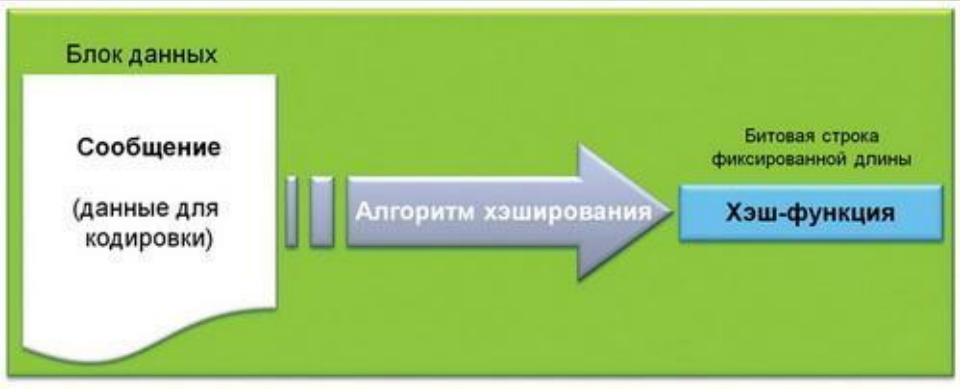
ХЭШ-ФУНКЦИЯ.

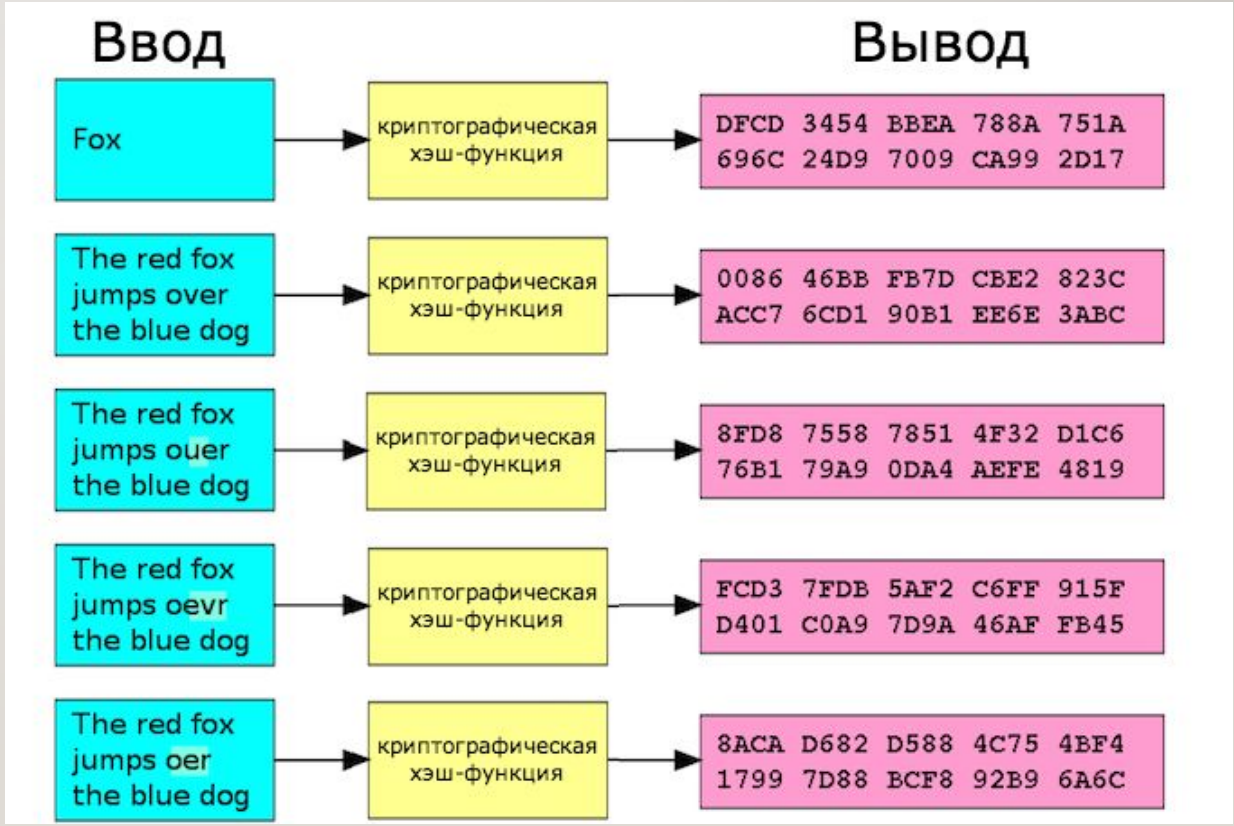
ХЭШ-ФУНКЦИЯ

Функция хэширования — это функция, которая принимает на вход строку битов (или байтов) произвольной длины и выдает результат фиксированной длины.



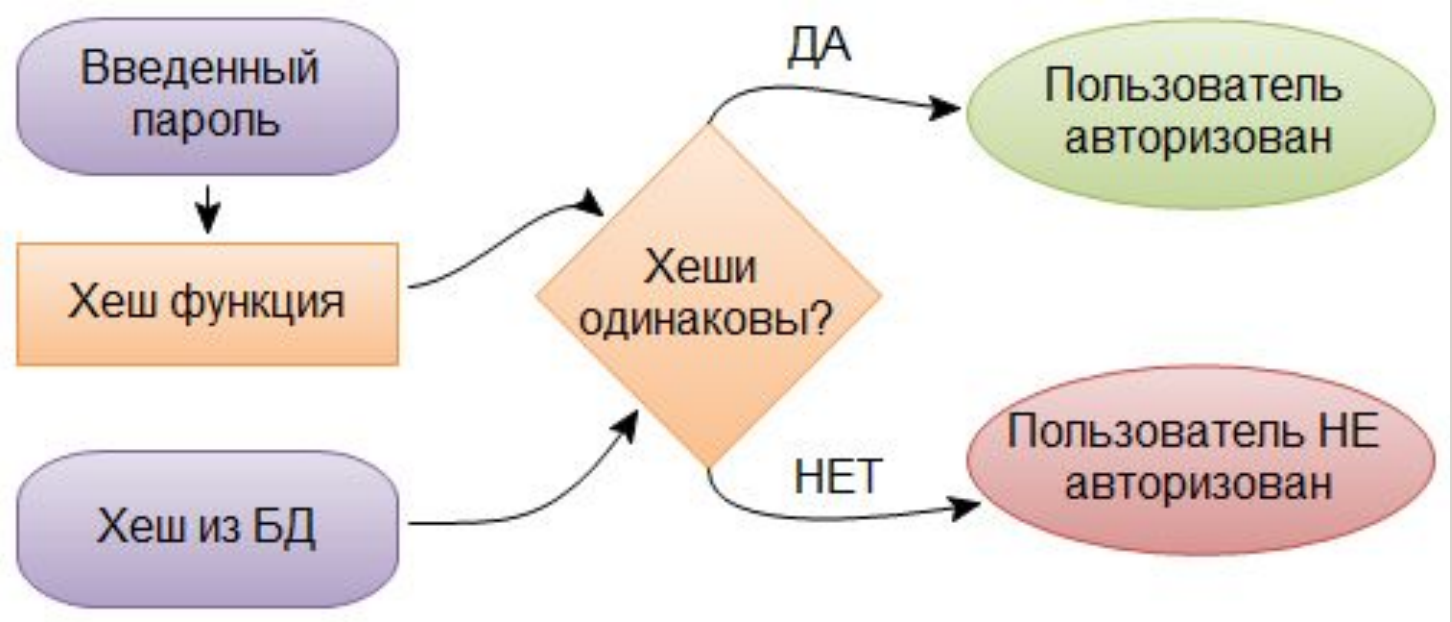
ХЭШ-ФУНКЦИЯ

- Длина хеш-функции полученной по заданному алгоритму одинакова для любой входной произвольной последовательности!
- Если буквы в тексте меняются местами, добавляется или удаляется любое количество символов – хэш-функция изменяется!



ОБЛАСТЬ ПРИМЕНЕНИЯ ХЭШ-ФУНКЦИЙ

- Аутентификация данных;
- Электронная подпись.



ОБЛАСТЬ ПРИМЕНЕНИЯ ХЭШ-ФУНКЦИЙ

- **Проверка целостности сообщений и файлов**
  Сравнивая хеш-значения сообщений, вычисленные до и после передачи, можно определить, были ли внесены какие-либо изменения в сообщение или файл.
- **Верификация пароля**
  Проверка пароля обычно использует криптографические хеши. Хранение всех паролей пользователей в виде открытого текста может привести к массовому нарушению безопасности, если файл паролей будет скомпрометирован. Одним из способов уменьшения этой опасности является хранение в базе данных не самих паролей, а их хешей. При выполнении хеширования исходные пароли не могут быть восстановлены из сохраненных хеш-значений, поэтому если вы забыли свой пароль вам предложат сбросить его и придумать новый.
- **Цифровая подпись**
  Подписываемые документы имеют различный объем, поэтому зачастую в схемах ЭП подпись ставится не на сам документ, а на его хеш. Вычисление хеша позволяет выявить малейшие изменения в документе при проверке подписи. Хеширование не входит в состав алгоритма ЭП, поэтому в схеме может быть применена любая надежная хеш-функция.

Пароль: A123

Сумма кодов символов:

65 («A») + 49 («1») + 50 («2») + 51 («3») = 215

Хэширование – это преобразование массива данных произвольного размера в битовую цепочку заданного размера (например, число).

? Можно ли по хэш-коду восстановить пароль?

! Хэширование – необратимое шифрование!

СВОЙСТВА ХЭШ-ФУНКЦИИ

- ***односторонность (однонаправленность)***: для любого сообщения m легко вычислить значение h(m), однако для любого значения x невозможно найти такое m, что h(m) = x.
- ***сопротивляемость коллизиям***: коллизией по отношению к функциям хэширования называют два разных значения m1 и m2, для которых h(m1) = h(m2). Каждая функция хэширования обладает бесконечным числом подобных коллизий сопротивляемости коллизиям означает лишь то, что, хотя коллизии и существуют, их невозможно обнаружить.
- ***лавинный эффект***.

КЛЮЧЕВЫЕ И БЕЗКЛЮЧЕВЫЕ ФУНКЦИИ ХЭШИРОВАНИЯ.

Все существующие функции хэширования можно разделить на два больших класса: бесключевые хэш-функции, зависящие только от сообщения, и хэш-функции с секретным ключом, зависящие как от сообщения, так и от секретного ключа.

- К ключевым функциям хеширования предъявляются следующие основные требования:

— невозможность фабрикации;

— невозможность модификации.

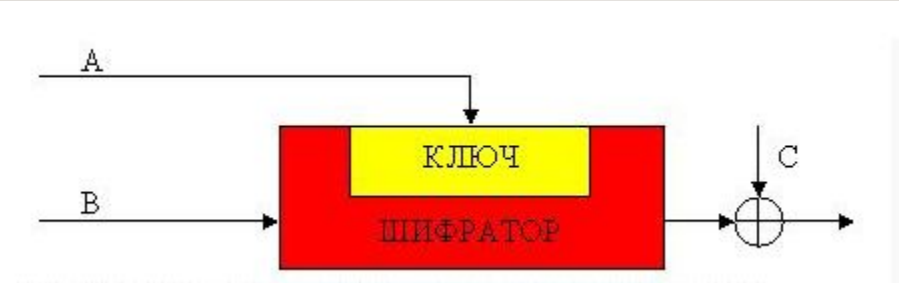
Первое требование означает высокую сложность подбора сообщения с правильным значением свертки. Второе — высокую сложность подбора для заданного сообщения с известным значением свертки другого сообщения с правильным значением свертки.

- Бесключевые функции хеширования обладают всеми классическими свойствами хэш-функций.

ПРИНЦИПЫ ПОСТРОЕНИЯ ХЭШ-ФУНКЦИИ

Ядром алгоритма является сжимающая функция

В качестве сжимающей функции можно использовать симметричный блочный алгоритм шифрования.



A, B и C могут принимать значения M_i, H_{i-1}, $(M_i \oplus H_{i-1})$ или быть константой, где M_i — i-ый блок входного потока, $\oplus$ — сложение по модулю 2, H_i — результат i-ой итерации.

«ГОСТ Р 34.11-2018. ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ФУНКЦИЯ ХЭШИРОВАНИЯ»

- Дата введения: 1 июня 2019 года
- Размер хэша: 256 или 512 бит
- Разработчики: Центр защиты информации и специальной связи ФСБ России с участием Открытого акционерного общества Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»)

ОСНОВНЫЕ ФУНКЦИИ

- сложение по модулю 2;
- преобразование замены;
- преобразование перестановки;
- линейное преобразование.

ФУНКЦИЯ СЖАТИЯ (LPS)

1. S — нелинейная биекция. 512 бит аргумента рассматриваются как массив из шестидесяти четырёх байт, каждый из которых заменяется по заданной стандартом таблице подстановки;

2. P — переупорядочивание байт. Байты аргумента меняются местами по определённому в стандарте порядку;

3. L — линейное преобразование. Аргумент рассматривается как 8 64-битных векторов, каждый из которых заменяется результатом умножения на определённую стандартом матрицу 64 × 64 над GF(2).

АТАКИ НА ФУНКЦИИ ХЭШИРОВАНИЯ

1) нахождение прообраза x по заданному значению y=h(x). Такая атака особенно опасна для систем аутентификации, использующих хэш-значения паролей и секретных ключей;

2) нахождение прообраза x′ по заданному прообразу x , для которого выполняется условие h(x)=h(x′). Эта атака может быть использована для фальсификации сообщения, подписанного цифровой подписью;

3) нахождение двух прообразов x и x′, $x \neq x'$, для которых выполнялось бы условие h(x)=h(x′).

ЗАДАНИЕ К ЛЕКЦИИ:

Исправьте ошибки в алгоритме:

Использование хэш-функций для хранения паролей

Процесс регистрации пользователя:

Пользователь заполняет регистрационную форму, в том числе и поле пароль.

- Веб-скрипт сохраняет всю информацию в базу данных.
- Пароль будет передан хэш-функции перед сохранением.
- Не зашифрованный пароль сохраняется.
  Процесс входа в систему:
- Пользователь вводит имя пользователя (или e-mail) и пароль.
- Скрипт передаёт пароль хэш-функцию.
- Скрипт находит записи пользователя в базе данных, и читает хранящийся в базе данных сохраненный пароль.
- Оба эти значения сравниваются, и, если они совпадают, то пользователь авторизуется.