АЛГОРИТМЫ КРИПТОГРАФИЧЕСКОГО ХЕШИРОВАНИЯ ДАННЫХ

П.И. Удалой, М.С. Коротыгин, Е.С. Белоусова

В настоящее время хеш-функции распространены в системах проверки целостности и подлинности сообщений, аутентификации пользователей, для формирования и передачи электронно-цифровой подписи. Также хеш-функции используются при проведении статистических экспериментов, при тестировании логических устройств, при построении алгоритмов быстрого поиска и проверки целостности записей в базах данных.

Хеш-функции – это функции, предназначенные для «сжатия» произвольного сообщения или набора данных в некоторую битовую комбинацию фиксированной длины, называемую сверткой. Основным требованием к хэш-функциям является равномерность распределения их значений при случайном выборе значений аргумента.

Криптографические хеш-функции – это выделенный класс хеш-функций, который имеет определенные свойства, делающие его пригодным для использования в криптографии, то есть, делающие его криптостойким.

В рамках данного доклада будет представлен сравнительный анализ наиболее распространенных алгоритмов криптографического хеширования, проведенный на основе углубленного изучения различных видов хеширования, их статистических свойств и требований, предъявляемых к таким алгоритмам, а также будут выделены проблемы, возникающие при их использовании.

В ходе сравнительного анализа установлено, что разработчики в нынешнее время при выборе алгоритма хеширования, учитывая настолько большое количество различных хеш-функций, сталкиваются с компромиссом. Компромиссом между скоростью хеширования и криптостойкостью свертки – если, например, разработчику нужен в первую очередь быстрый, а не надежный, алгоритм он выбирает MD5. А если же ситуация противоположная, когда на первом месте стоит степень криптостойкости функции, а не ее скорость, разработчик выбирает SHA-384 или SHA-512. Если ситуация более сложная, когда разработчику одновременно важна скорость алгоритма и ее криптостойкость, он выбирает SHA-1 или SHA-256 [1–5].

Литература

1. Хеш-алгоритмы [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/93226/. – Дата доступа: 25.04.2021.

2. Криптографические хеш-функции [Электронный ресурс]. – Режим доступа: https://utmagazine.ru/posts/21195-kriptograficheskaya-hesh-funkciya. – Дата доступа: 25.04.2021.

3. Hashing algorithm [Электронный ресурс]. – Режим доступа: https://www.sciencedirect.com/topics/computer-science/hashing-algorithm. – Дата доступа: 25.04.2021.

4. MD5 Problems [Электронный ресурс]. – Режим доступа: https://www.avira.com/en/blog/md5-the-broken-algorithm/. – Дата доступа: 25.04.2021.

5. Cryptography Hash functions [Электронный ресурс]. – Режим доступа: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm. – Дата доступа: 25.04.2021.