Свойство 1.

Детерминированность: независимо от того, сколько раз вычисляется H(M), M – const, при использовании одинакового алгоритма код хеш-преобразования h всегда должен быть одинаковым.

Свойство 2.

Скорость вычисления хеша h: если процесс вычисления h недостаточно быстрый, система просто не будет эффективной.

Свойство 3.

Сложность обратного вычисления: для известного H(М) невозможно (практически) определить М. Это важнейшее свойство хеш-функции для криптографических применений – свойство односторонности преобразования.

Свойство 4.

Даже минимальные изменения в хешируемых данных (М ≠ М') должны изменять хеш: Н(M) ≠ Н(М').

Свойство 5.

Коллизионная устойчивость (стойкость). Зная М, трудно найти такое М' (М ≠ М'), для которого H(М) = H(М').

Если последнее равенство выполняется, то говорят о коллизии 1-го рода.

Если случайным образом выбраны два сообщения (М и М'), для которых H(М) = H(М'), говорят о коллизии 2-го рода.

SHA-3 «криптографической губки». В этой конструкции реализован

итеративный подход для создания функции с произвольной длиной

на входе и произвольной длиной на выходе на основе определен

ного преобразования [49]. На основе технологии «губки» построен

ныне действующий в Беларуси стандарт хеширования [50].

SHA-256

Длина хеша: 256 бит.

Работает с 512-битными блоками.

Использует 8 регистров (A–H), 64 константы, 64 шага.

Основные функции:

Σ0, Σ1 — циклические сдвиги и XOR.

SHA-512

Длина хеша: 512 бит.

Работает с 1024-битными блоками.

80 шагов, 64-битные операции.

По структуре почти идентичен SHA-256, но рассчитан на 64-битные системы.

sha1 на выходе 160

sha2 - длина хешей соответствует числу, дополняющему через дефис название алгоритма

sha3 на вых произв длины

Яна, [28.05.2025 10:33]

иниц 4 константы к 3 из них нелин функция потом резтат складс с одной из 4 окнстант и потом опять этот результат склад с подблоком сообщения Ь потом с константой Т и сдвиг ввправо на С значений и этот результат склад с однй из 4 перем . пототм 4 этапа по 16 операция и коканнация этого всего