УДК 004.056

Студ. Д. Э. Юрашевич
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

КОЛЛИЗИИ И НЕОБРАТИМОСТЬ ХЕШ-ПРЕОБРАЗОВАНИЙ В АЛГОРИТМЕ SHA-256

Хэш-функция – функция, преобразовывающая входную последовательность данных произвольного размера в выходную последовательность фиксированного размера. Процесс преобразования данных называется хеширование [1-4] .

Использование хеш-преобразований:

– проверка целостности данных (обнаружение изменений),

– системы аутентификации,

– создание и проверка ЭЦП.

Основное свойство всех хеш-функций – их необратимость, то есть, по хэшу невозможно восстановить первоначальные данные, по которым он вычислен. Это свойство позволяет применять хеширование в таких важных областях человеческой деятельности, как компьютерная безопасность и криптография. При этом хеш-функции, применяемые в криптографии, должны отвечать требованиям криптографической стойкости: должно быть практически невозможно подобрать для заданных данных другую последовательность данных с совпадающей хеш-функцией, и, кроме того, должно быть практически невозможно подобрать наугад две последовательности данных с совпадающим хэшем. Слово "практически" подразумевает разумную сложность подбора, определяемую математически.

Виды хеш-функций

1.Хеш-функции, основанные на делении. Пусть x – хешируемое сообщение, а N – максимально возможное число хеш-кодов. Тогда метод хеширования посредством деления будет заключаться в вычислении остатка от деления k на N: $h(x)= x \bmod N$.

2. Хеш-функции, основанные на умножении. Получить из исходной последовательности последовательность хеш-кодов, используя метод умножения (мультипликативный метод), значит воспользоваться хеш-функцией: $h(x)=\lfloor N*(\{x*A\})\rfloor$. Здесь A – рациональное число, по модулю меньшее единицы ($0<A<1$).

Также правая часть функции содержит три пары скобок, означающих следующее:

- ( ) – скобки приоритета;
- ⌊⌋ – скобки вычисления целой части;
- { } – скобки определения дробной части.

Хеш-функции семейства SHA-2 построены на основе структуры Меркла–Дамгора: – метода построения криптографических хеш-

функций, предусматривающего разбиение входных сообщений произвольной длины на блоки фиксированной длины и работающего с ними по очереди с помощью функции сжатия, каждый раз принимающего входной блок с выходным от предыдущего прохода. Популярность структуры Меркла–Дамгора обусловлена следующим результатом: если односторонняя функция сжатия {\displaystyle f} устойчива к коллизиям, то и хеш-функция, построенная на её основе, будет также устойчива к коллизиям.

Схематично алгоритм *Sha-256* можно представить следующим образом (см. рис.1) [2].

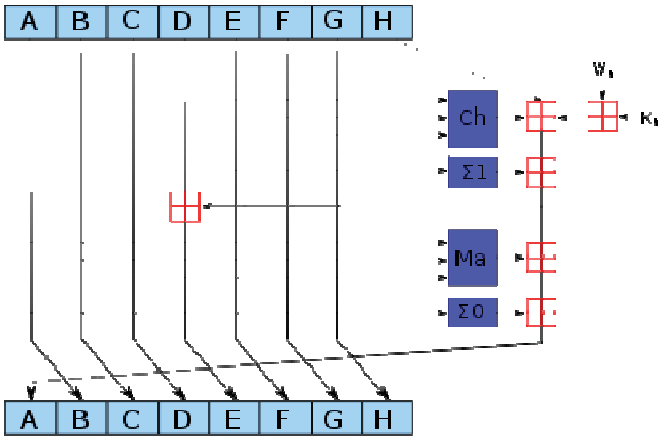

Рисунок 1 – Схема одной итерации алгоритмов SHA-256

Исходное сообщение после дополнения разбивается на блоки, каждый блок – на 16 слов. Алгоритм пропускает каждый блок сообщения через цикл с 64 или 80 итерациями (раундами). На каждой итерации 2 слова преобразуются, функцию преобразования задают остальные слова. Результаты обработки каждого блока складываются, сумма является значением хеш-функции. Тем не менее, инициализация внутреннего состояния производится результатом обработки предыдущего блока. Поэтому независимо обрабатывать блоки и складывать результаты нельзя.

Криптоанализ хеш-функции подразумевает исследование устойчивости алгоритма по отношению, по меньшей мере, к следующим видам атак:

– нахождение коллизий, то есть разных сообщений с одинаковым хешем,

– нахождение прообраза, то есть неизвестного сообщения по его хешу.

От устойчивости хеш-функции к коллизиям зависит безопасность электронной цифровой подписи с использованием данного хеш-алгоритма. От устойчивости к нахождению прообраза зависит, например, безопасность хранения хешей паролей для целей аутентифи-

кации, генерации ключей: клиент генерирует открытый ключ *pk* и секретный ключ *sk* для шифрования открытого текста. В большинстве случаев речь идет о безопасности сетевых технологий [1, 6].

Одной из причин необратимости является операция логического сдвига.Потеря некоторой части информации, совершить которую легко, а восстановить, что там было, можно только перебором. Схематично алгоритм сдвига можно представить в виде рис.2 [5].

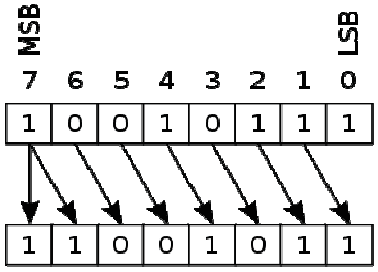

Рисунок 2 – Схема сдвига

Существуют и иные методы хеширования [7-8].

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ./ Урбанович П.П. – Минск: БГТУ, 2016. – 220 с.

2. Функции хэширования [Электронный ресурс]. – Режим доступа: http://mf.grsu.by/UchProc/livak/b_protect/zok_7.htm. Дата обращения: 10.04.2019.

3. Сингх, С. Книга шифров. Тайная история шифров и их расшифровки/ С. Сингх. – М.: Астрель, 2006. – Р. 150–215.

4. Мао, В. Современная криптография. Теория и практика / В. Мао. – М.: Вильямс, 2005. – Р. 16-80.

5. Алгоритмы / Хэш-функция SHA-256. [Электронный ресурс]. – Режим доступа: https://medium.com/dtechlog/алгоритмы-хэш-фнкция-sha-256-9862302f942f –Дата обращения: 09.04.2019.

6. Урбанович, П. П. Компьютерные сети: учебное пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. – Минск: БГТУ, 2011. – 399 с.

7. Urbanovich, P. The appearance of conflict when using the chaos function for calculating the hash code / P. Urbanovich, M. Plonkowski , K. Churikov // Przegląd elektrotechniczny. – 2012. – R. 88, № 11b. – P. 346-347.

8. Urbanovich, P. The appearance of conflict by using the chaos function to calculate the hash code /P. Urbanovich, M. Plonkowski, K. Churikau // 7th International Conference NEET'2011, Zakopane, Poland, June 28–July 1, 2011. – P. 151.