**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Информационная безопасность баз данных»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5**

«Шифрование в PostgreSQL»

Содержание

[Введение 3](#_Toc195789943)

[1 Шифрование в PostgreSQL 4](#_Toc195789944)

[1.1 Ход работы 4](#_Toc195789945)

[Заключение 7](#_Toc195789946)

[Список использованных источников 8](#_Toc195789947)

Введение

Цель работы – получение навыков работы с шифрованием в PostgreSQL.

Для достижения поставленной цели необходимо решить следующие задачи:

* создать таблицы для работы;
* зашифровать данные;
* расшифровать данные;
* сделать выводы.

# Шифрование в PostgreSQL

## Ход работы

Нужно добавить расширение для активации функции шифрования. Проверим список установленных расширений.

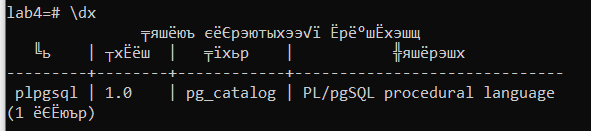


Рисунок 1 – проверка расширений

Далее устанавливаем расширение pgcrypto.



Рисунок 2 – установка расширения

Проверим, что оно установилось, еще раз посмотрев список всех расширений.

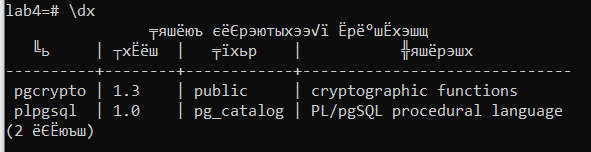


Рисунок 3 – проверка расширений

1. Создадим таблицу для дальнейшей работы. Пусть в таблице будет содержать 4 столбца: айди, текст, зашифрованный текст с помощью алгоритма SHA-1 и зашифрованный текст с помощью алгоритма md5. Заполним таблицу.

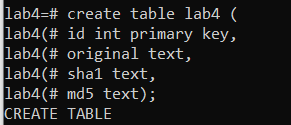


Рисунок 4 – создание таблицы

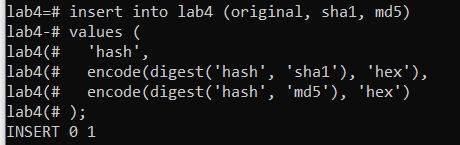


Рисунок 5 – заполнение таблицы

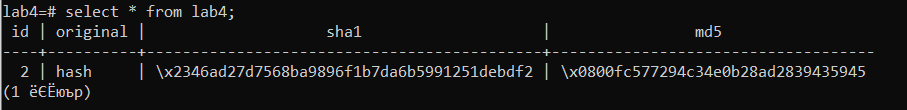


Рисунок 6 – заполненная таблица

Необходимо показать, как можно выполнить проверку, используя данные двух хешей. Для этого напишем запрос, который выбирает исходный текст из таблицы lab4 и проверяет, соответствуют ли сохранённые хеши sha1 и md5 результатам повторного хеширования этого текста. если оба хеша совпадают с пересчитанными, то результатом будет 'true', иначе — 'false'.

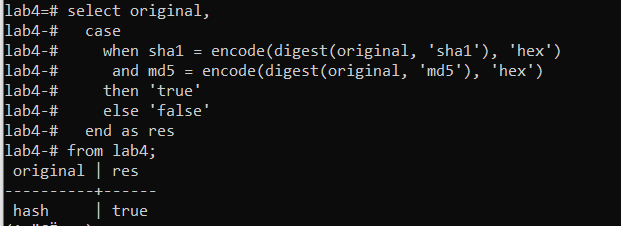


Рисунок 7 – проверка

1. Создадим таблицу, в которой данные имеют байтовый тип. Пусть первый столбец содержит не зашифрованную строку, а второй – зашифрованную строку.

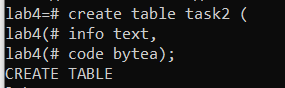


Рисунок – создание таблицы

Заполним таблицу. Причем, второе значение будет зашифровано с помощью pgp\_sym\_encrypt.



Рисунок – заполнение таблицы

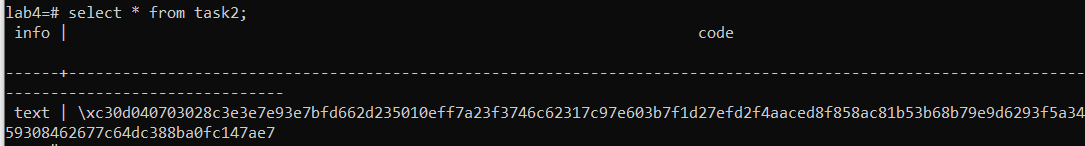


Рисунок – вывод заполненной таблицы

Теперь, расшифровать данные во время обычного select-запроса к зашифрованному столбцу. Это можно сделать с помощью команды pgp\_sym\_decrypt с ключом.

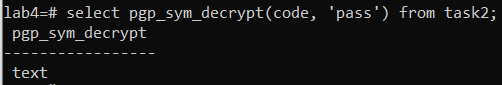


Рисунок – расшифровка данных

Заключение

В ходе данной лабораторной работы были изучены методы шифрование в PostgreSQL, а именно: хеширование паролей и шифрование столбцов таблицы. Были создана таблица, в которой данные зашифровывались с помощью алгоритмов sha1 и md5, затем была выполнена проверка хеширования с помощью двух хешей. Кроме этого, была создана таблица, в которой данные имеют байтовый тип. Этот столбец был зашифрован, дальше с помощью select-запроса и ключа расшифрован. Это позволило закрепить полученные знания и навыки. В ходе выполнения лабораторной работы были выполнены все задачи и достигнуты поставленные цели.

Список использованных источников

1. Основы технологий баз данных: учебное пособие Б. А. Новиков, Е. А. Горшкова, Н. Г. Графеева; под ред. Е. В. Рогова. — 2-е изд. — М.: ДМК Пресс, 2020. — 582 с.