Содержание:

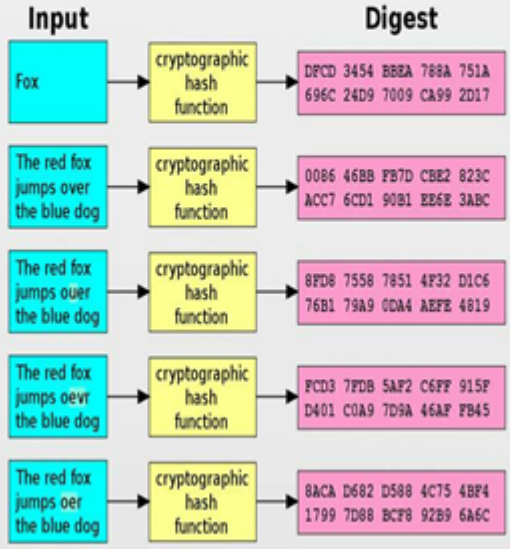
Функция хеширования.

Хеш-функция (англ. hash function от hash — «превращать в фарш», «мешанина»), другими словами функция свёртки — она занимается преобразованием массива входных данных произвольной длины в битовую строчку предустановленной ранее длины, выполняемым определённым алгоритмом. Хешированием называется преобразование, производимое хеш-функцией. Исходные данные называются «ключом» или «сообщением». Результат называется «хешем», «хеш-кодом», «хеш-суммой».

Примеры свойств алгоритмов хеширования:

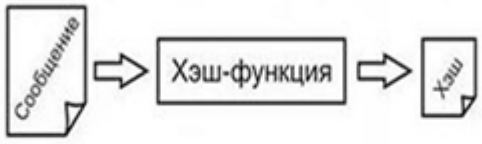
- разрядность;
- вычислительная сложность;
- криптостойкость.

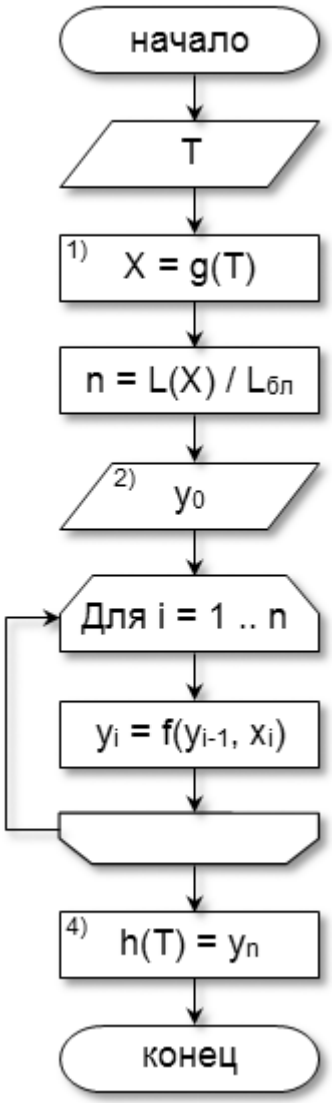
Cryptographic hash function



https://en.wikipedia.org/wiki/File:Cryptographic_Hash_Function.svg

ФУНКЦИЯ ХЭШИРОВАНИЯ





вычисления (стандартная схема хеш-функции

1)К исходному сообщению **T** прибавляется дополнительная информация так, чтобы длина **X** была кратной величине $\mathbf{L_{бл}}$, определенной спецификацией хеш-функции.

2)Для инициализации данной процедуры хеширования используется синхронизировнная ссылка $\mathbf{y_0}$.

3)Прообраз **X** разбивается на **n**-ое кол-во блоков $\mathbf{x_i}$ (i = 1 .. n) фиксированной длины $\mathbf{L_{бл}}$, над которыми будет производится однотипная процедура хеширования $\mathbf{f(y_{i-1}, x_i)}$, зависимая от результатов ключом предыдущего блока $\mathbf{y_{i-1}}$.

4)Хеш-образом **h(T)** изначального сообщения **T** будет является результат процедуры хеширования $\mathbf{y_n}$, полученный после обработки конечного

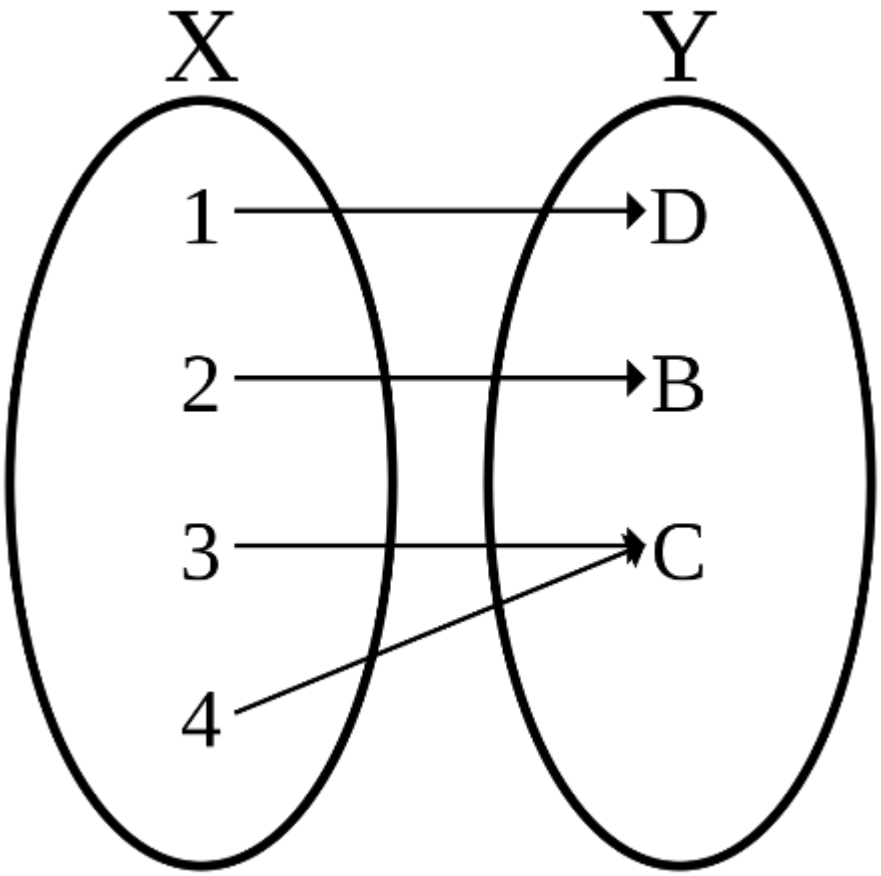
блока переменной $\mathbf{x_n}$.

Коллизией для функции **h** является одна пара значений **x, y, x ≠ y**, что **h(x) = h(y)**. За этим следует, что образ хеш-функции должна принять следующие свойства:

- для данного значения **h(x)** нет возможности найти значение аргумента **x**. Данные хеш-функции называют **стойкими в вплане обращения** или **стойкими в сильном понимании**;

- для данного аргумента **x** нет возможности найти другой аргумент **y** , что **h(x) = h(y)**. А уже эти хеш-функции называют **стойкими в плане вычисления коллизий** или **стойкими в слабом смысле**.

В другом исходе, когда значение хеш-функции будет зависит не только от прообраза, но и от ключа, который закрыт, то это значение будет называться кодом проверки подлинности сообщений (Message Authentication Code, MAC) или кодом проверки подлинности данных (Data Authentication Code, DAC), иначе **имитовставкой**.



Коллизии будет возникать только тогда, когда хеш-функция не инъективна. Значениям 3 и 4 в области определения представленной на рисунке функции относится одно и то же значение C этой функции; иначе говоря, пара 4 и 3 является коллизией функции

Самую простую хеш-*функцию* можно составить с использованием *операции* "сумма по модулю 2" таким образом: мы получим входную строку, далее складываем все байты по модулю 2 и *байт*-результат возвращаем в качестве значения хеш-фукнции. *Длина* значения хеш-функции будет составлять в этом случае 8 *бит* независимо от размера входного сообщения.

Например, пусть изначальное сообщение, переведенное в цифровой формат, было таким (в 16-ом формате):

3E 54 A0 1F B4

Мы преобразуем сообщение в двоичную систему счисления, запишем байты друг под другом, а затем сложим биты в каждом столбике по модулю 2:

0011 1110

0101 0100

1010 0000

0001 1111

1101 0100

0110 0101

Результатом ($0110\ 0101_{(2)}$ или $65_{(16)}$) и будет значением хеш-функции.

Хеш-функции применяются в следующих направлениях:

- для построения ассоциативных массивов;
- для поиска дубликатов в сериях наборов данных;
- построении уникальных идентификаторов;
- так же для вычислении контрольных сумм от сигнала для последующего обнаружения в них ошибок, появляющихся при хранении или передаче каких либо данных;
- не мало важным направлением является сохранении паролей в системах защиты в виде хеш-кода
- а еще при создании электронной подписи

Список литературы:

- https://info-farm.ru/alphabet_index/kh/khehsh-funkciya.html
- https://kvodo.ru/hesh-funktsii.html
- https://intuit.ru/studies/courses/691/547/lecture/12381
- https://intuit.ru/studies/courses/12181/1174/lecture/25261 *(полезная ссылка, там более подробно описаны принципы работы тех или иных функций)*
- https://ru.wikipedia.org/wiki/Коллизия_хеш-функции
- https://abcdwork.ru/kriptovalyuta/chto-takoe-xeshirovanie-i-dlya-chego-ono-nuzhno.html
- https://cryptoperson.ru/cryptography/chto-takoe-hjesh-kod-i-hjesh-funkcija-prakticheskoe-primenenie-obzor-populjarnyh-algoritmov
- https://ru.wikipedia.org/wiki/Хеш-функция
- https://www.sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema9

- https://wreferat.baza-referat.ru/Хэш-функция