**ПРИЛОЖЕНИЕ**

**Варианты заданий для лабораторной работы:**

**«Система электронного голосования на основе гомоморфных свойств криптосистемы Пэйе»**

Внимание:Основание системы счисления выбрать равным b=Nv+1

**Вариант №1. Дано: p= 13; q= 11.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 | v |  |  |  |  | m= |
| A2 |  |  |  |  | v | m= |
| A3 |  | v | v |  |  | m= |
| A4 |  |  |  |  |  | m= |
| A5 | v |  |  | v |  | m= |
| A6 |  | v | v |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 16 |  |  |
| A2 | 12 |  |  |
| A3 | 23 |  |  |
| A4 | 37 |  |  |
| A5 | 11 |  |  |
| A6 | 9 |  |  |
| Подсчет: |  |  |  |

**Вариант №2. Дано: p= 7; q= 11.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  |  | v |  |  | m= |
| A2 | v |  |  |  | v | m= |
| A3 |  |  | v |  |  | m= |
| A4 |  | v |  |  |  | m= |
| A5 | v |  |  | v |  | m= |
| A6 |  |  | v |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 19 |  |  |
| A2 | 21 |  |  |
| A3 | 13 |  |  |
| A4 | 7 |  |  |
| A5 | 11 |  |  |
| A6 | 8 |  |  |
| Подсчет: |  |  |  |

**Вариант №3. Дано: p= 5; q= 19.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  |  | v |  |  | m= |
| A2 | v |  |  |  | v | m= |
| A3 |  |  | v |  |  | m= |
| A4 |  |  |  | v |  | m= |
| A5 | v |  |  | v | v | m= |
| A6 |  |  | v |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 9 |  |  |
| A2 | 21 |  |  |
| A3 | 13 |  |  |
| A4 | 7 |  |  |
| A5 | 11 |  |  |
| A6 | 18 |  |  |
| Подсчет: |  |  |  |

**Вариант №4. Дано: p= 11; q= 3.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 | v |  | v |  |  | m= |
| A2 |  |  | v |  | v | m= |
| A3 |  |  | v |  |  | m= |
| A4 |  | v |  |  |  | m= |
| A5 | v |  |  | v |  | m= |
| A6 |  |  | v |  |  | m= |
| Итог: |  |  |  |  |  |  |

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

**Вариант №5. Дано: p= 7; q= 17.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  |  | v |  |  | m= |
| A2 | v |  |  |  | v | m= |
| A3 | v |  |  |  |  | m= |
| A4 |  | v |  |  |  | m= |
| A5 | v |  |  | v |  | m= |
| A6 |  |  | v |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 19 |  |  |
| A2 | 21 |  |  |
| A3 | 11 |  |  |
| A4 | 7 |  |  |
| A5 | 21 |  |  |
| A6 | 8 |  |  |
| Подсчет: |  |  |  |

**Вариант №6. Дано: p= 5; q= 13.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  |  | v |  |  | m= |
| A2 | v |  | v |  |  | m= |
| A3 |  |  | v |  |  | m= |
| A4 |  | v |  |  |  | m= |
| A5 | v |  |  | v |  | m= |
| A6 |  |  | v |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 21 |  |  |
| A2 | 2 |  |  |
| A3 | 13 |  |  |
| A4 | 7 |  |  |
| A5 | 11 |  |  |
| A6 | 18 |  |  |
| Подсчет: |  |  |  |

**Вариант №7. Дано: p= 7; q= 23.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 | v |  |  |  |  | m= |
| A2 |  |  |  |  | v | m= |
| A3 | v |  |  |  | v | m= |
| A4 |  |  |  |  | v | m= |
| A5 | v |  |  |  |  | m= |
| A6 |  |  | v |  | v | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 16 |  |  |
| A2 | 12 |  |  |
| A3 | 23 |  |  |
| A4 | 7 |  |  |
| A5 | 11 |  |  |
| A6 | 9 |  |  |
| Подсчет: |  |  |  |

**Вариант №8. Дано: p= 5; q= 23..**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  |  | v |  |  | m= |
| A2 | v |  |  |  | v | m= |
| A3 |  |  |  | v |  | m= |
| A4 |  | v |  |  |  | m= |
| A5 | v |  | v |  | v | m= |
| A6 |  |  | v |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 16 |  |  |
| A2 | 5 |  |  |
| A3 | 23 |  |  |
| A4 | 7 |  |  |
| A5 | 11 |  |  |
| A6 | 9 |  |  |
| Подсчет: |  |  |  |

**Вариант №9. Дано: p= 19; q= 5.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  |  | v |  |  | m= |
| A2 | v |  |  |  | v | m= |
| A3 |  |  | v |  |  | m= |
| A4 |  | v |  |  |  | m= |
| A5 | v |  |  | v |  | m= |
| A6 |  |  | v |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 19 |  |  |
| A2 | 5 |  |  |
| A3 | 13 |  |  |
| A4 | 7 |  |  |
| A5 | 11 |  |  |
| A6 | 19 |  |  |
| Подсчет: |  |  |  |

**Вариант №10. Дано: p= 11; q= 23.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  | v | v |  |  | m= |
| A2 | v |  |  |  | v | m= |
| A3 | v |  | v |  | v | m= |
| A4 |  | v |  |  |  | m= |
| A5 | v |  |  | v | v | m= |
| A6 |  |  |  |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 19 |  |  |
| A2 | 12 |  |  |
| A3 | 15 |  |  |
| A4 | 2 |  |  |
| A5 | 11 |  |  |
| A6 | 9 |  |  |
| Подсчет: |  |  |  |

**Вариант №11. Дано: p=17; q=13.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  | v | v |  |  | m= |
| A2 | v |  |  |  | v | m= |
| A3 |  | v |  |  |  | m= |
| A4 |  | v |  |  |  | m= |
| A5 | v | v |  | v |  | m= |
| A6 |  |  | v |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 18 |  |  |
| A2 | 7 |  |  |
| A3 | 23 |  |  |
| A4 | 4 |  |  |
| A5 | 11 |  |  |
| A6 | 9 |  |  |
| Подсчет: |  |  |  |

**Вариант №12. Дано: p= 3; q= 23.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  |  | v |  |  | m= |
| A2 | v |  |  | v | v | m= |
| A3 |  |  | v |  |  | m= |
| A4 |  | v | v |  |  | m= |
| A5 | v |  |  | v |  | m= |
| A6 |  | v |  |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 19 |  |  |
| A2 | 12 |  |  |
| A3 | 13 |  |  |
| A4 | 5 |  |  |
| A5 | 11 |  |  |
| A6 | 9 |  |  |
| Подсчет: |  |  |  |

**Вариант №13. Дано: p= 2; q=11.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  |  | v |  |  | m= |
| A2 |  | v |  |  | v | m= |
| A3 |  |  |  |  | v | m= |
| A4 |  | v |  |  | v | m= |
| A5 | v |  |  | v |  | m= |
| A6 |  |  | v |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 13 |  |  |
| A2 | 12 |  |  |
| A3 | 19 |  |  |
| A4 | 7 |  |  |
| A5 | 11 |  |  |
| A6 | 9 |  |  |
| Подсчет: |  |  |  |

**Вариант №14. Дано: p= 17; q=5.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  | v | v |  |  | m= |
| A2 |  |  |  |  |  | m= |
| A3 |  | v | v |  |  | m= |
| A4 |  | v |  |  | v | m= |
| A5 | v |  |  | v |  | m= |
| A6 |  |  |  |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 16 |  |  |
| A2 | 12 |  |  |
| A3 | 13 |  |  |
| A4 | 5 |  |  |
| A5 | 11 |  |  |
| A6 | 9 |  |  |
| Подсчет: |  |  |  |

**Вариант №15. Дано: p=19; q= 7.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  |  | v |  |  | m= |
| A2 | v |  |  |  | v | m= |
| A3 | v |  |  |  | v | m= |
| A4 | v |  |  | v |  | m= |
| A5 | v |  |  | v |  | m= |
| A6 |  |  | v |  |  | m= |
| Итог: |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 7 |  |  |
| A2 | 16 |  |  |
| A3 | 13 |  |  |
| A4 | 21 |  |  |
| A5 | 11 |  |  |
| A6 | 9 |  |  |
| Подсчет: |  |  |  |