**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 № 11

**СИСТЕМА ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ НА ОСНОВЕ ГОМОМОРФНЫХ СВОЙСТВ КРИПТОСИСТЕМЫ ПЭЙЕ**

Выполнил: ст. г. ИКТЗ-83

Громов А. А.

Проверил: Яковлев В. А.

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

**Цель лабораторной работы:**

Изучение принципов построения системы электронного голосования на основе криптосистемы Пэйе и анализ выполнения требований по обеспечению ее безопасности.

**Исходные данные:**

**Вариант №4.**

| **Избиратель** | **B1**  **(70)** | **B2**  **(71)** | **B3**  **(72)** | **B4**  **(73)** | **B5**  **(74)** | **Голос (m)** |
| --- | --- | --- | --- | --- | --- | --- |
| A1 | v |  | v |  |  | m=50 |
| A2 |  |  | v |  | v | m=2450 |
| A3 |  |  | v |  |  | m=49 |
| A4 |  | v |  |  |  | m=7 |
| A5 | v |  |  | v |  | m=344 |
| A6 |  |  | v |  |  | m=49 |
| Итог: | 2 | 1 | 4 | 1 | 1 | 2949 |

294910 = 114127

Nv = 6, Nc = 5

Основание системы счисления b = Nv + 1 = 7

**Выполнение работы:**

**Генерация ключей:**

Максимальное число сообщений, которые можно зашифровать

mmax = 74 + 73 + 72 + 71 + 70 = 2801

Следовательно, максимально возможная сумма всех голосов

*Tmax = Nv\* mmax* =

По условию Tmax*;*

Для генерации ключа выберем случайным образом 2 простых больших числа

и , где

Вычисляем ,

Пусть

*=*

**Шифрование:**

Зашифруем сообщения, содержащие выбор избирателей: *E(mi)= ci ==*  *r Z\*n*

| **Избиратель** | **Случайное число (ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| --- | --- | --- | --- |
| A1 | 21 | m=50 |  |
| A2 | 68 | m=2450 |  |
| A3 | 13 | m=49 |  |
| A4 | 7 | m=7 |  |
| A5 | 45 | m=344 |  |
| A6 | 9 | m=49 |  |
| Подсчет: |  |  |  |

Вычислим произведение криптограмм:

**Дешифрование:**

Таким образом, подсчет зашифрованных голосов дает сумму всех голосов. Для определения победителя голосования необходимо преобразовать получившееся значение в числовую форму, представленную в начале выборов. В данном случае сервер для подсчетов голосов работает с десятичными числами, поэтому перевод не обязателен.

294910 = 1 \* 74 +1 \* 73 + 4 \* 72 +1 \* 71 +2 \* 70 = 114127

В силу гомоморфности криптосистемы индекс максимального элемента результирующего вектора и будет индексом победившего кандидата. Следовательно, можно сделать вывод о том, что победителем электронных выборов является кандидат B3.

**Вывод:**

В ходе выполнения данной лабораторной работы был изучен алгоритм электронного голосования на основе КС Пэйе и определен победитель электронного голосования.