КРАТКИЕ СВЕДЕНИЯ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Функция | Разработчик | Год | Размер вывода (бит) | Размер слова | Количе ство раундов |
| MD5 | **Рональд Ривест** | **1992** | **128** | **32** | 64 |
| SHA-256 SHA-384 SHA-512 | **АНБ** | **2002** | **256/384/512** | **64** | 80 |
| SHA-224 | **2004** | **224** | **32** | 64 |
| BLAKE2b | 1. **Жан-Филипп Аумассон** 2. **Сэмюэл Невес Зуко** 3. **Уилкокс-О'Хирн** 4. **Кристиан Виннерляйн** |  | **512** | **64** | 12 |
| BLAKE2s | 2012 | 256 | 32 | 10 |

ПОДРОБНОЕ ОПИСАНИЕ

1. MD5 (Message Digest 5)

♦️**Принцип работы:** MD5 — это устаревшая криптографическая хеш-функция. Она обрабатывает данные блоками по 512 бит и выводит хеш размером 128 бит.

♦️**Как работает:** MD5 использует серию побитовых операций, модульных сложений и обращений к таблице для перемешивания входных данных. Работает в несколько этапов и раундов.

♦️**Безопасность:** MD5 считается криптографически сломанным. Коллизии можно найти относительно легко, что делает его непригодным для большинства приложений безопасности (например, хранение паролей, цифровые подписи, контрольные суммы, где требуется защита от несанкционированного изменения). В настоящее время его основное применение — контрольная сумма для проверки целостности файлов (где защита от вредоносного вмешательства не является важной) или как простой идентификатор в базе данных.

**Размер вывода:** 128 бит (16 байт)

2. Семейство SHA-2 (Secure Hash Algorithm 2) (SHA-256, SHA-384, SHA-512, SHA-224)

♦️**Принцип работы:** SHA-2 — это семейство криптографических хеш-функций, разработанных NSA. Работает аналогично MD5, но использует более сложные шаги и блоки большего размера для повышения безопасности.

♦️**Как работает:** Алгоритмы SHA-2 используют те же принципы, что и MD5 (побитовые операции, модульные сложения, функции смешивания), но имеют более сложные раунды, больше раундов и блоки большего размера, что увеличивает сложность вычислений. В семействе есть несколько вариантов, которые генерируют хеши разного размера.

♦️**Безопасность:** Алгоритмы SHA-2 по-прежнему считаются достаточно безопасными для большинства приложений, хотя были обнаружены некоторые уязвимости, и исследования продолжаются. Они гораздо более безопасны, чем MD5. Широко используются в веб-безопасности, цифровых подписях и криптовалютах.

• SHA-256 и SHA-512 являются наиболее широко используемыми членами этого семейства.

• SHA-224 и SHA-384, по сути, являются усеченными версиями SHA-256 и SHA-512 соответственно.

**Размер вывода:**

• SHA-256: 256 бит (32 байта)

• SHA-384: 384 бита (48 байт)

• SHA-512: 512 бит (64 байта)

• SHA-224: 224 бита (28 байт)

3. Семейство BLAKE2 (BLAKE2b, BLAKE2s)

♦️**Принцип работы:** BLAKE2 — это семейство криптографических хеш-функций, разработанное как более быстрая и безопасная альтернатива MD5 и SHA-1, а также для обеспечения лучшей производительности, чем SHA-2.

♦️**Как работает:** BLAKE2 основан на потоковом шифре ChaCha, который известен своей скоростью и безопасностью. Он использует более эффективную внутреннюю структуру по сравнению с MD5 и SHA-2.

♦️**Безопасность:** BLAKE2 считается очень безопасным и имеет очень хорошую производительность. Он широко используется в высокопроизводительных приложениях безопасности.

• BLAKE2b оптимизирован для 64-битных платформ и имеет переменный размер вывода.

• BLAKE2s оптимизирован для 32-битных платформ и имеет переменный размер вывода.

**Размер вывода:** - переменный, но обычно:

• BLAKE2b: 256 бит (32 байта) или больше

• BLAKE2s: 256 бит (32 байта) или меньше

**❗️Ключевые различия:**

• **Безопасность:** MD5 взломан, SHA-2 считается достаточно безопасным (с широко используемыми SHA-256 и SHA-512), а BLAKE2 считается очень безопасным.

• **Скорость:** BLAKE2 обычно быстрее, чем SHA-2, особенно на современном оборудовании. MD5 самый быстрый (но очень небезопасный).

• **Размер вывода:** Размер вывода различается. Больший размер хеша (например, SHA-512, BLAKE2b) обычно обеспечивает лучшую устойчивость к коллизиям, но с небольшими затратами производительности.

• **Сложность:** MD5 самый простой, SHA-2 более сложный, а BLAKE2 имеет более современную и эффективную внутреннюю структуру, основанную на блочном шифровании.

**❗️Рекомендации:**

• Избегайте MD5 для всего, что связано с безопасностью.

• SHA-256 или SHA-512 — хороший выбор общего назначения, если BLAKE2 недоступен.

• BLAKE2b/BLAKE2s — отличный выбор для быстрого и высокопроизводительного хеширования.

• Всегда обновляйте ваши криптографические библиотеки