Хеширование строк

1 Хеш-функции

Хеш-функция предназначена для свертки входного массива любого размера в битовую строку, для MD5 длина выходной строки равна 128 битам. Для чего это нужно? К примеру у вас есть два массива, а вам необходимо быстро сравнить их на равенство, то хеш-функция может сделать это за вас, если у двух массивов хеши разные, то массивы гарантировано разные, а в случае равенства хешей — массивы скорее всего равны.

Хеш-функции используются в криптографических алгоритмах, электронных подписях, кодах аутентификации сообщений, обнаружении манипуляций, сканировании отпечатков пальцев, контрольных суммах (проверка целостности сообщений), хеш-таблицах, хранении паролей и многом другом. К примеру, скачивая файл из интернета, вы часто видите рядом с ним строку вида b10a8db164e0754105b7a99be72e3fe5 — это и есть хеш, прогнав этот файл через алгоритм MD5 вы получите такую строку, и, если хэши равны, можно с большой вероятностью утверждать что этот файл действительно подлинный (конечно с некоторыми оговорками, о которых расскажу далее). [1]

2 MD5

Default2.

3 SHA-1

Default3.

Список литературы

[1] Марков А. С. and Цирлов В. Л. *Спецификация системы управления информационной безопасностью.* APS, 2021.