## **Лабораторная работа №9-2**

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

**Цель 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.

**Используемое программное обеспечение**

Для работы используется программа “SearchPOIs” и вспомогательная программа “Maxima”, используемая в предыдущих лабораторных работах. Для работы программы “SearchPOIs” необходимо иметь на компьютере установленное программное обеспечение java8.

**Описание работы программы**

Программа “SearchPOIs” реализует протокол скрытого определения “точек интереса” мобильного пользователя с учетом типа POI.

Целью данного протокола является получение пользователем информации о ближайших точках интереса определенного типа без раскрытия серверу своего местоположения и типа запрашиваемой точки интереса.

На вкладке “Карта” представлена карта, заранее разделенная на ячеек. На карте изображены 4 типа точек интереса: банкомат, велосипедная парковка, аптека и почта, которые закодированы числами 1, 2, 3, 4 соответственно. Для дальнейших вычислений будем считать, что количество типов точек интереса – , а размер карты - ячеек.

Сервер имеет базу данных, в которой хранится информация о ближайших точках интереса определенного типа относительно центра каждой ячейки. Информация о ближайших точках интереса для ячейки типа обозначается как . состоит из 8 бит. Первые три бита содержат первую координату, следующие три бита – вторую координату, последние два бита – тип точки интереса .

Протокол состоит из четырех алгоритмов: генерация ключей, формирование запроса, формирование ответа и получение ответа.

Первые два алгоритма выполняются пользователем на вкладке “Генерация запроса”. Пользователь генерирует 4 ключа, 2 секретных и 2 открытых и производит шифрование координат своего местоположения и тип интересующей точки интереса.

Генерация ключей происходит следующим образом:

Выбраются два больших простых числа , таких что , где – самое большое целое число из базы данных сервера, содержащей информацию о ближайших POIs. С учетом того, что ,.

2.Выбираются следующие два больших простых числа , так, чтобы , где .

Так как на втором этапе сервер производит вычисления, используя криптосистему Рабина, необходимо, чтобы все сгенерированные числа удовлетворяли условию: , где – сгенерированное простое число.

Рекомендации по выбору чисел :

Числа выбрать из диапазона 122-160. Проверить их на простоту с помощью теста Ферма, используя программу “Maxima”. Вероятность того, что число не простое, должна быть не больше 0,125. Далее проверить условие , также используя программу “Maxima”. Если выбранные числа являются простыми и условие соблюдено, посчитать модуль и перейти к выбору следующих чисел , если нет, то выбрать другие числа и повторить процедуру проверки.

Числа выбрать, исходя из диапазона: . Провести процедуру проверки такую же как при выборе чисел . Если выбранные числа являются простыми и условие соблюдено, посчитать модуль и перейти к следующему шагу, если нет, то выбрать другие числа и повторить процедуру проверки.

Генерируются числа из множества и из множества , удовлетворяющие условию:

Секретными ключами являются: и , а открытыми ключами: и .

Далее пользователь формирует запрос на основе своего местоположения и типа запрашиваемой точки интереса, используя алгоритм шифрования криптосистемы Пэйе.

Формирование запроса выполняется в три этапа и происходит следующим образом:

1. Шифрование типа POI на первом открытом ключе.

Для каждого пользователь выбирает случайное целое число и вычисляет криптограммы :

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

Таким образом, пользователь зашифровывает 1, если , и 0 в любом другом случае, используя алгоритм шифрования криптосистемы Пэйе.

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.

Таким образом, пользователь зашифровывает 1, если , и 0 в любом другом случае, используя алгоритм шифрования криптосистемы Пэйе.

3. Шифрование координаты своей ячейки на втором открытом ключе.

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

где – вторая координата ячейки, в которой находится пользователь.

Все полученные криптограммы пользователь отправляет на сервер в качестве запроса.

Третий алгоритм выполняется сервером на вкладке генерация ответа. Сервер, получив зашифрованный запрос от пользователя, производит вычисления, состоящие из двух этапов. Сервер импользует шифрование Рабина и Пэйе для того, чтобы пользователь не мог расшифровать данные ни для какой ячейки, кроме своей.

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 :

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

Четвертый алгоритм выполняется пользователем на вкладке получение ответа. Получив ответ от сервера в виде , пользователь выбирает только то значение, порядковый номер которого соответствует второй координате его местоположения и выполняет расшифровку данных, состоящую из четырех шагов.

1.Расшифровывается криптограмма , полученная от сервера секретным ключом , используя алгоритм дешифрования криптосистемы Пэйе.

2.Расшифровывается криптограмма секретным ключом , используя алгоритм дешифрования криптосистемы Рабина.

3.Расшифровывается криптограмма секретным ключом , используя алгоритм дешифрования криптосистемы Пэйе.

4.Расшифровывается криптограмма секретным ключом , используя алгоритм дешифрования криптосистемы Рабина.

В результате четвертого шага дешифровки, пользователь получает запрашиваемую информацию о k ближайших точках интереса типа для своей ячейки .

**Задание:**

1. Запустить программу “SearchPOIs”.
2. Изучить карту, представленную на вкладке “Карта”.
3. Выбрать ячейку (свое местоположение), относительно которого программа будет искать ближайшую точку интереса и тип точки интереса(при первой генерации ключей берем значение ).

Выбор ячейки производится следующим образом:

координата ,

координата ,

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

1. Сгенерировать ключи в соответствии с требованиями, представленными в описании работы программы.
2. Провести проверку выполнения условия сгенерированных , используя программу “Maxima”.
3. Сформировать запрос.
4. На вкладке “Генерация ответа” получить запрос пользователя и произвести вычисления.
5. На вкладке “Получение ответа” получить ответ от пользователя и произвести расшифровку.
6. Сравнить полученные результаты с данными на карте. Сделать выводы.
7. Повторить пункты 5-8 для всех типов точек интереса. Сделать выводы.
8. Попробовать расшифровать криптограмму полученную от сервера, порядковый номер которой не равен второй координате . Сделать выводы.

**Отчет:**

1. Титульный лист.
2. Цель работы.
3. Скриншоты всех алгоритмов выполнения лабораторной работы с пояснениями.
4. Скриншоты из программы “Maxima”.
5. Выводы.

**Контрольные вопросы:**

1. Что такое гомоморфное шифрование?
2. Какими гомоморфными свойствами обладает криптосистема Пэйе?
3. Как производится шифрование и расшифрование в криптосистеме Пэйе?
4. Как производится шифрование и расшифрование в криптосистеме Рабина?
5. В чем состоит основная задача алгоритма скрытого определения точек интереса мобильного пользователя?