

**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 К БЛИЖАЙШИХ ТОЧЕК ИНТЕРЕСА БЕЗ  
УЧЕТА ТИПА POIs**

Выполнил:

ст. г. ИКТЗ-83

Громов А.А.

Проверил:

Яковлев В. А.

---

Санкт-Петербург  
2021

**Цель лабораторной работы:**

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

**Исходные данные:**

Вариант 4:

$d_{1,1}$	11	$d_{2,1}$	33	$d_{3,1}$	36	$d_{4,1}$	27
$d_{1,2}$	12	$d_{2,2}$	18	$d_{3,2}$	26	$d_{4,2}$	34
$d_{1,3}$	25	$d_{2,3}$	35	$d_{3,3}$	33	$d_{4,3}$	11
$d_{1,4}$	10	$d_{2,4}$	11	$d_{3,4}$	9	$d_{4,4}$	27

Местоположение  $(i, j) = (2, 1)$

$p = 7, q = 23$

**Выполнение работы:****Генерация ключей:**

Вычисляем модуль  $N$ :  $N = pq = 161$ .

Максимальная запись на сервере  $M = 36$ , следовательно, простые числа выбраны, верно.

Пусть  $\alpha = 3, \beta = 17$

$$g = (\alpha n + 1)\beta^n \bmod n^2 = (3 * 161 + 1)17^{161} \bmod 161^2 = 17477$$

Открытый ключ:  $pk = \{g, N\} = \{17477, 161\}$ ;

Секретный ключ:  $sk = \{p, q\} = \{7, 23\}$ .

**Шифрование запроса:**

Для каждого  $l \in \{1, 2, \dots, n\}$  выбирается случайное целое число  $r_l \in Z_N^*$  и вычисляется:

$$c_l = \begin{cases} \text{Encrypt}(1, pk) = g^1 r_l^N \bmod N^2 & \text{если } l = i \\ \text{Encrypt}(0, pk) = g^0 r_l^N \bmod N^2 & \text{если } l \neq i \end{cases}$$

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

Так как область имеет размер  $4 \times 4$ , то  $n = 4$

Пусть  $r_1 = 6, r_2 = 11, r_3 = 19, r_4 = 5$

$$c_1 = 6^{161} \bmod 25921 = 3821;$$

$$c_2 = 17477 * 11^{161} \bmod 25921 = 16033;$$

$$c_3 = 19^{161} \bmod 25921 = 2775;$$

$$c_4 = 5^{161} \bmod 25921 = 6940.$$

Отправляем на сервер зашифрованный запрос  $Q$  и открытый ключ:

$$Q = \{3821, 16033, 2775, 6940\}, pk = \{17477, 161\}.$$

**Получение ответа:**

Вычисляем  $R = \{C_1, C_2, C_3, C_4\}$ , где  $\gamma = \{1, 2, 3, 4\}$ :

$$C_\gamma = \prod_{l=1}^n c_l^{d_{l,\gamma}} \bmod N^2.$$

$$C_1 = 3821^{11} \cdot 16033^{33} \cdot 2775^{36} \cdot 6940^{27} \bmod 161^2 = 23701;$$

$$C_2 = 3821^{12} \cdot 16033^{18} \cdot 2775^{26} \cdot 6940^{34} \bmod 161^2 = 8058;$$

$$C_3 = 3821^{25} \cdot 16033^{35} \cdot 2775^{33} \cdot 6940^{11} (\text{mod } 161^2) = 17266;$$

$$C_4 = 3821^{10} \cdot 16033^{11} \cdot 2775^9 \cdot 6940^{27} (\text{mod } 161^2) = 75.$$

Сгенерированный ответ  $R = \{23701, 8058, 17266, 75\}$  сервер отправляет пользователю.

### Гомоморфные свойства:

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

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

Расшифровываем криптограмму, используя алгоритм дешифрования КС Пэ́йе

$$d = \frac{(C_j^\lambda (\text{mod } N^2) - 1)/N}{(g^\lambda (\text{mod } N^2) - 1)/N} (\text{mod } N)$$

$$\lambda = \text{lcm}(p-1, q-1) = \text{lcm}(6, 22) = 66$$

$$d = \frac{\frac{23701^{66} (\text{mod } 25921) - 1}{161}}{\frac{17477^{66} (\text{mod } 25921) - 1}{161}} (\text{mod } 161) = 94 * 37^{-1} \text{ mod } 161$$

$$= 94 * 74 \text{ mod } 161 = 33$$

Преобразуем  $d$  в двоичный вид и получим  $d_2 = 100001$ . Отсюда видим, что ближайшая точка интереса для ячейки  $(2, 1)$  находится в подячейке  $(4, 1)$

### Вывод:

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