Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические методы защиты информации

Студент: Сенченя В.И.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Лабораторная работа №13**

**Тема «****исследование криптографических**

**алгоритмов на основе эллиптических**

**кривых»**

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

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию и геометрическому представлению операций над эллиптическими кривыми (ЭК).
2. . Разработать приложение для реализации указанных преподавателем методов криптопреобразования на основе ЭК.
3. Разработать приложение для реализации заданных алгоритмов генерации и верификации ЭЦП.
4. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Выполнение операций над точками кривой**

Для нахождения точек ЭК для значений *x* используется следующая формула:

*y*2 = *x*3+*ax*+*b*

Для перемножения точки на константу используется следующая формула:

*kP* = *P* + *P* + ... + *P* (*k* раз)

Для суммирования двух точек необходимо действовать по следующему алгоритму:

1. Если *P* = *Q*, то необходимо выполнить операцию удвоения точки *P*, то есть сложить точку *P* с самой собой.
2. Если *P* ≠ *Q*, то нужно выполнить операцию сложения точек *P* и *Q*. Для этого можно воспользоваться формулой сложения точек на эллиптической кривой:

*λ* = (*y*2 - *y*1) / (*x*2 - *x*1)

*x*3 = *λ*^2 - *x*1 - *x*2

*y*3 = *λ*(*x*1 - *x*3) - *y*1

Здесь *λ* – это наклон прямой, проходящей через точки *P* и *Q*, а *x*3 и *y*3 - координаты новой точки, которая является результатом операции сложения точек *P* и *Q*.

1. Если результатом операции является бесконечно удаленная точка (т.е. точка на бесконечности), то результатом перемножения двух точек является нейтральный элемент на кривой.

Операция вычитания двух точек на эллиптической кривой также определяется как операция сложения, но с использованием специального обратного элемента, который называется обратной точкой.

Предположим, что у нас есть две точки на кривой: *P* = (*x*1, *y*1) и *Q* = (*x*2, *y*2), и мы хотим найти разность *R* = *P* - *Q*.

Для того, чтобы выполнить операцию вычитания, нужно найти обратную точку *Q*' для точки *Q*. Обратная точка *Q*' имеет те же координаты, что и точка *Q*, но с отрицательным знаком *y*-координаты:

*Q*' = (*x*2, -*y*2)

Пример кода операций с точками на кривой предоставлен на рисунке 1.1, а результат работы на рисунке 1.2.

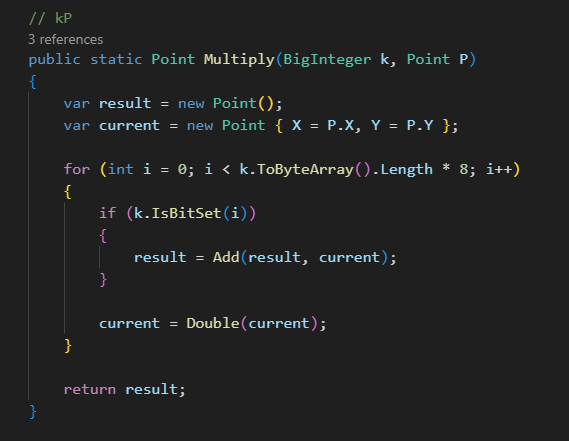


Рисунок 1.1 – Код программы

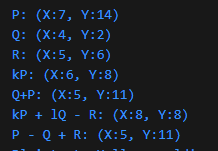


Рисунок 1.2 – Результат работы программы

**Вычисление открытого ключа**

Для вычисления открытого ключа используем следующую формулу:

C2=*P*+*kQ*

Вычисляем точку *R*, если *P* ≠ *Q*, то используем:

*λ* = (*у*2 – *у*1) / (*х*2 – *х*1)

Если *P* = *Q*, то используем

*λ* = (3(х1)2 + *а*)/(2 *у*1)

Используя точку *R* вычисляем *Q*:

*Q* = *P* + *kR*

**Шифрование**

Шифрование на основе эллиптических кривых происходит с использованием алгоритма шифрования, известного как *ECIES* Он использует конечные поля и математические функции на эллиптических кривых для защиты данных.

*ECIES* работает следующим образом:

1. Генерация ключей: Изначально создаются публичный и приватный ключи. Приватный ключ является случайным числом, а публичный ключ представляет собой точку на эллиптической кривой, которая вычисляется как произведение приватного ключа на базовую точку кривой.
2. Шифрование: При шифровании сообщения используется публичный ключ, алгоритм ECIES генерирует новый временный ключ шифрования для каждого сообщения. На этом ключе вычисляются точки на кривой, и одна из этих точек используется для зашифрования сообщения. Зашифрованное сообщение вместе с координатами точки отправляется получателю.
3. Расшифрование: Получатель использует свой приватный ключ для вычисления общей точки на кривой, которая соответствует координатам отправленной точки. Затем он использует эту точку и свой приватный ключ для вычисления временного ключа шифрования, который использовался для шифрования сообщения. Получатель расшифровывает сообщение, используя временный ключ шифрования.

Код предоставлен на рисунке 1.3, а результат работы на рисунке 1.4

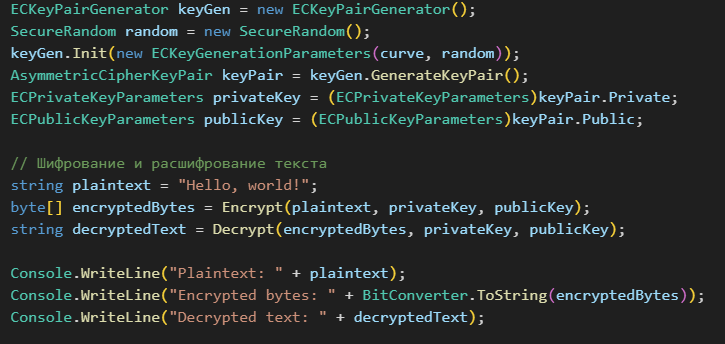


Рисунок 1.3 – Код программы

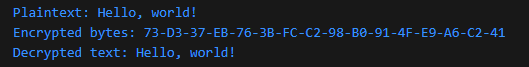


Рисунок 1.4 – Результат работы программы

**Вычисление точек на ЭК по *x***

Точки на кривой по x вычисляются по следующей функции:

*y*2=*x*3+*ax*+*b*

График и значения, полученные для значения *x*min=621 и *x*max=655 предоставлены на рисунке 1.5.

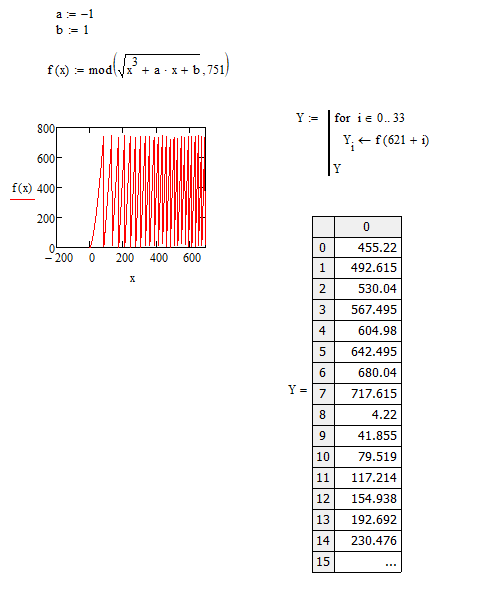


Рисунок 1.5 – График и значения *y*

Мы можем заключить результат, что если у нас выполняется условие функции, то найденные точки принадлежат эллиптической кривой.

**Вывод**

В ходе выполнения лабораторной работы я приобрёл и закрепил навыки практические навыки разработки приложения для реализации криптографических алгоритмов на основе эллиптических кривых.