**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 № 10-1

**ИССЛЕДОВАНИЕ ПРОТОКОЛА СКРЫТОГО ОПРЕДЕЛЕНИЯ *K* БЛИЖАЙШИХ ТОЧЕК ИНТЕРЕСА БЕЗ УЧЕТА ТИПА POIs**

Выполнил: ст. г. ИКТЗ-83

Громов А.А.

Проверил: Яковлев В. А.

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

Цель лабораторной работы:

Практическое применение криптосистемы Пэйе и ее гомоморфных свойств при определении местоположения точек интереса.

Исходные данные:

Вариант 4:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 11 |  | 33 |  | 36 |  | 27 |
|  | 12 |  | 18 |  | 26 |  | 34 |
|  | 25 |  | 35 |  | 33 |  | 11 |
|  | 10 |  | 11 |  | 9 |  | 27 |

Местоположение (i, j) = (2, 1)

p = 7, q = 23

**Выполнение работы:**

**Генерация ключей:**

Вычисляем модуль : .

Максимальная запись на сервере , следовательно, простые числа выбраны, верно.

Пусть

Открытый ключ: ;

Секретный ключ: .

**Шифрование запроса:**

Для каждого выбирается случайное целое число и вычисляется:

где 𝑖 – первая координата ячейки, в которой находится пользователь.

Так как область имеет размер 4x4, то n = 4

Пусть r1 = 6, r2 = 11, r3 = 19, r4 = 5

;

;

;

.

Отправляем на сервер зашифрованный запрос Q и открытый ключ:

*.*

**Получение ответа:**

Вычисляем , где :

Сгенерированный ответ сервер отправляет пользователю.

**Гомоморфные свойства:**

Получив ответ от сервера, пользователь выполняет расшифровку при помощи сгенерированного на первом этапе секретного ключа, используя алгоритм дешифрования криптосистемы Пэйе.

Из вектора R выбираем . Все остальные данные, полученные от сервера, можно отбросить, так как только содержит информацию о k ближайших POIs для ячейки (i, j).

Расшифровываем криптограмму, используя алгоритм дешифрования КС Пэйе

Преобразуем d в двоичный вид и получим d2 = 100001. Отсюда видим, что ближайшая точка интереса для ячейки (2, 1) находится в подъячейке (4, 1)

**Вывод:**

В ходе выполнения данной лабораторной работы было получено представление о практическом применении КС Пэйе в протоколе скрытого определения k ближайших точек без учета типа POIs, был изучен алгоритм данного протокола.