**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Дисциплина Основы криптографии с открытыми ключами

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4**

Исследование побочных атак на криптосистему РША

*(тема отчета)*

**Выполнил:**

Ковалев И. А., ИКТЗ-73

*(Ф.И.О., № группы)*

**Проверил:**

д.т.н., профессор Яковлев В.А.

*(должность, Ф.И.О.)*

**Цель лабораторной работы**

Изучить влияние параметров и способов проектирования криптосистемы РША на возможность ее криптоанализа, используя побочные атак, а также закрепить знания, полученные на лекциях курса «Основы криптографии с открытым ключом» , «Криптографические протоколы».

**Ход работы**

1. Запустить программу «RSA attacks lab.exe». После запуска сразу откроется окно для демонстрации атаки на малую шифрующую экспоненту (атака Хастада).
2. Сгенерировать 3 набора ключей РША с одинаковой малой открытой экспонентой *e*=3.

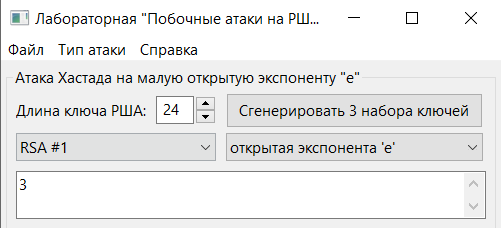


Рисунок 1. Генерация набора ключей с экспонентой e=3.

1. Сгенерировать случайное сообщение и зашифровать его.

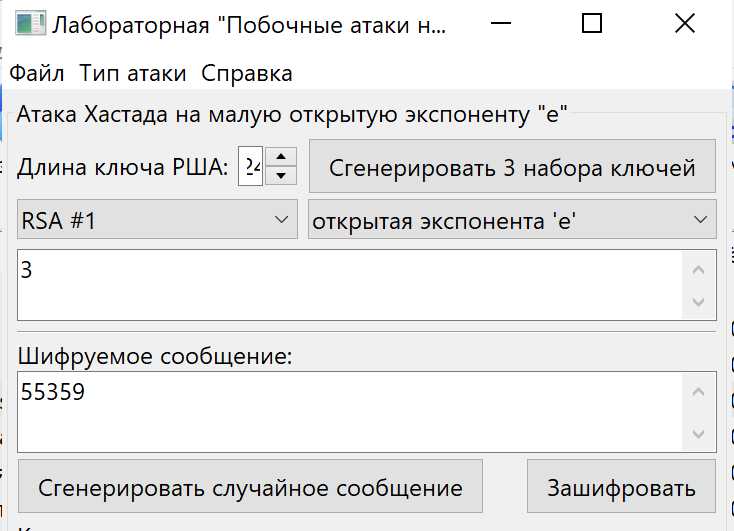


Рисунок 2. Генерация случайного сообщения и его шифрование.

1. Вычислить решение системы сравнений, используя китайскую теорему об остатках.

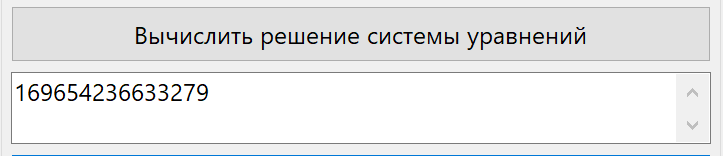


Рисунок 3. Вычисление решения системы уравнений.

1. Найти кубический корень методом Ньютона из решения системы, полученного на предыдущем шаге. Убедиться в том, что это и есть исходное сообщение, сгенерированное в п.3.

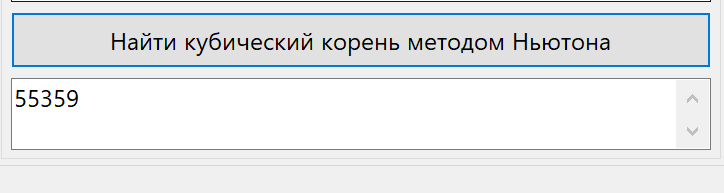


Рисунок 4. Вычисление кубического корня.

Видим, что результат вычисления равен исходному сообщению (см. рис. 2).

1. Переключиться на окно демонстрации атаки при малом количестве возможных сообщений.
2. Сгенерировать ключи криптосистемы и список возможных сообщений заданной длины.

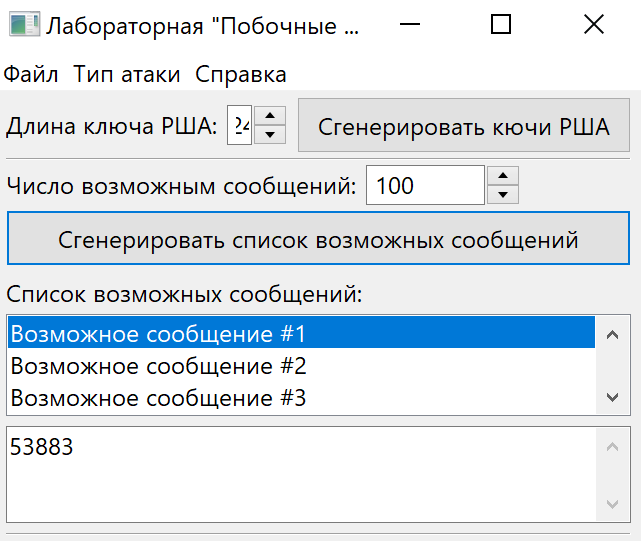


Рисунок 5. Генерация ключей и списка возможных сообщений.

1. Зашифровать случайным образом одно из возможных сообщений.

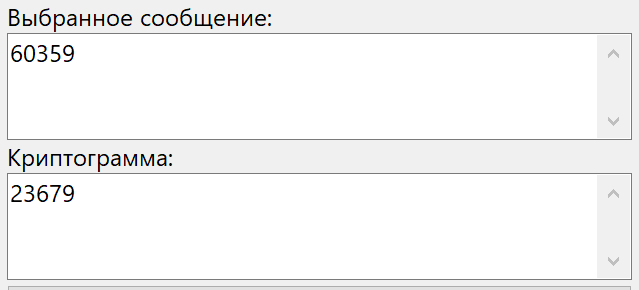


Рисунок 6. Шифрование случайного сообщения из списка.

1. Путем последовательного шифрования возможных сообщений по списку и сравнения с криптограммой из п.8 найти исходное сообщение. Оценить скорость выполнения данной атаки в зависимости от количества возможных сообщений и длины модуля.

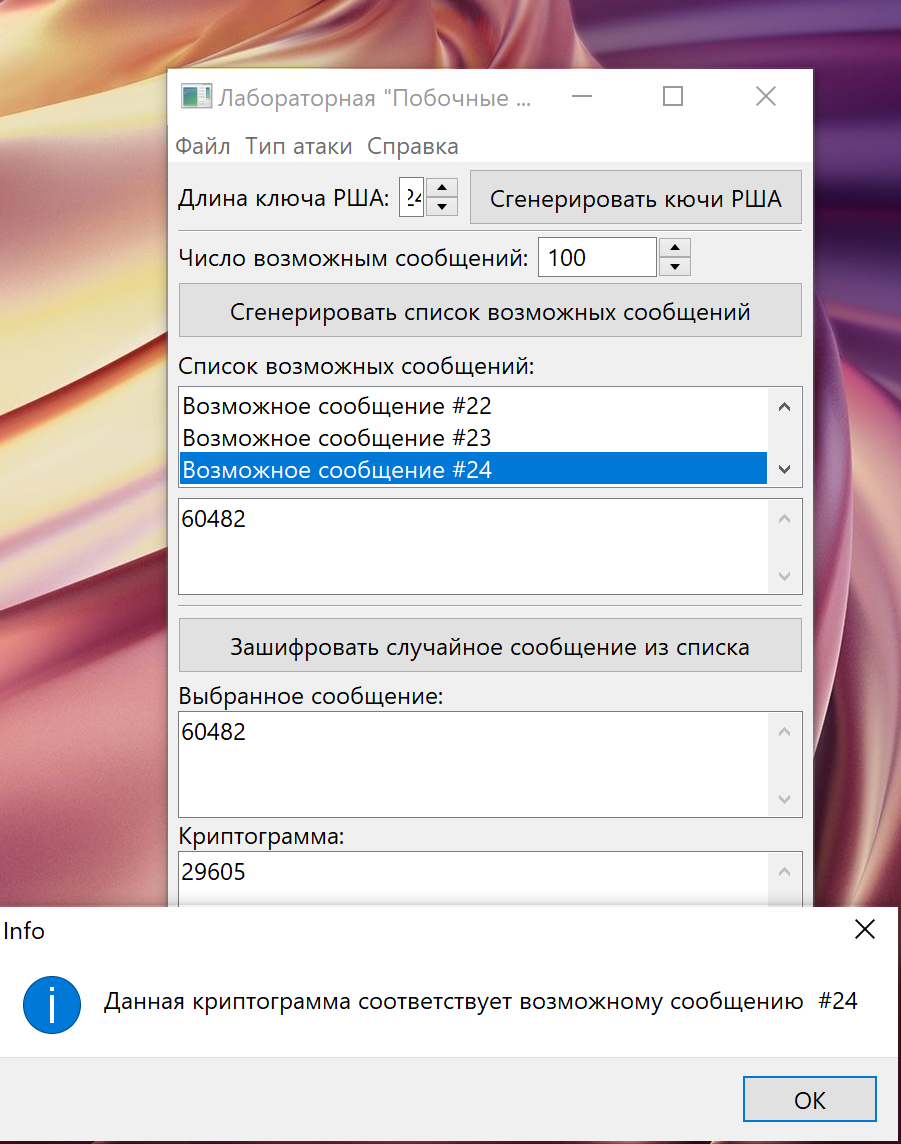


Рисунок 7. Поиск исходного сообщения при малом количестве возможных сообщений.

При увеличении количества возможных сообщений и длины модуля скорость проведения атаки снижается, однако для человека эта разница практически незаметна.

1. Переключиться на окно демонстрации атаки Винера (атака на малую секретную экспоненту).
2. Сгенерировать ключи криптосистемы (длина секретной экспоненты = 8; длина модуля РША = 32).

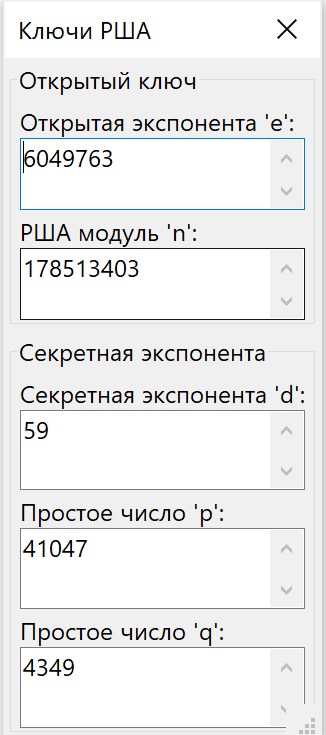
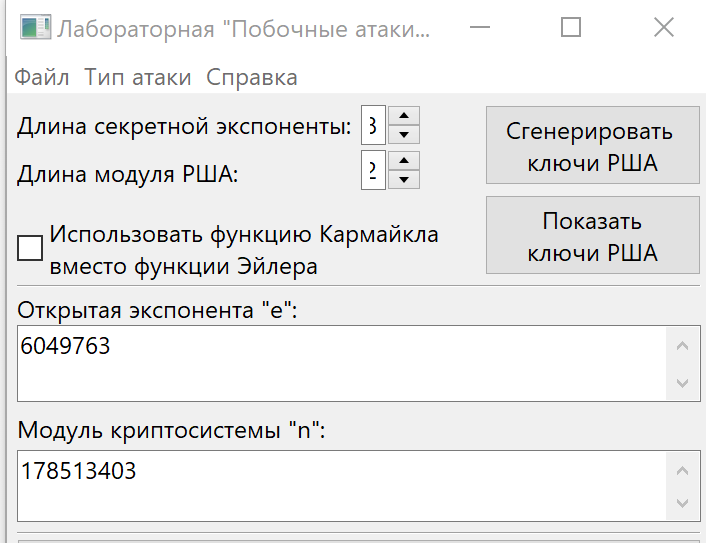


Рисунок 8. Генерация ключей при атаке Винера.

1. Выполнить атаку Винера. Убедиться в том, что найденные в результате выполнения атаки секретная экспонента и делители модуля криптосистемы действительно соответствуют параметрам заданной криптосистемы.

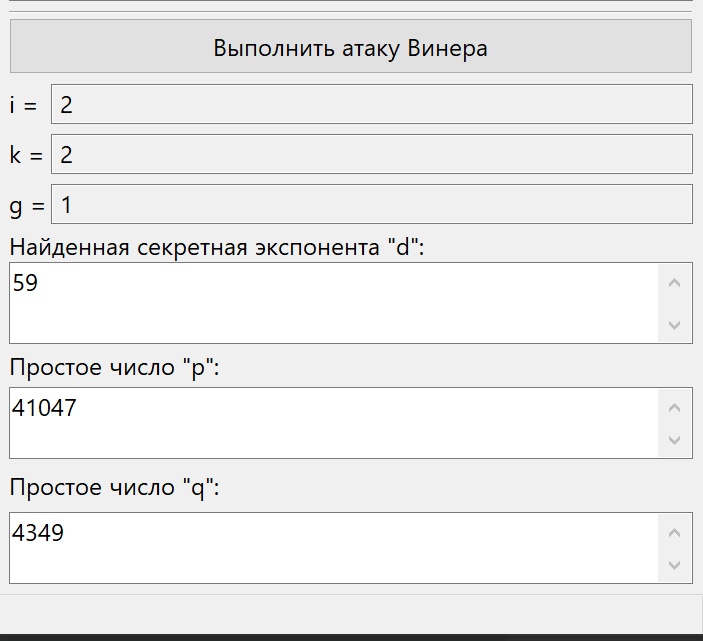


Рисунок 9. Проведение атаки Винера.

Видим, что полученные в результате проведения атаки секретная экспонента и делители модуля криптосистемы действительно соответствуют параметрам заданной криптосистемы (см. рис. 8).

**Проведем данную атаку «вручную»:**

Значение *d* может быть легко вычислено как знаменатель одной из подходящих дробей *k/d* – разложения *e/N* в цепную дробь.

Исходные данные:

Алгоритм Евклида:

= \*0 +

= \*29 + 3070276

= 3070276\*1 + 2979487

3070276= 2979487\*1 + 90789

2979487= 90789\*32 + 74239

90789= 74239\*1 + 16550

74239 = 16550\*4 + 8039

16550= 8039\*2 + 472

8039= 472\*17 + 15

472= 15\*31 + 7

15 = 7\*2 + 1

7 = 1\*0 + 7

Получаем следующие подходящие дроби:

***.***

***.***

***.***

Далее перебором, для каждой *k/d* подходящей дроби, вычисляется



и решается квадратное уравнение



Проверяется, является ли *p* простым множителем.

Предположим *k/d = = 2*/59, тогда:

Откуда:

Проверка:

1. Задавая различные длины модуля и секретной экспоненты, убедиться в том, что атака Винера дает результат при битовой длине секретной экспоненты приблизительно меньше четверти битовый длины модуля криптосистемы.

При длине модуля 128 бит и длине секретной экспоненты 40 бит (> 1/4) выполнить атаку Винера не удалось.

При длине модуля 128 бит и длине секретной экспоненты 30 бит (< 1/4) атака Винера была успешно выполнена.

1. Переключиться на окно демонстрации атаки, связанной с мультипликативным свойством шифра РША.
2. Сгенерировать ключи криптосистемы (длина ключа РША = 24).

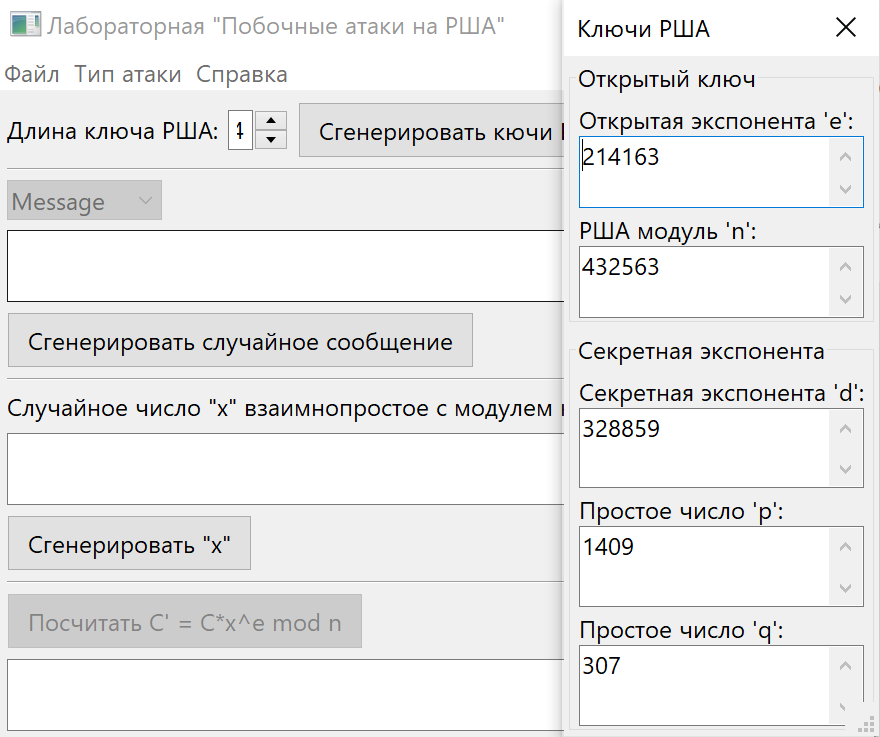


Рисунок 10. Генерация ключей при атаке, связанной с мультипликативным свойством шифра РША.

1. Сгенерировать случайное сообщение M и зашифровать его.

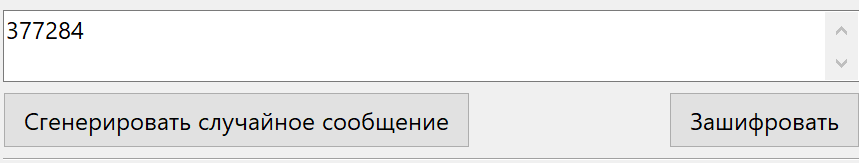


Рисунок 11. Генерация случайного сообщения при атаке, связанной с мультипликативным свойством шифра РША.

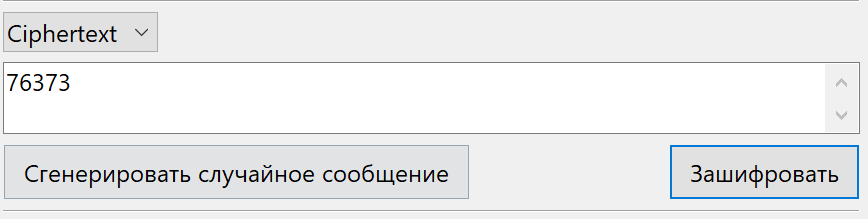


Рисунок 12. Шифрование сообщения при атаке, связанной с мультипликативным свойством шифра РША.

1. Сгенерировать случайное число *x* взаимно простое с модулем криптосистемы и вычислить специальную криптограмму *C'*.

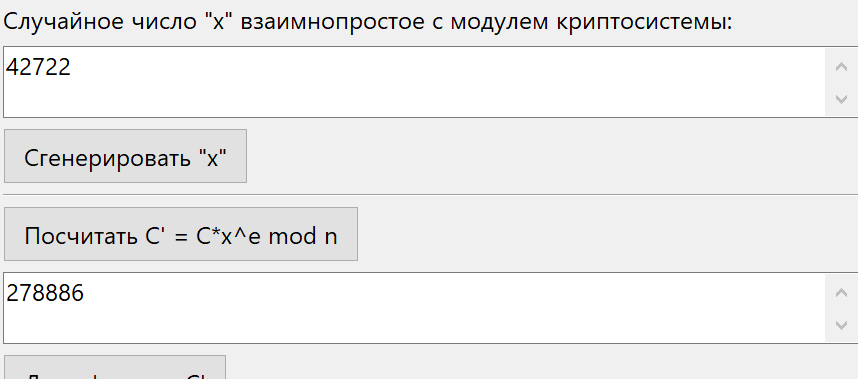


Рисунок 13. Генерация числа “x” взаимно простого с модулем криптосистемы и вычисление специальной криптограммы C'.

1. Дешифровать *C'*, получив тем самым некое сообщение *M'*.



Рисунок 14. Дешифрование C'.

1. Извлечь исходное сообщение *M* из *M'*. Убедиться в том, что полученное в результате выполнения атаки сообщение совпадает с исходным сообщением из п.16.

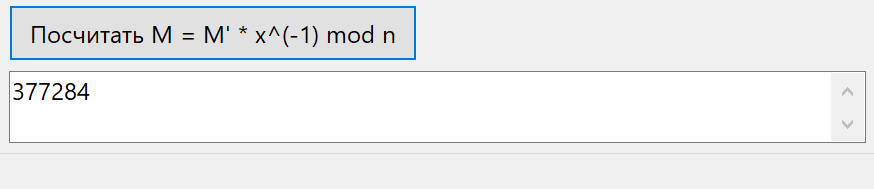


Рисунок 15. Получение исходного сообщения при атаке, связанной с мультипликативным свойством шифра РША.

Видим, что результат вычисления равен исходному сообщению (см. рис. 11).

1. Переключиться на окно демонстрации циклической атаки.
2. Сгенерировать ключи криптосистемы (дина ключа РША = 16).

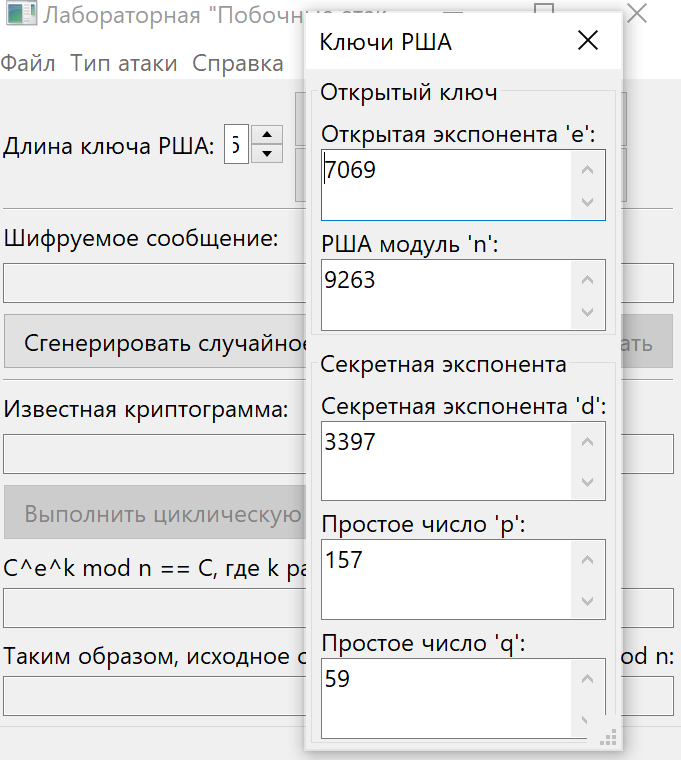


Рисунок 16. Генерация ключей при циклической атаке.

1. Сгенерировать случайное сообщение и зашифровать его.

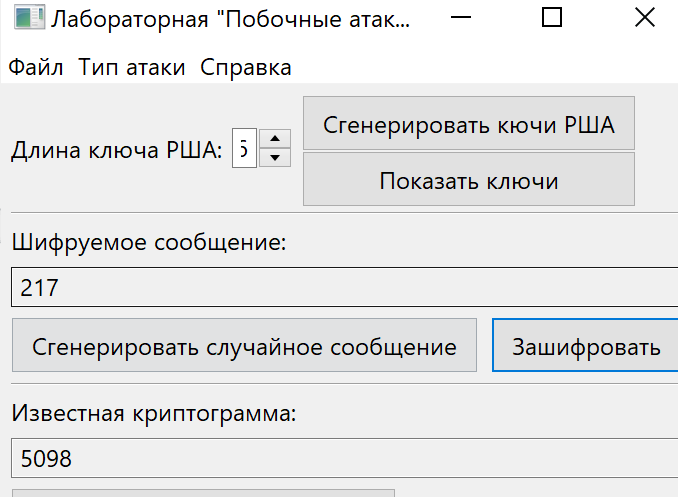


Рисунок 17. Генерация сообщения и его шифрование при циклической атаке.

1. Выполнить циклическую атаку. Убедиться в том, что найденное сообщение соответствует исходному сообщению из п.19.

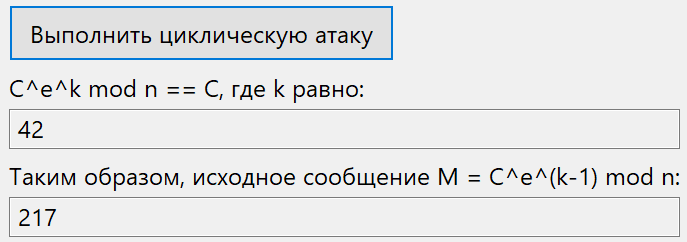


Рисунок 18. Проведение циклической атаки.

Видим, что результат вычисления равен исходному сообщению (см. рис. 17).

1. Увеличив длину модуля криптосистемы, убедиться в том, что алгоритм выполнения данной атаки обладает не полиномиальной сложностью.

При увеличении длины модуля криптосистемы (проверялась длина 32 бита) время выполнения атаки значительно увеличивается (см. рис. 19) - алгоритм выполнения циклической атаки обладает не полиномиальной сложностью

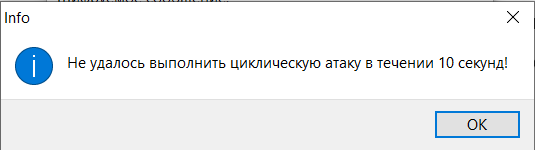


Рисунок 19. Сообщение об ошибке при проведении циклической атаки с большим модулем.

1. Переключиться на окно демонстрации атаки на общие модули.
2. Сгенерировать 2 набора ключей с общим модулем.

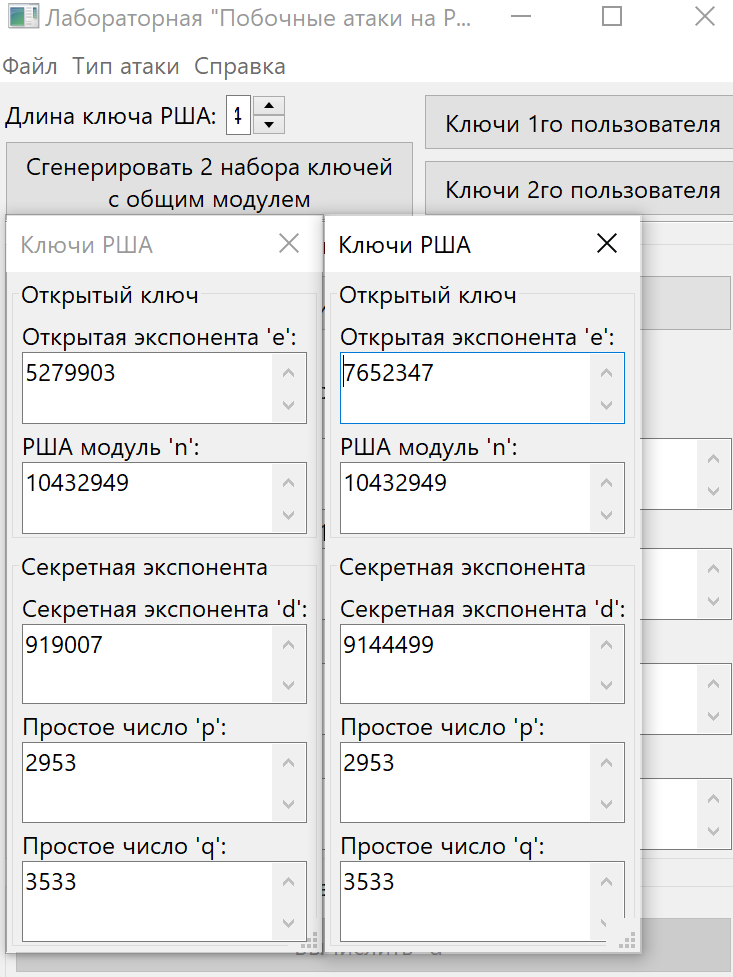


Рисунок 20. Генерация ключей при атаке на общие модули.

1. Выполнить факторизацию общего модуля, зная обе секретные экспоненты.

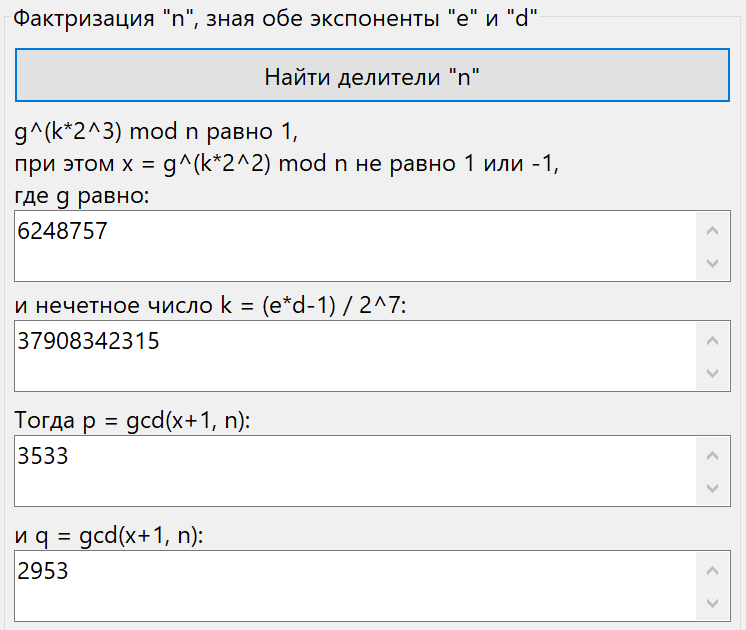


Рисунок 21. Факторизация общего модуля.

1. Вычислить секретную экспоненту второго набора ключей, зная делители общего модуля криптосистемы. Просмотрев исходные параметры обоих наборов ключей и результаты выполнения атаки, убедиться в том, что атака на общие модули привела к взлому криптосистемы.

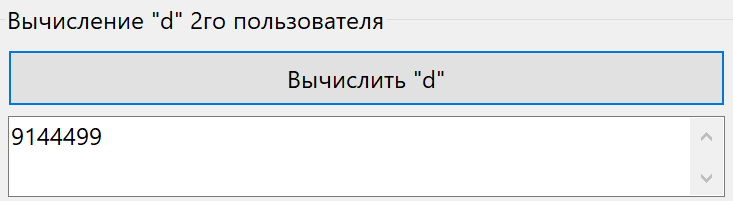


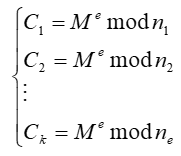
Рисунок 22. Вычисление секретной экспоненты второго набора ключей.

Видим, что результат вычисления равен секретной экспоненте второго набора ключей (см. рис. 20).

**Контрольные вопросы**

1. Каковы необходимые условия для выполнения атаки на малую шифрующую экспоненту?

Для выполнения атаки злоумышленнику достаточно иметь систему из любых *e* уравнений системы:



где *e* – открытая экспонента малой величины.

1. Каким образом можно противостоять атаке при малом числе возможных сообщений?

Для защиты от этой атаки необходимо либо не использовать малые e, либо не отправлять одни и те же сообщения разным пользователям. Если в этом есть объективная необходимость, то сообщение нужно немного изменить, добавляя, например, в конце его небольшие различные случайные числа. Такой метод называется методом «подсаливания» сообщения.

1. Какова приблизительная длина секретной экспоненты, при которой атака Винера выполняется успешно?

Битовая длина секретной экспоненты должна быть приблизительно меньше четверти битовый длины модуля криптосистемы.

1. Каково главное условие выполнения атаки, связанной с мультипликативным свойством шифра РША?

Проведение данной атаки возможно, если легитимный пользователь криптосистемы согласен расшифровать любую другую криптограмму кроме той, что интересует злоумышленника.

1. Почему с увеличением модуля криптосистемы время выполнения циклической атаки возрастает экспоненциально?

Доказано, что сложность алгоритма эквивалентна сложности разложения числа *n* на множители, т.е. задаче факторизации. Соответственно при больших *n* данный подход не лучше прямого метода факторизации модуля криптосистемы РША. Другими словами, нет никакого эффективного алгоритма, который может завершить эту атаку в полиномиальное время, если *n* является большим.