунок 1.3 — Результат 1 задания

Условия для второго задания:

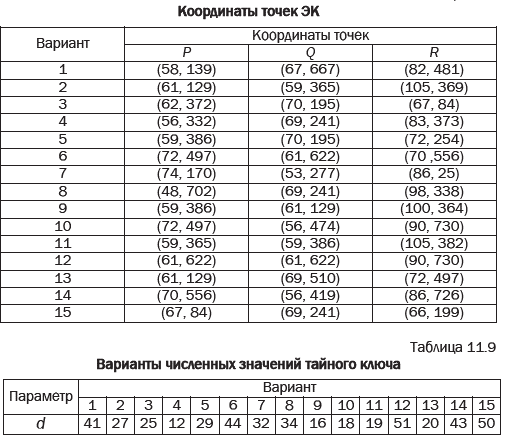


Рисунок 1.4 — Параметры для задания 2

Для второго задания возьмем следующие параметры. Координаты точек *P*, *Q*, *R* будут равны (56, 332), (69, 241), (83, 373). Параметр *d* будет равен 12.

Проверим работоспособность приложения 2:

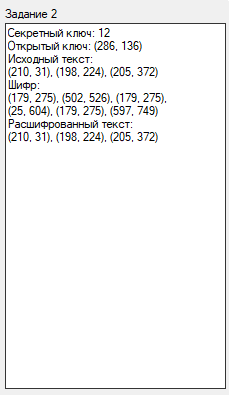


Рисунок 1.5 — Результат 2 задания

Условия для задания 3:



Рисунок 1.6 — Параметры для задания 3

Сообщение состоит из букв «Ф», «И», «О». Этим буквам соответствуют следующие координаты: (210, 31), (198, 224), (205, 372). Параметр *d* будет равен 4.

Проверим работоспособность выполнения задания 3:

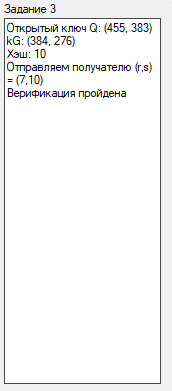


Рисунок 1.7 — Результат 3 задания

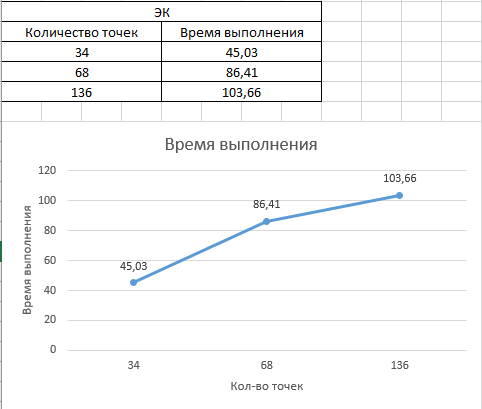


Рисунок 1.8 — Анализ результатов

**Вывод**

В ходе лабораторной работы были изучены и приобретены практические навыки разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых.