# Encryption and Decryption in PostgreSQL

## Introduction

This document provides a detailed guide on how to configure and implement encryption and decryption in PostgreSQL using the pgcrypto extension. The encryption ensures data security, and the decryption mechanism allows authorized access to sensitive information.

## Step 1: Enable pgcrypto Extension

PostgreSQL provides the pgcrypto extension for cryptographic functions. To enable it, execute the following command:

CREATE EXTENSION IF NOT EXISTS pgcrypto;

## Step 2: Create a Table with Encrypted Data

Create a table to store encrypted data, such as employee salary details:

CREATE TABLE emp\_sal\_details (  
 empid SERIAL PRIMARY KEY,  
 name TEXT NOT NULL,  
 salary BYTEA NOT NULL,  
 deptid INT NOT NULL  
);

## Step 3: Create an Encryption Function

Define a function that encrypts sensitive data using AES encryption with a secret key:

CREATE OR REPLACE FUNCTION encrypt\_text(input\_text TEXT, key TEXT) RETURNS BYTEA AS $$  
BEGIN  
 RETURN pgp\_sym\_encrypt(input\_text, key);  
END;  
$$ LANGUAGE plpgsql;

## Step 4: Create a Decryption Function

Define a function that decrypts encrypted data:

CREATE OR REPLACE FUNCTION decrypt\_text(encrypted\_data BYTEA, key TEXT) RETURNS TEXT AS $$  
BEGIN  
 RETURN pgp\_sym\_decrypt(encrypted\_data, key);  
END;  
$$ LANGUAGE plpgsql;

## Step 5: Insert Encrypted Data

Insert employee records with encrypted salary values:

INSERT INTO emp\_sal\_details (name, salary, deptid)  
VALUES ('John Doe', encrypt\_text('75000', '123456789'), 101);

## Step 6: Retrieve and Decrypt Data

Query to retrieve decrypted salary details:

SELECT empid, name, decrypt\_text(salary, '123456789') AS decrypted\_salary, deptid  
FROM emp\_sal\_details;

## Step 7: Security Best Practices

1. Use strong encryption keys and store them securely (e.g., environment variables, secret managers).

2. Restrict access to sensitive data using proper user roles and privileges.

3. Regularly rotate encryption keys and update encrypted data accordingly.

4. Ensure pgcrypto extension is installed and enabled in the database schema.