Хэш сумма

Что это такое

Хэш-функция - это математическая функция, которая принимает на вход произвольный набор данных и преобразует его в некоторое фиксированное значение фиксированной длины. Это значение называется хэш-кодом или хэш-значением.

Что это такое

Хэш-функция является одной из основных компонентов при проектировании и разработке различных информационных систем и программного обеспечения. Она позволяет быстро и эффективно выполнять операции поиска, вставки и удаления данных в различных структурах данных, таких как хэш-таблицы, множества и другие.

Принципы работы хэш-функций

- Детерминизм
- Равномерность
- Стойкость к коллизиям
- Быстрота

Где применяются

Хэш-таблицы

Криптография

Проверка целостности данных

Индексация и поиск в базах данных

Пример

Когда вы регистрируетесь социальной сети ваш логин и пароль пропускает через определенную хэш-функцию и значение хэша записываются в базу данных. После регистрации, когда вы используете логин и пароль для входа они опять пропускаются через хэш-функцию и значение хэша сравнивается с тем значением хэша которая была записана в базу данных изначально после вашей регистрации.

Беда

Когда пароль хэшируется, получается уникальная хэш-сумма. Если два пользователя используют одинаковый пароль, то их хэши-суммы также будут одинаковыми. Это позволяет злоумышленникам проводить атаку по словарю, где для каждой хэш-суммы используется заранее известное значение пароля.

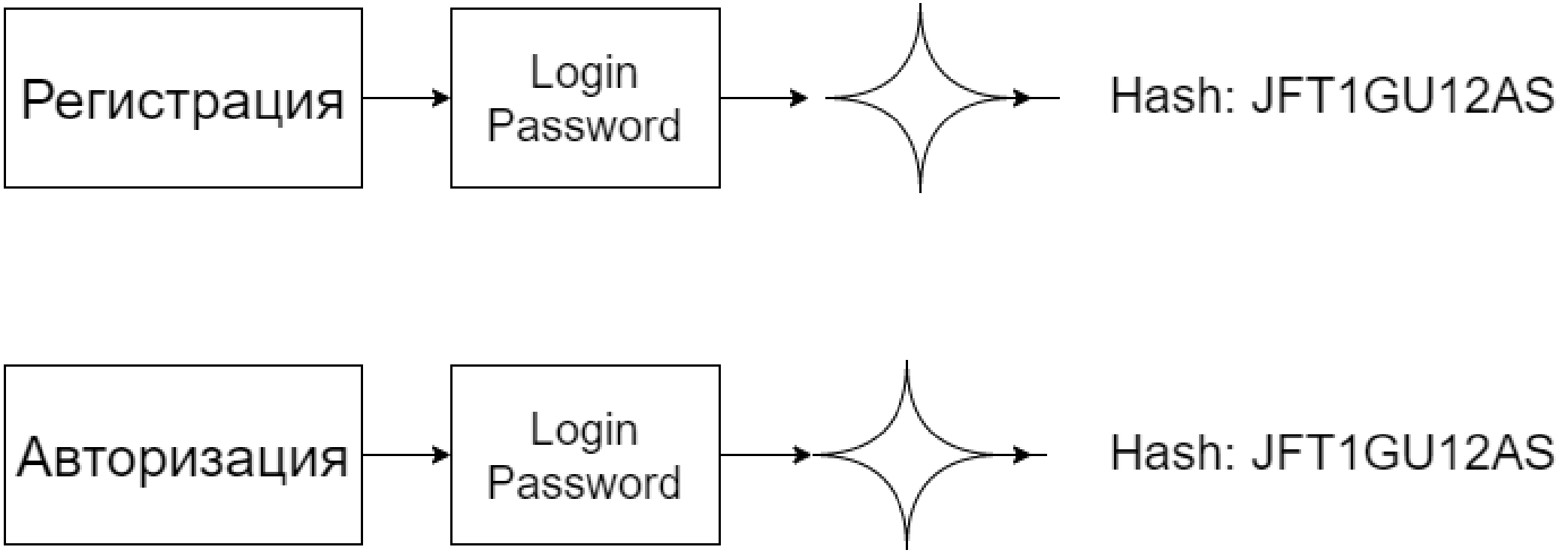
Соль

Соль (salt) в хэш-функциях - это случайное значение, которое добавляется к паролю перед хэшированием. Использование соли позволяет увеличить безопасность хранения паролей и усложнить подбор их значений методом перебора.

Соль

Соль решает проблему с одинаковыми паролями, добавляя к паролю случайное значение перед хэшированием. Два пользователя, использующих одинаковый пароль, будут иметь разные хэш-суммы, потому что они будут использовать разные соли. Это усложняет атаку по словарю, поскольку злоумышленник должен знать не только значение пароля, но и значение соли, чтобы подобрать правильную хэш-сумму.

Соль


Регистрация
Login
Password
Hash: JFT1GU12AS
Авторизация
Login
Password
Hash: JFT1GU12AS

Соль

Атака по словарю

- это метод криптоанализа, при котором злоумышленник пытается подобрать правильный пароль или ключ путем перебора известного списка возможных значений. В этом списке могут быть слова из словаря, наиболее распространенные пароли, имена пользователей, даты рождения и т.д.

Атака по словарю

Для защиты от атаки по словарю рекомендуется использовать длинные и сложные пароли, которые состоят из комбинации букв, цифр и символов. Также важно использовать разные пароли для разных сервисов и периодически их менять. Для усиления защиты паролей можно применять также дополнительные методы, такие как соль или двухфакторная аутентификация.

Радужные таблицы

Для создания радужных таблиц используются алгоритмы, которые генерируют большое количество случайных паролей, хешируют их и сохраняют полученные хеш-суммы в таблице. Затем происходит сокращение размера таблицы путем удаления дублирующихся хеш-сумм и сохранения только первого пароля, соответствующего каждой хеш-сумме.

Атака перебором

Злоумышленник перебирает все возможные комбинации символов, пока не найдет значение хеш-суммы, которое соответствует заданной хеш-сумме.

Как защититься?

- Использование сложных паролей
- Использование солей
- Использование медленных хэш-функций
- Ограничение числа неудачных попыток авторизации
- Двухфакторная аутентификация

Хэш-функция MD5

Один из наиболее известных примеров хэш-суммы - это MD5 (Message-Digest Algorithm 5). Она была разработана Рональдом Ривестом в 1991 году и с тех пор широко использовалась для хеширования данных в различных областях, включая криптографию и проверку целостности файлов.

Хэш-функция MD5

MD5 принимает на вход произвольный блок данных произвольной длины и генерирует для него уникальную 128-битную хэш-сумму. Полученный хэш-код может использоваться для проверки целостности данных, а также для хранения и передачи данных в форме, которая не раскрывает оригинальные данные.

Пример

хэш-сумма MD5 для строки "Hello, world!":

1.Строка преобразуется в последовательность байтов: 48 65 6C 6C 6F 2C 20 77 6F 72 6C 64 21

2. Для последовательности байтов вычисляется хэш-код с помощью MD5.

3.Полученный хэш-код имеет вид: 0x65a8e27d8879283831b664bd8b7f0ad4

Пример

Изменение только одного байта в исходной строке приводит к существенному изменению хэш-кода, что позволяет использовать MD5 для проверки целостности данных и обнаружения любых изменений в них

C#

System.Security.Cryptography.MD5 - это класс, который предоставляет реализацию алгоритма хеширования MD5 в .NET Framework. Этот класс является частью пространства имен **System.Security.Cryptography,** которое содержит различные классы для реализации криптографических алгоритмов.

```
using System.Security.Cryptography;

string text = "Hello world";
byte[] hash;

using (var md5 = MD5.Create())
{

    byte[] inputBytes = System.Text.Encoding.ASCII.GetBytes(text);
    hash = md5.ComputeHash(inputBytes);

}

Console.WriteLine("MD5 hash of file {0} is {1}", text,
BitConverter.ToString(hash).Replace("-", "").ToLower());
```

C#

Метод ComputeHash() вычисляет хэш-сумму для переданного потока в виде массива байтов. Массив байтов, представляющий хэш-сумму файла, сохраняется в переменной hash.

C#

Выводим хэш-сумму файла на экран с помощью методов BitConverter.ToString() и ToLower(). Метод BitConverter.ToString() преобразует массив байтов хэш-суммы в строку в шестнадцатеричном формате, разделяя каждый байт дефисом. Метод ToLower() приводит строку к нижнему регистру.

SHA

SHA (Secure Hash Algorithm) - это семейство криптографических хэш-функций, разработанных Национальным институтом стандартов и технологий (NIST) США. Они являются одними из самых распространенных алгоритмов хэширования в мире.

SHA

Класс System.Security.Cryptography.SHA1 в .NET Framework представляет алгоритм хэширования SHA-1 (Secure Hash Algorithm 1), который является одним из наиболее распространенных алгоритмов хэширования. SHA-1 генерирует хэш-сумму фиксированной длины в 160 битов (20 байтов).

SHA

Основной метод класса `ComputeHash` принимает массив байтов в качестве входных данных и возвращает массив байтов, представляющий хэш-сумму в формате SHA-1. Можно использовать различные перегрузки

```
using System;
using System.Security.Cryptography;
using System.Text;

class Program
{
    static void Main(string[] args)
    {
        string inputString = "hello world";
        byte[] hash;

        using (var sha = SHA256.Create())
        {
            hash = sha.ComputeHash(Encoding.UTF8.GetBytes(inputString));
        }

        Console.WriteLine("SHA-1 hash of string '{0}' is {1}", inputString,
BitConverter.ToString(hash).Replace("-", "").ToLower());
    }
}
```

Задание

Создать консольную программу проверяющую правильность ввода пароля, сравнивая введенную пользователем строку с паролем хранящимся в виде хэш-суммы.