Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование криптографических**

**алгоритмов на основе эллиптических**

**кривых**

Студент: Буданова К. А.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

1. **Цель работы**

Изучение и приобретение практических навыков разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых.

1. **Задания**

**Задание 1:**

1.1. Найти точки ЭК для значений *х*.

1.2. Разработать приложение для выполнения операций над точками кривой: а) *k ⋅ Р*; б) *Р* + *Q*; в) *k ⋅ Р* + *l ⋅ Q* – *R*; г) *Р* – *Q* + *R*.

**Задание 2**:

2.1. Создать оконное приложение для зашифрования/расшифрования собственной фамилии на основе ЭК, указанной в задании, для генерирующей точки *G* = (0, 1).

2.2. Вычислить самостоятельно значение открытого ключа *Q*. Принять, что шифруемым блоком является один символ сообщения.

**Задание 3**:

3.1. Создать оконное приложение для генерации/верификации ЭЦП на основе алгоритма ЕСDSA: ЭК *Е751*(–1, 1) c генерирующей точкой *G* = (416, 55); порядок точки *q* = 13.

3.2. Вычислить самостоятельно значение открытого ключа *Q*.

3.3. Хешем подписываемого сообщения (*Н*(*М*)) является модуль по основанию 13 координаты *х* точки ЭК, соответствующей первому символу собственной фамилии.

1. **Ход работы**

В основе задания – ЭК вида *у2* = *х3 – х* + 1 (mod 751): *а* = –1, b = 1, р = 751, т. е. Е751(–1, 1). В соответствии с вариантом, *k* = 7, *l* = 8, *xmin* = 71, *xmax*= 105.

В первом задании необходимо было найти точки ЭК для значений *х*. Для этого воспользуемся формулой выше, которая реализована в коде и представлена на рисунке 3.1. В результате получим вывод, представленный на рисунке 3.2.

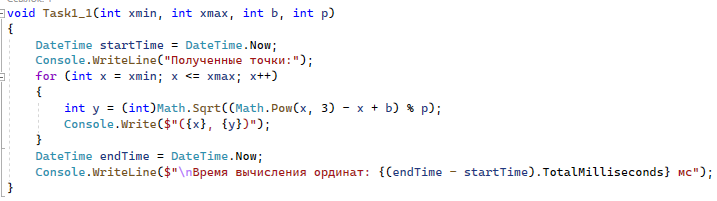


Рисунок 3.1 – Код, реализующий ЭК вида *у2* = *х3 – х* + 1

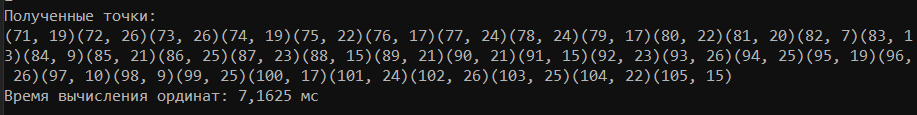


Рисунок 3.2 – Полученные точки

Кроме того, посмотрим, как изменение диапазона абсцисс влияет на скорость вычисления ординат. Результаты представлены на гистограмме на рисунке 3.3.

Рисунок 3.3 – Скорость вычисления ординат

Следующим шагом необходимо было провести операции над точками. Точки в соответствии с вариантом, следующие: *P* = (62, 372), *Q* = (70, 195), *R* = (67, 84). Для операций был разработан класс EllipticCurve, представленный на рисунке 3.4.

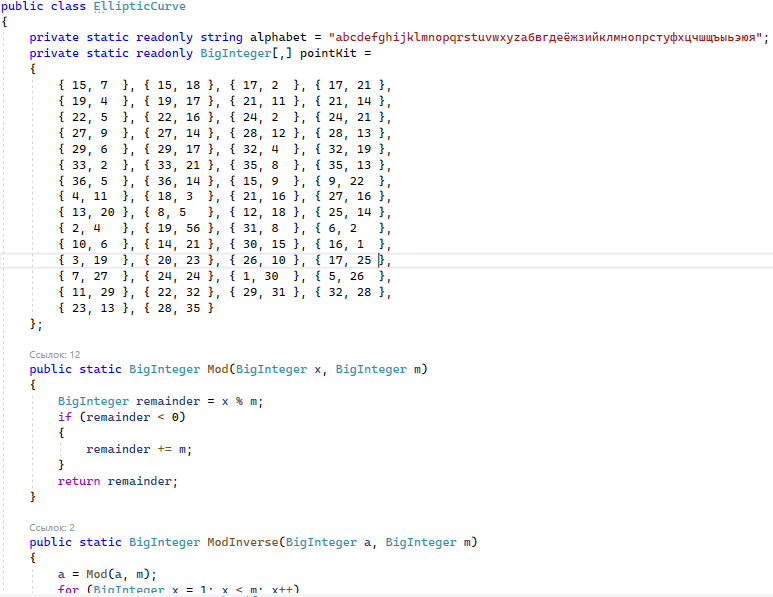


Рисунок 3.4 – Класс EllipticCurve, реализующий основные операции с точками

В результате получаем вывод, представленный на рисунке 3.5.

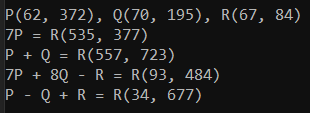


Рисунок 3.5 – Результат операций над точками

Далее, нужно было реализовать зашифрование и расшифрование текста на основе ЭК для генерирующей точки *G* = (0,1), ключ *d* =25, *k* – случайное число в диапазоне от 2 до *d*. Входные данные представлены на рисунке 3.6.

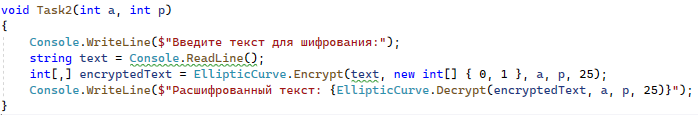


Рисунок 3.6 – Входные данные для методов Encrypt и Decrypt

Сами методы для шифрования и расшифрования представлены на рисунке 3.7.

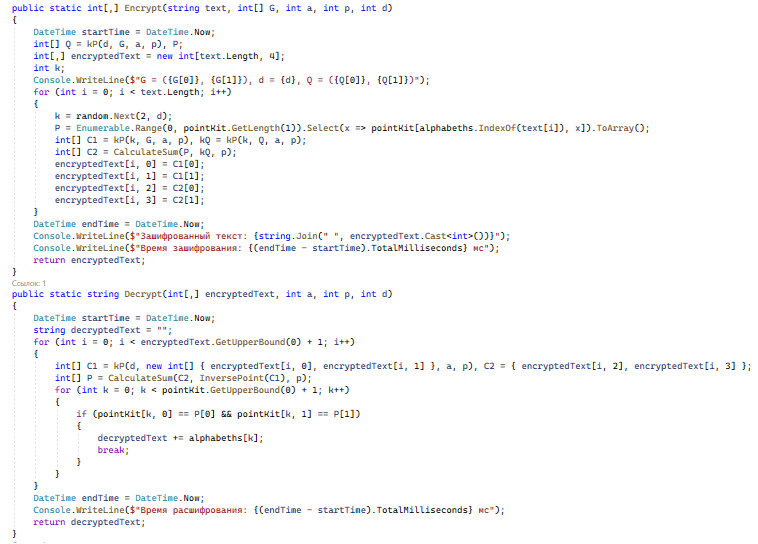


Рисунок 3.7 – Методы Encrypt и Decrypt

В результате получим следующий вывод, представленный на рисунке 3.8.

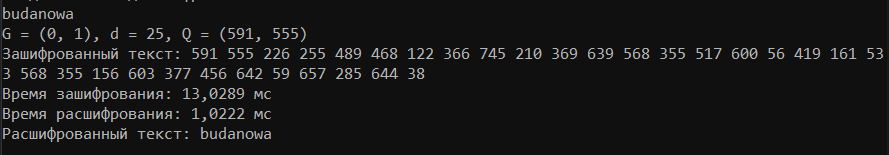


Рисунок 3.8 – Шифрование и дешифрование данных

Также, изменим количество шифруемых и расшифруемых символов и посмотрим, как изменилось время шифрования и расшифрования. Результаты представлены на рисунке 3.9.

Рисунок 3.9 – Скорость шифрования и дешифрования данных в зависимости от длины исходного сообщения

Для реализации последнего задания были разработаны методы CreateDS и VerifyDS для создания и верификации ЭЦП на основе ЭК. Они представлены на рисунке 3.10.

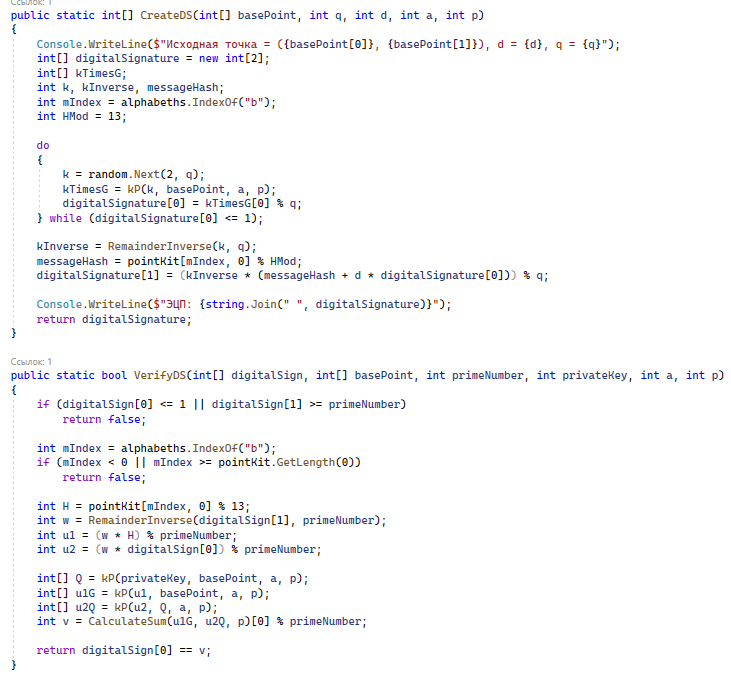


Рисунок 3.10 – Методы CreateDS и VerifyDS

Исходя из задания параметры следующие:

ЭК *Е*751(–1, 1) c генерирующей точкой *G* = (416, 55); порядок точки q = 13. Хешем подписываемого сообщения (*Н*(*М*)) является модуль по основанию 13 координаты *х* точки ЭК, соответствующей первому символу собственной фамилии(в моём случае «b»). *d* = 7 в соответствии с вариантом.

Входные данные указаны на рисунке 3.11.

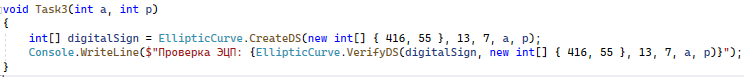


Рисунок 3.11 – Входные данные создания и верификации ЦП

В результате получим следующий вывод, представленный на рисунке 3.12.

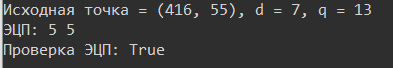


Рисунок 3.12 – Результат создания и верификации ЦП

**Вывод**

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

Также было разработано авторское приложение в соответствии с целью лабораторной работы.