Группа: ИУ7-54Б; Исследовательская группа: 12ZEM; ФИО: Цховребова Я.Р.]

Хэширование - это процесс преобразования входных данных в фиксированный размер выходных данных с использованием хэш-функции.

Хэш-функция - это функция, которая принимает на вход произвольные данные и генерирует хэш-код (или хэш-значение), которое представляет собой уникальную строку байтов, идентифицирующую входные данные.

Криптографические хэш-функции предназначены для использования в криптографических приложениях, где безопасность данных играет критическую роль. Их основные свойства:

- Стойкость к коллизиям;
- Стойкость к нахождению первого прообраза;
- Стойкость к нахождению второго прообраза.

Криптографические хэш-функции формируются с использованием определенных математических и алгоритмических методов, которые обеспечивают стойкость к различным видам атак, непредсказуемость и равномерное распределение хэш-значений.

Большинство хэш-функций, предложенных в прошлом, были основаны на так называемой конструкции Меркла-Дамгаарда.

Контрукция Меркла-Дамгарда - это метод создания криптографических хэш-функций из блочных функций сжатия. Основная идея заключается в том, что сообщение разбивается на блоки, затем каждый блок итеративно преобразуется с использованием функции сжатия, а результаты объединяются, чтобы получить хэш-значение. Контрукция Меркла-Дамгарда широко используется для создания криптографических хэш-функций, таких как MD5 и SHA-1.

Формирование хэш-функций:

1. Хэш-функции, основанные на блочных шифрах: используют блочные шифры как часть процесса создания хэш-значения для входных данных. Они часто применяются в режиме Меркла-Дамгарда, где сообщение разбивается на блоки, и каждый блок сжимается с использованием блочного шифра. Это обеспечивает преобразование произвольно длинного входного сообщения в фиксированную длину хэш-значения.

1.1. Однодлинные конструкции: каждый блок данных, который обрабатывается хэш-функцией, имеет тот же размер, что и блок внутри блочного шифра. К ним относятся: конструкция Дейвиса-Мейера (используется в специализированных конструкциях хэш-функций, например, в семействе SHA-2, где "ключ" (блок сообщения) в два раза больше чем "блок открытого текста" (значение цепочки)); конструкция Матьяса-Мейера-Осеаса; конструкция Миягучи-Прениела (хэш-функции N-Hash и Whirlpool); конструкция Рабин.

1.2. Конструкции двойной длины - имеют двойной размер вывода по сравнению с размером блока данных, обрабатываемых хэш-функцией. Основные конструкции: MDC-2 и MDC-4; Tandem Davies-Meyer; Abreast Davies-Meyer; Hirose, FSE 2006.

2. Хэш-функции, основаные на использовании перестановок: предполагают использование только небольшого набора фиксированных ключей вместо ключевого расписания блочного шифра, что позволяет уменьшить сложность.

3. Специализированные дизайны хэш-функций.

MD2 (для 8-битных процессоров), MD4 (для 32-битных систем). Множество других хэш-функций были разработаны с использованием MD4 как основы. Все они основаны на конструкции Меркла-Дамгарда.

3.1. Семейство MD4: MD5, SHA-0, HAVAL, SHA-1, SHA-2 и другие.

Общие характеристики или особенности хэш-функций в семействе MD4:

- Обычно строятся на основе вариантов конструкции Меркла-Дамгарда;

- Используемая в этих хэш-функциях компрессионная функция часто может рассматриваться как блочный шифр в режиме Дэвиса-Мейера.

- Компрессионная функция состоит из нескольких простых шагов, каждый из которых обновляет состояние, содержащее несколько регистров;

- Каждый регистр в состоянии обычно является 32-битным или 64-битным значением;

- Используется относительно простое расширение сообщения или ключевое расписание (генерация подключей из основного ключа).