## *ЛАБОРАТОРНАЯ РАБОТА № 2*

## Атаки на криптосистему RSA без разложения числа на множители

Цель работы – изучение уязвимостей криптосистемы RSA по отношению к атакам без разложения на множители, генерация параметров криптосистемы RSA.

### Теоретические сведения

Как показывает практика, правильный выбор множителей  и  не всегда гарантирует стойкость криптосистемы. Существует множество атак, нарушающих безопасность криптосистемы RSA без разложения числа  на множители. Существование таких атак накладывает значительные ограничения на выбор значений различных параметров криптосистем на основе алгоритма RSA.

1. **Случай общего модуля**

Если в системе RSA у пользователей *A* и *B* общее составное число , но различные открытые ,  и закрытые ,  ключи, причем , то каждый пользователь может найти разложение числа  и тем самым узнать закрытый ключ другого пользователя. Для этого нарушителю (например, пользователю *B*) достаточно найти значение квадратного корня из единицы, отличное от . Если , , то , и ,  имеют нетривиальные общие делители с . Разложение можно выполнить по аналогии с псевдопростым тестом Миллера–Рабина следующим алгоритмом.

**Алгоритм** **2.1.** Разложение составного числа на множители по известным показателям RSA

*Вход*. Число , показатели ,  такие, что .

*Выход*. Делители  и  числа , закрытый ключ другого пользователя .

* 1. Положить . Представить  в виде , где –  нечетное число.
  2. Выбрать случайное  и вычислить .
  3. Вычислять , , , … до получения  такого, что . Если , то вернуться на шаг 2, иначе положить .
  4. Положить , .
  5. Вычислить  и найти закрытый ключ другого пользователя: .
  6. Результат:, . ◼

1. **Случай малого закрытого показателя**

Атака Винера на схему RSA основана на предположении, что значение закрытого показателя  достаточно мало. Пусть , ,  − открытый ключ, − закрытый ключ схемы RSA. Тогда если , то значение закрытого показателя  может быть вычислено за полиномиальное от *n* время.

Для доказательства этого предположения используется математический аппарат непрерывных дробей, который позволяет найти приближение к некоторому вещественному числу  с помощью подходящих дробей. Пусть  − несократимая рациональная дробь, и выполняется условие: , тогда  представляет собой подходящую дробь к числу .

Открытый и закрытый показатели связаны соотношением , т.е. существует такое , что , или . При делении последнего равенства на  может быть получено, что:

.

Так как значение  неизвестно, вместо  можно использовать соотношение известных значений  ввиду относительной близости *n* и  друг к другу:

 .

Тогда при  и  выполняется: , из чего следует:

.

Таким образом, подходящая дробь  со знаменателем, близким к , является хорошим приближением к . Действуя таким образом, можно найти закрытый показатель , если его длина достаточно мала.

**Алгоритм 2.2.** Атака Винера на криптосистему RSA

*Вход*. Число , показатель .

*Выход*. Закрытый показатель 

1. Представить  в виде непрерывной дроби , .
2. Для  выполнить следующие действия.
   1. Вычислить *i*-ю подходящую дробь  к :, где .
   2. Проверить выполнение сравнения , где – произвольное сообщение. Если сравнение выполняется, то положить  и перейти на шаг 3.
3. Результат: *d*. ◼
4. **Случай специальных открытых показателей**

Каждый пользователь  системы связи с шифрованием по схеме RSA должен иметь свое персональное число . Для ускорения процесса шифрования иногда используются малые открытые показатели , причем они могут быть одинаковыми, например, 3 или 5. В этом случае, даже если числа  различны, можно выполнить бесключевое дешифрование сообщения. Предположим, что отправитель посылает одно и то же сообщение  трем получателям, открытые ключи которых равны , причем  и . Обозначим . Тогда выполняются сравнения , , и значение  как целое число может быть восстановлено по китайской теореме об остатках по известным  и взаимно простым модулям . Для нахождения сообщения  нужно извлечь кубический корень из  в кольце целых чисел, эта операция имеет полиномиальную сложность. Очевидно, то же справедливо и в случае других малых одинаковых открытых показателей.

**Алгоритм 2.3.** Бесключевое дешифрование широковещательного сообщения в случае малого общего показателя 

*Вход*. Открытые ключи нескольких пользователей:, шифртексты широковещательного сообщения: .

*Выход*. Сообщение .

1. По известным шифртекстам  и характеристикам  колец по китайской теореме об остатках восстановить число .
2. Вычислить .
3. Результат: *m*. ◼

Еще один вариант атаки на схему шифрования может быть использован, если порядок элемента  в группе  является малым. В этом случае для нахождения сообщения  по шифртексту  выполняется последовательное зашифрование   
шифртекста: ,  и т. д.  до получения открытого текста (предполагается, что открытый текст обладает избыточностью, позволяющей его распознать).

**Алгоритм 2.4.** Бесключевое дешифрование сообщения в случае малого порядка  в 

*Вход*. Составное число , шифртекст , открытый показатель .

*Выход*. Открытый текст .

1. Для  выполнить следующие действия.
   1. Вычислить , где .
   2. Проверить выполнение сравнения . Если сравнение выполняется, то положить  и перейти на шаг 3.
2. Результат: *m*. ◼

Отметим, что порядок элемента  в группе  мал лишь в том случае, если он мал в обеих группах  и . Однако, если этот порядок мал хотя бы в одной из указанных групп, то можно разложить число  следующим образом. Сначала сгенерировать случайное . Затем для  вычислять последовательно  и проверять с помощью бинарного алгоритма Евклида условие . Если это условие будет выполнено, то указанный наибольший общий делитель является нетривиальным делителем числа .

Для исключения этой атаки числа  и  выбирают так, чтобы порядки групп  и  имели большие простые делители.

В случае малых открытых показателей можно не только осуществить бесключевое дешифрование, но и вскрыть закрытый показатель . Для этого достаточно знать четверть двоичных разрядов одного из делителей числа .

Рассмотрим другой простой вариант атаки на систему RSA на основе «частично известных» открытых текстов. Если два сообщения ,  не одинаковы, но связаны с помощью аффинного соотношения с известными параметрами, например, , где  и  известны, то по шифртекстам ,  можно восстановить оба сообщения. Например, для  сообщение  восстанавливается по формуле

.

Сообщение  выражается через  и коэффициенты , . В случае произвольного показателя  имеют место соотношения:

, .

Обозначим неизвестное сообщение  через переменную . Тогда, переходя к кольцу полиномов , можно записать:

.

Вычислив этот наибольший общий делитель, можно определить .

**Алгоритм** **2.5.** Нахождение двух открытых текстов по двум шифртекстам и параметрам аффинного преобразования

*Вход*. Составное число , шифртексты , , параметры , , открытый показатель .

*Выход*. Открытые тексты , .

* 1. Вычислить  как свободный член линейного полинома  в кольце .
  2. Положить .
  3. Результат: . ◼

Алгоритм 2.5 допускает обобщение на случай, когда  задается произвольным полиномом от  над :. Тогда  в кольце полиномов . Если  и  задаются полиномами от  над кольцом 



и известны шифртексты , , то



в кольце полиномов .

**Пример** **2.1.** Восстановление пары сообщений без разложения числа .

Пусть . Вычисляем  в кольце . Получаем последовательность вычетов для алгоритма Евклида (с учетом нормирования полиномов по старшему коэффициенту):





то есть .

Второе сообщение: . ◼

Операция вычисления наибольшего общего делителя полиномов степени  над кольцом  предусматривает выполнение на каждой итерации следующих действий:

* одну операцию обращения по модулю ;
*  операций умножения чисел по модулю ;
*  операций сложения чисел по модулю .

Число итераций равно .

При использовании умножения «в столбик» и арифметики Монтгомери сложность алгоритма 2.5 равна . При использовании умножения с помощью быстрого преобразования Фурье сложность алгоритма равна .

Для того чтобы стойкость к методу дешифрования на основе частично известных открытых текстов была не хуже, чем сложность разложения, открытый показатель  должен быть достаточно велик. Минимально возможные значения показателя  для различных размеров задачи разложения, для которых сложность указанной атаки равна сложности разложения, приведены в таблице 2.1.

Таблица 2.1 – Минимальный размер открытого показателя    
в системе RSA, при котором атака по алгоритму 2.5 неэффективна

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 512 | 768 | 1024 | 2048 | 4096 | 8192 |
|  | 108 | 1010 | 2⋅1011 | 3⋅1015 | 1021 | 1029 |

Сложность разложения оценивалась по отношению к методу решета числового поля. Сложность атаки на основе алгоритма Евклида в  оценивалась по отношению к умножению с помощью быстрого преобразования Фурье.

### Контрольные вопросы

1. При каком условии возможна атака Винера?
2. Перечислите методы противодействия атаке Винера.
3. Почему числа  и  необходимо выбирать таким образом, чтобы  имели большие простые делители?
4. Предложите способы защиты от атаки бесключевого дешифрования широковещательных сообщений без отказа от использования общих малых закрытых показателей.
5. Обеспечивают ли часто используемые открытые показатели вида  стойкость к методу криптоанализа на основе частично известных открытых текстов?

### Порядок выполнения работы

1. Получить у преподавателя вариант задания.
2. Разработать программу (**П-1**), которая реализует разложение составного числа на множители по известным показателям RSA и вычисляет закрытый ключ другого пользователя в случае общего модуля *n*.
3. Разработать программу (**П-2**), которая реализует атаку Винера на криптосистему RSA.
4. Разработать программу (**П-3**), которая, в соответствии с вариантом задания, реализует одну из следующих атак:

* бесключевое дешифрование широковещательного сообщения в случае малого общего показателя *e*. Для восстановления числа  по китайской теореме об остатках и нахождения корня степени  допускается использовать готовые процедуры. Тело сообщения – файл, зашифрованный алгоритмом AES-256 в режиме CBC. При длине исходного файла, не кратной 16 байтам, открытый текст дополняется символами с кодом 0x03 так, чтобы длина сообщения (файла) перед зашифрованием была кратна 16 байтам. Изначальная длина доступна в элементе данных «Длина сообщения» заголовка. Удаление выравнивания не обязательно;
* бесключевое дешифрование сообщения в случае малого порядка *e* в .

1. Разработать программу (**П-4**), которая осуществляет генерацию параметров криптосистемы RSA. Разработка процедур генерации случайных чисел и проверки числа на простоту не требуется. Генерация ключей должна обеспечивать выработку безопасных параметров криптосистемы с учетом произведенных атак. Выполнить анализ сгенерированных параметров с помощью инструмента CrypTool. Для этого в пункте «Asymmetric» раздела «Encrypt/Decrypt» выбрать «RSA Demonstration», ввести значение модуля *n* и открытого показателя *e* и запустить процедуру тестирования параметров, нажав «Factorize RSA modulus».

### Содержание отчета

1. Формулировка задания.
2. Выполненная работа:
3. описание осуществленных атак;
4. параметры схемы RSA, используемые при атаках.
5. содержимое дешифрованных файлов и его тип, найденные значения закрытого ключа;
6. описание созданного алгоритма генерации параметров и ключей системы RSA;
7. пример сгенерированных ключей и параметров криптосистемы как последовательности модуля и экспоненты;
8. результаты тестирования сгенерированных параметров криптосистемы с помощью программы CrypTool.
9. Ответы на контрольные вопросы.
10. Выводы по работе.
11. Листинги программ.