**Лабораторная работа №8**

**«Изучение системы шифрования Пэйе и ее гомоморфных свойств»**

**Цель работы:** Закрепление теоретических знаний, приобретение навыков шифрования и дешифрования информации с помощью КС Пэйе и изучение его гомоморфных свойств.

**Теоретические сведения:**

Функция шифрования гомоморфна относительно операции над открытыми текстами, если существует эффективный алгоритм , который получив на вход любую пару криптограмм вида выдает криптограмму такую, что при ее дешифровании будет получен открытый текст .

В лабораторной работе исследуется криптосистема Пэйе, являющейсянедетерминированной схемой с открытым ключом.

Используемые математические понятия:

1. *Наибольшим общим делителем* двух чисел *a* и *b* называется такое наибольшее число *d*, которое делит оба этих числа*.* Наибольший общий делитель двух чисел обозначается обычно как , а иногда просто (*a,b).*
2. Целые числа а и b называются взаимно простыми, если их наибольший общий делитель равен 1. Например, числа 9 и 28 являются взаимно простыми.
3. *Наименьшее общее кратное* (lcm) двух или более целых положительных чисел - это наименьшее целое число, которое делится на каждый член набора чисел без остатка. Примечание:, поэтому .
4. Пусть *п* – целое натуральное число, тогда *функцией Эйлера*называется количество целых не отрицательных чисел, меньших *п* и взаимно простых с *п*, т. е.:

, где означает количество элементов множества *Х*. Легко проверить, что , , если *р* – простое число. Например, φ (9) = 6, так как шесть чисел 1, 2, 4, 5, 7 и 8 взаимно просты, исключая число 9. Если n можно разложить на различные простые числа p и q, то ); Например, .

1. *Мультипликативно обратное целое число по модулю m* для элемента *a* является целое число такое, что , эквивалентно . Мультипликативно обратный элемент по модулю *m* существует тогда и только тогда, когда a и m взаимно простые,

т.е. gcd(a, m) = 1.

***Алгоритм шифрования данных с помощью КС Пэйе***

*Генерация ключей:* выбираются два больших простых числа *p* и *q,* такие что .

Вычисляется *q*  Выбирается случайное целое число *g*, такое что *g* ∈

Вычисляется , где u – наибольшее целое число, удовлетворяющее

Принимаем в качестве открытого ключа пару (*n*, *g*), а закрытого -

Стоит отметить, что при использовании эквивалентной длины, нахождение элементов для генерация ключей происходит по следующему принципу: *g= n+1*, , , где .

*Шифрование* :

Предположим, что необходимо зашифровать открытый текст где . Выбираем случайное число *k* ∈ и вычисляем криптограмму:

*gm .*

*Дешифрование* криптограммы :

*Гомоморфные свойства:*

Криптосистема обладает следующими свойствами гомоморфности:

1. при дешифровании произведения двух шифротекстов будет получена сумма соответствующих им открытым текстам:

;

1. при дешифровании криптограммы, возведенной в степень , будет получено произведение открытого текста и показателя степени d:

.

**Задание на лабораторную работу**

Вручную произвести шифрование и дешифрование сообщения согласно криптосистеме Пэйе, используя значения, представленные в таблице. В качестве проверки необходимо использовать соответствующий программный продукт, и предоставить скриншоты, получившихся результатов. Обратите внимание, что числа необходимо сгенерировать случайным образом в программе.

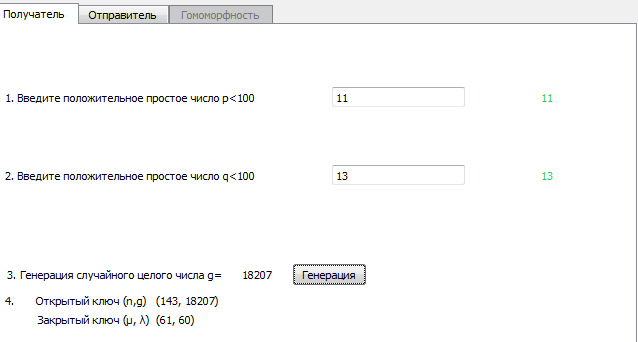
**Таблица 5. Варианты задания для выполнения лабораторной работы.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nвар** | ***p*** | ***q*** | ***M*** |
| 13 | 7 | 5 | 8 |
| 14 | 19 | 7 |
| 15 | 5 | 19 |
| 16 | 23 | 5 | 22 |
| 17 | 11 | 3 |
| 18 | 29 | 3 |
| 19 | 19 | 5 | 7 |
| 20 | 5 | 29 |
| 21 | 3 | 11 |
| 22 | 17 | 13 | 18 |
| 23 | 23 | 3 |
| 24 | 5 | 13 |
| 25 | 3 | 23 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Nвар** | ***p*** | ***q*** | ***M*** |
| 1 | 5 | 7 | 13 |
| 2 | 19 | 11 |
| 3 | 13 | 17 |
| 4 | 17 | 3 | 11 |
| 5 | 11 | 7 |
| 6 | 7 | 13 |
| 7 | 13 | 19 | 16 |
| 8 | 7 | 17 |
| 9 | 5 | 3 |
| 10 | 11 | 13 | 14 |
| 11 | 7 | 23 |
| 12 | 5 | 17 |

**Пример выполнения лабораторной работы:**

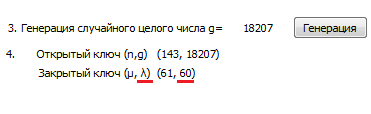
1. Запуск программы «Paillier.exe»
2. *Генерация ключей:* вводим параметры *p* и *q*, которые находятся в диапазоне [1... 100]. Напомним, что для генерации ключа эти числа должны быть простыми. Если при вводе число отображается красным цветом, значит, оно не является простым. Предположим, что



**Рисунок 3.1 Генерация ключа.**

Далее нажимаем на поле «Генерация» и получаем значение случайного числа . После выполнения этих действий происходит вычисление параметров открытого и закрытого ключей, которые будут использованы для шифрования и дешифрования сообщения. В нашем примере , а значения

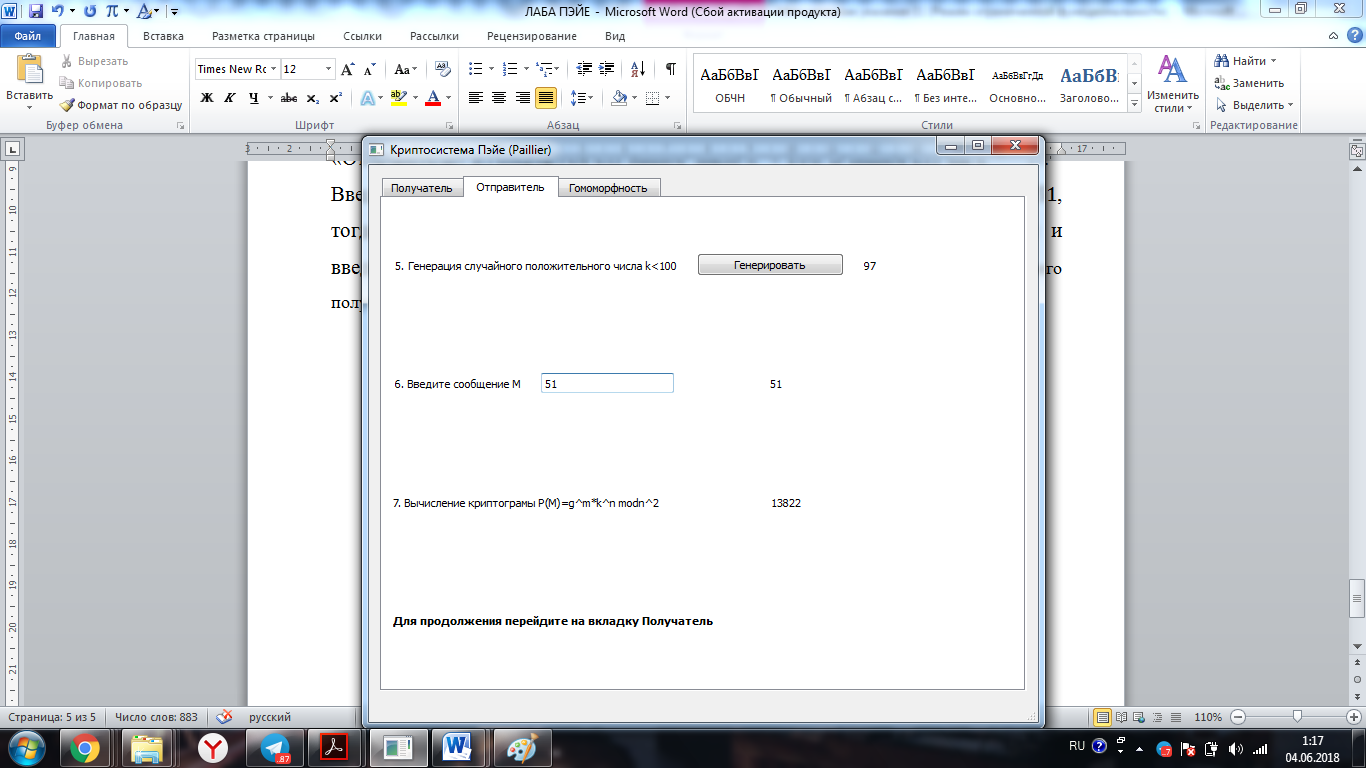
Перед выполнением следующего пункта необходимо обратить внимание на значение закрытого ключа, если , то следует повторно нажать кнопку «Генерация» для изменения параметра.

**

**Рисунок 3.2 Параметр закрытого ключа.**

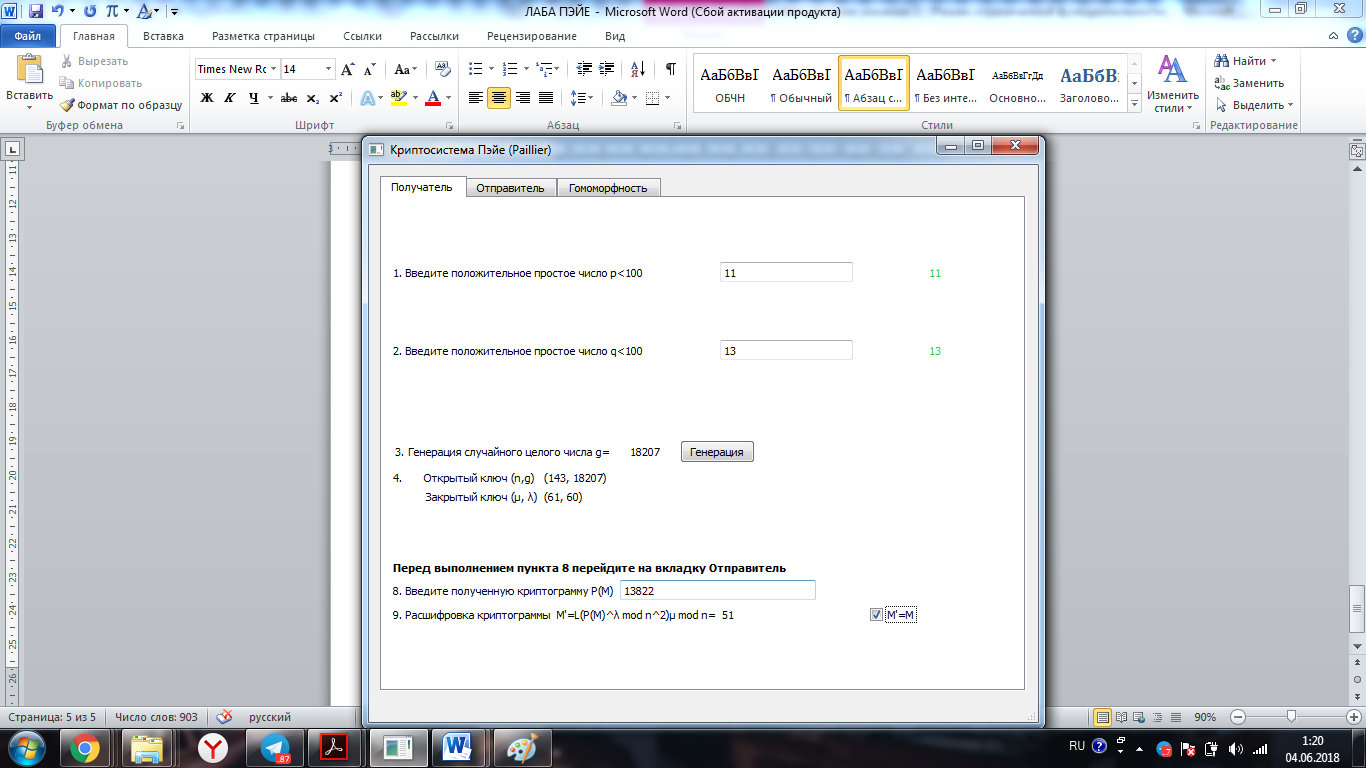
1. *Шифрование:* для получения криптограммы переходим на вкладку «Отправитель» и генерируем случайное число *.* В нашем случае *.*

Введем значение сообщения *,* которое нужно зашифровать. Допустим, , тогда с помощью открытого ключа , сгенерированного значения и введенного , вычисляется криптограмма:  *gm .*  В результате чего получаем .



**Рисунок 3.3 Процедура шифрования сообщения.**

1. *Дешифрование:* после получения переходим на вкладку «Получатель» и в пункте 8 вводим значение получившейся криптограммы для дальнейшего расшифрования.



**Рисунок 3.4 Процедура дешифрования сообщения.**

Как видим, значение дешифрованного сообщения равно истинному значению , поэтому ставим галочку рядом с этим тождеством и переходим к проверке гомоморфных свойств.

1. *Проверка гомоморфности криптосистемы Пэйе.*

Убедиться, что данная криптосистема обладает двумя свойствами гомоморфности.

Первое свойство, заключается в следующем: криптограмму можно возвести в степень и дешифровать, что равносильно умножению сообщения на эту константу

Для проверки этого свойства выбрать сообщение m и число r. Зашифровать m по схеме Пейе. Найти  (для выполнения операции возведения числа в степень использовать калькулятор экспонент в ЛР «Анализ системы РША»). Дешифровать () по схеме Пэйе. Сравнить полученный результат с числом . Совпадение свидетельствует о выполнении первого свойства гомоморфности.

Согласно второму свойству, при дешифровании произведения двух криптограмм будет получена сумма соответствующих им открытых сообщений:

Чтобы выполнить проверку данного свойства необходимо: Выбрать два сообщения m1 и m2 и зашифровать их по схеме Пэйе на одном и том же ключе. Далее перемножить криптограммы Расшифровать криптограмму-произведение Полученный результат сравнить с суммой Совпадение будет свидетельствовать о выполнении второго свойства гомоморфности КС Пэйе.

**Содержание отчёта:**

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

1. Цель и назначение работы.
2. Исходные данные, подробные результаты расчетов с пояснениями назначения каждого шага, а так же скриншоты программы, подтверждающие их правильность.
3. При проверке свойств гомоморфности числа m1, m2,r должны быть новыми (не используемыми в предыдущих пунктах работы) и явно записанными.
4. Выводы о проделанной работе.

**Контрольные вопросы:**

1. Что такое гомоморфное шифрование?
2. Что такое функция Эйлера?
3. Как проверить, что число *р*простое?
4. Каким образом генерируются ключи в криптосистеме Пэйе?
5. Чем определяется стойкость исследуемой криптосистемы?
6. Какими гомоморфными свойствами обладает данная система шифрования?