

**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 СВОЙСТВ**

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 Пэе и изучение его гомоморфных свойств.

Исходные данные:

Вариант 4: $p = 17$, $q = 3$, $M = 11$

Выполнение работы:

Генерация ключей:

Вычислим $n = p \cdot q = 17 \cdot 3 = 51$ и $\lambda = \text{lcm}(p - 1, q - 1) = \text{lcm}(16, 2) = 16$
 $g = 11$

Криптосистема Пэе

Получатель Отправитель Гомоморфность

1. Введите положительное простое число $p < 100$: $p = 17$

2. Введите положительное простое число $q < 100$: $q = 3$

3. Сгенерированное случайное число g : Генерировать $g = 11$

4. Открытый ключ (n, g) $(n, g) = (51, 11)$
Закрытый ключ (μ, λ) $(\mu, \lambda) = (40, 16)$

Перед выполнением пункта 8 перейдите на вкладку "Отправитель".

8. Введите полученную криптограмму $P(M)$: $P(M) =$

9. Расшифровка криптограммы:

Рис. 1 Генерация g и формирование ключей

Вычислим $\mu = [L(g^{\lambda} \bmod n^2)]^{-1}$, где $L(u) = \left\lfloor \frac{u-1}{n} \right\rfloor$, 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:

$k = 44$

Криптосистема Пэйе

Получатель Отправитель Гомоморфность

5. Генерация случайного положительного числа k: Генерировать k = 44

6. Введите сообщение M: M = 16

7. Вычисление криптограммы P(M): P(M) = 2207

Для продолжения перейдите на вкладку Получатель.

Рис. 3 – Генерация k и формирование криптограммы
 $Pai(m) = c = g^m \cdot k^n \pmod{n^2}$.

```

(%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:

$$m = L (c^\lambda \bmod n^2) * \mu \bmod n.$$

```

(%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 $P(M)$:

$P(M) =$

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:

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

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

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

Рис. 8 – Дешифрование (Результат = 10)

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

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

Рис. 9 – Вычисление модуля суммы сообщений

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

Утверждение 2. при дешифровании криптограммы, возведенной в степень $d \in \mathbb{Z}_n^*$, будет получено произведение открытого текста и показателя степени d : $D(Pai(m))^d \bmod n^2 = d \cdot m \bmod n$.

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 $D(Pai(m))^d \bmod n^2$

```
(%i79) d:4;  
  
u: power_mod(Pai^d,lambda,n^2);  
L: (u-1)/n;  
D: mod(L*mu,n);  
  
(%o76) 4  
(%o77) 1429  
(%o78) 28  
(%o79) 49
```

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

Проверим, вычислив $d \cdot t \bmod n$

```
(%i80) mod(d*m,n);  
(%o80) 49
```

Рис. 12 – Проверка

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

Подтвердим расчеты в программе «КС Пэё»

Проверка свойств гомоморфности:

| | |
|--|---|
| $D(P(m)^r) \bmod n^2 = (r * m) \bmod n$ | $D(P(m1) * P(m2) \bmod n^2) = (m1 + m2) \bmod n$ |
| 1. Введите значение r: r = <input type="text" value="4"/> | 1. Введите значение P(m1): P(m1) = <input type="text" value="790"/> |
| Введите значение P(m): P(m) = <input type="text" value="934"/> | Введите значение P(m2): P(m2) = <input type="text" value="1549"/> |
| 2. $D(P(m)^r) \bmod n^2 = 49$ | 2. $D(P(m1) * P(m2) \bmod n^2) = 10$ |
| 3. $(r * m) \bmod n = 49$ | 3. $(m1 + m2) \bmod n = 10$ |

Рис. 12 – Проверка свойств гомоморфности

Вывод:

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