Оглавление

1. Цель лабораторной работы:

Реализовать алгоритм шифрования RC5.

2. Описание алгоритма шифрования

RC5 — это блочный шифр, разработанный Роном Ривестом из компании RSA Security с переменным количеством раундов, длиной блока и длиной ключа. Это расширяет сферу использования и упрощает переход на более сильный вариант алгоритма.

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

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. Все операции сложения и вычитания выполняются по модулю 2^w.

Расширение ключа:

Перед непосредственно шифрованием или расшифрованием данных выполняется процедура расширения ключа. Процедура генерации ключа состоит из четырёх этапов:

- Генерация констант
- Разбиение ключа на слова
- Построение таблицы расширенных ключей
- Перемешивание

Шифрованиение:

Перед первым раундом выполняются операции наложения расширенного ключа на шифруемые данные:

$$A = (A + S_0) \mod 2^w$$
$$B = (B + S_1) \mod 2^w$$

В каждом раунде выполняются следующие действия:

$$A = ((A \oplus B) \lll B) + S_{2i}$$
$$B = ((B \oplus A) \lll A) + S_{2i+1}$$

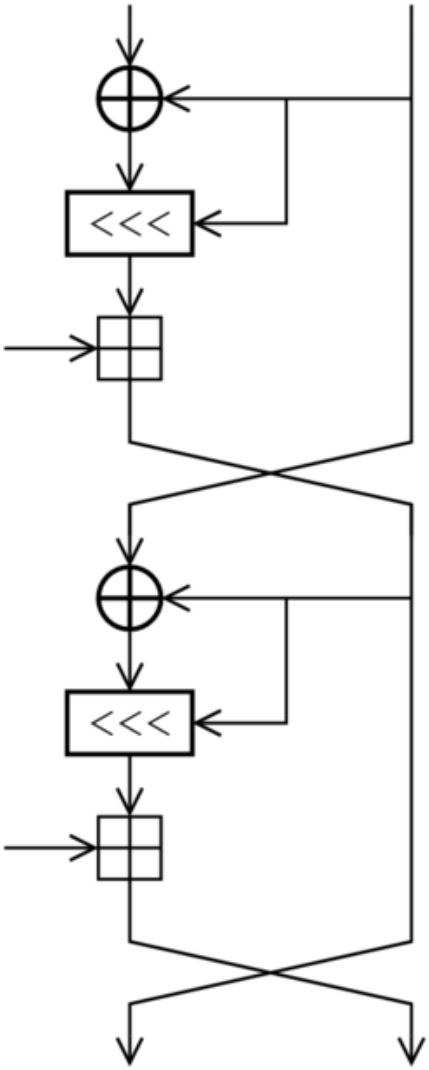


Рисунок 1. Схема алгоритма RC5

Дешифрование:

Для дешифрования данных используются обратные операции, то есть для $i = R, R-1, \ldots, 1$ выполняются следующие раунды:

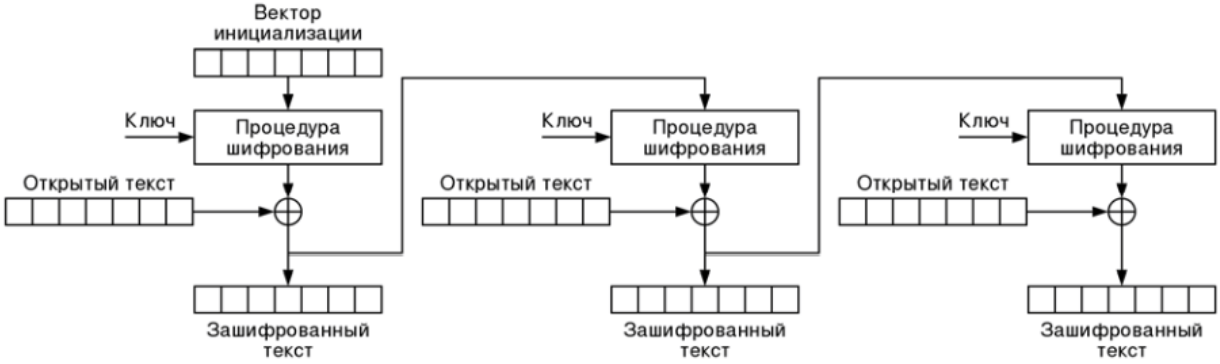
$$B = ((B - S_{2i+1}) \ggg A) \oplus A$$
$$A = ((A - S_{2i}) \ggg B) \oplus B$$

После выполнения всех раундов, исходное сообщение находится из выражения:

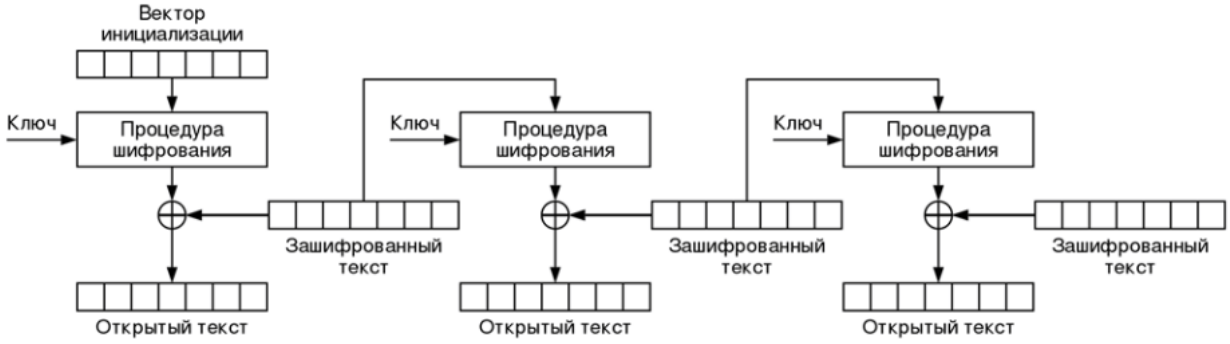
$$B = (B - S_1) \mod 2^w$$
$$A = (A - S_0) \mod 2^w$$

Режим CFB:

Режим обратной связи по шифротексту, режим гаммирования с обратной связью (англ. Cipher Feedback Mode, CFB) — один из вариантов использования симметричного блочного шифра, при котором для шифрования следующего блока открытого текста он складывается по модулю 2 с перешифрованным (блочным шифром) результатом шифрования предыдущего блока.



Шифрование в режиме CFB



Дешифрование в режиме CFB

Особенность режима CFB в том, что ошибка, которая возникает в шифротексте при передаче (например, из-за помех), сделает невозможным расшифровку как блока, в котором ошибка произошла, так и следующего за ним, однако не распространяется на последующие блоки

3. Пример работы программы

Рисунок 2. Исходное Изображение.

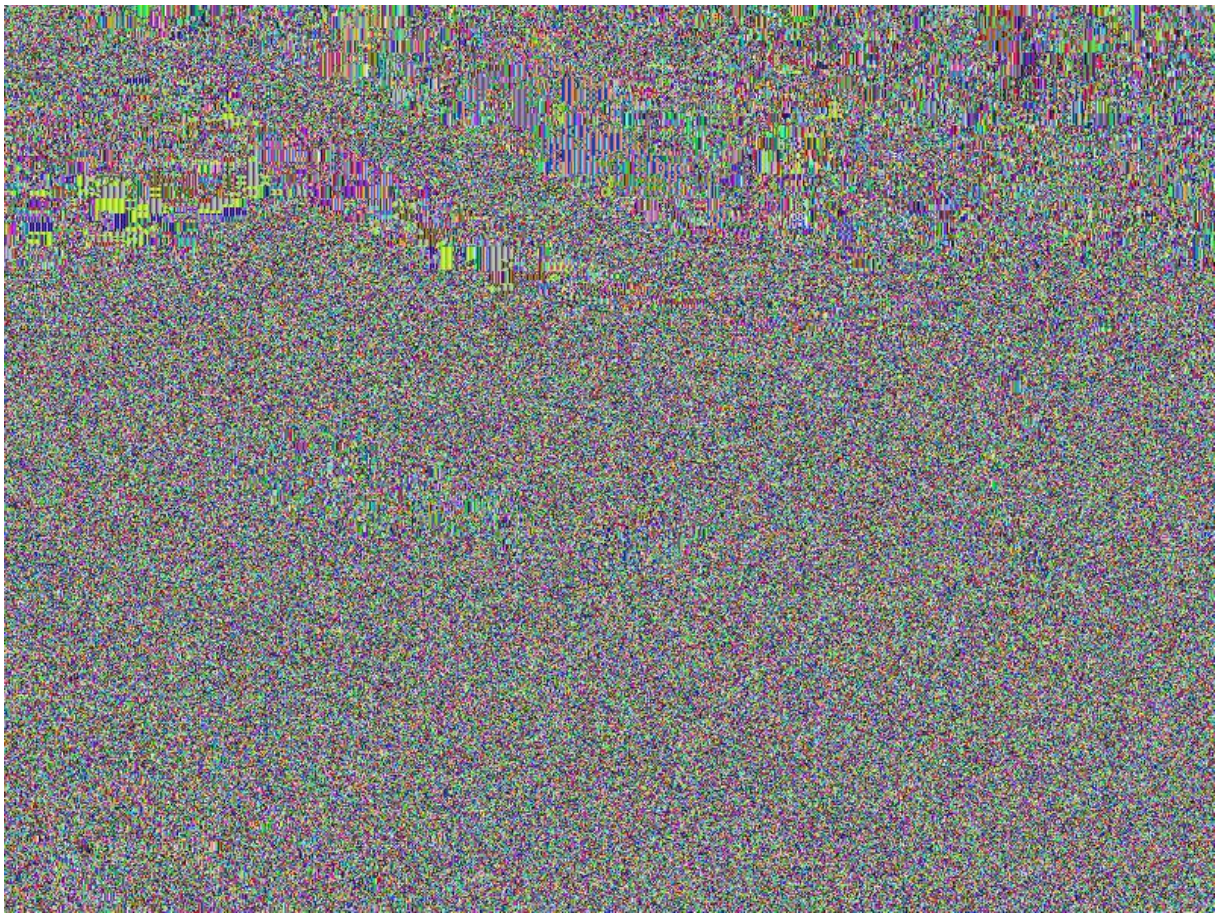


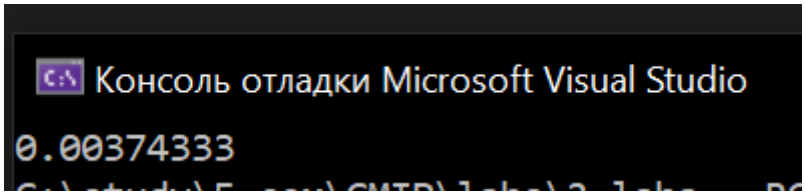
Рисунок 3. Закодированное изображение.

Рисунок 4. Раскодированное изображение.

Коэффициент корреляции:

$$\hat{r}_{A,B} = \frac{\hat{M}[(A - \hat{M}[A])(B - \hat{M}[B])]}{\hat{\sigma_A}\hat{\sigma_B}}$$

Результат вычисления коэффициента корреляции программой:



Полученное значение близко к нулю. Это свидетельствует о том, что исходное и зашифрованное изображения практически полностью различаются, и дешифрование без знания основного ключа не представляется возможным.

4. Криптостойкость

RSA потратила много времени на анализ его работы с 64-битным блоком. Так в период с 1995 по 1998 г. они опубликовали ряд отчётов, в которых подробно проанализировали криптостойкость алгоритма RC5. Оценка для линейного криптоанализа показывает, что алгоритм безопасен после 6 раундов. Дифференциальный криптоанализ требует 2^{24} выбранных

открытых текстов для алгоритма с 5 раундами, 2^{45} для 10 раундов, 2^{53} для 12 раундов и 2^{68} для 15 раундов. А так как существует всего лишь 2^{64} возможных различных открытых текстов, то дифференциальный криптоанализ невозможен для алгоритма в 15 и более раундов. Так что рекомендуется использовать 18-20 раундов, или по крайней мере не меньше 15 вместо тех 12 раундов которые рекомендовал сам Ривест.

5. Атака на алгоритм RC5

На платформах, где операция циклического сдвига на переменное число битов выполняется за различное число тактов процессора, возможна атака по времени исполнения на алгоритм RC5. Два варианта подобной атаки были сформулированы криптоаналитиками Говардом Хейзом и Хеленой Хандшух . Они установили, что ключ может быть вычислен после выполнения около 220 операций шифрования с высокоточными замерами времени исполнения и затем от 228 до 240 пробных операций шифрования. Самый простой метод борьбы с подобными атаками — принудительное выполнение сдвигов за постоянное число тактов (например, за время выполнения самого медленного сдвига)

6. Вывод

Таким образом, наиболее реальным методом взлома алгоритма RC5 (не считая варианты с небольшим количеством раундов и с коротким ключом) является полный перебор возможных вариантов ключа шифрования. Что означает, что у алгоритма RC5 практически отсутствуют недостатки с точки зрения его стойкости.

7. Список литературы.

1) Черчхаус. Коды и шифры

2) С.В. Беззатеев, Е.А. Крук, А.А. Овчинников “Блоковые Шифры. Учебное пособие”

3) М.Р. Гильмутдинов, А.М. Тюрликов, Е.М. Линский “Цифровая обработка изображений