|  |
| --- |
|  |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** |

**Задание по практике**

|  |  |
| --- | --- |
| **Криптографические методы защиты информации** | |
| *(наименование дисциплины (модуля) в соответствии с учебным планом)* | |
| Уровень | специалитет |
|  | *(бакалавриат, магистратура, специалитет)* |
| Форма обучения | очная |
|  | *(очная, очно-заочная, заочная)* |
| Направление  подготовки |  |
|  | *(код(-ы) и наименование(-я))* |
|  |  |
| Институт |  |
|  | *(полное и краткое наименование)* |
| Кафедра |  |
|  | *(полное и краткое наименование кафедры, реализующей дисциплину (модуль))* |
| Лектор | Ермакова Алла Юрьевна |
|  | *(сокращенно – ученая степень, ученое звание; полностью – ФИО)* |

|  |  |  |  |
| --- | --- | --- | --- |
| Используются в данной редакции с учебного года | 2022/23 | | |
|  | *(учебный год цифрами)* | | |
| Проверено и согласовано «\_\_\_\_» \_\_\_\_\_\_\_\_2020\_г. |  |  |  |
|  | *(подпись директора Института/Филиала с расшифровкой)* | | |

Москва 2020 г.

**Лабораторная работа.**

**Разработка криптографического протокола.**

**Цель работы: изучение способа построения и разработка криптографического протокола.**

**Протокол** – совокупность правил, регламентирующих последовательность шагов, предпринимаемых двумя или большим количеством сторон для совместного решения некоторой задачи, а также регламентирующих форматы сообщений, пересылаемых между участниками обмена, и действия при возникновении сбоев.

**Ход работы:**

Используется язык программирования python с помощью PYqt5. Было разработано приложение для шифрования с помощью криптосистемы Шмидта-Самоа.

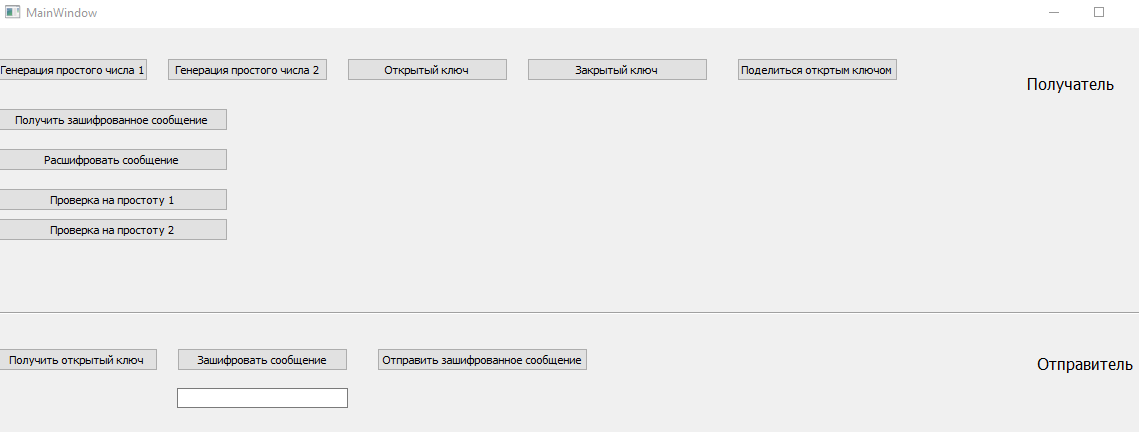


Рис.1. Запуск приложения.



Рис.2. Генерация первого простого числа p.

Генерируется большое случайное число, которое после генерации проверяется на простоту перебором чисел. Числа для проверки начинаются с 2 до корня из сгенерируемого числа.



Рис.3. Генерация второго простого числа q.

Второе большое простое число генерируется аналогично первому.



Рис.4. Расчет открытого ключа N.

Открытый ключ рассчитывается по формуле N=p^2\*q.



Рис.5. Расчет закрытого ключа d.

Закрытый ключ рассчитывается по формуле

d=N^(-1)mod(НОК(p-1,q-1).(Обратное число N по модулю НОК(p-1,q-1).



Рис.6. Отправка открытого ключа получателем.



Рис.7.Полученный открытый ключ отправителем.

Полученный открытый ключ совпадает с открытым ключом получателя.



Рис.8.Сообщение для шифрования m.



Рис.9.Зашифрованное сообщение с.

Рассчитывается по формуле c=m^N mod N.



Рис.10.Отправление зашифрованного сообщения.



Рис.11.Полученное зашифрованное сообщение.

Полученное зашифрованное сообщение совпадает с зашифрованным сообщением отправителя.



Рис.12. Расшифрованное сообщение.

Расшифрованное сообщение совпадает с исходным.

Сообщение расшифровывается по формуле m= c^d mod p\*q.



Рис.13.Первая проверка чисел на простоту.

Проверка производится с помощью теста простоты ферма.

Если n простое число то для a работает выражение

a^(n-1) = 1 mod n.Берется 5 проверок.



Рис.14.Вторая проверка чисел на простоту.

Проверка производится с помощью решета Эратосфена. Это алгоритм нахождения простых чисел до заданного числа путем отсеивания простых чисел.

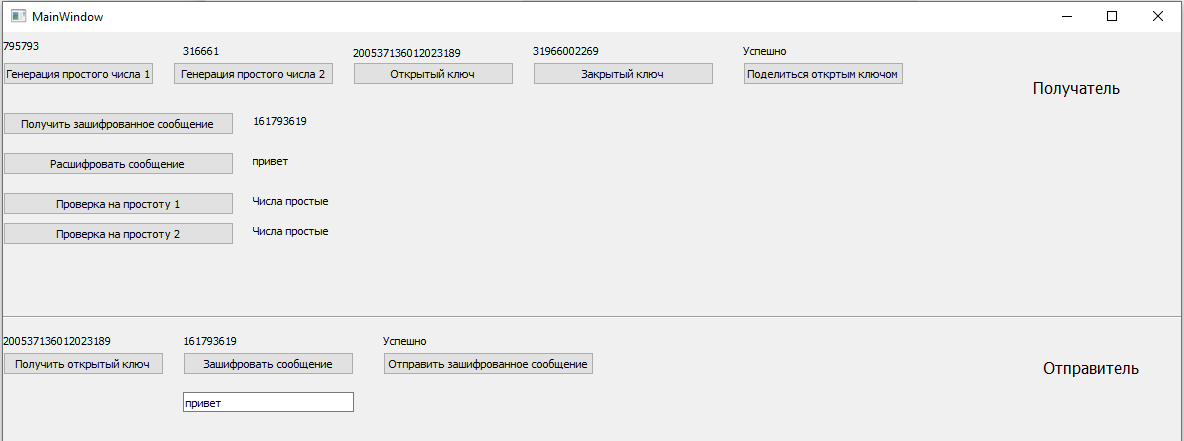


Рис.15.Окно приложения после прохождения всех действий.

**Вывод:**

В результате выполнения лабораторной был изучен способ построения и разработки шифрования с использованием криптосистемы Шмидта-Самоа.

Стойкость алгоритма основывается на сложности разложения больших чисел на множители.

Атака на протокол может быть осуществлена перехватом сообщением.