

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №2**

**В РАМКАХ ДИСЦИПЛИНЫ «МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»**

Выполнил:

Студент 4-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Действия отправителя (инициатора обмена)

Генерируются . Вычисляется

Вычисляется функция Эйлера

Выбирается случайное число , такое что

Из чисел – открытый ключ отправителя

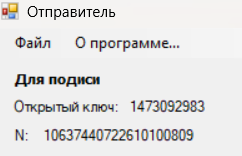


Рисунок 1 - Генерация открытых ключей отправителя

При помощи алгоритма Евклида вычисляется из формулы RSA так что

Из пары – формируется закрытый ключ

Действия получателя

Генерируются . Вычисляется

Вычисляется функция Эйлера

Выбирается случайное число , такое что

Из чисел – открытый ключ отправителя

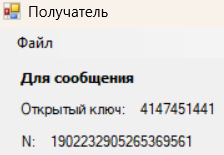


Рисунок 2 - генерация открытого ключа получателя

При помощи алгоритма Евклида вычисляется из алгоритма RSA, так что

Из пары – формируется закрытый ключ

Происходит обмен открытыми ключами

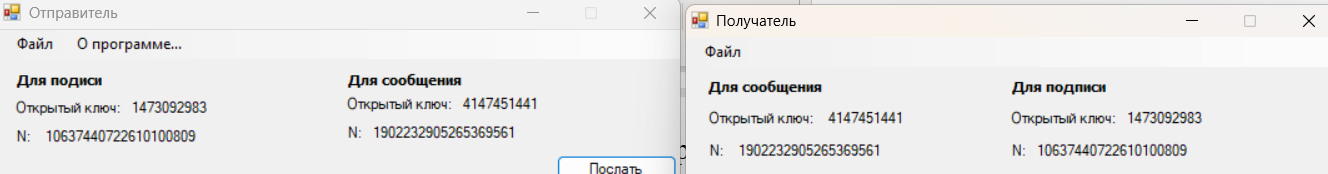


Рисунок 3 - обмен ключами

Действия отправителя (шифрование и подпись сообщения)

Берется символ исходного сообщения , и с помощью закрытых ключа для него генерируется подпись такое, что

Далее каждый подписанный символ шифруется для передачи при помощи открытых ключей и преобразуется в символ ,такой что

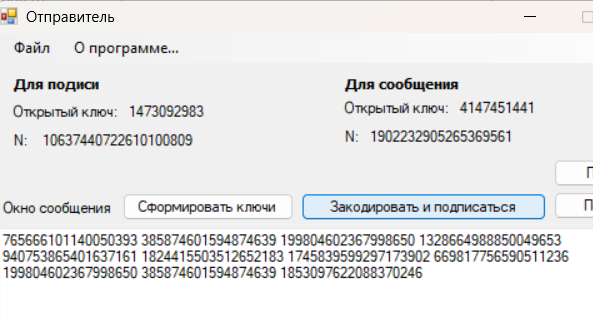


Рисунок 4 - зашифрованное подписанное сообщение

Последовательность символов передается получателю

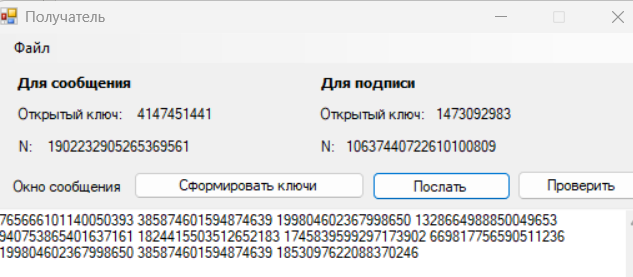


Рисунок 5 - получение зашифрованного сообщение получателем

Действия получателя (проверка подписи, расшифровка)

Берется символ сообщения и при помощи закрытых ключей преобразуется в расшифрованный символ , такой что

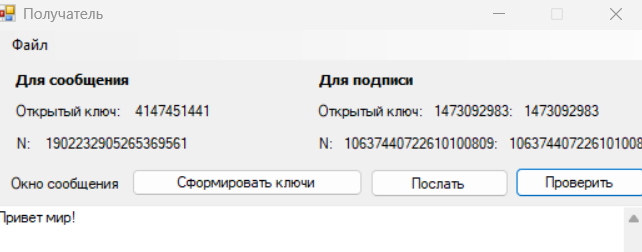


Рисунок 6 - расшифрованное сообщение

Для каждого символа при помощи открытых ключей проверяется подпись и вычисляется символ , такой что .

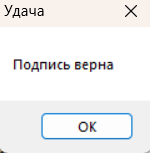


Рисунок 7 - проверка подписи и расшифровка сообщения

Так как как из множества осмысленных текстов при заданных параметрах выделяется один уникальный, полученный получателем, можно сделать вывод, что во время передачи сообщения были соблюдены условия неотказуемости, целостности и авторства сообщения.