ПРИМЕНЕНИЕ ТЕСТА КАСИСКИ ПРИ ПОТОКОВОМ ШИФРОВАНИИ

Шлык П. А., Болтак С. В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Болтак С. В. – ассистент

В работе описываются условия применимости теста Касиски для криптоанализа шифротекстов, полученных как результат потокового шифрования. Потоковое шифрование реализуется с использованием регистра сдвига с линейной обратной связью.

Функцией потокового шифрования определяется такой вид преобразования, результат которого зависит не только от значения используемого ключа шифрования, но и положения единицы шифрования в исходном тексте [1]. Используемой функцией потокового шифрования является функция, основанная на работе регистра сдвига с линейной обратной связью. Регистр сдвига с линейной обратной связью является конечным автоматом с конкретным количеством возможных состояний. Уникальное количество состояний регистра определяет размерность ключа. Элементом шифрования является бит информации. Предполагается, что исходным текстом для потокового шифрования является осмысленная последовательность символов естественного языка. Рассматриваемый язык задаётся соответствующим алфавитом. Так как максимальная размерность алфавита существующих языков не превышает количества возможных значений одного байта [2], то каждый символ исходного текста представлен в однобайтовой кодировке (например, КОИ-8).

Процесс расшифровки можно разделить на два этапа:

1. определение размерности ключа;
2. определение значения самого ключа.

Для определения размерности ключа предполагается использование частной реализации теста Касиски. Тест основан на следующих допущениях:

1. Ключ для шифрования имеет ограниченную размерность. Следовательно, использование ключа для заданного исходного текста носит периодический характер.
2. Периодическое применение ключа на различные фрагменты текста может привести к тому, что конкретные последовательности символов в исходном тексте будут отображены на соответствующие символы в шифротексте.
3. Размерность ключа достаточно мала по сравнению с размерами шифротекста, что позволяет установить периодический, неслучайный характер появления одинаковых последовательностей.

Значение самого ключа определяется с помощью перебора всех значений ключа заданного размера и поиска такого значения, при котором текст можно считать расшифрованным.

Вероятность появления случайной последовательности байтов, не соответствующей ни одной последовательности символов исходного текста, есть величина меньшая, чем при анализе соответствующих текстов, зашифрованных простым полиалфавитным шифром (например, шифром Вижинера). Это объясняется тем, что функция потокового шифрования переводит значение из пространства значений исходного текста, задающегося частичным, ограниченным диапазоном байта, в пространство значений шифротекста, задающегося всеми возможными значениями байта.

Неслучайный характер отображения последовательностей исходного текста на соответствующие последовательности шифротекста определяется следующим:

1. Если размерность ключа кратна 8, то результат функции потокового шифрования аналогичен результату применения полиалфавитного шифра. Но в данном случае тест Касиски даёт ответ, который необходимо перевести в битовую форму.
2. Если размерность ключа не кратна 8, то полученные значения расстояний между L-граммами будут находиться в линейной зависимости от размерности ключа (то есть, возможны значения, которые не будут определены как L-граммы вообще). По эмпирическим наблюдениям, результат теста Касиски будет кратным или равным истинному значению длины ключа шифрования.

Таким образом, реализация теста Касиски исходит из того, что:

1. количество L-грамм определённого размера мало;
2. количество случайных L-грамм мало.

Предлагается разделить значения расстояний между L-граммами одного размера на сильный пул и слабый пул значений. В сильном пуле поддерживается следующий инвариант: наибольший общий делитель значений отличен от 1. Новое значение добавляется в пул, если изменение общего делителя пула не превысит установленной величины. Иначе значение добавляется в слабый пул. В слабом пуле ведётся создание группы чисел, конкурирующей со значениями сильного пула. Если размер конкурирующей группы превысит размер сильного пула, то сильный пул будет заменён

конкурирующей группой. Ответом частной реализации теста Касиски является наибольший общий делитель среди всех общих делителей сильных пулов L-грамм конкретного размера.

Список использованных источников:

1. Ярмолик, В. Н. Элементы теории информации: Практикум / В. Н. Ярмолик, А. П. Занкович, С. С. Портянко. — Минск: БГУИР, 2007. — 39 с.

2.Guiness World Records — [Электронный ресурс]. — Режим доступа: https://www.guinnessworldrecords.com/world-records/longest-alphabet — Дата доступа: 31.03.2023.