**Лабораторная работа №10**

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

**Цель лабораторной работы:** изучение принципов построения системы электронного голосования на основе криптосистемы Пэйе и анализ выполнения требований по обеспечению ее безопасности.

**Теоретические сведения:**

Система электронного голосования должна удовлетворять следующим требованиям:

1.Участвовать в выборах могут только те легитимные пользователи, которые были предварительно включены в списки, составленные *избирательной комиссией* (ИК);

2. Результат голосования каждого легитимного участника должен сохраняться в тайне от всех участников процедуры голосования (в том числе от других легитимных пользователей, ИК и всех посторонних), за исключением, конечно, самого подавшего голос;

3. Результат голосования каждого участника должен быть правильно учтен ИК и учтен лишь единожды;

4. При отсутствии легитимного избирателя в списке ИК или при неправильном учете результатов голосования в ИК, эти ошибки должны быть исправлены без нарушения тайны голосования;

5. ИК не может сфальсифицировать результаты тех легитимных избирателей, которые не захотели принять участие в голосовании.

Напомним, что эта система шифрования обладает аддитивным гомоморфным свойством. Так как при дешифровании произведения двух шифротекстов будет получена сумма соответствующих им открытых текстов:

;

Используя КС Пэйе, можно организовать выборы между несколькими кандидатами, используя следующую схему:

Предположим, что *Nv-* число избирателей, а *Nc* - число кандидатов. Сначала необходимо перевести каждый голос избирателя в числовую форму и зашифровать их с помощью шифрования Пэйе. Голос, поданный за того или иного кандидата, будет обозначаться числами следующим образом: 1-ый кандидат - число *,* 2-ой кандидат- число *,* … - й кандидат- число Тогда максимальное возможное число mmax =(если избиратель выбрал всех кандидатов). Отсюда следует что, максимально возможная сумма всех голосов в системе:(случай, когда все избиратели сделали выбор в пользу всех кандидатов).

Далее выполняются три основных шага алгоритма шифрования голоса:

**Генерация ключа (избирательная комиссия):**

Выбираются два простых больших числа , такие, что наибольший общий делитель и *,* где

Выбирается случайное число  и .

*(n,g)-* открытый ключ.

Закрытым ключом будет являться пара (: для этого вычисляются и  *,* где *,* гденаибольшее целое число, удовлетворяющее .

**Шифрование:**

Каждый избиратель шифрует свой голос

*E(mi)= ci =,* где *r Z\*n*

и отправляет криптограмму на сервер.

Даже если два разных избирателя проголосовали за одного и того же кандидат, их зашифрованные голоса будут отличаться друг от друга, так как число *r* случайно генерируется и используется в каждом шифровании.

Сервер в конце выборов имеет не более –криптограмм ,соответствующих голосам. Он производит вычисления над зашифрованными данными:

(количествовсех зашифрованных данных по модулю ) и отправляет в избирательную комиссию.

**Дешифрование**

Дешифрование криптограммы произведения Т осуществляется избирательной комиссией. Согласно гомоморфному свойству криптосистемы Пэйе:

*D(T)= =,* где расшифрование *T.* Расшифрование выполняется по формуле *.*

Далей число ** представляется в b-ичной системе счисления и по коэффициентам разрядов этого числа определяются кандидаты-победители.

**Пример выполнения процедуры голосования:**

Предположим, что имеется 9 избирателей и 5 кандидатов , тогда , .

Если мы обозначим систему счисления, которую мы используем для шифрования сообщений, как число , тогда должно быть выполнено следующее условие: *b* > *.*

Определим, что . По условиям избирательной Комиссии осуществляется выбор двух новых членов студсовета. Предпочтительным является выбор двух кандидатов, однако возможны варианты выбора одного кандидата или же оставление бюллетеня пустым. Сообщения, которые должны быть зашифрованы, показаны в следующей таблице:

**Таблица 6. Пример заполнения бюллетеня избирателей.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Избиратель** | **B1**  **(100)** | **B2**  **(101)** | **B3**  **(102)** | **B4**  **(103)** | **B5**  **(104)** | **Голос (m)** |
| A1 |  | v |  |  |  | m=101=10 |
| A2 |  |  | v |  | v | m=102 +104=10100 |
| A3 |  |  |  |  |  | m=0 |
| A4 |  |  |  | v |  | m=103=1000 |
| A5 | v |  |  | v |  | m=100+103=1001 |
| A6 |  | v |  | v |  | m=101+103=1010 |
| A7 |  |  | v | v |  | m=102+103=1100 |
| A8 |  | v |  | v |  | m=101+103=1010 |
| A9 | v |  |  |  |  | m=100=1 |
| Итог: | 2 | 3 | 2 | 5 | 1 |  |

Максимальное возможное число сообщений, которые можно зашифровать:

*mmax =*  . Следовательно, максимально возможная сумма всех голосов: *Tmax = Nv\* mmax* = . По условию Tmax*; ;*

Предполагается, что числа  и имеют одинаковую длину.

*Генерация ключей:*

Для генерирования ключа выберем случайным образом два простых больших числа и , где

Вычисляем , ;

Используем случайно сгенерированное число *Z\*n*, удовлетворяющее условию  *.*

*=*  mod 16095743161- -1 .

*Шифрование:*

Зашифруем сообщения, содержащие выбор избирателей: *E(mi)= ci ==*  16095743161 *r Z\*n..*

**Таблица 7. Результат шифрования голосов избирателей.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Избиратель** | **Случайное число**  **(ri)** | **Голос (m)** | **Зашифрованное значение голоса (ci)** |
| A1 | 35145 | m=101=10 | 13039287935 |
| A2 | 74384 | m=102 +104=10100 | 848742150 |
| A3 | 96584 | m=0 | 7185465039 |
| A4 | 10966 | m=103=1000 | 80933260 |
| A5 | 17953 | m=100+103=1001 | 722036441 |
| A6 | 7292\* | m=101+103=1010 | 350667930 \* |
| A7 | 24819 | m=102+103=1100 | 4980449314 |
| A8 | 4955\* | m=101+103=1010 | 7412822644 \* |
| A9 | 118037 | m=100=1 | 3033281324 |
| Подсчет: |  | 23251 |  |

Вычислим произведение криптограмм:

*T=*

*Дешифрование:*

*=\**53022

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.

В силу гомоморфности криптосистемы индекс максимального элемента результирующего вектора и будет индексом победившего кандидата. Следовательно, можно сделать вывод о том, что победителями электронных выборов являются кандидаты B2 и B4.

**Порядок выполнения работы:**

1. Провести моделирование работы системы электронного голосования на основе криптографической системы Пэйе, согласно варианту задания.
2. Определить победивших кандидатов
3. Результаты представить в виде отчета.

**Примечание**. Основание системы счисления выбрать равным b=Nv+1

**Содержание отчета:**

Лабораторная работа оформляется в виде отчета с указанием фамилии, группы и варианта студента. Он должен содержать следующие пункты:

1. Цель работы.
2. Исходные данные (таблица с выбором кандидатов).

**Примечание**. Основание системы счисления выбрать равным b=Nv+1.

1. Подробное описание процедур шифрования/дешифрования с пояснениями каждого шага, объявлением победивших кандидатов и указанием исполнителей избирательной процедуры.
2. Выводы о проделанной работе.
3. Ответы на контрольные вопросы.

**Контрольные вопросы:**

1. Какими свойствами гомоморфности обладает КС Пэйе?
2. Перечислите кратко основные требования к системе электронного голосования?
3. Назовите основные преимущества электронных выборов?
4. Каким образом обеспечивается анонимность избирателя с использованием системы шифрования Пэйе?
5. Каким образом обеспечивается тайна выбора избирателя в этой системе голосования?
6. Проведите анализ выполнения требований к системе голосования, перечисленных в задании, и подробно опишите, какие из них выполняются, а какие нет. Что бы Вы предложили для выполнения всех требований?

**ПРИЛОЖЕНИЕ Б**

**Варианты заданий для лабораторной работы:**

**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: |  |  |  |