# АНАЛИЗ УЯЗВИМОСТЕЙ ПОТОКОВЫХ КРИПТОСИСТЕМ НА БАЗЕ М-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Болтак С. В., Русакович Е. С.
Кафедра программного обеспечения информационных технологий,
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: s.boltak@bsuir.by

*Исследована криптостойкость потоковых криптосистем на базе М-последовательностей. Показана уязвимость данных систем. Предложен алгоритм, основанный на оптимизации метода Касиски. Разработано программное средство для взлома потоковых шифров.*

## Введение

Характерной особенностью потоковых криптосистем является использование криптографического ключа большой длины, равного длине шифруемого сообщения, для чего применяются генераторы псевдослучайных последовательностей [1].

М-последовательность – псевдослучайная двоичная последовательность максимальной длины, сгенерированная регистром сдвига с линейной обратной связью (Linear Feedback Shift Register – LFSR).

Генераторы М-последовательностей являются одним из наиболее часто используемых типов генераторов, так как обладают хорошими статистическими свойствами, которые практически не отличаются от свойств случайных последовательностей, и воспроизводимостью [2].

## I. Анализ предметной области

Для потоковых систем шифрования наиболее известными являются следующие методы криптоанализа: метод полного перебора ключей, метод Берлекэмпа-Мэсси, побочные атаки, корреляционные методы. Полный перебор требует больших затрат по времени, а также вычислительных мощностей и при большой длине ключа практически невозможен, так как основан на переборе всех возможных ключей и одновременного дешифрования. Алгоритм Берлекэмпа-Мэсси строит эквивалентный линейный рекуррентный регистр (ЛРР) с помощью которого генерируется исходная ключевая последовательность. Однако для построения ЛРР необходимо знать часть исходной информации и соответствующую ей криптограмму. Побочные атаки возможны при повторении шифрующих битов в ключевой последовательности, когда они повторяются и шифруют разную информацию, таким образом возникает уязвимость и шифр может быть вскрыт. Корреляционные атаки – наиболее распространённые атаки, что обусловлено построением поточных шифров. Они направлены на восстановление начального состояния регистров и используют корреляцию между их входными состояниями и выходной (ключевой) последовательностью схемы [3].

LFSR в качестве генераторов М-последовательностей имеют уязвимость, которая обусловлена линейным характером генерируемой последовательности. Если злоумышленнику удалось завладеть парой «исходный текст – шифротекст» длиной 2m бит, где m – длина регистра, то он может восстановить характеристический многочлен и, как результат, дешифровать сообщение [1].

Использование метода Касиски предполагает наличие периодического ключа. Суть метода заключается в том, что одинаковые биты шифруемой информации дают одинаковые фрагменты (l-граммы) криптограмм, если были зашифрованы одной и той же битовой ключевой последовательностью. Однако данный метод не исключает случайные l-граммы, что часто затрудняет определение периода ключа и позволяет определить его лишь с той или иной вероятностью [1].

При большом объёме шифруемой информации ключевая битовая последовательность будет иметь повторения, что делает возможным использование метода Касиски.

## II. Реализация

Предлагаемый алгоритм состоит из двух частей – определения расстояний между повторяющимися l-граммами и анализа расстояний для нахождения длины М-последовательности.

Для определения расстояний алгоритм выделяет первую l-грамму, ищет ее повторения до конца файла и заносит их в специальную структуру данных. Для увеличения быстродействия длина l-граммы берётся 5 байт, а поиск происходит многопоточно. В результате поиска будет сформирована структура, хранящая повторяющиеся l-граммы и соответствующие им расстояния, через которые данная l-грамма повторилась. Основная часть алгоритма – это анализ найденных расстояний и нахождение длины ключа. Классический тест Касиски предполагает нахождение наибольшего общего делителя найденных расстояний (НОД), это и есть предполагаемая длина периода ключа. Схема алгоритма функции анализа найденных расстояний между повторяющимися l-граммами изображена на рисунке 1.

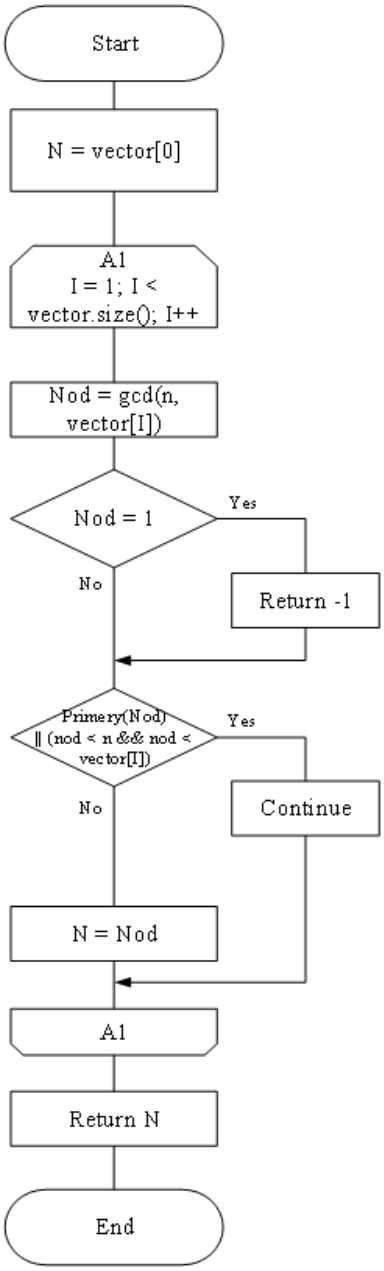


Рис. 1 – Алгоритм анализа расстояний

Для более точного нахождения длины ключа в существующий метод были внесены некоторые ограничения. Задача анализа расстояний состоит в том, чтобы исключить те расстояния, которые могут привести к нарушению корректности нахождения длины ключа, так как если хотя бы одно из расстояний случайно, оно изменит результат вычисления длины ключа для всех остальных расстояний. Например, если это случайное число простое, то нахождение НОД с этим числом приведёт к получению либо 1, либо самого числа, где 1 — всегда неверно, то есть вероятность правильного ответа низкая. Следовательно, необходимо на уровне анализа одной l-граммы получить непростое число с максимальным количеством делителей (чтобы повысить вероятность нахождения истинной длины ключа в делителях на дальнейшем этапе).

Шаги алгоритма:

1. взять первое расстояние;
2. взять следующее расстояние;
3. найти НОД двух расстояний;
4. если НОД равен 1, записать в результирующий массив -1;
5. если НОД не равен 1, то шаг 6;
6. если полученное значение не является простым числом, а также не равно ни одному из чисел, участвующих в вычислении НОД – текущему расстоянию присвоить найденный НОД;
7. повторять шаги 2-6 пока в массиве расстояний не останется одно число.

Описанный выше алгоритм применяется для всех найденных ранее l-грамм. В результате каждому массиву расстояний будет поставлено в соответствие одно число. Далее из массива удаляются все -1 и находится НОД оставшихся чисел. Найденное число и будет являться длиной искомого ключа.

## III. Выводы

Тестирование работы предложенного алгоритма проводилось для шифротекстов, полученных с помощью M-последовательностей на базе примитивных многочленов степени два, четырнадцать, восемнадцать и двадцать три. Время, понадобившееся для взлома, отображено в таблице 1.

Таблица 1 – Время взлома

| Степень полинома | Время взлома, мс |
|---|---|
| 2 | 2 |
| 4 | 122221 |
| 18 | 27843 |
| 23 | 3022844 |

Вероятность взлома для предлагаемого метода зависит от наличия повторений в шифрующей битовой последовательности, а также ограничена вычислительной мощностью используемого для вычислений компьютера.

Проведенные исследования могут быть использованы разработчиками потоковых криптосистем.

## Список литературы

1. Ярмолик, В. Н. Элементы теории информации: Практикум / В. Н. Ярмолик, А. П. Занкович, С. С. Портянко. – Минск: БГУИР, 2007. – 7–11 с.
2. Golomb, S. W. Shift register sequences. –San Francisco: Holden-Day, 1967. – 24 p.
3. Кутузов, А. В. Методы криптоанализа блочных и поточных систем шифрования / А. В. Кутузов, Н. В. Старченков, Д. А. Кудряшов // Современная техника и технологии. 2016. №9. – [Электронный ресурс]. Режим доступа: https://technology.snauka.ru/2016/09/10571. – Дата доступа: 12.08.2023.