АМЕРИКАНСКИЙ СТАНДАРТ ХЭШ-ФУНКЦИИ (SHS)

Стандарт функции хеширования SHS (Secure Hash Standard) -

Стандарт США, определяющий алгоритмы вычисления значения хеш-функции: алгоритм SHA-1(введен в действие в 1995 г.) и алгоритмы SHA-256, SHA-384, SHA-512 (введены в действие в 2002 г.)

Алгоритм SHA-1

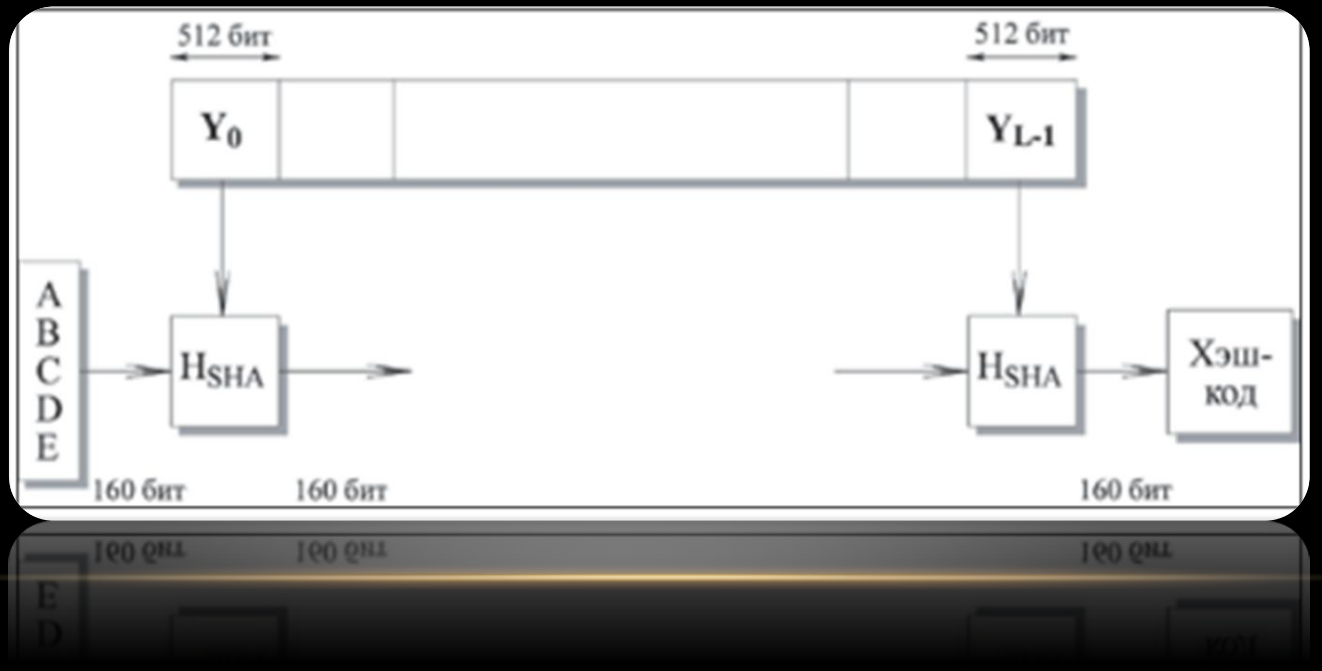
Хэш-функция SHA-1

Алгоритм состоит из следующих шагов:

Шаг 1: добавление недостающих битов

Шаг 2: добавление длины

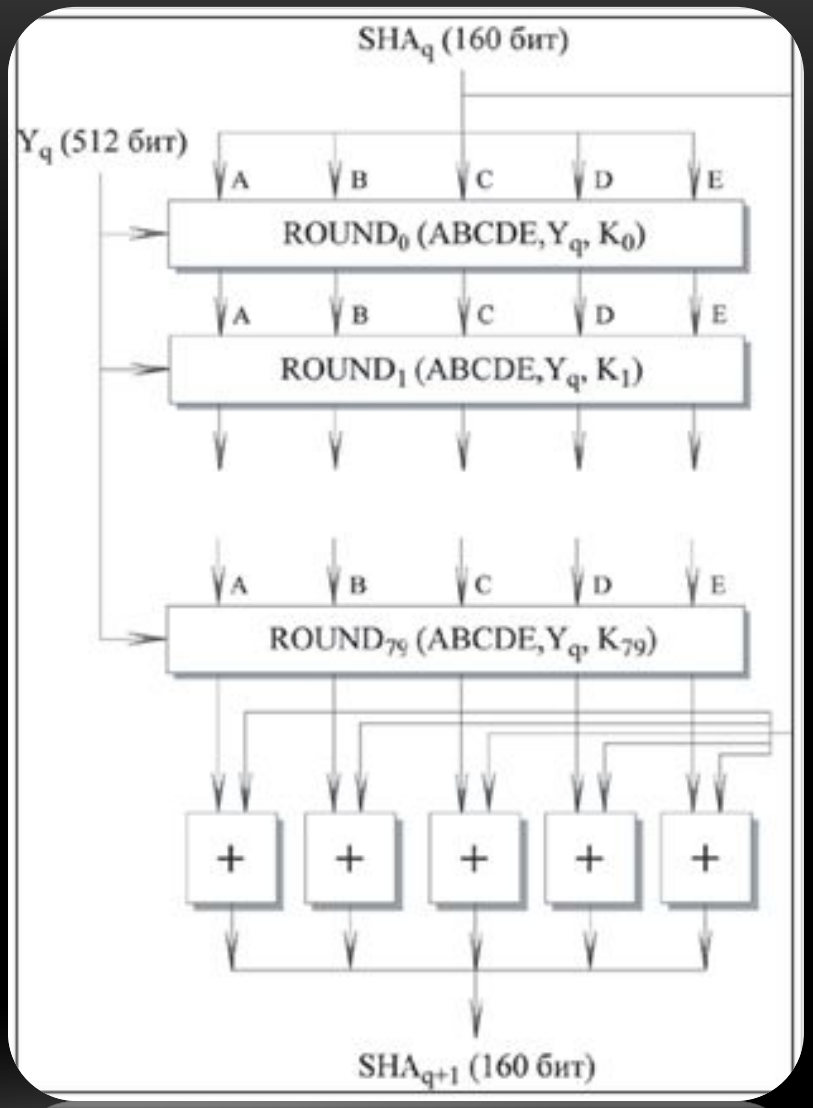
Шаг 3: инициализация SHA-1 буфера



Шаг 4:

обработка сообщения в 512-битных (16-словных) блоках

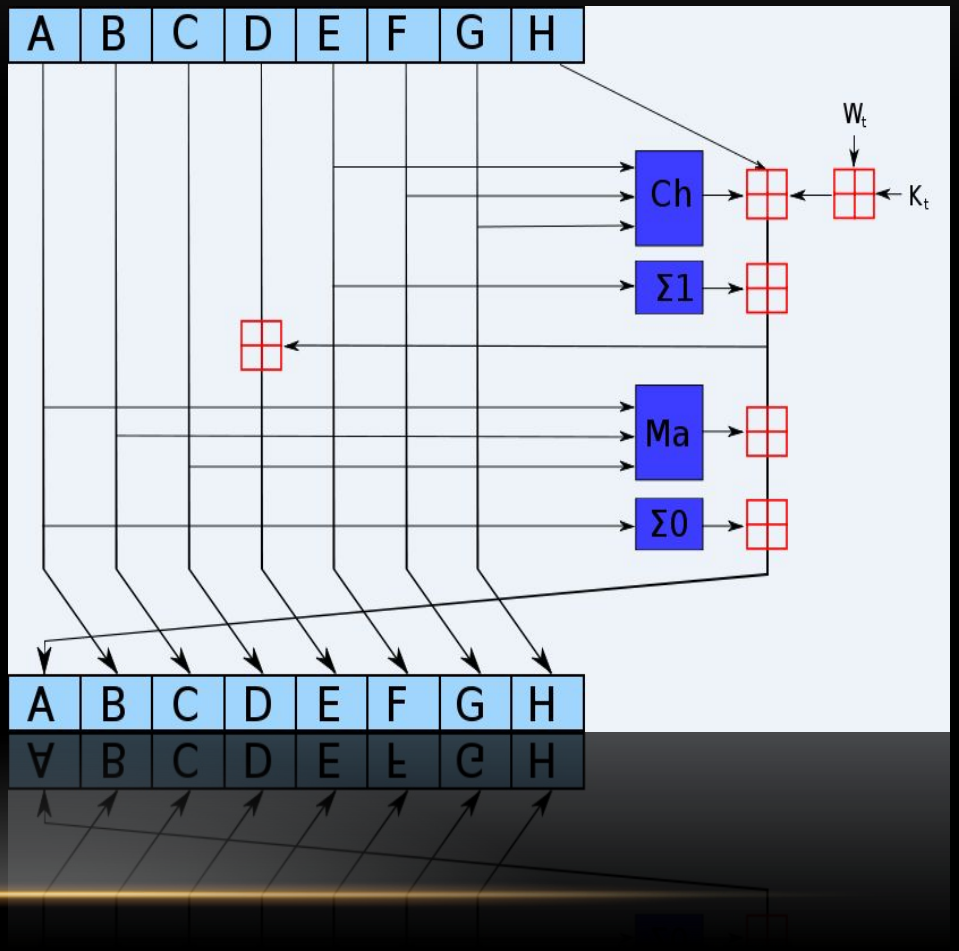
Шаг 5: выход



АЛГОРИТМ SHA-2

Хеш-функции семейства SHA-2 построены на основе структуры Меркла — Дамгарда.

Исходное сообщение после дополнения разбивается на блоки, каждый блок — на 16 слов. Алгоритм пропускает каждый блок сообщения через цикл с 64-мя или 80-ю итерациями (раундами). На каждой итерации 2 слова преобразуются, функцию преобразования задают остальные слова. Результаты обработки каждого блока складываются, сумма является значением хеш-функции. Тем не менее, инициализация внутреннего состояния производится результатом обработки предыдущего блока. Поэтому независимо обрабатывать блоки и складывать результаты нельзя.



СРАВНЕНИЕ ВАРИАЦИЙ АЛГОРИТМА SHA

Вариации алгоритма		Размер выходного хеша (бит)	Промежуточный размер хеша (бит)	Размер блока (бит)	Максимальная длина входного сообщения (бит)	Размер слова (бит)	Количество раундов	Используемые операции	Найденные коллизии
SHA-0		160	160	512	$2^{64} - 1$	32	80	+,and, or, xor, rotl	Есть
SHA-1		160	160	512	$2^{64} - 1$	32	80	+,and, or, xor, rotl	2^{52} операций
SHA-2	*SHA-256/224*	256/224	256	512	$2^{64} - 1$	32	64	+,and, or, xor, shr, rotr	Нет
	SHA-512/384	512/384	512	1024	$2^{128} - 1$	64	80	+,and, or, xor, shr, rotr	Нет