

# MySQL 내장함수를 이용한 Data 암호화



## 과제 개요



- ✓ DB에서 **개인정보**를 처리하는 경우에는 **개인정보보호법** 등에서 규정하는 보호조치를 모두 적용해야 한다.

# 개인정보보호법



## ✓ 법령상 준수해야하는 보호조치 중 암호화 관련 부분

근거	준수 항목	상세 내용
안전성확보조치 제7조 제2항 기술적관리적보호조치 제6조 제1항	비밀번호 일방향 암호화	이용자, 개인정보취급자 등의 비밀번호가 노출 또는 위변조되지 않도록 일방향 암호화해서 저 장하고, 난수 추가(Salting) 등의 조치를 취한다.
안전성확보조치 제7조 제5항 기술적관리적보호조치 제6조 제2항	개인정보 양방향 암호화	주민등록번호, 여권번호, 운전면허번호, 외국인 등록번호, 신용카드번호, 계좌번호, 바이오정보 는 안전한 알고리즘으로 양방향 암호화하여 저 장한다.

## 과제 개요



- ✓ DB에서 **개인정보**를 처리하는 경우에는 **개인정보보호법** 등에서 규정하는 보호조치를 모두 적용해야 한다.
- ✓ 이번 과제에서는 법령상 준수해야 하는 보호조치 중 **데이터 암호화**와 관련된 부분을 MySQL에서 제공하는 **내장함수**를 이용하여 회원관리 기능을 구현해 본다.

# MySQL 내장함수



- ✓ MySQL은 다양한 내장함수를 제공하고 있음.
- ✓ 자주 쓰는 내장함수
  - ✓ 집계 함수 : COUNT, SUM, AVG, MAX, MIN 등
  - ✓ Math 함수 : ABS, MOD, CEILING, FLOOR 등
  - ✓ String 함수 : LENGTH, CONCAT, LEFT, RIGHT, SUBSTRING 등
  - ✓ Date 함수 : NOW, SYSDATE, DATE\_ADD, 등

<https://dev.mysql.com/doc/refman/8.0/en/built-in-function-reference.html>

## 일방향 암호화



- ✓ 복호화가 불가능한 암호화 방식
- ✓ 비교를 통해 올바른 데이터인지 확인
- ✓ 비밀번호와 같이 복호화가 필요 없는 데이터 저장시 사용
- ✓ SHA-2 알고리즘으로 암호화 진행

# 양방향 암호화



- ✓ 복호화가 가능한 암호화 방식
- ✓ 대칭키 암호화, 공개키 암호화 방식이 있음
- ✓ 주민등록번호, 계좌번호 등 필요에 따라 복호화가 필요한 데이터 저장시 사용
- ✓ 대칭키 암호화 방식 중 AES 알고리즘으로 암호화 진행
- ✓ 양방향이기때문에 암호화 함수와 복호화 함수가 별도로 존재

## 오늘의 과제



- ✓ 회원기능이 있는 서비스 개발에 필요한 기능 개발해 보기
- ✓ 회원 관리 테이블 생성
  - ✓ 회원아이디, 회원비밀번호, 회원계좌번호 반드시 포함
- ✓ 회원가입 쿼리 작성
- ✓ 회원정보조회 쿼리 작성
- ✓ 회원정보수정 쿼리 작성
- ✓ 로그인 쿼리 작성
- ✓ 비밀번호 변경 쿼리 작성



