**Лабораторная работа. ИССЛЕДОВАНИЕ ПОБОЧНЫХ АТАК НА КРИПТОСИСТЕМУ РША**

**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».

**Используемое программное обеспечение**

Для выполнения работы используется специально разработанный программный комплекс «RSA attacks lab.exe»

**Задание**

1. Для выполнения каждой из атак сгенерировать набор ключей РША (или несколько наборов).

2. Выполнить необходимые для осуществления криптоанализа шаги.

3. Проанализировать результаты выполнения атак.

**Порядок выполнения**

Для начала работы перейти в каталог, содержащий описание лабораторных работ, и убедиться в установке программы «RSA attacks lab». Проделать нижеописанные шаги сначала для небольших чисел, которые можно занести в отчет (длина модуля РША ~20 бит). Затем убедиться в том, что данные атаки выполняются также быстро и при больших длинах ключей (за исключением циклической атаки).

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.

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.

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.

13. Задавая различные длины модуля и секретной экспоненты, убедиться в том, что атака Винера дает результат при битовой длине секретной экспоненты приблизительноменьше 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.13.

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.19.

24.Увеличив длину модуля криптосистемы, убедиться в том, что 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.

**Отчет**

1. Титульный лист.

2. Сгенерированные параметры криптосистем.

3. Сгенерированные сообщения и соответствующие им криптограммы.

4. Результаты промежуточных вычислений, выводимые программой.

5. Результаты выполнения атак.

**Пример отчета**

1. Атака на малую шифрующую экспоненту

Параметры криптосистем:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Набор ключей | Модуль *n* | Экспонента *e* | Экспонента *d* | Простое *p* | Простое *q* |
| 1 | 110767 | 3 | 73387 | 431 | 257 |
| 2 | 243043 | 3 | 161339 | 677 | 359 |
| 3 | 81247 | 3 | 53611 | 719 | 113 |

Шифруемое сообщение: 64945

Криптограмма 1: 19255

Криптограмма 2: 176455

Криптограмма 3: 1363

Общее решение системы сравнений: 273928464708625

Кубический корень из общего решения: 64945

2. Атака Винера

Шифрующая экспонента *e*: 51470893

Модуль криптосистемы*n*: 1071303463

Найденная секретная экспонента: 37

Найденные делители модуля: 33931 и 31573

*i* = 37, *k*=16, *g*=9

3. Атака с использованием мультипликативного свойства шифра РША

Параметры криптосистемы:

* Открытая экспонента*e*: 692923
* Секретная экспонента*d*: 327283
* Модуль криптосистемы*n*: 697483

Выбранное сообщение*M*: 81662

Зашифрованное сообщение*C*: 511286

Случайное число *x* взаимно простое с модулем *n*: 449665

Комбинированная криптограмма 

Расшифрованное *M'*: 155729

Исходное сообщение 

4. Циклическая атака

Открытая экспонента *e*: 112031

Модуль криптосистемы *n*: 117197

Шифруемое сообщение *M*: 31990

Криптограмма *C*: 64361

, где *k* = 3222

Исходное сообщение 

5. Атака на общие модули

Открытая экспонента *e*1: 374263

Открытая экспонента *e*2: 294143

Секретная экспонента *d*1: 16327

Общий модуль: 385241

Случайное число *g*, используемое для факторизации: 302073



Делители модуля: 601 и 641

Секретная экспонента *d*2: 139007

**Контрольные вопросы**

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

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

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

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

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