Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра «Информационных систем и технологий»**

**Лабораторная работа №13**

Исследование криптографических алгоритмов на основе эллиптических кривых

Выполнил:

Студент 3 курса, 10 группы

Баранчук Владислав

Минск, 2021 г.

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

**Теоретическая часть**

Эллиптическая кривая – это набор точек, описывающихся уравнением Вейерштрассе.

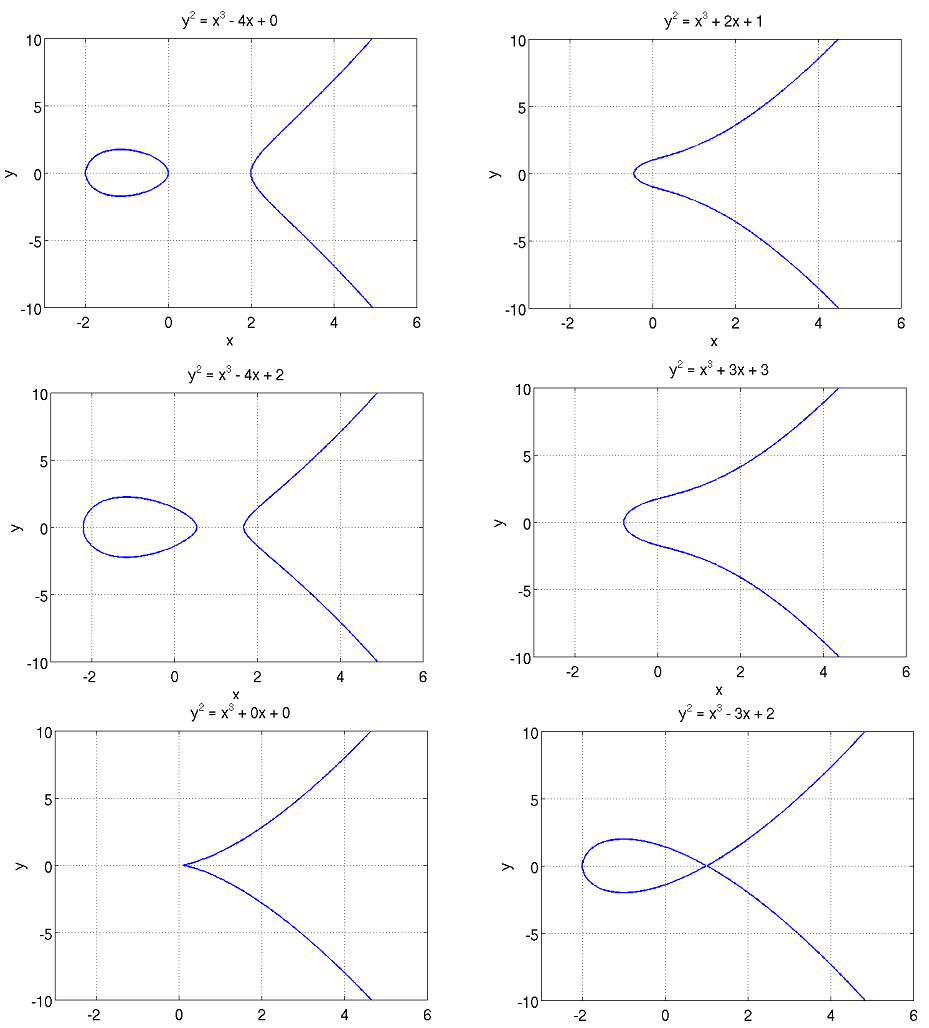


Рис. 1.1 – Примеры графиков ЭК.

Точки эллиптической кривой над конечным полем представляют собой группу. Для этой группы определена операция сложения. Соответственно мы можем представить умножение числа k на точку G как G+G+...+G с k слагаемыми.

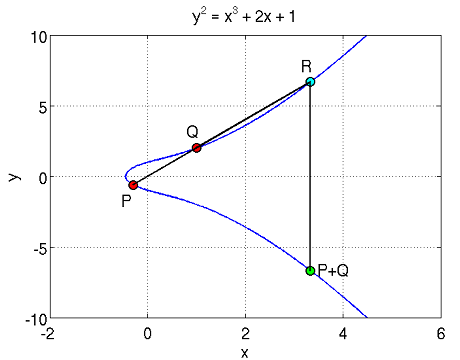


Рис. 1.2 – Графическое представление сложения двух точек ЭК.

Теперь представим, что у нас имеется сообщение M представленное в виде целого числа. Мы можем зашифровать его используя выражение  
C=M\*G.

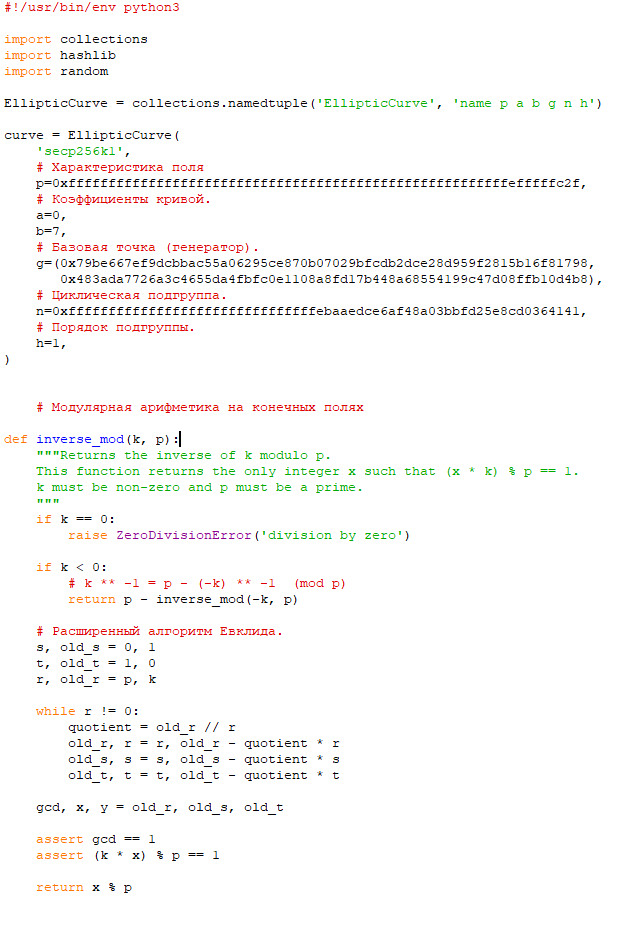
Вопрос в том, насколько сложно восстановить M зная параметры кривой E(a,b), шифротекст С и точку G. Данная задача называется дискретным логарифмом на эллиптической кривой и не имеет быстрого решения. Более того, считается, что задача дискретного логарифма на эллиптической кривой является более трудной для решения, чем задача дискретного логарифмирования в конечных полях.

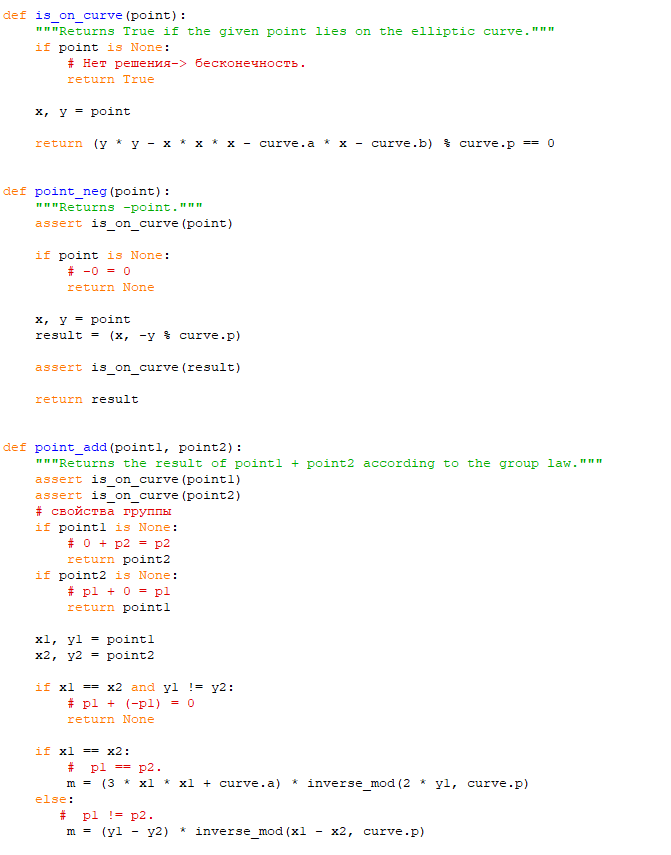
Наиболее быстрые методы, разработанные для конечных полей оказываются бесполезны в случае эллиптических кривых.  
Так для решения дискретного логарифма существуют достаточно быстрые алгоритмы имеющие сложность https://habrastorage.org/getpro/habr/post_images/6eb/d2f/38d/6ebd2f38df6ad717b6f674e2d5a03182.png, где c и d – некоторые константы, а p — размер поля. Такие алгоритмы называются субэкспоненциальными и позволяют сравнительно легко вскрывать дискретный логарифм в конечном поле, если размер поля не выбран очень большим, порядка 21024.

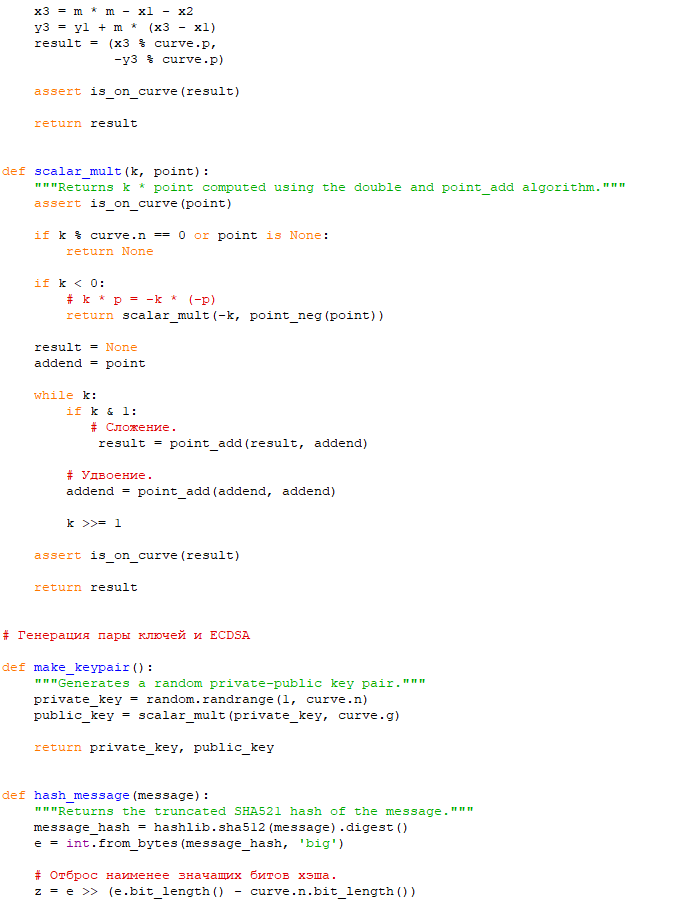
В тоже время наиболее быстрые методы решения дискретного логарифма на эллиптической кривой имеют сложность https://habrastorage.org/getpro/habr/post_images/6c2/205/3fd/6c22053fdc2e65e2126cbe856b1bd56e.png, где q — количество точек эллиптической кривой. Таким образом, для обеспечения уровня стойкости в 280 операций необходимо чтобы q=2160. Напомню, для того, чтобы получить аналогичный уровень сложности при вычислении дискретного логарифма в конечном поле необходимо поле порядка q=21024.

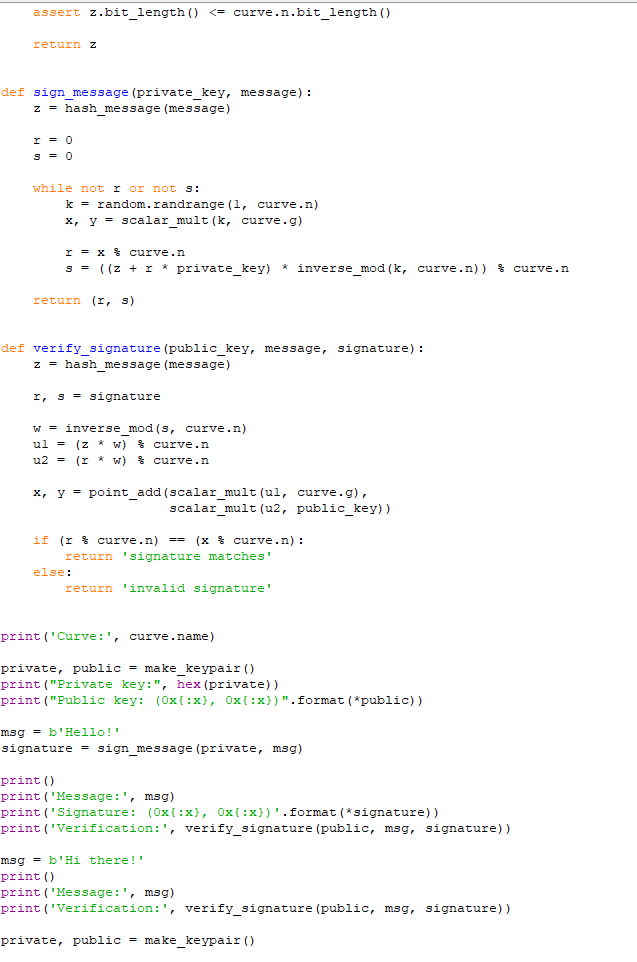
**Практическая часть**

Алгоритмы для генерирования и проверки ЭЦП на основе ЭК









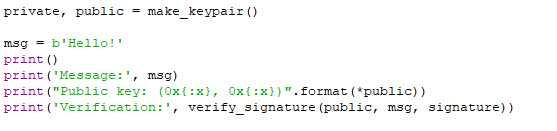


Рис. 1.3 – Листинг ЭЦП и её верификации

Код копирует некоторые части из скрипта ECDH, в частности, параметры области определения и алгоритм генерирования пары закрытого/открытого ключей. Скрипт сначала подписывает сообщение (байтовую строку «Hello!»), а затем проверяет подпись. После чего он пробует проверить ту же подпись для другого сообщения («Hi there!») и проверка не удаётся. Наконец, он пробуем проверить подпись для правильного сообщения, но с другим случайным открытым ключом, после чего проверка тоже не удаётся.

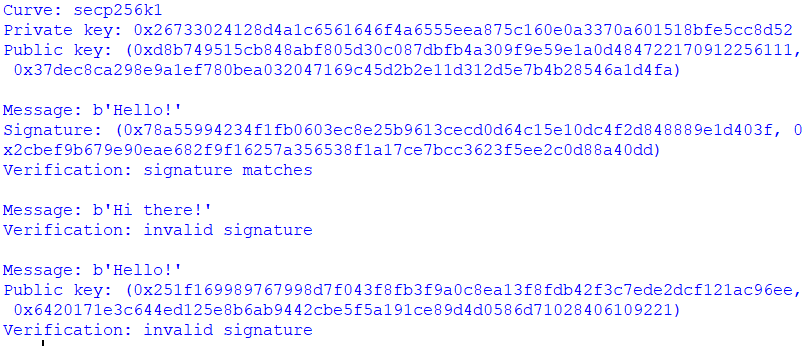


Рис. 1.4 – результат выполнения алгоритма

**Вывод**

В ходе лабораторной работы были получены знания принципах работы эллиптических кривых. Изучены алгоритмы генерации ключевой информации, верификации цифровой подписи на основе ЭК. Так же был реализован программный код, который осуществляет процесс генерации и верификации ЭЦП по описанным алгоритмам.