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 СИСТЕМЫ ШИФРОВАНИЯ ПЭЙЕ И ЕЁ ГОМОМОРФНЫХ СВОИСТВ

Выполнил: ст. г. ИКТЗ-83

Громов А. А.

Проверил: Яковлев В. А.

____

Санкт-Петербург
2021

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 $\lambda = lcm(p-1, q-1) = lcm(16,2) = 16$

g = 11

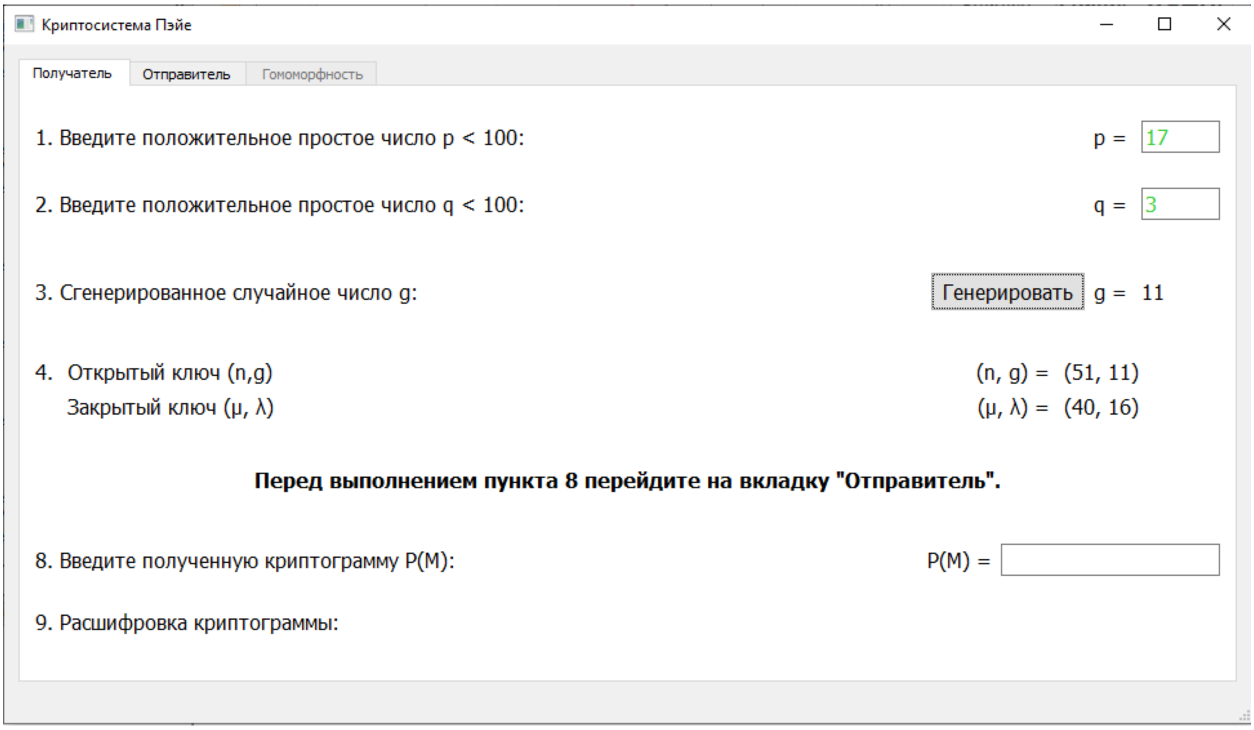

Рис. 1 Генерация g и формирование ключей

Вычислим $\mu = \left[L\left(g^{\lambda} mod n^2\right)\right]^{-1}$, где $L(u) = \left[\frac{u-1}{n}\right]$, u – наибольшее целое число, удовлетворяющее $u - 1 \geq x \cdot n$

Проведем вычисления с помощью программы wxMaxima

```
(%i36) n:51;
       λ:16;
       g:11;

       u:power_mod(g,λ,n^2);
(%o33) 51
(%o34) 16
(%o35) 11
(%o36) 1888

(%i37) L:(u−1)/n;
(%o37) 37

(%i38) μ:power_mod(L,−1,n);
(%o38) 40
```

Рис. 2 – Вычисление μ

$$\mu = 40$$

Шифрование:

Предположим, что необходимо зашифровать открытый текст m, где $m \in Z_n$. Выбираем случайное число $k \in Z_n^*$ и вычисляем криптограмму:

k = 44

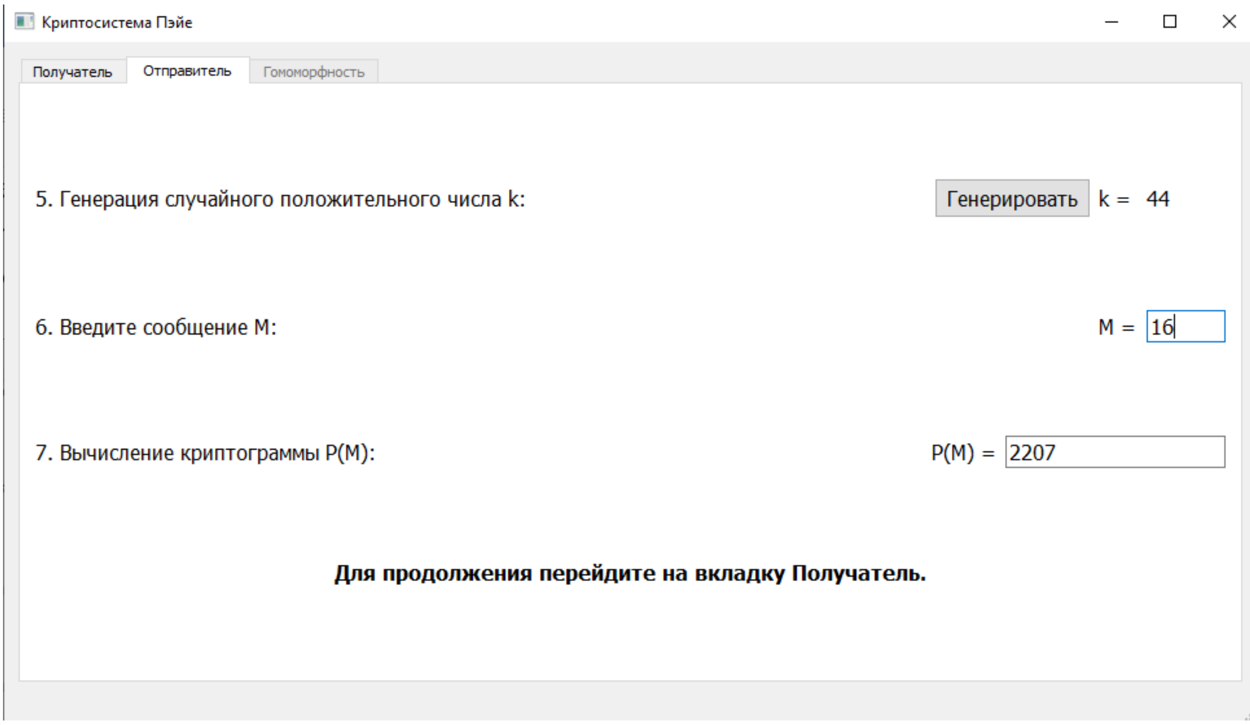

Рис. 3 – Генерация k и формирование криптограммы

$Pai(m) = c = g^m \cdot k^n \ (mod\ n^2).$

```
(%i43) m:16;
       k:44;
       n:51;
       g:11;


       Pai : mod(mod(g^m,n^2)·power_mod(k,n,n^2),n^2);
(%o39) 16
(%o40) 44
(%o41) 51
(%o42) 11
(%o43) 2207
```

Рис. 4 – Вычисление криптограммы

Дешифрование:

$$m = L\,(c^{\lambda}\,mod\;n^2)\,*\,\mu\,mod\;n.$$

```
(%i46) u: power_mod(Pai,λ,n^2);
       L: (u−1)/n;
       m: mod(L·μ,n);
(%o44) 1582
(%o45) 31
(%o46) 16
```

Рис. 5 – Дешифрование криптограммы

В результате дешифрования было получено исходное сообщение m = 16

Проверим его в программе «КС Пэйе»

8. Введите полученную криптограмму P(M):	P(M) = 2207
9. Расшифровка криптограммы:	16

Рис. 5 – Проверка расшифровки

Дешифрование произведено корректно

Гомоморфные свойства:

Для проверки гомоморфных свойств положим $m_1 = 7$ и $m_2 = 3$ 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:

$$D(Pai(m_1)\cdot Pai(m_2) mod\;n^2) = (m_1 + m_2) mod\;n;$$

Сначала вычислим криптограммы $Pai(m_1)$и $Pai(m_2)$

```
(%i51) m1:7;
       k:44;
       n:51;
       g:11;;
       Pai1 : mod(mod(g^m1,n^2)·power_mod(k,n,n^2),n^2);
(%o47) 7
(%o48) 44
(%o49) 51
(%o50) 11
(%o51) 790
```

Рис. 6 – Криптограмма $Pai(m_1) = 790$

```
(%i66) m2:3;
       k:44;
       n:51;
       g:11;;
       Pai2 : mod(mod(g^m2,n^2)·power_mod(k,n,n^2),n^2);
(%o62) 3
(%o63) 44
(%o64) 51
(%o65) 11
(%o66) 1549
```

Рис. 7 – Криптограмма $Pai(m_2) = 1549$

Вычислим $D(P(m_1) \cdot P(m_2) mod\ n^2)$

```
(%i69) u: power_mod(Pai1·Pai2,λ,n^2);
       L: (u−1)/n;
       D: mod(L·μ,n);
(%o67) 664
(%o68) 13
(%o69) 10
```

D

Рис. 8 – Дешифрование (Результат = 10)

Сравним результат предыдущего шага с $(m_1 + m_2) mod\ n$

```
(%i70) mod(m1+m2,n);
(%o70) 10
```

Рис. 9 – Вычисление модуля суммы сообщений

В результате вычислений было подтверждено выполнение условия $(Pai(m_1) \cdot Pai(m_2) mod\ n^2) = (m_1 + m_2) mod\ n = 10$

Утверждение 2. при дешифровании криптограммы, возведенной в степень $d \epsilon Z_n^*$, будет получено произведение открытого текста и показателя степени d: $D(Pai(m))^d mod\, n^2 = d \cdot m\, modn.$

Пусть d = 4 и m = 25

Вычислим криптограмму $Pai(m)$

```
(%i75) m:25;
       k:44;
       n:51;
       g:11;;
       Pai : mod(mod(g^m,n^2)·power_mod(k,n,n^2),n^2);
(%o71) 25
(%o72) 44
(%o73) 51
(%o74) 11
(%o75) 934
```

Рис. 10 – Вычисление криптограммы

Определим $D(Pai(m))^d mod\, n^2$

```
(%i79) d:4;

       u: power_mod(Pai^d,λ,n^2);
       L: (u−1)/n;
       D: mod(L·μ,n);
(%o76) 4
(%o77) 1429
(%o78) 28
(%o79) 49
```

Рис. 11 – Определение $D(Pai(m))^d mod\, n^2 = 49$

Проверим, вычислив $d \cdot m\, modn$

```
(%i80) mod(d·m,n);
(%o80) 49
```

Рис. 12 – Проверка

По итогам подсчетов было выполнено условие $D(Pai(m))^d mod\, n^2 = d \cdot m\, modn$ = 49.

Подтвердим расчеты в программе «КС Пэйе»

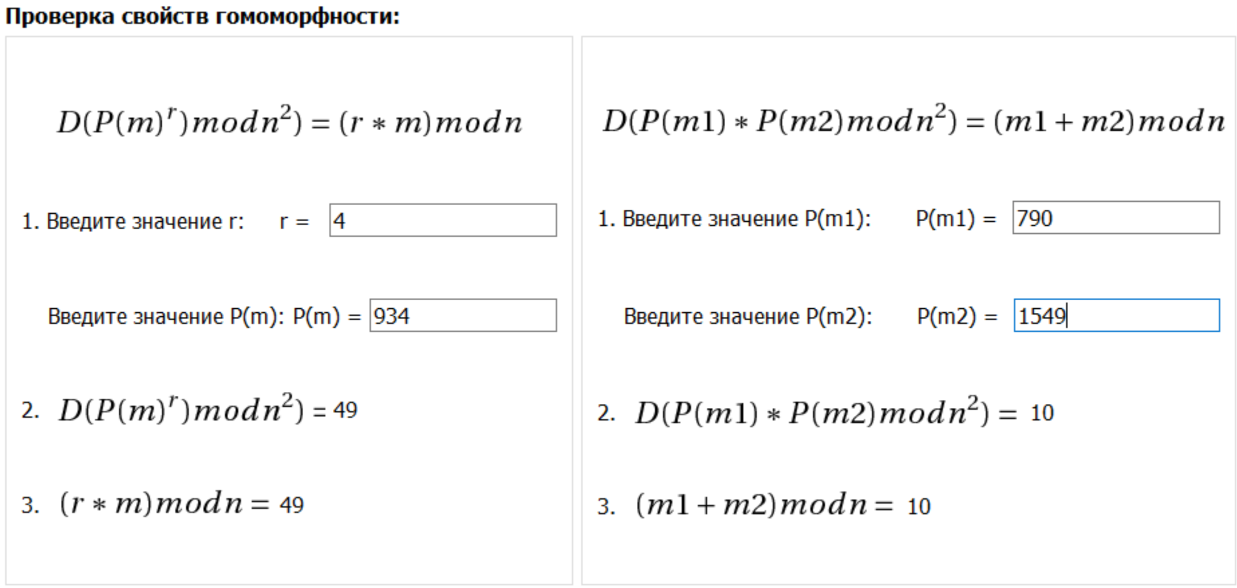

Рис. 12 – Проверка свойств гомоморфности

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.