Содержание:

Введение

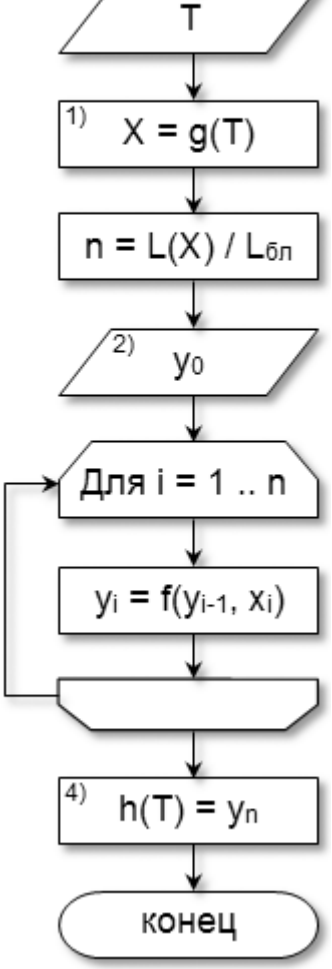
Хеш-функция (англ. hash function от hash — «превращать в фарш», «мешанина»), или функция свёртки — функция, осуществляющая преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом. Преобразование, производимое хеш-функцией, называется хешированием. Исходные данные называются входным массивом, «ключом» или «сообщением». Результат преобразования (выходные данные) называется «хешем», «хеш-кодом», «хеш-суммой», «сводкой сообщения».

Хеширование (иногда хэширование, англ. hashing) - преобразование входного массива данных произвольной длины в выходную строку фиксированной длины. Такие преобразования также называются **хеш-функциями** или **функциями свёртки**, входной массив – **прообразом**, а результаты преобразования - **хешем, хеш-кодом, хеш-образом, цифровым отпечатком** или **дайджестом сообщения** (англ. message digest).

Существует множество алгоритмов хеширования, отличающихся различными свойствами. Примеры свойств:

- разрядность;
- вычислительная сложность;
- криптостойкость.

Процедура вычисления (стандартная схема алгоритма) хеш-функции



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

2)Для инициализации процедуры хеширования используется синхропосылка $\mathbf{y_0}$.

3)Прообраз **X** разбивается на **n** блоков $\mathbf{x_i}$ (i = 1 .. n) фиксированной длины $\mathbf{L_{бл}}$, над которыми выполняется однотипная процедура хеширования $\mathbf{f(y_{i-1}, x_i)}$, зависящая от результата хеширования предыдущего блока $\mathbf{y_{i-1}}$.

4)Хеш-образом **h(T)** исходного сообщения **T** будет результат процедуры хеширования $\mathbf{y_n}$, полученный после обработки последнего блока $\mathbf{x_n}$.

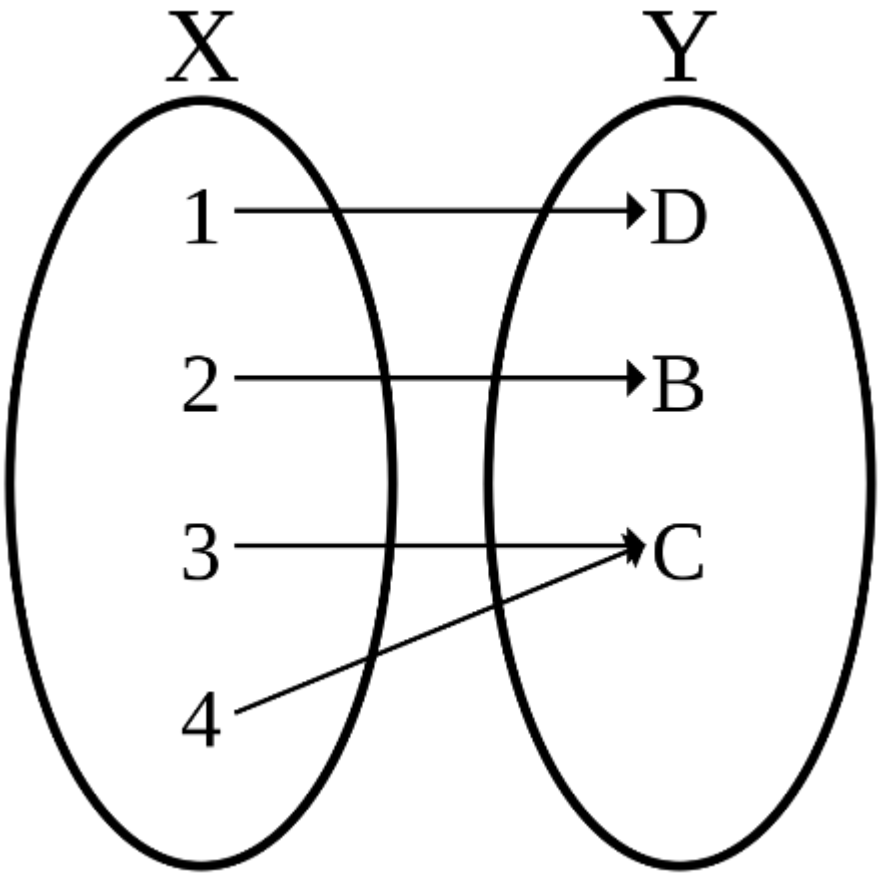
Коллизией для функции **h** называется пара значений **x, y, x ≠ y**, такая, что **h(x) = h(y)**. Таким образом хеш-функция должна обладать следующими свойствами:

- для данного значения **h(x)** невозможно найти значение аргумента **x**. Такие хеш-функции называют **стойкими в смысле обращения** или **стойкими в сильном**

смысле;

- для данного аргумента **x** невозможно найти другой аргумент **y** такой, что **h(x) = h(y)**. Такие хеш-функции называют **стойкими в смысле вычисления коллизий** или **стойкими в слабом смысле**.

В случае, когда значение хеш-функции зависит не только от прообраза, но и закрытого ключа, то это значение называют кодом проверки подлинности сообщений (Message Authentication Code, MAC), кодом проверки подлинности данных (Data Authentication Code, DAC)w или имитовставкой.



Коллизии возникают, когда хеш-функция не инъективна. Значениям 3 и 4 в области определения представленной на рисунке функции соответствует одно и то же значение C этой функции; иными словами, пара 3 и 4 является коллизией функции

Простейшая хеш-*функция* может быть составлена с использованием *операции* "сумма по модулю 2" следующим образом: получаем входную строку, складываем все байты по модулю 2 и *байт*-результат возвращаем в качестве значения хеш-фукнции. *Длина* значения хеш-функции составит в этом случае 8 *бит* независимо от

размера входного сообщения.

Например, пусть исходное сообщение, переведенное в цифровой вид, было следующим (в шестнадцатеричном формате):

3E 54 A0 1F B4

Переведем сообщение в двоичный вид, запишем байты друг под другом и сложим биты в каждом столбике по модулю 2:

0011 1110

0101 0100

1010 0000

0001 1111

1101 0100

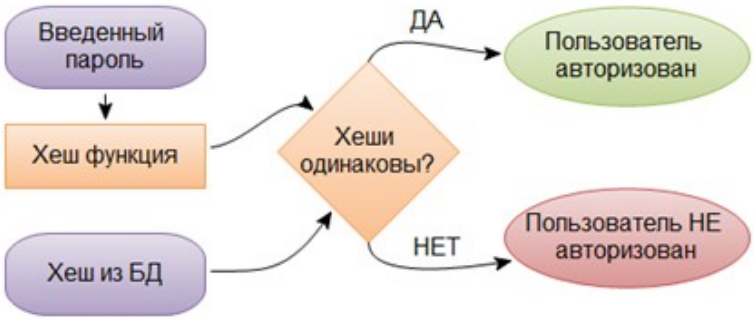
0110 0101

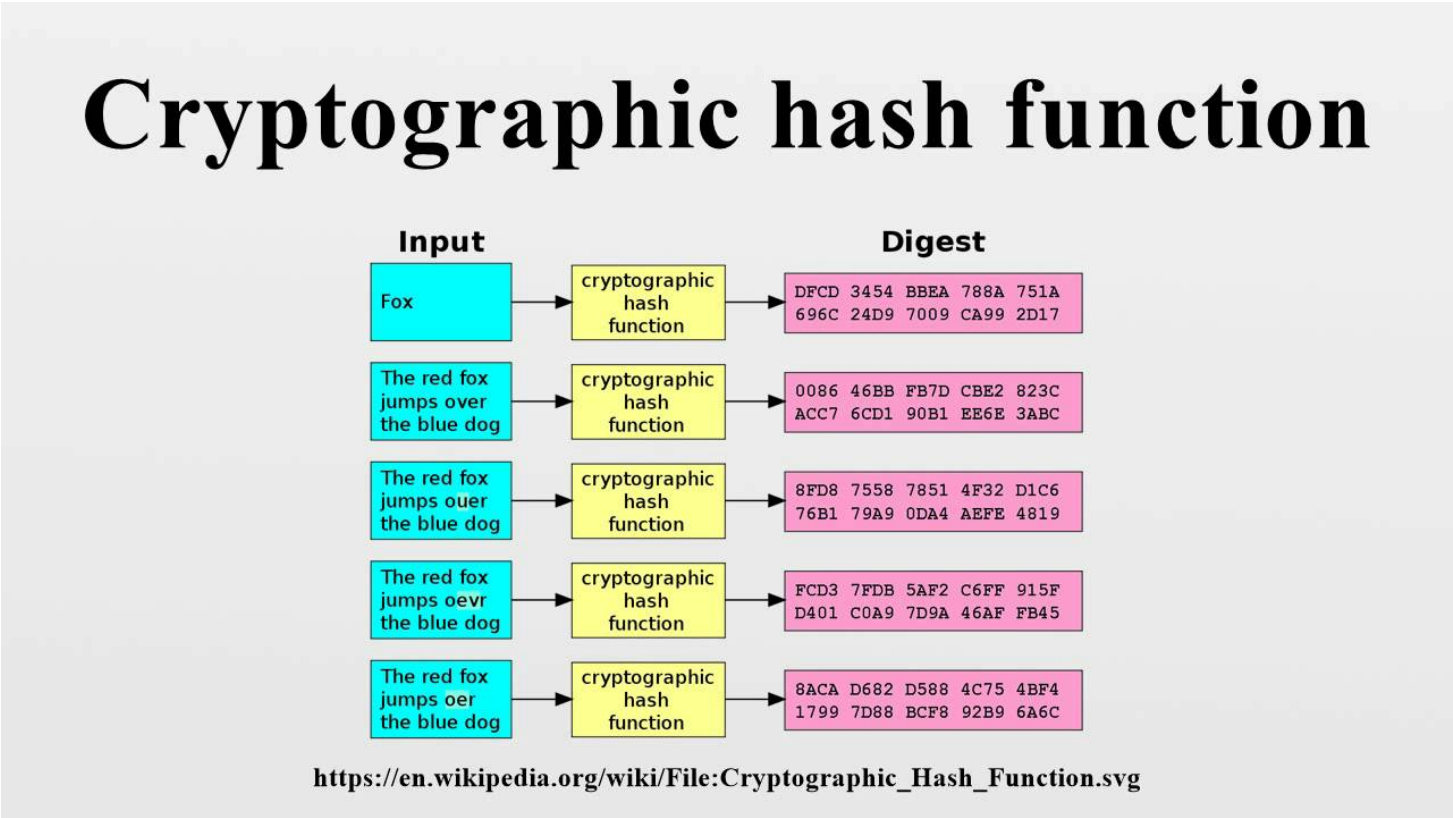
Результат ($0110\ 0101_{(2)}$ или $65_{(16)}$) и будет значением хеш-функции.

Хеш-функции применяются в следующих случаях:

- при построении ассоциативных массивов;
- при поиске дубликатов в сериях наборов данных;
- при построении уникальных идентификаторов для наборов данных;
- при вычислении контрольных сумм от данных (сигнала) для последующего обнаружения в них ошибок, возникающих при хранении и/или передаче данных;
- при сохранении паролей в системах защиты в виде хеш-кода
- при выработке электронной подписи

ФУНКЦИЯ ХЭШИРОВАНИЯ





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