Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических алгоритмов на основе эллиптических кривых

Студент: Валдайцев А. Д.

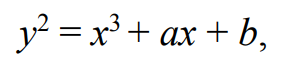
ФИТ 3 курс 5 группа

Пр*еп*одаватель: Савельева М. Г.

Минск 2023

# Эллиптические кривые

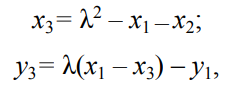
Эллиптическая кривая над вещественными числами – это множество точек, описываемых уравнением:



при этом константы (*а* и *b* – вещественные числа) должны удовлетворять условию:



Если *P* = (*х1*, *у1*) и *Q* = (*х2*, *у2*), то *P* + *Q* = (*х3*, *у3*) определяется в соответствии с правилами:



где



Эллиптическая кривая над полем *Fp* задается теми же уравнениями, что и ЭК над действительными числами, только все вычисления производятся по модулю *р*. Формально ЭК над полем задается так: *Ер*(*а*, *b*).

# Нахождение точек ЭК в диапазоне значений

В основе задания лежит ЭК вида:



где *а* = –1, *b* = 1, *р* = 751, т. е. *Е*751(–1, 1).

Для нахождения точек ЭК среди диапазоне значений x необходимо подставить *a*, *b*, *p* и *x* в формулу, задающую ЭК. Функция, реализующая данный функционал, представлена на рисунке 1.1.

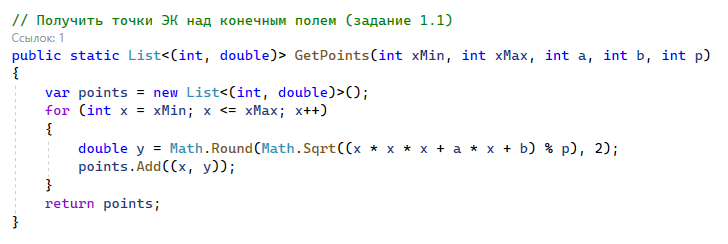


Рисунок 1.1 – Код функции получения точек ЭК над конечным полем

Вывод данной функции представлен на рисунке 1.2.

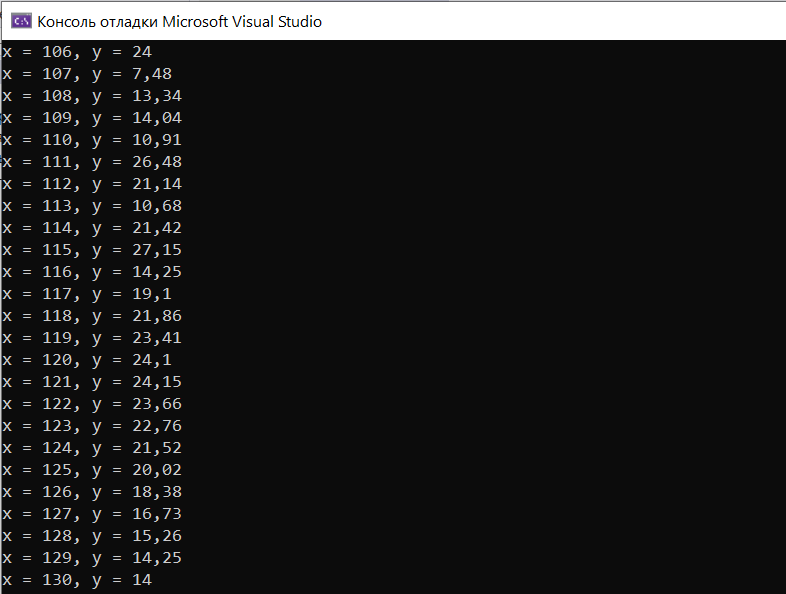


Рисунок 1.2 – Вывод функции получения точек ЭК

# Операции над точками ЭК

Для выполнения операции умножения натурального числа *k* на точку эллиптической кривой *P* реализована следующая функция, представленная на рисунке 1.3.

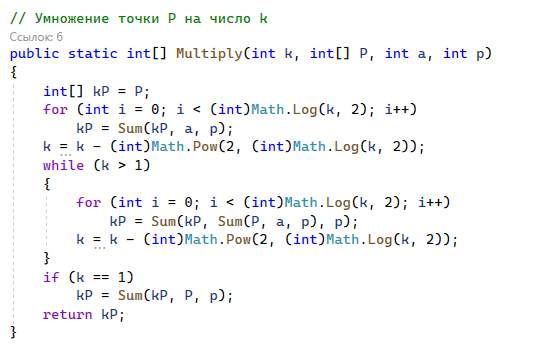


Рисунок 1.3 – Код функции вычисления произведения точки на число

Для реализации алгоритма сложения двух точек ЭК необходимо рассмотреть два случая: когда *P* = *Q* и когда *P* **≠** *Q*. В каждом случае будет использована своя формула для вычисления параметра *λ*.

Код функции, выполняющей вычисления суммы двух точек ЭК, представлен на рисунке 1.4.

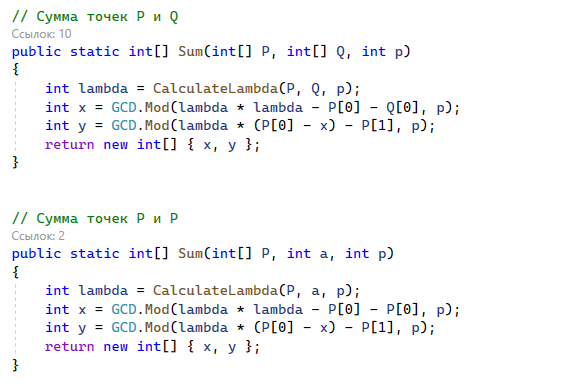


Рисунок 1.4 – Код функции вычисления суммы точек ЭК

Для выполнения оставшихся преобразований над точками ЭК необходимо использовать обратные точки в ЭК и комбинацию прочих функций. Код данных преобразований представлен на рисунке 1.5.

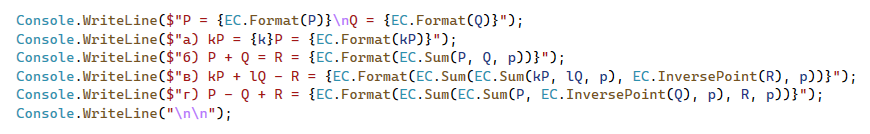


Рисунок 1.5 – Преобразования точек эллиптической кривой

Вывод данных функций представлен на рисунке 1.6.

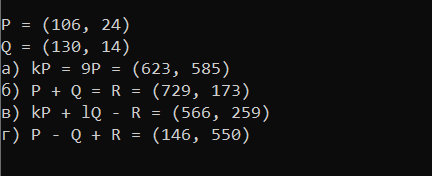


Рисунок 1.6 – Вывод функций преобразований точек ЭК

# Зашифрование с помощью ЭК

При зашифровании данных с использованием ЭК зашифрованное сообщение *М* или каждый зашифрованный блок *mi* этого сообщения состоят из двух чисел.

Зашифрование предполагает представление сообщения в виде точки *Р* (или представления каждого блока сообщения в виде разных точек *Рi*) ЭК с известной точкой *G* и известным *Q*. Соответственно шифртекст – это две точки на той же ЭК: *С*1 и *C*2 или *Сi*1 и *Ci*2. Отправитель выбирает некоторое случайное число *k* и далее выполняет вычисления с использованием открытого ключа получателя:



Получатель для расшифрования сообщения вычисляет:



Для реализации зашифрования с помощью ЭК реализована данная функция, представленная на рисунке 1.7.

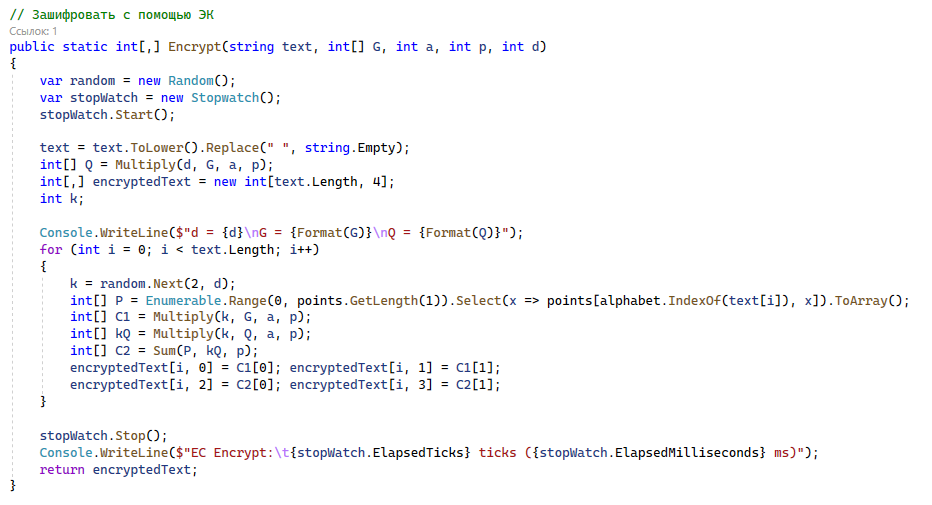


Рисунок 1.7 – Код функции зашифрования при помощи ЭК

Для расшифрования же применяется следующая функция, представленная на рисунке 1.8.

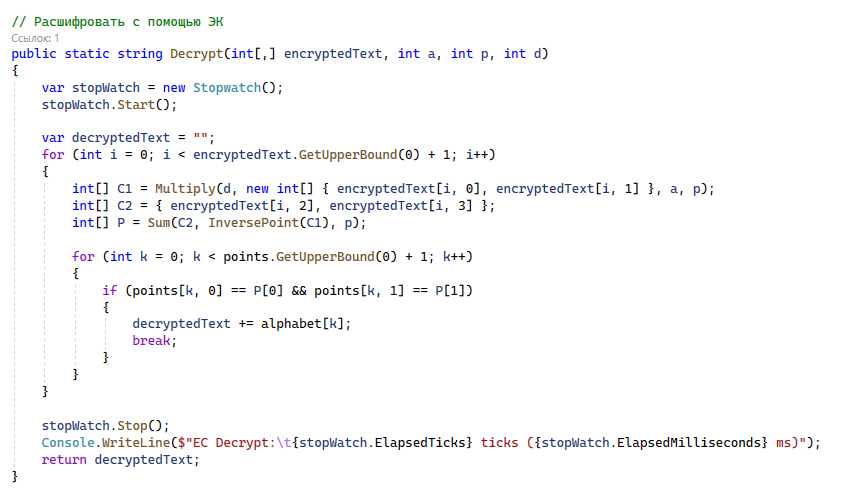


Рисунок 1.8 – Код функции расшифрования при помощи ЭК

Вывод функций зашифрования и расшифрования представлен на рисунке 1.9.

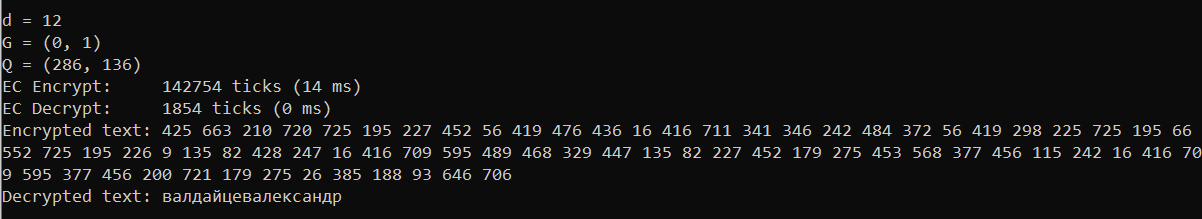


Рисунок 1.9 – Вывод функций шифрования при помощи ЭК

# Анализ полученных результатов

Как видно из рисунка 1.9, зашифрованный текст был успешно расшифрован, что свидетельствует о том, что алгоритм работает корректно. Также стоит отметить, что при каждом новом зашифровании того же текста получается новый шифротекст. Это происходит за счёт того, что каждый раз выбирается новое случайное число *k*.

Также можно заметить, что алгоритмы зашифрования на основе ЭК являются немного более производительными, чем алгоритмы RSA и Эль-Гамаля. Это связано с особенностями математических операций над точками на кривых, которые требуют меньше вычислительных ресурсов.

# Вывод

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