

Выбор хеш- алгоритма

Хеш-алгоритмы



- MD2
- MD4
- MD5
- SHA
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Хеш-алгоритм MD2, MD4, MD5



На данный момент данные алгоритмы
считаются взломанными

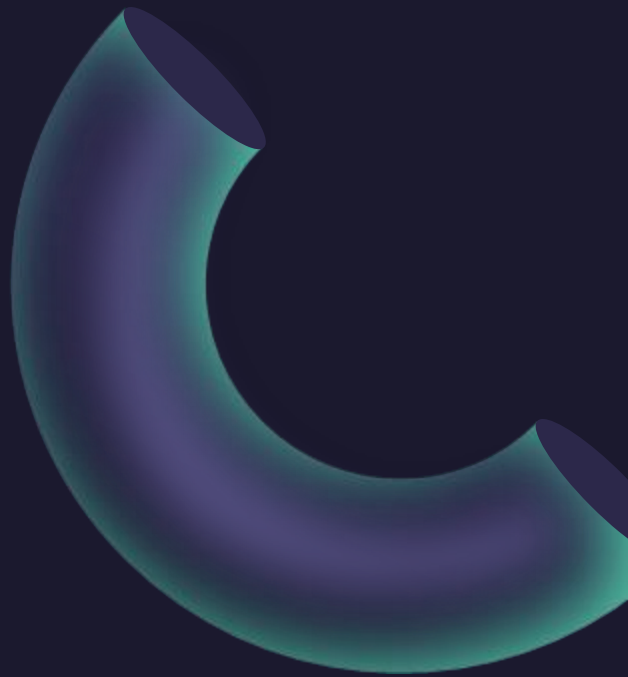
- MD2 – 1996;
- MD4 – 1996;
- MD5 – 2004;





Алгоритм SHA-1

Также была найдена коллизия на 64-раундовый алгоритм с вычислительной сложностью около 2^{35} операций.



Отказ браузеров от SHA-1

С 2017 года основные браузеры отказываются от использования алгоритма SHA-1:

- Mozilla
- Chrome
- Opera
- Яндекс.Браузер

Оптимальный выбор алгоритма

В настоящее время оптимальным алгоритмом хеширования является SHA-256.
Основными преимуществами данного алгоритма:

- Скорость работы
- Надежность

