МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт искусственного интелекта
Базовая кафедра №252 – информационной безопасности

ПРАКТИЧЕСКАЯ РАБОТА

Тема практической работы: «Алгоритм шифрования RC 5 XOR»

Студент группы ККСО-05-21	Копытин А.А.	_____ (*подпись*)
Руководитель практической работы	старший преподаватель Плешаков А.С.	_____ (*подпись*)
Работа представлена к защите	<___>_____2022 г.	
Допущен к защите	<___>_____2022 г.	

Москва - 2022

Содержание

1 RC 5

RC5 (*Ron's Code 5* или *Rivest's Cipher 5* — это блочный шифр, разработанный в 1994 году Роном Ривестом из компании RSA Security Inc. с переменным количеством ра ундов, длиной блока и длиной ключа. Это расширяет сферу использования и упрощает переход на более сильный вариант алгоритма.

1.1 Описание

Существует несколько различных вариантов алгоритма, в которых преобразования в "пол-раундах" классического RC5 несколько изменены. В классическом алгоритме используются три примитивных операции и их инверсии:

- сложение по модулю
- побитовое исключающее ИЛИ (XOR)
- операции циклического сдвига на переменное число бит ( ).

Основным нововведением является использование операции сдвига на переменное число бит, не использовавшиеся в более ранних алгоритмах шифрования. Эти операции одинаково быстро выполняются на большинстве процессоров, но в то же время значительно усложняют дифференциальный и линейный криптоанализ алгоритма.

Шифрование по алгоритму RC5 состоит из двух этапов. Процедура расширения ключа и непосредственно шифрование. Для расшифровки выполняется сначала процедура расширения ключа, а затем операции, обратные процедуре шифрования.

1.2 Параметры

Т.к. алгоритм RC5 имеет переменные параметры, то для спецификации алгоритма с конкретными параметрами принято обозначение RC5-W/R/b, где

- W — половина длины блока в битах, возможные значения 16, 32 и 64. Для эффективной реализации величину W рекомендуют брать равным машинному слову. Например, для 32-битных платформ оптимальным будет выбор W=32, что соответствует размеру блока 64 бита.
- R — число раундов, возможные значения от 0 до 255. Увеличение числа раундов обеспечивает увеличение уровня безопасности шифра. Так, при R=0 информация шифроваться не будет. Также алгоритм RC5 использует таблицу расширенных ключей размера слов, которая получается из ключа, заданного пользователем.
- b — длина ключа в байтах, возможные значения от 0 до 255.

2 Варианты алгоритма

Т.к. одним из свойств RC5 является его простота в реализации и анализе, вполне логично, что многие криптологи захотели усовершенствовать классический алгоритм. Общая структура алгоритма оставалось без изменений, менялись только действия выполняемые над каждым блоком в процессе непосредственно шифрования. Так появилось несколько различных вариантов этого алгоритма.

2.1 RC5XOR

В этом алгоритме сложение с ключом раунда по модулю заменено операцией XOR:

Этот алгоритм оказался уязвим к дифференциальному и линейному криптоанализу. Бирюкову и Кушилевицу удалось найти атаку методом дифференциального криптоанализа для алгоритма RC5XOR-32/12/16, используя 228 выбранных открытых текстов.

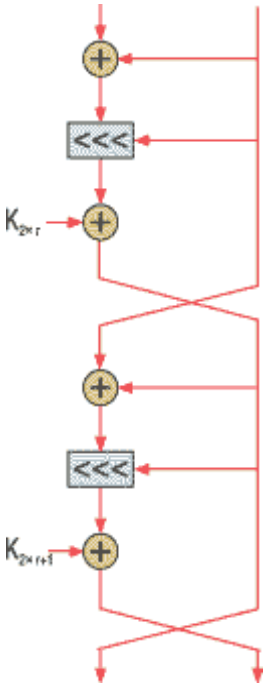

Рис.1

Алгоритм RC5XOR, в котором сложение с ключом раунда по модулю 2 заменено операцией XOR (рис.1):

A = ((A (+) B) <<< B) E K2*r mod 2w **.

Здесь и далее в качестве примера приведено только преобразование для вычисления левого субблока; правый вычисляется в следующей половине раунда аналогичным образом.

Данный алгоритм оказался менее стоек, чем RC5, как к линейному, так и к дифференциальному криптоанализу. В частности, Бирюков и Кушилевиц предложили атаку методом дифференциального криптоанализа, вскрывающую алгоритм RC5XOR-32/12/16 на основе 228 выбранных открытых текстов.