**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 № 9

**ИЗУЧЕНИЕ CИСТЕМЫ ШИФРОВАНИЯ ПЭЙЕ И ЕЁ ГОМОМОРФНЫХ СВОИСТВ**

Выполнил: ст. г. ИКТЗ-83

Громов А. А.

Проверил: Яковлев В. А.

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

Цель лабораторной работы:

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

Исходные данные:

Вариант 4: p = 17, q = 3, M = 11

**Выполнение работы:**

**Генерация ключей:**

Вычислим n = p\*q = 17\*3 = 51 и

g = 11

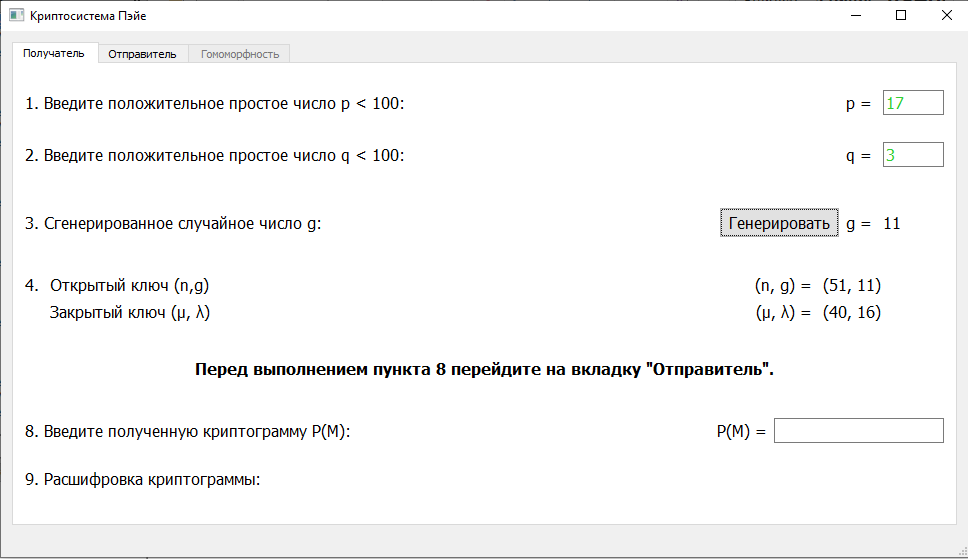


Рис. 1 Генерация g и формирование ключей

Вычислим , где u – наибольшее целое число, удовлетворяющее

Проведем вычисления с помощью программы wxMaxima

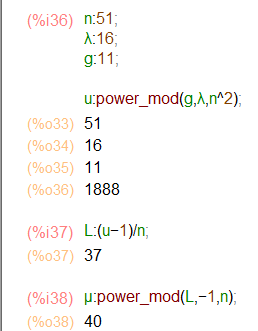


Рис. 2 – Вычисление

**Шифрование:**

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

k = 44

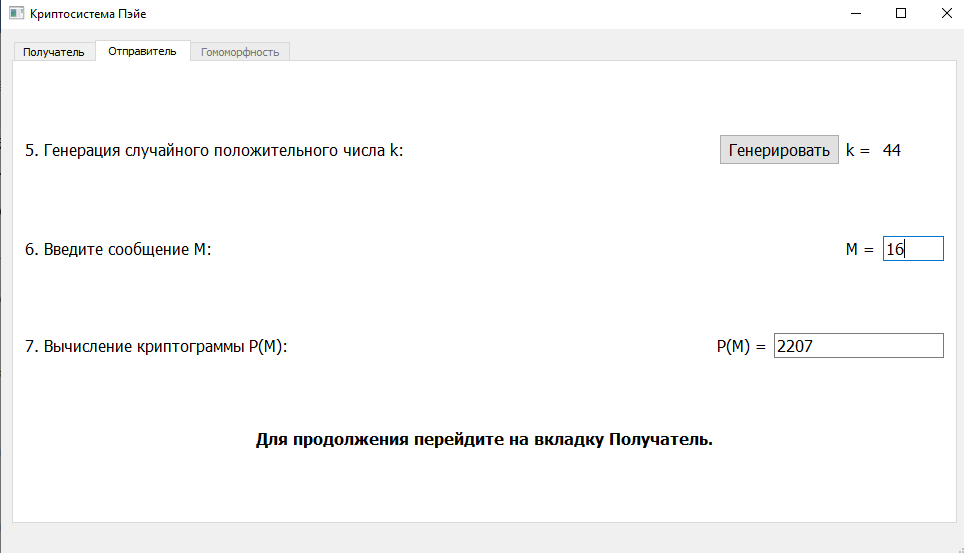


Рис. 3 – Генерация k и формирование криптограммы

*gm .*

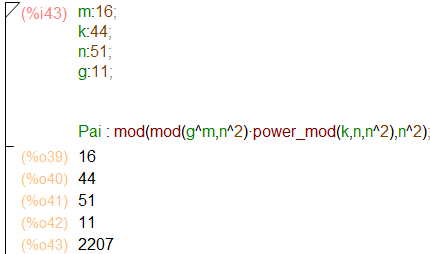


Рис. 4 – Вычисление криптограммы

**Дешифрование:**

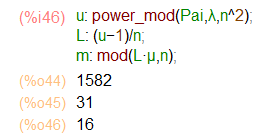


Рис. 5 – Дешифрование криптограммы

В результате дешифрования было получено исходное сообщение m = 16

Проверим его в программе «КС Пэйе»



Рис. 5 – Проверка расшифровки

Дешифрование произведено корректно

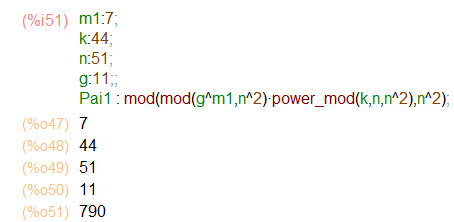
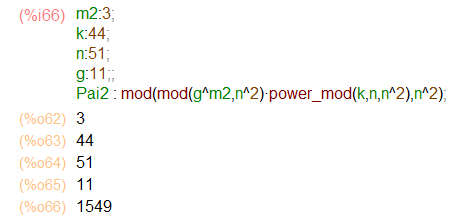
**Гомоморфные свойства:**

Для проверки гомоморфных свойств положим m1 = 7 и m2 =3 и зашифруем их по вышеизложенному алгоритму, при этом оставим остальные параметры неизменными

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

;

Сначала вычислим криптограммы

Рис. 6 – Криптограмма Рис. 7 – Криптограмма

Вычислим

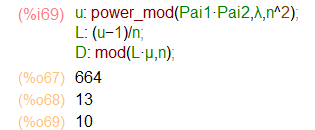


Рис. 8 – Дешифрование (Результат = 10)

Сравним результат предыдущего шага с



Рис. 9 – Вычисление модуля суммы сообщений

В результате вычислений было подтверждено выполнение условия

Утверждение 2. при дешифровании криптограммы, возведенной в степень , будет получено произведение открытого текста и показателя степени d: .

Пусть d = 4 и m = 25

Вычислим криптограмму

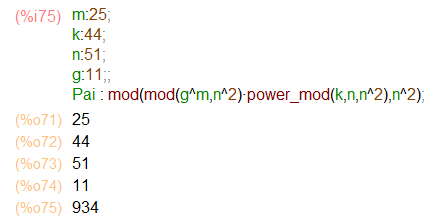


Рис. 10 – Вычисление криптограммы

Определим

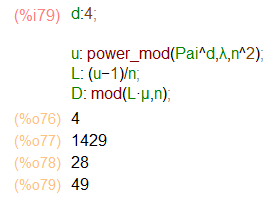


Рис. 11 – Определение

Проверим, вычислив



Рис. 12 – Проверка

По итогам подсчетов было выполнено условие = 49.

Подтвердим расчеты в программе «КС Пэйе»

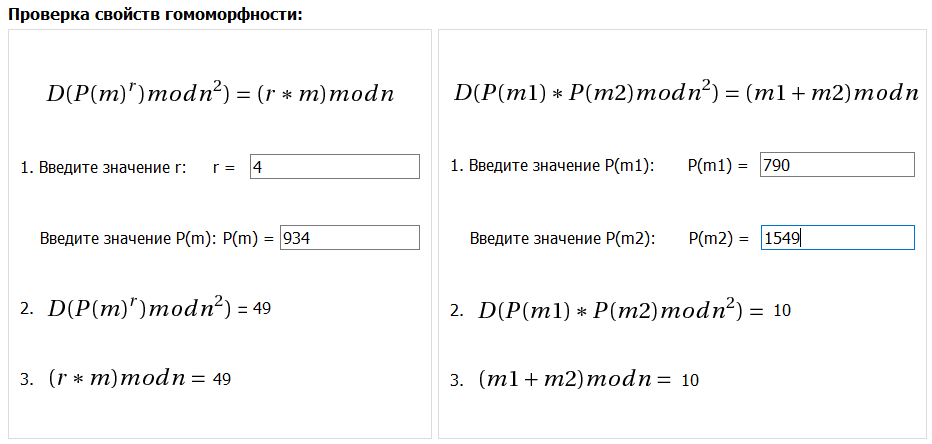


Рис. 12 – Проверка свойств гомоморфности

**Вывод:**

В результате выполнения данной лабораторной работы была изучена криптосистема Пэйе и её гомоморфные свойства. Были произведены шифрование и дешифрование сообщения, а также доказаны свойства гомоморфности.