**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное**

**учреждение высшего образования**

**«Санкт-Петербургский государственный университет телекоммуникаций**

**им. проф. М. А. Бонч-Бруевича»**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Кафедра Защищенных систем связи

Дисциплина «Основы криптографии с открытыми ключами»

# Лабораторная работа № 10-2

**Исследование протокола скрытого определения местоположения точек интереса пользователя с учетом типа POI**

**Вариант 4**

Выполнил: ст. г. ИКТЗ-83

Громов А. А.

Проверил: Яковлев В. А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Цель лабораторной работы**

Закрепить теоретические знания студентов по разделу: “Гомоморфное шифрование”. Ознакомиться с протоколом скрытого определения точек интереса мобильного пользователя на основе изученных алгоритмов криптосистем Пэйе и Рабина.

**Исходные данные**

Выбор ячейки производится следующим образом:

координата ,

координата ,

где – номер студента по журналу, – день выполнения лабораторной работы.

Получаем:

**Ход работы**

**Генерация ключей**

Выбираем два больших простых числа , таких что , где – самое большое целое число из базы данных сервера, содержащей информацию о ближайших POIs. С учетом того, что ,. Числа выбрать из диапазона 122-160.

Также необходимо, чтобы все сгенерированные числа удовлетворяли условию: , где – сгенерированное простое число.

Выбираем следующие два больших простых числа , так, чтобы  
, где . Числа выбрать, исходя из диапазона: .

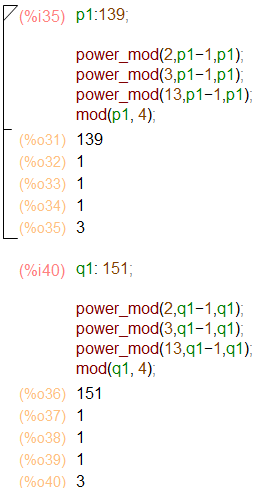


Рисунок 1. Проверка соответствия чисел заданным условиям.

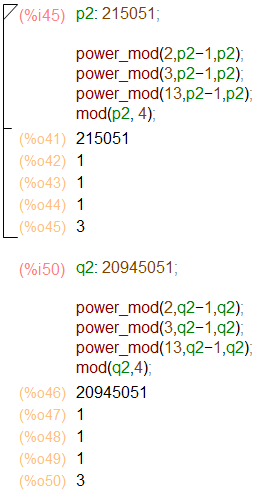


Рисунок 2. Проверка соответствия чисел заданным условиям.

Генерируем числа из множества и из множества , удовлетворяющие условию:



Рисунок 3. Генерация чисел .

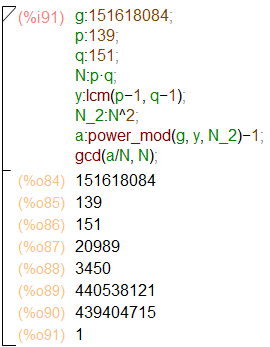
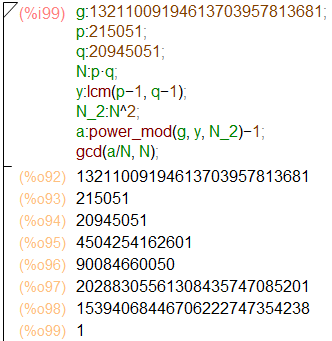
 

Рисунок 4. Проверка соответствия чисел заданным условиям.

Таким образом, имеем следующие ключи:

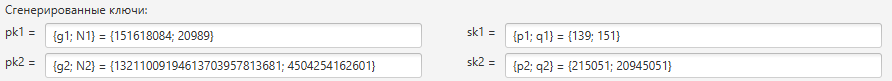


Рисунок 5. Сгенерированные ключи.

**Формирование запроса**

1. Шифрование POI типа на первом открытом ключе

Для каждого пользователь выбирает случайное целое число и вычисляет криптограммы :

где – тип точек интереса, про который пользователь запрашивает информацию.

Вычисляем криптограммы с при :



Рисунок 6. Вычисление криптограмм .

2. Шифрование координаты своей ячейки на втором открытом ключе.

Для каждого пользователь выбирает случайное целое число и вычисляет криптограммы :

где – первая координата ячейки, в которой находится пользователь.

Вычисляем криптограммы :



Рисунок 7. Вычисление криптограмм .

3. Шифрование координаты своей ячейки на втором открытом ключе

Далее пользователь выбирает случайное целое число и вычисляет еще одну криптограмму :

где – вторая координата ячейки, в которой находится пользователь.

Вычисляем криптограмму :

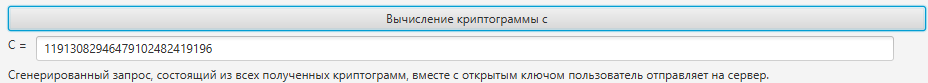


Рисунок 8. Вычисление криптограммы .

Все полученные криптограммы пользователь отправляет на сервер в качестве запроса.

**Генерация ответа сервера**

1. Шифрование значений POIs для всех ячеек на первом открытом ключе.

Вычисляется , где , :

2. Вторичное шифрование POIs и дополнительное шифрование для координаты на втором открытом ключе.

Для каждого выбирается – целое число из множества и вычисляется :

Вычисление криптограмм R:

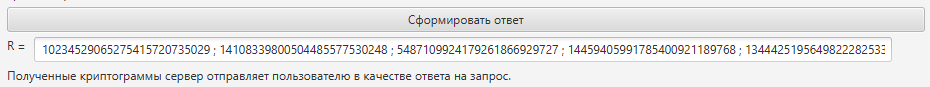


Рисунок 9. Вычисление криптограмм .

После того, как сервер вычислил криптограммы R, он посылает их пользователю в качестве ответа на полученный запрос.

**Получение ответа**

Пользователь получает ответ от сервера в виде :

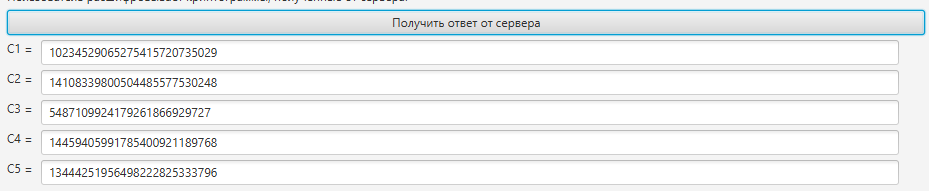


Рисунок 10. Получение пользователем криптограмм .

Далее пользователь выбирает только то значение, порядковый номер которого соответствует второй координате его местоположения и выполняет расшифровку данных, состоящую из четырех шагов.

В нашем случае выбираем криптограмму .

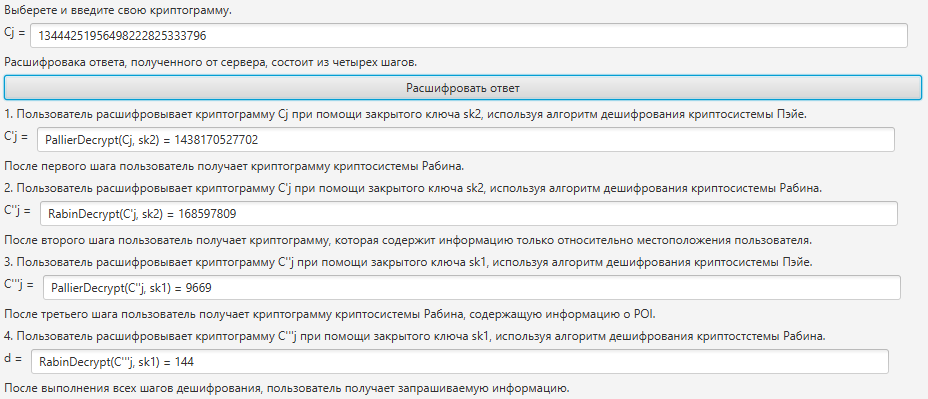


Рисунок 11. Выполнение алгоритма дешифрования.

В результате четвертого шага дешифровки, пользователь получает информацию о ближайшей точке интереса типа для своей ячейки , представленную в десятичном виде.

Для вычисления координат и типа POI переводим d в двоичную форму (длиной 8 бит):

Первые три бита содержат первую координату, следующие три бита – вторую координату, последние два бита – тип точки интереса. При этом к значениям каждой группы битов нужно добавить 1. Таки образом видим, что ближайший банкомат (t = 1) находится в ячейке: {5; 5}.

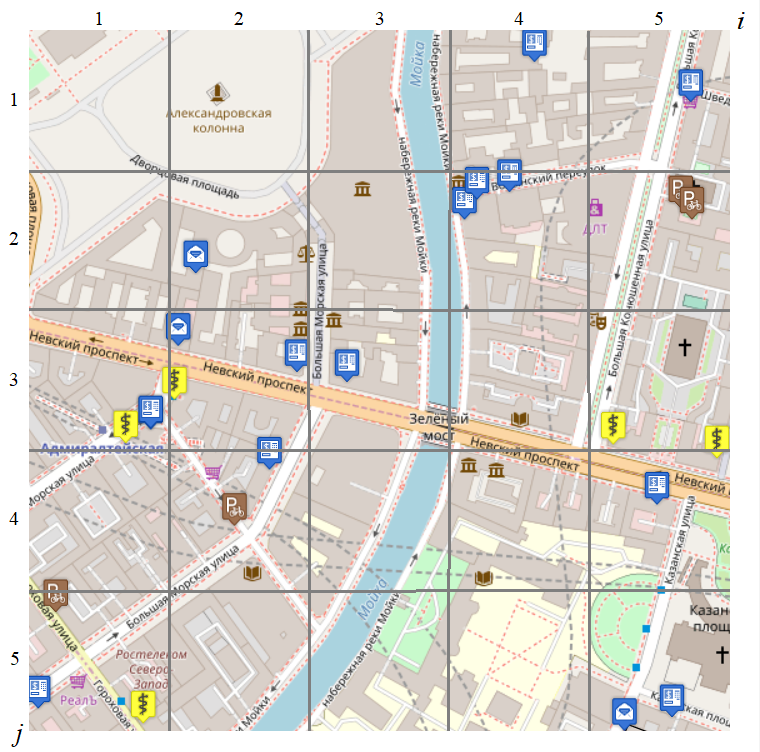
Видим, что полученное значение совпадает с данными на карте:

Рисунок 12. Проверка по карте.

Попробуем расшифровать криптограмму полученную от сервера, порядковый номер которой не равен второй координате :

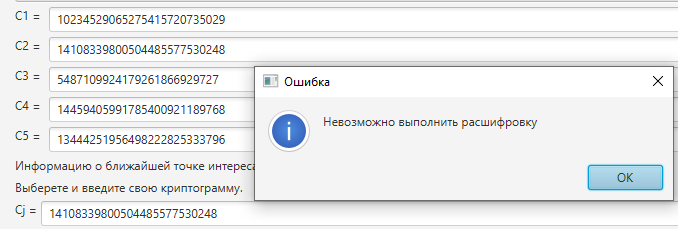


Рисунок 13. Попытка расшифровки криптограммы с индексом .

Видим, что благодаря тому, что для формирования ответа сервер использует шифрование Рабина и Пэйе, пользователь не может расшифровать данные ни для какой ячейки, кроме своей.

Повторим процедуру скрытого определения POIs для остальных типов POIs (при использовании тех же ключевых данных). Получаем следующие результаты:

Ближайшая велопарковка: (5, 2)

Ближайшая аптека: (5, 4)

Ближайшее отделение почты: (5, 5)

Видим, что полученные значения также совпадают с данными на карте:

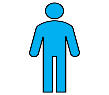
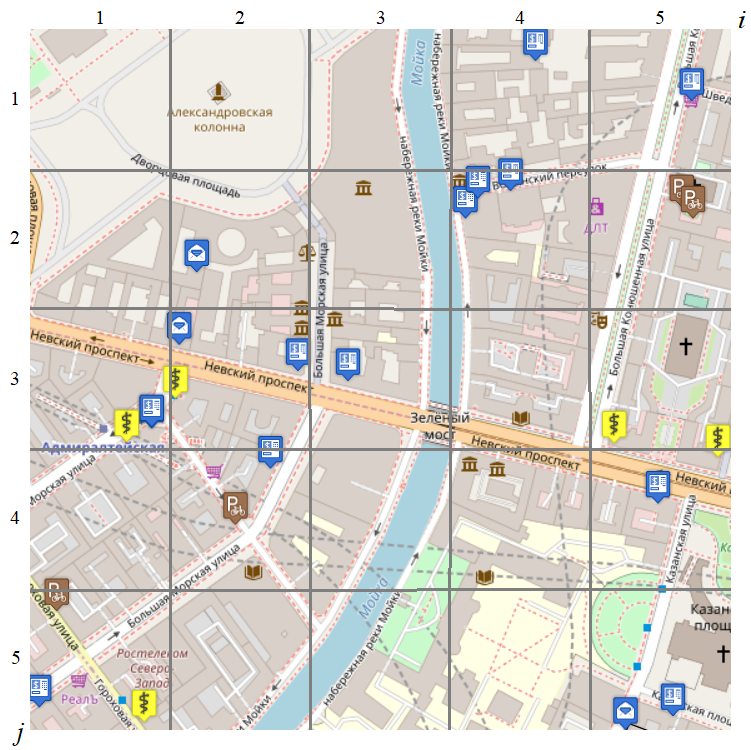
 

Рисунок 14. Проверка по карте.

Вывод:

В ходе выполнения данной лабораторной работы были закреплены теоретические знания по разделу «Гомоморфное шифрование», произведено ознакомление с протоколом скрытого определения точек интереса мобильного пользователя на основе алгоритмов КС Пэйе и Рабина.