Государственный Университет Молдовы

Факультет Математики и Информатики

Департамент Информатики

“Криптография и информационная безопасность”

Индивидуальная работа №1

Алгоритм RC2

Преподаватель: O.Cerbu

Выполнил: Маруневич Николай группа I1902

Кишинев 2022

Алгоритм шифрования RC2 был разработан в конце 1980-х гг. (в различных источниках указаны 1987 и 1989 гг.) Рональдом Ривестом, который, в частности, разработал алгоритм RC5.

Является собственностью компании RSA Data Security, при этом известен тот факт, что разработку данного алгоритма инициировала и частично спонсировала фирма Lotus, которой требовался сильный (но не являющийся широко распространенным) алгоритм шифрования для последующего использования в программной системе Lotus Notes. Причем криптостойкость алгоритма должна была быть проверена Агентством Национальной Безопасности (АНБ) США. АНБ также внесло свой вклад в разработку алгоритма, предложив некоторые детали реализации, внедренные в алгоритм Ривестом.

Еще одна интересная особенность состоит в том, что RC2 был разрешен к экспорту за пределы США. Есть источники, в которых утверждается, что взамен на такое благоволение со стороны контролирующих органов Ри- вест внес в процедуру расширения ключа некие ослабляющие алгоритм действия. Автору данной книги не удалось, однако, найти об этом подробную информацию, поэтому алгоритм RC2 далее будет рассмотрен в варианте без подобных ослаблений.

Не менее интересен и тот факт, что долгое время после разработки RC2 структура данного алгоритма оставалась в секрете, но в начале 1996 г. анонимный автор опубликовал в Usenet-конференции исходные тексты алгоритма. Причем не ясно, была ли это утечка информации из RSA Data Security или результат реверс-инжиниринга какой-либо программной реализации алгоритма RC2.

Не известно, насколько долго алгоритм оставался бы в секрете, не будь этой анонимной публикации, но в марте 1998 г. Ривест полностью опубликовал алгоритм в виде RFC 2268.

Получил широкое распространение, как минимум, благодаря тому факту, что он является основным и обязательным для реализации алгоритмом шифрования согласно стандарту защиты сообщений электронной почты S/MIME.

**Структура алгоритма**

Алгоритм шифрует данные блоками по 64 бита с использованием ключей переменного размера: от 8 до 1024 битов включительно; рекомендуемым размером ключа является 64 бита.

Алгоритм является сетью Фейстеля, в нем выполняются 18 раундов преобразований. Причем раунды алгоритма делятся на 2 типа: смешивающие (mix) раунды и объединяющие (mesh) раунды. Общая структура алгоритма такова:

1.     Выполняются 5 смешивающих раундов.

2.     Выполняется 1 объединяющий раунд.

3.    Выполняются 6 смешивающих раундов.

4.     Выполняется 1 объединяющий раунд.

5.     Выполняются 5 смешивающих раундов.

Предполагается, что шифруемый блок данных разделен на 4 16-битных слова*R****q***…*R*3 \* наД ко~

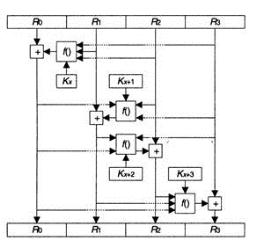
которыми смешивающий раунд в цикле по*i* от 0 до 3 выполняет следующие

операции

[http://crypto.pp.ua/img/shifr_image824-min-vs.jpg](http://crypto.pp.ua/img/shifr_image824.jpg)

где:

* Kj — фрагмент расширенного ключа, определяемый глобальной переменной*j\* данная переменная изначально равна нулю и увеличивается на 1 (как показано выше) в каждом смешивающем раунде; процедура расширения ключа подробно описана далее;
* & — побитовая логическая операция «и»;
* *~ х* — побитовый комплемент к*х\*

[](http://crypto.pp.ua/img/shifr_image826.jpg)

http://crypto.pp.ua/img/shifr_image850.jpg

http://crypto.pp.ua/img/shifr_image852.jpg

http://crypto.pp.ua/img/shifr_image854.jpg

6.     Для использования в шифрующих преобразованиях 128-байтная последовательность Lq.-.Lj27 представляется в виде 16-битных слов*К0…Квз:*

**Расшифровывание**

Расшифровывание выполняется по той же общей схеме, что и зашифровыва- ние. Однако при расшифровывании используются другие операции, выполняемые в смешивающем и объединяющем раундах.

Смешивающий раунд расшифровывания в цикле по*i* от 3 до 0 выполняет следующие операции:

где:

* циклический сдвиг вправо на число битов, определяемое значением St.
* начальное значение*j* устанавливается не в 0, а в 63.

Аналогичным образом изменен и объединяющий раунд при расшифровывании по сравнению с зашифровыванием. В нем в цикле по*i* от 3 до 0 выполняется следующая операция:

http://crypto.pp.ua/img/shifr_image856.jpg

**Криптостойкость алгоритма**

Почти сразу после опубликования RC2 вышла работа ряда известных криптологов: Рональда Ривеста, Ларса Кнудсена, Винсента Риджмена и Мэта Робшоу, — в которой исследовалось воздействие дифференциального и линейного криптоанализа на алгоритм RC2. Результаты оказались таковы:

* алгоритм не подвержен атаке методом линейного криптоанализа;
* алгоритм может быть теоретически вскрыт методом дифференциального криптоанализа, для чего необходимо наличие не менее 259 пар выбранных открытых текстов и соответствующих им шифртекстов — такая атака вряд ли реализуема на практике.

Не более практичной является атака на связанных ключах, для успешного проведения которой требуется наличие 234 выбранных открытых текстов и соответствующих им шифртектов, причем зашифровывание должно выполняться на ключе, связанном с искомым определенным простым соотношением. Данная атака изобретена не менее известными криптологами: Джоном Келси, Брюсом Шнайером и Дэвидом Вагнером.

Других методов вскрытия алгоритма RC2 на настоящий момент не известно.