**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 № 7

**ИЗУЧЕНИЕ КВАНТОВОГО АЛГОРИТМА ШОРА ФАКТОРИЗАЦИИ МОДУЛЯ КРИПТОСИСТЕМЫ RSA**

Выполнил: ст. г. ИКТЗ-83

Громов А.А.

Проверил: Яковлев В. А.

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

Цель лабораторной работы:

Ознакомление с квантовым алгоритмом факторизации Шора и основами квантовых вычислений, наблюдение принципа работы квантового алгоритма в симуляции. Изучение способа факторизации модуля методом поиска периода для взлома криптосистем РША.

Программное обеспечение:

Для работы используются программы QuantumSimulator.exe и ContFrac.exe из учебного каталога.

**Выполнение работы:**

1. Найти период функции , где x = 1, 2, 3…, методом простого перебора. Использовать найденный период для факторизации модуля.,

|  |  |  |
| --- | --- | --- |
| **№** |  |  |
| **4** | 2 | 21 |

Таблица 1. Функция 2x mod 21

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| ax | 1 | 2 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| ax mod 21 | 1 | 2 | 4 | 8 | 16 | 11 | 1 | 2 | 4 | 8 |

Из таблицы 1 видно, что период функции r=6, и, так как он четный, его можно представить как r=2k. Тогда получим ar = a2k = 1 mod M или a2k - 1 = 0 mod M. Таким образом, используя формулу разности квадратов, запишем (ak)2 -1 = (ak -1)(ak +1) и (ak -1)(ak +1) 0 mod M, что означает наличие общего множителя у M и (ak ±1). То есть, применив алгоритм Евклида, можно найти числа p и q как НОД(ak + 1, М) = p и НОД(ak - 1, М) = q.

Для r = 6 получим

p = НОД(23 + 1, 21) = НОД(9, 21) = 3

q = НОД(23 - 1, 21) = НОД(7, 21) = 7

Проверим: p\*q = 7\*3 = 21 = M. Факторизация модуля произведена успешно.

2. Ознакомиться с квантовой частью алгоритма Шора и выполнить квантовое возведение в степень для двух периодов. Для y = 4 составить суперпозицию состояний регистра |x⟩.

Дано , . Тогда , а состояние будет иметь вид

.

Тогда каждому фиксированному состоянию регистра соответствует последовательность значений регистра

Таблица 2. Состояния регистров

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| … | … | … | … | … | … |
|  |  |  |  |  |  |
| … | … | … | … | … | … |
|  |  |  |  |  |  |

Измерив состояние регистра согласно заданию, мы получили фиксированное состояние , которому соответствует последовательность значений x вида

*,*

где , – сдвиг относительно начала координат (нулевого состояния регистра , ). Таким образом, было рассмотрено состояние регистров на этапе выполнения квантового возведения в степень и получена суперпозиция состояний в регистре , соответствующих фиксированному состоянию регистра – .

3. Рассчитать непрерывную дробь вида , где – номер студента по варианту (для номеров 01–09 взять 31–39), – номер группы, а – сгенерированное на основе полученного знаменателя в программе CoutFrac.exe число.

В соответствии с заданием для данного варианта знаменатель непрерывной дроби имеет вид 3483. Запустим программу CountFrac.exe и сгенерируем числитель для данного знаменателя (Рис. 1):

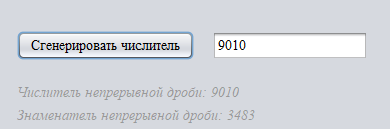


Рис. 1 Генерация числителя непрерывной дроби в соответствии со знаменателем

Выполним разложение дроби:

Алгоритм Евклида:

9010 = 3483\*2 + 2044

3483 = 2044\*1 + 1439

2044 = 1439\*1 + 605

1439 = 605\*3 + 229

605 = 229\*2 + 147

229 = 147\*1 + 82

147 = 82\*1 + 65

82 = 65\*1 + 17

65 = 17\*3 + 14

|  |  |
| --- | --- |
| |  | | --- | | [2;1,1,2,2,1,1,1,3,1,4,1,2] | |

Проверим правильность разложения дроби в программе CountFrac.exe:

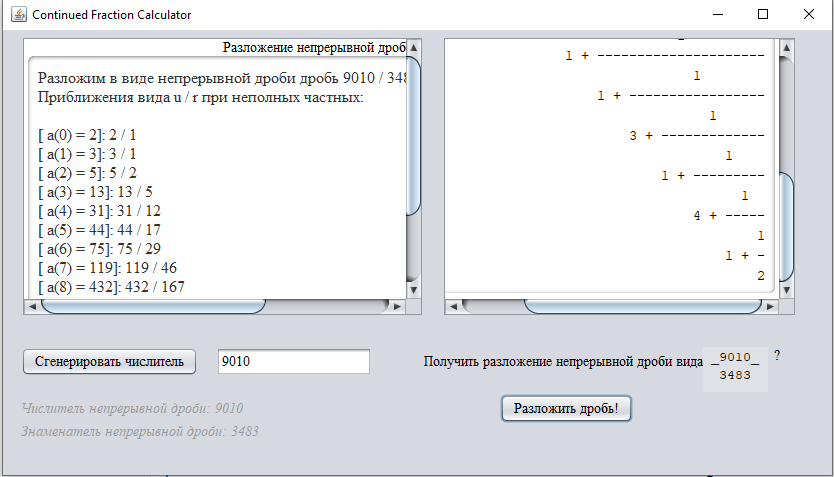


Рис. 2 Разложение непрерывной дроби в программе

После прохождения проверки путем ввода последнего знаменателя (в данном случае числа 2) можно получить результат разложения дроби с вычислением промежуточных дробей (здесь они названы приближением при неполных частных), знаменатели которых в действительной постобработке выполнения квантового алгоритма Шора могут быть периодами

4. Ознакомиться с выполнением квантового алгоритма Шора с помощью программы-симулятора QuantumSimulator.exe, проанализировать полученные результаты и сделать выводы.

Рассмотрим процесс симуляции выполнения квантового алгоритма Шора для модуля . Выбираем целое число , количество кубит, необходимое для задания размера квантовых регистров и, соответственно, в этом случае количество состояний каждого регистра (Рис. 3).

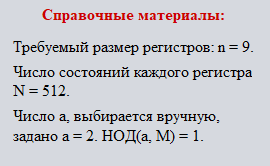


Рис. 3 Вычисленные программой справочные данные

Проверим: – верное, – верное.

В результате выполнения квантового возведения в степень для функции для всех состояний регистра , в регистре были получены следующие значения: , как можно увидеть на Рис. 4:

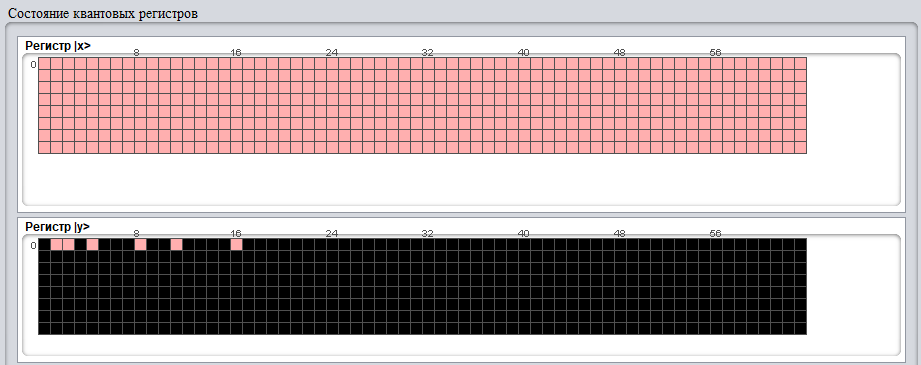
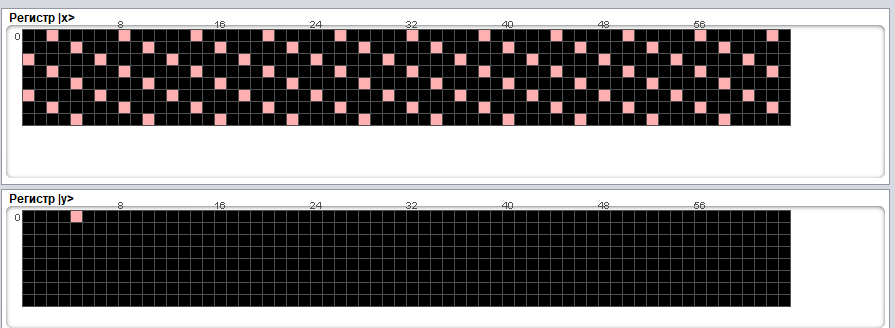


Рис. 4 Квантовое возведение в степень

В результате измерения состояния регистра было получено фиксированное значение , которому соответствует суперпозиция периодических последовательностей состояний в регистре , как можно увидеть на Рис. 5:

Рис. 5 Измерение состояния квантового регистра

Данная суперпозиция может быть описана как:

В результате применения для суперпозиции, содержащейся в регистре , квантового преобразования Фурье, были получены следующие значения {много} (Рис. 6):

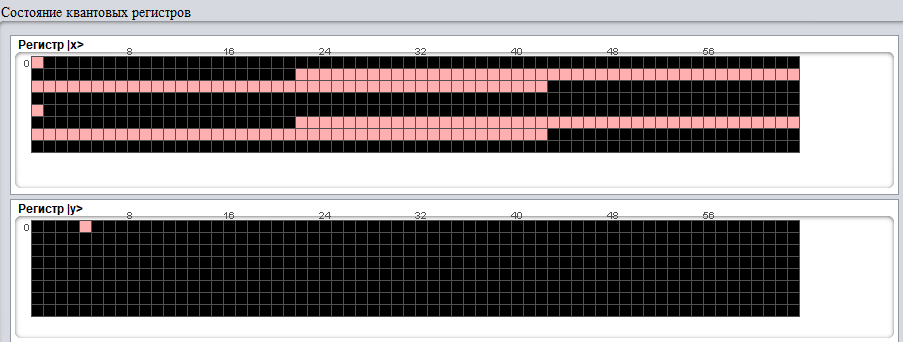


Рис. 6 Квантовое преобразование Фурье над регистром

В результате измерения состояния регистра из полученной выше последовательности значений было выбрано фиксированное значение m = 171, как можно увидеть на Рис. 7:

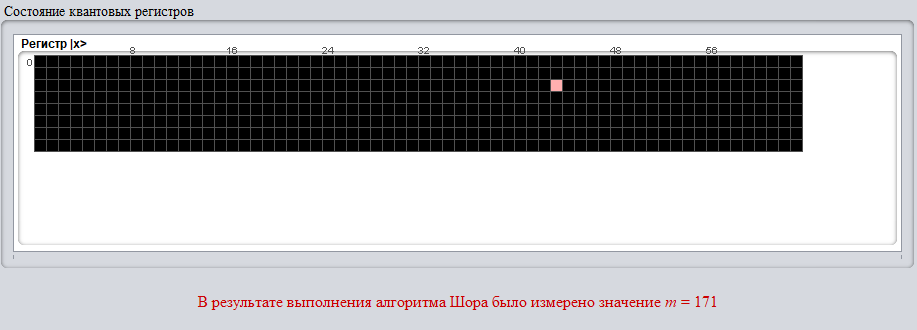


Рис. 7 Измерение состояния квантового регистра

Дробь вида передана на постобработку, выполняемую классическим компьютером. Произведено разложение непрерывной дроби и получены возможные периоды {1, 2, 3}. Из них условиям, необходимым для определения периода, удовлетворяет только r = 2: r = 2 < M – 1 = 20 и r – четное число. Можно убедиться в этом на Рис. 8

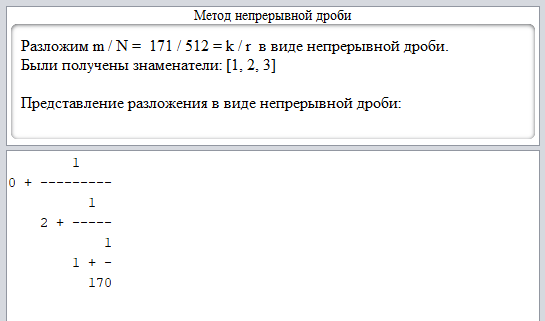
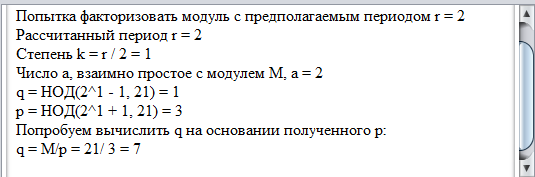


Рис. 8 Разложение непрерывной дроби в симуляторе квантовых вычислений

На основании полученного значения r = 2 рассчитаем коэффициенты разложения M = 21

Попробуем определить q на основании полученного p: q = M/p = 21/3 = 7



Проверим: M = p\*q = 3\*7 = 21. Факторизация выполнена успешно, а значит, криптосистема может быть взломана.

**Вывод:**

В ходе выполнения данной лабораторной работы, мы познакомились с квантовым алгоритмом факторизации Шора и основами квантовых вычислений. Также был изучен способ факторизации модуля методом поиска периода для взлома криптосистем РША.