

Аутентификация

Аутентификация

Процедура проверки подлинности

Может быть основана на:

- чем то, что известно пользователю
- чем то, что есть у пользователя
- чем то, что он собой представляет
- на местоположении пользователя
- на совокупности факторов

Биометрическая аутентификация (критерии)

- Всеобщность: Данный признак должен присутствовать у всех людей без исключения.
- Уникальность: Биометрия отрицает существование двух людей с одинаковыми физическими и поведенческими параметрами.
- Постоянство: для корректной аутентификации необходимо постоянство во времени.
- Измеримость: специалисты должны иметь возможность измерить признак каким-либо устройством для дальнейшего занесения в базу данных.
- Приемлемость: общество не должно быть против сбора и измерения биометрического параметра.

Статическая биометрия

- Аутентификация по отпечатку пальца
- Аутентификация по радужной оболочке глаза
- Аутентификация по сетчатке глаза
- Аутентификация по геометрии руки
- Аутентификация по геометрии лица
- Аутентификация по термограмме лица

Динамическая биометрия

- Аутентификация по голосу
- Аутентификация по рукописному почерку

Аутентификация по схеме "Отклик-отзыв"

- Контрольный вопрос
- Заранее настраивается при регистрации

Аутентификация с помощью физического объекта

- Карта с хранимой суммой
- Смарт-карта

Аутентификация (cont)

Парольная аутентификация

- Аутентификация по секретному тексту.
- Проста для понимания и реализация
- Поддержка реестра (имя пользователя:пароль)
- Одноразовые и многоразовые пароли

Шифрование и Хэширование

Шифрование

обратимое преобразование информации с секретом (ключом) в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней.

Шифр

какая-либо система преобразования текста с секретом (ключом) для обеспечения секретности передаваемой информации.

Шифротекст

результат операции шифрования

Хэширование

необратимое преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом.

Хэш-функция

функция, выполняющая хеширование.

Хэш

результат хэширования

Симметричное шифрование

использует один и тот же ключ и для зашифровывания, и для расшифровывания.

Асимметричное шифрование

шифрование использует два разных ключа: один для зашифровывания (который также называется открытым), другой для расшифровывания (называется закрытым).

Шифрование и Хэширование (cont)

Применение хэширования

- 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 (возникших случайно или внесённых намеренно), возникающих при хранении и/или передаче данных;
- при сохранении паролей в системах защиты в виде хеш-кода (для восстановления пароля по хеш-коду требуется функция, являющаяся обратной по отношению к использованной хеш-функции);
- при выработке электронной подписи (на практике часто подписывается не само сообщение, а его «хеш-образ»);

Электронно-цифровая подпись

C

By **Hideru_Azava**
cheatography.com/hideru-azava/

Not published yet.
Last updated 11th January, 2019.
Page 2 of 2.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>