БФУ им. И. Канта – Компьютерный практикум по криптографии на эллиптических кривых

Преподаватель С. Новоселов Осень 2024

Лабораторная работа № 2b

Опубликована **27.09.2024**

Дедлайн **24.10.2024**

Разработать программу в системе компьютерной алгебры Sage для выработки общего ключа sk с удалённым сервером и обмена сообщениями зашифрованными симметричным шифром на ключе sk.

1. Сервер доступен по адресу:
   `tasks.crypto-kantiana.com`
   порт: 10781

2. Сообщения шифровать с помощью шифра Camellia в режиме OFB с начальным вектором (iv), полученным от сервера.

3. Для работы с симметричной криптографией рекомендуется использовать модуль `cryptography` для Python 3. Если он не установлен, то установить с помощью команды:
   `pip install cryptography`

4. В качестве общего секретного ключа использовать координату x точки, переведенную в байтовую строку кодом:
   `int(x).to_bytes(len(p.binary())/8, "big")`

5. Все байтовые строки, передаваемые по сети должны кодироваться/декодироваться с помощью base64.

Требования к сдаче

- При выработке общего ключа со своей стороны, использовать разработанные при выполнении предыдущих лабораторных методы (сложение точек, скалярное умножение и т.д.). Использование встроенных методов Sage для этой цели **не допускается**.

- Исходный код должен содержать комментарии к каждой из функций с описанием входных и выходных параметров

- Студент должен понимать, что он написал, зачем, а также ответить на теоретические вопросы.