

**ІІТМО**

**Семейство алгоритмов  
SHA-2**

# История появления SHA-2

- В 1993г. разработан алгоритм SHA-0
- В 1995г. опубликован исправленный и доработанный SHA-1
- В 2002г. разработан SHA-2
- В марте 2012 вышла последняя на текущий момент редакция стандарта
- В 2015 опубликован новый алгоритм шифрования SHA-3



SHA-1 и SHA-2 - две разные версии алгоритма SHA. Они различаются в конструкциях (как создается хеш из исходных данных) и в битовой длине подписи. SHA-2 является «семейством» хэшей и имеет различную длину.



Алгоритм SHA-3 мало похож на SHA-2, у них мало общего кроме имени. SHA-2 использует структуру Дэвиса-Мейера с блочным шифром; SHA-3 использует структуру губки с перестановкой Кекчака. SHA-3 более новый (и надежный) стандарт шифрования, но функции SHA-2 имеют более высокую производительность по сравнению с SHA-3.

Исходное сообщение после дополнения разбивается на блоки, каждый блок на 16 слов.

Алгоритм пропускает каждый блок сообщения через цикл с 64 или 80 итерациями (раундами).

На каждой итерации 2 слова преобразуются, функцию преобразования задают остальные слова.

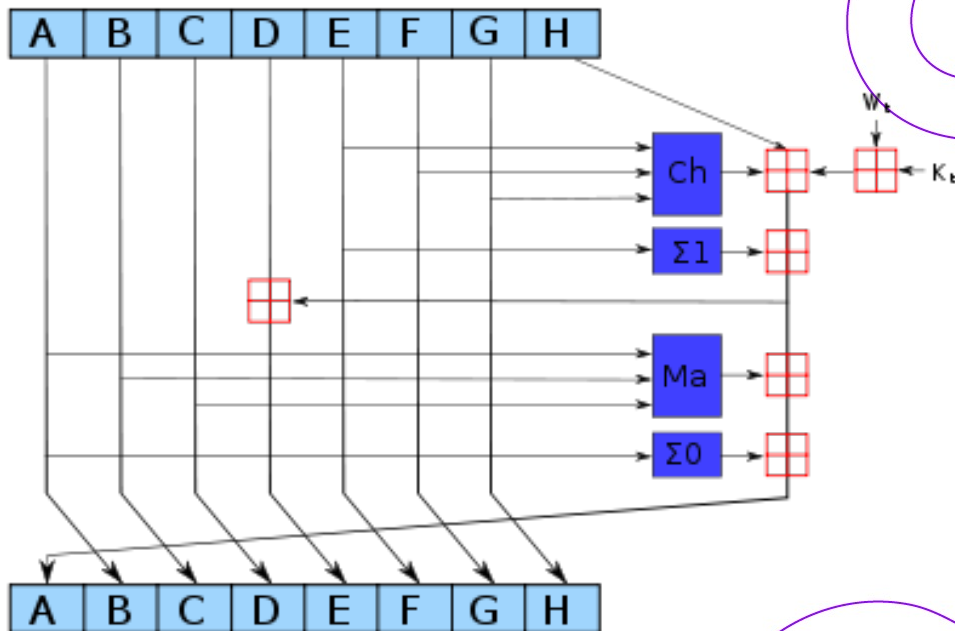
Результаты обработки каждого блока складываются, сумма является значением хеш-функции.



Инициализация внутреннего состояния производится результатом обработки предыдущего блока. Поэтому **независимо обрабатывать блоки и складывать результаты нельзя.**



# Алгоритм работы SHA-256 (семейство SHA-2)

ІТМО



Каждый блок SHA-256   имеет фиксированный размер 512 бит. Если длина сообщения превышает размеры блока, то создаются дополнительные до тех пор, пока все сообщение не уместится. Если последний из дополнительных блоков заполнен не полностью, то его дополняют до конца нулями.

# Сравнение хеш-функций семейства SHA-2



Хеш-функция	Длина дайджеста сообщения (бит)	Длина внутреннего состояния (бит)	Длина блока (бит)	Максимальная длина сообщения (бит)	Длина слова (бит)	Количество итераций в цикле	Скорость (MiB/s) <sup>[7]</sup>
SHA-256, SHA-224	256/224	256 (8 × 32)	512	$2^{64} - 1$	32	64	139
SHA-512, SHA-384, SHA-512/256, SHA-512/224	512/384/256/224	512 (8 × 64)	1024	$2^{128} - 1$	64	80	154

В 2003 году Гилберт и Хандшух провели исследование *SHA-2*, но не нашли каких-либо уязвимостей. Однако в марте 2008 года индийские исследователи нашли коллизии для 22 итераций *SHA-256* и *SHA-512*. В сентябре того же года они представили метод конструирования коллизий для усечённых вариантов *SHA-2* (21 итерация). Позднее были найдены методы конструирования коллизий для 31 итерации *SHA-256* и для 27 итераций *SHA-512*.

Ввиду алгоритмической схожести *SHA-2* с *SHA-1* и наличия у последней потенциальных уязвимостей принято решение, что *SHA-3* будет базироваться на совершенно ином алгоритме. В 2012 года NIST утвердил в качестве *SHA-3* алгоритм Кецсак.

**Спасибо  
за внимание!**

**it**MO *re than a*  
**UNIVERSITY**

Соловьев Артемий Александрович,  
студент группы Р32151