# Доклад на тему ‘Хэш-функции’

Явкина Анастасия Юрьевна

12 октября 2024

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

# Содержание

# Содержание

# Докладчик

# Докладчик


- Явкина Анастасия Юрьевна
- студент 4-го курса НПМбд-02-21
- Российский университет дружбы народов им. Патриса Лумумбы
- 1032216503@pfur.ru
- https://github.com/ayyavkina/-

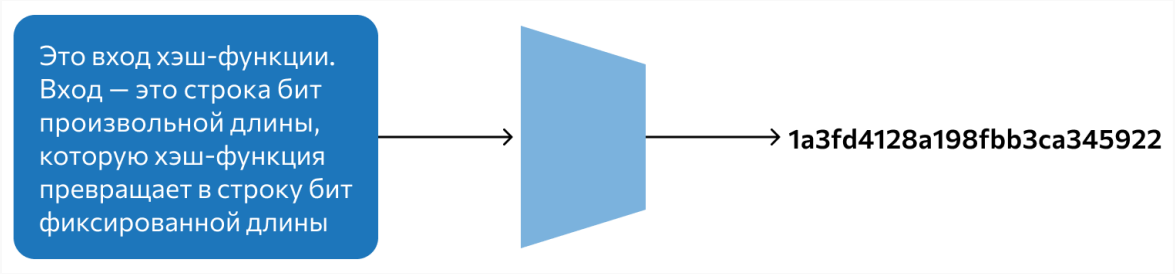
# Цель

# Цель

Целью данного доклада является объяснить основные концепции, принципы работы и применения хэш-функций в информатике, а также подчеркнуть их важность для обеспечения безопасности данных и оптимизации вычислительных процессов.

# Глава 1. Хэш-функции.

# Глава 1. Хэш-функции.



# Глава 1.1 Применение хэш-функций

# Глава 1.1 Применение хэш-функций

Основное назначение хеширования – проверка информации. Эта задача важна в огромном количестве случаев: от проверки паролей на сайте до сложных вычислений в блокчейне. Так как хеш – это уникальный код определенного набора данных, по нему можно понять, соответствует ли информация ожидаемой. Поэтому программа может хранить хеши вместо образца данных для сравнения. Это может быть нужно для защиты чувствительных сведений или экономии места.

# Глава 2. Свойства хеш-функций.

# Глава 2. Свойства хеш-функций.

1. Необратимость.
2. Детерминированность.
3. Уникальность.
4. Разнообразие.
5. Высокая скорость генерации.

# Глава 3. Принцип работы хэш-функции.

# Глава 3. Принцип работы хэш-функции.

Возможных преобразований для получения хеша бесконечное количество. Это могут быть формулы на основе умножения, деления и других операций, алгоритмы разного уровня сложности. Но если хеш применяется для защиты данных, его функция должна быть криптографической – такие хеш-функции обладают определенными свойствами. Именно криптографические хеш-функции используются, например, при хранении паролей. Если говорить о криптографической хеш-функции, то она чаще всего работает в несколько шагов. Данные разбиваются на части и проходят через сжимающую функцию, которая преобразовывает информацию в меньшее количество бит. Функция должна быть криптостойкой – такой, результат которой практически невозможно вскрыть. А вот хеш-функции для более простых случаев, например построения таблиц, не обязаны быть криптографическими. Там преобразования могут быть проще.

# Глава 4. Безопасность криптографической хеш-функции.

# Глава 5. Пример.

# Заключение

# Заключение

Таким образом, хэш-функции – это важный инструмент в арсенале компьютерных технологий. Они играют ключевую роль в обеспечении безопасности данных, проверке целостности информации и оптимизации вычислений. Важно выбирать хэш-функции с учетом их надежности и области применения. Современные криптографические хэш-функции, такие как SHA-256 и SHA-3, продолжают оставаться надежными и востребованными.

# Список литературы

# Список литературы


1. Винокуров, С.Ф. Избранные вопросы теории булевых функций / С.Ф. Винокуров. - М.: [не указано], 2012. - 564 с.
2. Дэвенпорт, Дж. Интегрирование алгебраических функций / Дж. Дэвенпорт. - М.: [не указано], 2013. - 726 с.
3. Евграфов, М.А. Асимптотические оценки и целые функции / М.А. Евграфов. - М.: [не указано], 2014. - 285 с.
4. Катленд, Н. Вычислимость. Введение в теорию рекурсивных функций / Н. Катленд. - М.: [не указано], 2011. - 707 с.
5. Ленг, С. Введение в алгебраические и абелевы функции / С. Ленг. - М.: [не указано], 2014. - 601 с.
6. 2012. - 833 с.
7. Шевалле, К. Введение в теорию алгебраических функций от одной переменной / К. Шевалле. - М.: [не указано], 2014. - 226