**Отчет по Лабораторной работе   
Криптосистема на основе эллиптических кривых**

В рамках лабораторной работы был разобран материал по эллиптическим кривым, а также, разработано приложение, реализующее алгоритмы из материала, предоставленного к лабораторной работе. Возникли проблемы при реализации алгоритма выбора G так как не всегда порядок полученных подгрупп совпадает с ожиданием (есть подозрение что ошибка в описываемом алгоритме). Для проверки был использован модуль M равный 73, ап значение a и b были приняты 1 что удовлетворяет необходимому условию.