МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«Исследование криптографических алгоритмов на основе эллиптических кривых»**

Студент: Высоцкий Я.А.

ФИТ 3 курс 5 группа

Вариант 4

Преподаватель: Савельева М. Г.

Минск 2023

1. **Нахождения точки эллиптической кривой и выполнения операций**

Для нахождения точек эллиптических кривых мы будет использовать следующею формулу

(1.1)

Код реализующий расчет точек ЭК предоставлен на рисунке 1.1

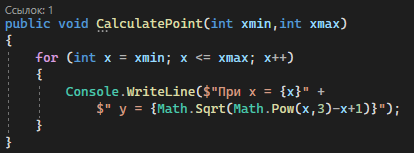
****

Рисунок 1.1 – Код расчета ЭК

Так же по заданию мы должны были выполнить различные операции над точками ЭК. Два основных метода будут расмотренны ниже.

Метод CalculateKP расчитывает произведение числа на точку. Код данного метода предоставлен ниже.

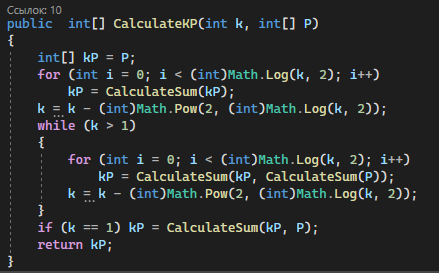


Рисунок 1.2 – Метод CalculateKp

Для выполнения операции сложения точек используется метод CalculateSum.Код данного метода предоставлен ниже.

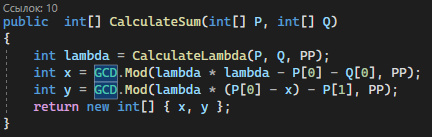


Рисунок 1.3 – Метод CalculateSum

Результат выполнения нахождения точек предоставлен на рисунке 1.4.

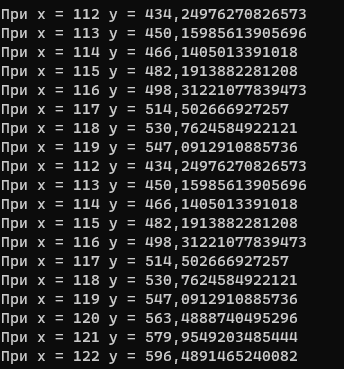


Рисунок 1.4 – Метод CalculateSum

1. **Шифрование и расшифрование с использованием ЭК**

Для шифрования и расшифрования текста, но основе ЭК было разработано два метода: GetEncryptTextByPointAndGenerator и GetEncryptTextByGenerator.

Метод GetEncryptTextByPointAndGenerator принимает 3 параметра: строка для шифрования, точка, выбираемая в качестве открытого ключа, и секретный ключ. Далее каждый символ строки сравнивается с таблицей соответствия. Код данного метода предоставлен на рисунке 2.1.

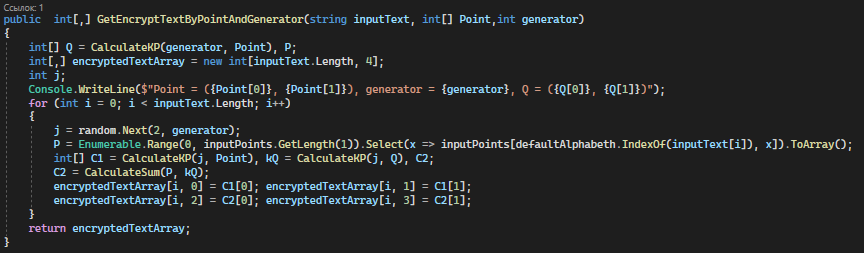


Рисунок 2.1 – Код метода GetEncryptTextByPointAndGenerator

Для расшифрования текст применяется метод GetEncryptTextByGenerator. Он принимает массив чисел, которые собой представляют зашифрованный текст, и закрытый ключ. Код метода предоставлен на рисунке 2.2.

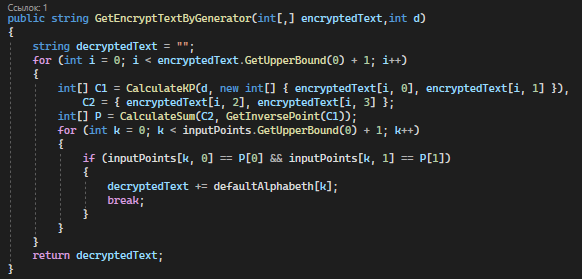


Рисунок 2.2 – Код метода GetEncryptTextByGenerator

1. **Генерация и верификация ЭЦП c помощью ЭК**

Для генерации и верификации ЭЦП на основе алгоритма ECDSA было разработано 2 метода: GenerateDigitalSign и CheckDigitalSign.

Метод GenerateDigitalSign принимает 3 параметра: генерирующую точку, порядок точки и значение тайного ключа. Код данного метода предоставлен на рисунке 3.1.

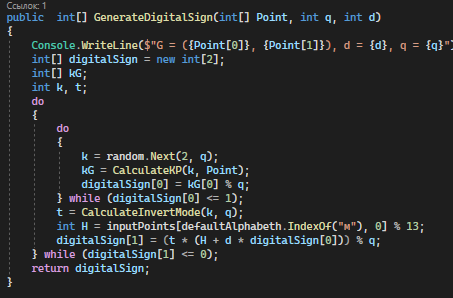


Рисунок 3.1 – Код метода GenerateDigitalSign

Далее для проверки валидности подписи применяется метод CheckDigitalSign. Он принимает 4 параметра: саму подпись, генерирубщую точку, порядок точки и значений тайного ключа. Код данного метода предоставлен на рисунке 3.2.

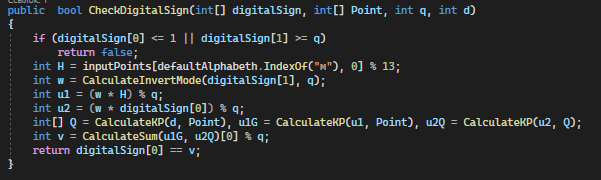


Рисунок 3.1 – Код метода CheckDigitalSign

1. **Анализ результатов**

В сравнении с генерацией ЭЦП на основе Rsa, Эль-Гамаля и Шнора генерация ЭЦП с ЭК занимает больше времени, но ее верификация занимает значительно меньше. На рисунке 4.1 оранжевым цветом отображено время верификации, а синим время генерации.

Рисунок 4.1 – Гистограмма сравнения времени

**Вывод**

При выполнении лабораторной работы были изучены и приобретены практические навыки разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических прямых.