**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 «Защищенные системы связи»

Дисциплина «Основы криптографии с открытыми ключами»

# Лабораторная работа № 5

**«ИССЛЕДОВАНИЕ ПОБОЧНЫХ АТАК НА КРИПТОСИСТЕМУ РША»**

**4 вариант**

Выполнил: Громов А. А.

ИКТЗ-83

Проверил: Яковлев В. А.

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

Санкт-Петербург

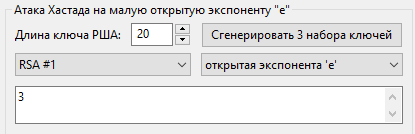
2021

**Цель 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».

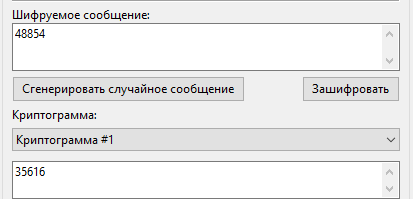
**Ход выполнения работы**

1. Запустить программу «RSA attacks lab.exe». После запуска сразу откроется окно для демонстрации атаки на малую шифрующую экспоненту.

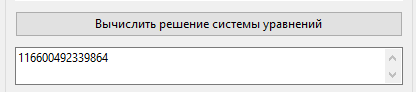
2. Сгенерировать 3 набора ключей РША с одинаковой малой открытой экспонентой *e*=3.



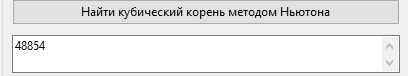
3.Сгенерировать случайное сообщение и зашифровать его.



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



5. 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.



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Набор ключей | Модуль *n* | Экспонента *e* | Экспонента *d* | Простое *p* | Простое *q* |
| 1 | 59953 | 3 | 39619 | 359 | 167 |
| 2 | 142663 | 3 | 94459 | 179 | 797 |
| 3 | 163903 | 3 | 108667 | 653 | 251 |

Шифруемое сообщение: 48854,

Криптограмма 1: 35616,

Криптограмма 2: 49176,

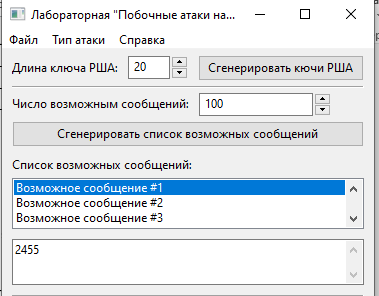
Криптограмма 3: 87530,

Общее решение системы сравнений: 116600492339864,

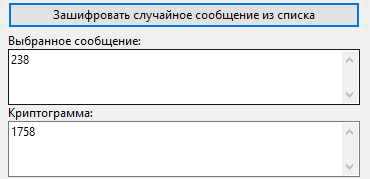
Кубический корень из общего решения: 48854.

6. Переключиться на окно демонстрации атаки при малом количестве возможных сообщений.

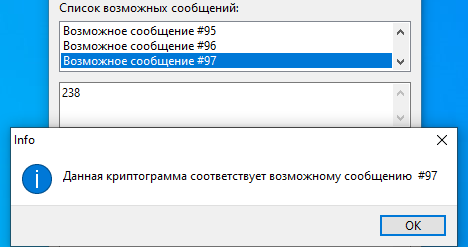
7. Сгенерировать ключи криптосистемы и список возможных сообщений заданной длины.



8. Зашифровать случайным образом одно из возможных сообщений.



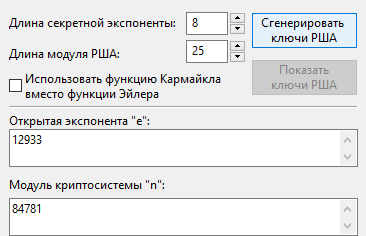
9. Путем последовательного шифрования возможных сообщений по списку и сравнения с криптограммой из п.8 найти исходное сообщение. Оценить скорость выполнения данной атаки в зависимости от количества возможных сообщений и длины модуля.

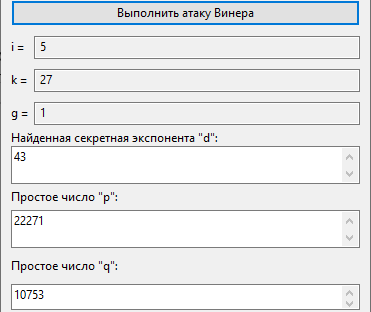
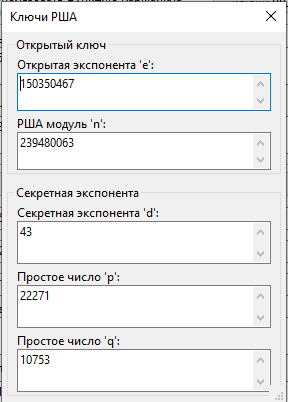


Скорость выполнения данной атаки очень высока при малой длине ключа или при малом числе возможных сообщений. С увеличением обоих показателей скорость снижается.

10. Переключиться на окно демонстрации атаки Винера (атака на малую секретную экспоненту).

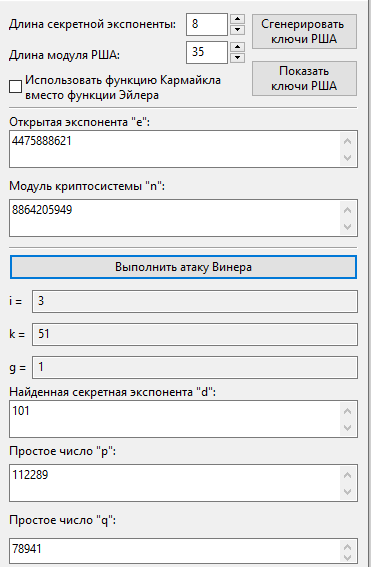
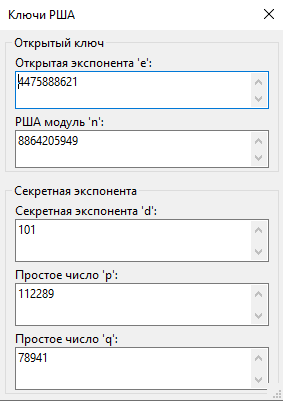
11. Сгенерировать ключи криптосистемы.



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

Действительно, атака успешно выполняется! Полученная секретная экспонента и делители модуля криптосистемы действительно соответствуют параметрам заданной криптосистемы.

* Шифрующая экспонента e: 150350467,
* Модуль криптосистемы n: 239480063,
* Найденная секретная экспонента: 43,
* Найденные делители модуля: 22271 и 10753,
* i = 5, k = 27, g = 1.

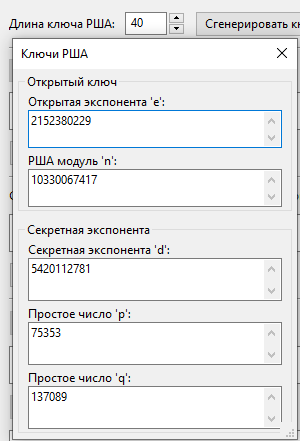
13. Задавая различные длины модуля и секретной экспоненты, убедиться в том, что атака Винера дает результат при битовой длине секретной экспоненты приблизительно меньше четверти битовый длины модуля криптосистемы.

* Шифрующая экспонента e: 4475888621,
* Модуль криптосистемы n: 8864205949,
* Найденная секретная экспонента: 101,
* Найденные делители модуля: 112289 и 78941,
* i = 3, k = 51, g = 1.

В ходе выполнения данного пункта была выбрана длина экспоненты, равная 8 и длина модуля, равная 35. 8 чуть меньше четверти от 35. Таким образом, мы убедились в том, что атака Винера дает результат при битовой длине секретной экспоненты приблизительно меньше четверти битовый длины модуля криптосистемы.

14. Переключиться на окно демонстрации атаки, связанной с мультипликативным свойством шифра РША.

15. Сгенерировать ключи криптосистемы.

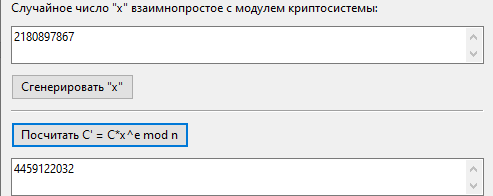


16. Сгенерировать случайное сообщение*M* и зашифровать его.





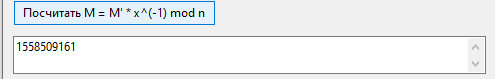
17. Сгенерировать случайное число *x*взаимно простое с модулем криптосистемы и вычислить специальную криптограмму *C'*.



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



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



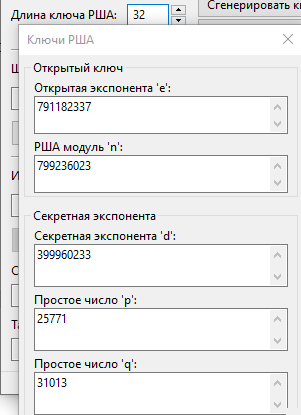
Сообщение, полученное в результате выполнения атаки, совпадает с исходным сообщением из п.16.

Параметры криптосистемы:

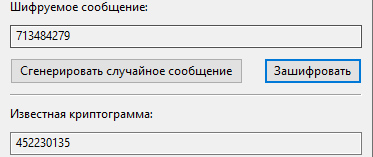
* Открытая экспонента e: 2152380229,
* Секретная экспонента d: 5420112781,
* Модуль криптосистемы n: 10330067417.
* Выбранное сообщение M: 1558509161,
* Зашифрованное сообщение C: 3032071503,
* Случайное число x взаимно простое с модулем n: 2180897867,
* Комбинированная криптограмма
* Расшифрованное M': 3971186480,
* Исходное сообщение

20. Переключиться на окно демонстрации циклической атаки.

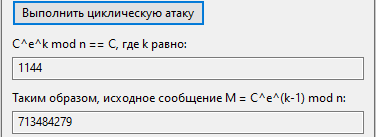
21. Сгенерировать ключи криптосистемы.



22. Сгенерировать случайное сообщение и зашифровать его.



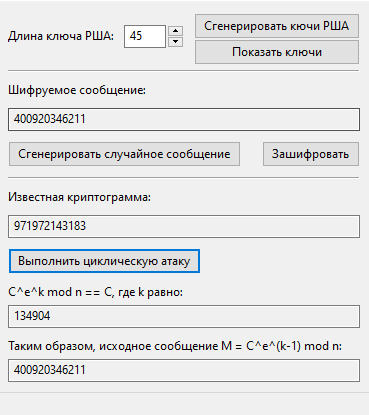
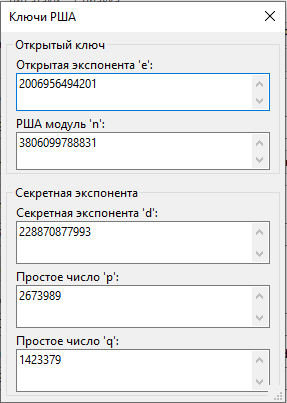
23. Выполнить циклическую атаку. Убедиться в том, что найденное сообщение соответствует исходному сообщению из п.22.



REWRITE

Найденное сообщение соответствует исходному сообщению из п.22.

* Открытая экспонента *e*: 791182337,
* Модуль криптосистемы *n*: 799236023,
* Шифруемое сообщение *M*: 713484279,
* Криптограмма *C*: 452230135,
* , где *k* = 1144,
* Исходное сообщение

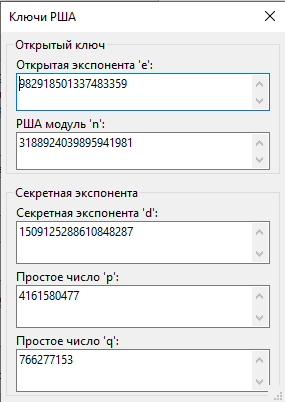
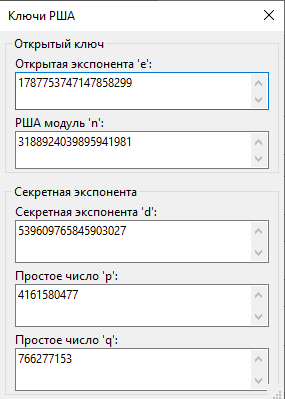
24.Увеличив длину модуля криптосистемы, убедиться в том, что алгоритм выполнения данной атаки обладает не полиномиальной сложностью.

* Открытая экспонента *e*: 2006956494201,
* Модуль криптосистемы *n*: 3806099788831,
* Шифруемое сообщение *M*: 400920346211,
* Криптограмма *C*: 971972143183,
* , где *k* = 134904,
* Исходное сообщение

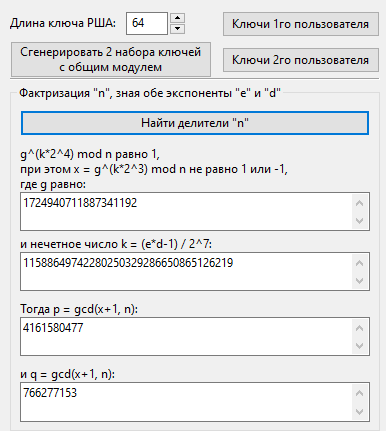
Таким образом мы убедились, что, при увеличении длины модуля криптосистемы, алгоритм выполнения данной атаки обладает не полиномиальной сложностью.

25. Переключиться на окно демонстрации атаки на общие модули.

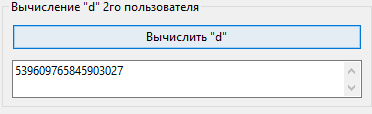
26. Сгенерировать 2 набора ключей с общим модулем.

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



28. 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.



* Открытая экспонента e1: 982918501337483359,
* Открытая экспонента e2: 178775374147858299,
* Секретная экспонента d1: 1509125288610848287,
* Общий модуль: 3188924039895941981,
* Случайное число g, используемое для факторизации: 72494071187341192,
* k =
* Делители модуля: 4161580477 и 766277153,
* Секретная экспонента d2: 539609765845903027.

Изучив исходные параметры наборов ключей и результаты выполнения атаки, мы убедились в том, что атака на общие модули приводит к взлому криптосистемы.

**Вывод:**

В ходе выполнения данной лабораторной работы было изучено влияние параметров и способов проектирования криптосистемы РША на возможность ее взлома, используя побочные атаки.

Также были закреплены знания, полученные на лекциях курса «Основы криптографии с открытым ключом», «Криптографические протоколы».