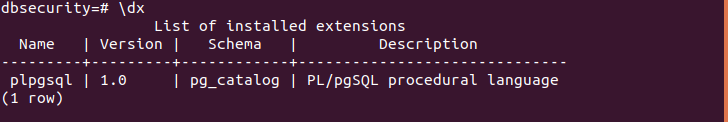
**Шифрование в PostgreSQL**

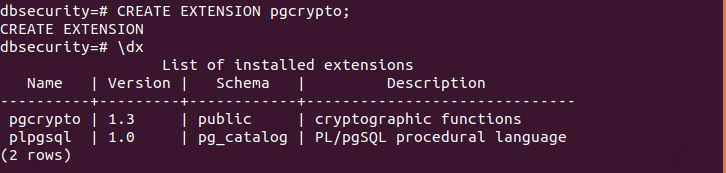
*Хеширование паролей*

PostgreSQL предлагает несколько типов шифрования данных. Первым типом является хеширование паролей, которое позволяет хранить в базе данных хеши парольных фраз и ключей для работы приложения. Обычно в процессе аутентификации проверяется именно совпадение хешей паролей. Хеширование – это необратимый процесс без возможности расшифровать входные значения. Однако хеш можно проверить путем повторного хеширования входного значения.

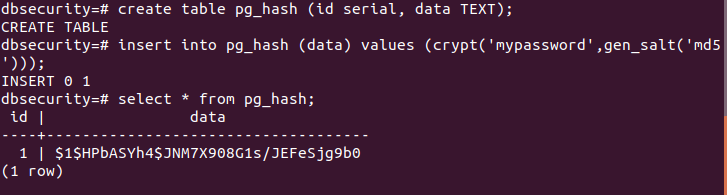
Во-первых, нужно добавить расширение для активации функции шифрования. Проверьте список установленных расширений:



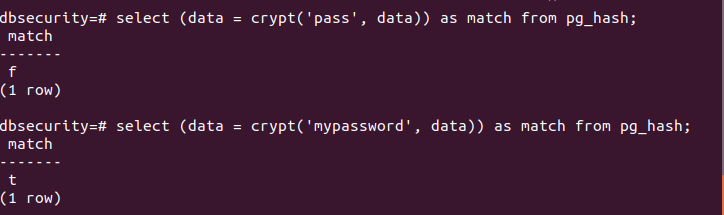
Далее устанавливаем расширение **pgcrypto:**



Создадим выделенную таблицу для хешированных значений и вставим в нее хеш с помощью следующих нескольких запросов:

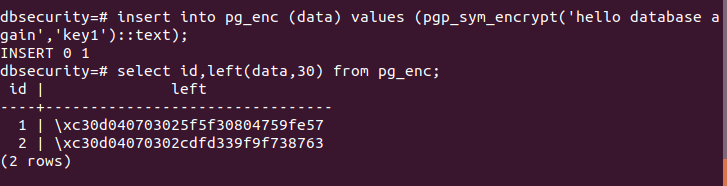


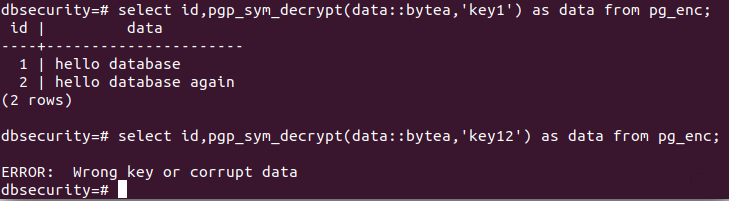
Введенный пароль можно проверить запросом вызова функции ***crypt ()***.



*Шифрование столбцов таблицы*

Еще одной особенностью PostgreSQL является возможность шифрования выделенных столбцов таблицы. Клиент может зашифровать критичные значения с точки зрения безопасности, которые находятся в некоторых столбцах. Вместо одностороннего хеширования шифрование может быть обратимым (симметричным). Пользователь может расшифровать данные, если знает ключ, который использовался при шифровании.





**Задачи для практической работы:**

1. Создайте таблицу, в которой два столбца содержат хешированные значения, где одно из них сгенерировано с помощью алгоритма SHA-1. Покажите, как можно выполнить проверку, используя данные двух хешей.

2. Создайте таблицу, в которой данные имеют байтовый тип. Зашифруйте этот столбец и покажите, как пользователь может расшифровать данные во время обычного select-запроса к зашифрованному столбцу.

**Вопросы к защите**

1. Особенности криптографической защиты в СУБД. Перечислите основные подходы к шифрованию в распределенных СУБД.
2. Шифрование на уровне устройств хранения информации.
3. Шифрование на уровне СУБД
4. Шифрование на уровне приложения.
5. Роль аппаратных модулей безопасности (HS модулей) в структуре криптографической защиты современных СУБД.
6. Роль гомоморфных криптосистем для облачных сервисов и систем хранения. Существующие решения и перспективы развития.
7. Перспективные направления исследований в области КМЗИ в БД.