-- 사용자 정보 테이블 생성

CREATE TABLE Users\_Encrypted (

id INT AUTO\_INCREMENT PRIMARY KEY,

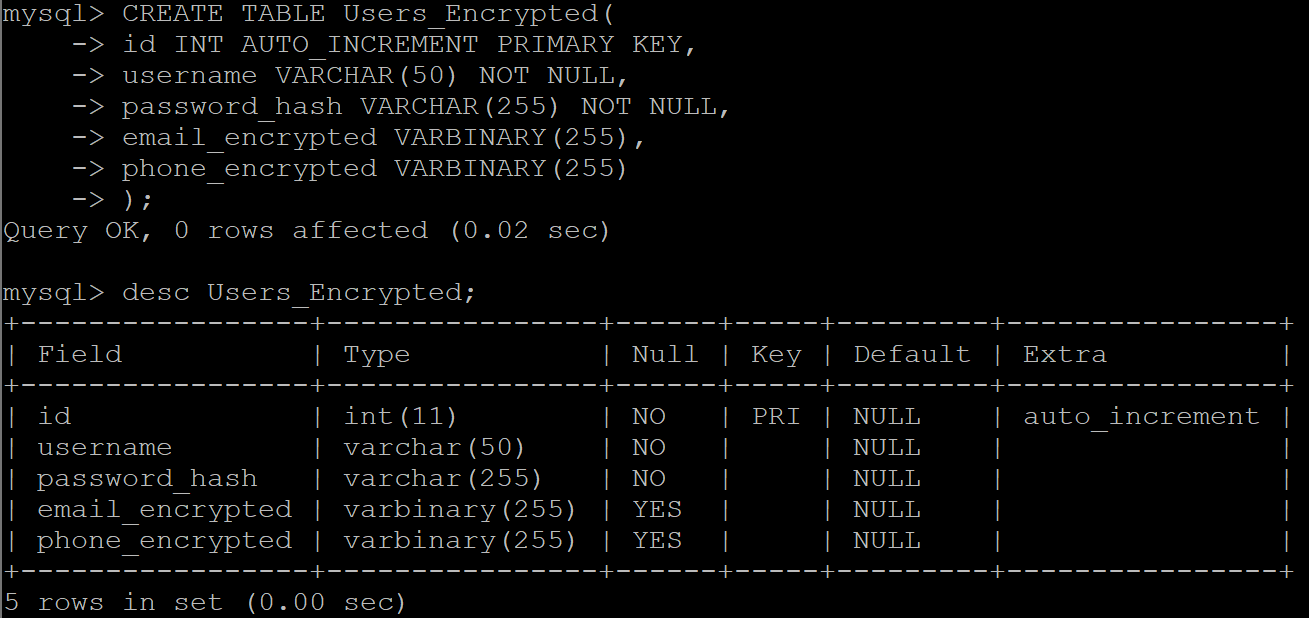
username VARCHAR(50) NOT NULL,

password\_hash VARCHAR(255) NOT NULL, -- 비밀번호 해시 값 저장

email\_encrypted VARBINARY(255), -- 암호화된 이메일 저장 (VARBINARY 타입 사용)

phone\_encrypted VARBINARY(255) -- 암호화된 전화번호 저장

);



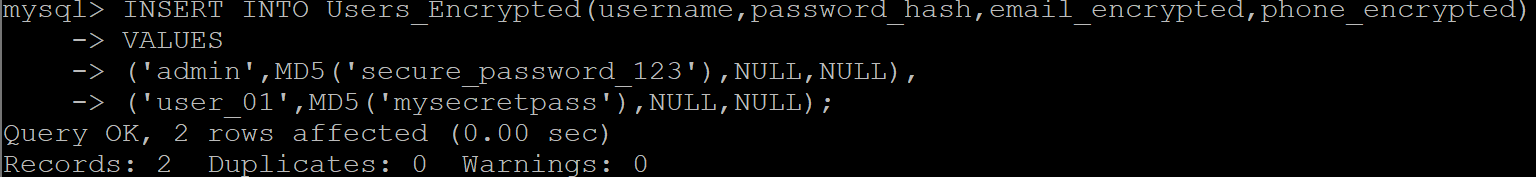
**단방향 암호화**

-- 사용자 등록 시 비밀번호를 MD5로 해싱하여 저장

INSERT INTO Users\_Encrypted (username, password\_hash, email\_encrypted, phone\_encrypted) VALUES

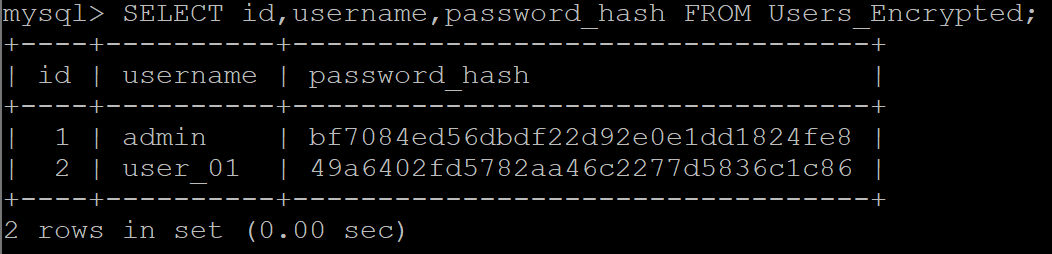
('admin', MD5('secure\_password\_123'), NULL, NULL), -- 비밀번호를 MD5로 암호화

('user\_01', MD5('mysecretpass'), NULL, NULL);



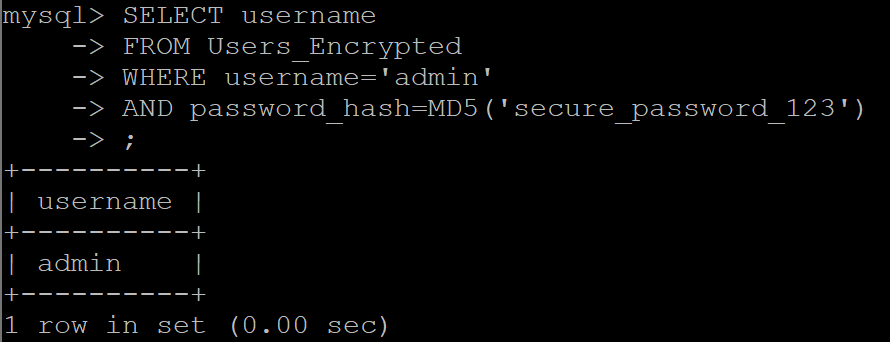
-- 저장된 비밀번호 해시 값 확인 (원본 비밀번호는 알 수 없음)

SELECT id, username, password\_hash FROM Users\_Encrypted;



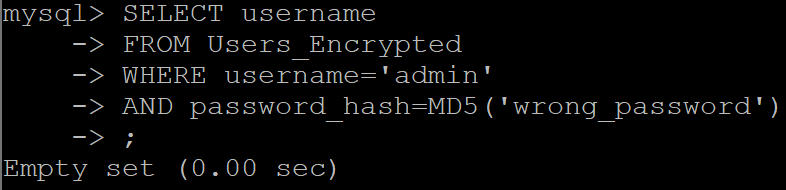
-- 로그인 시 비밀번호 확인 (입력된 비밀번호를 다시 MD5로 해싱하여 비교)

SELECT username FROM Users\_Encrypted WHERE username = 'admin' AND password\_hash = MD5('secure\_password\_123');



-- 결과가 나오면 로그인 성공

SELECT username FROM Users\_Encrypted WHERE username = 'admin' AND password\_hash = MD5('wrong\_password');



-- 결과가 없으면 로그인 실패

**양방향 암호화**

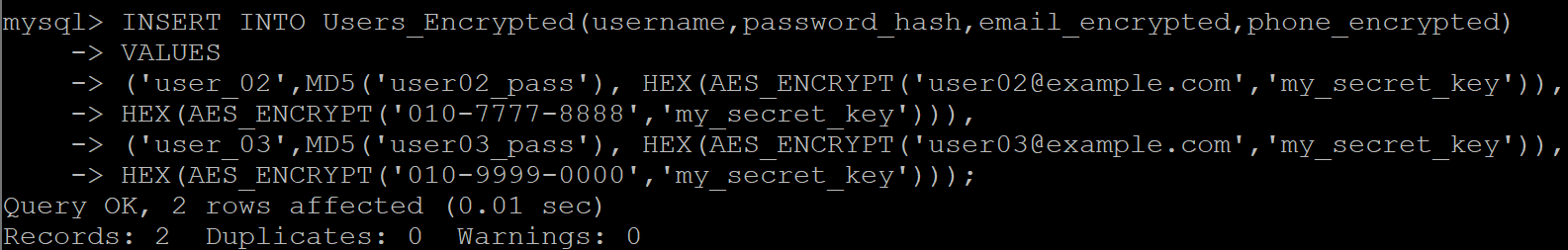
-- 양방향 암호화된 데이터 삽입

-- 'my\_secret\_key'는 암호화/복호화에 사용될 비밀 키

INSERT INTO Users\_Encrypted (username, password\_hash, email\_encrypted, phone\_encrypted) VALUES

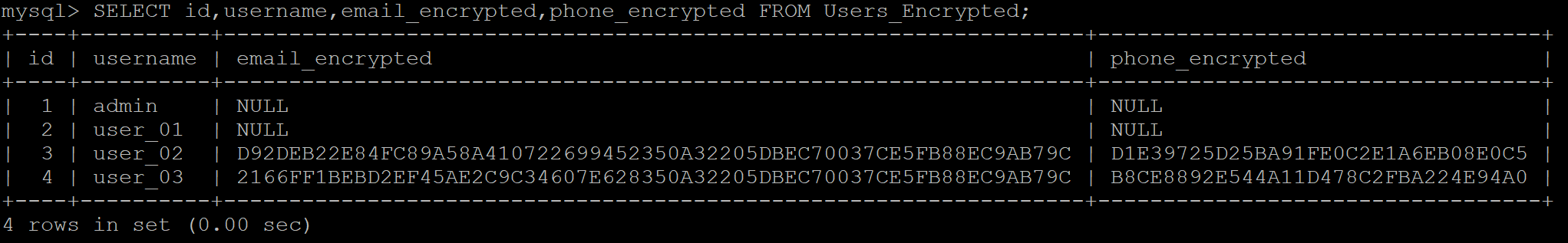
('user\_02', MD5('user02\_pass'), HEX(AES\_ENCRYPT('user02@example.com', 'my\_secret\_key')), HEX(AES\_ENCRYPT('010-7777-8888', 'my\_secret\_key'))),

('user\_03', MD5('user03\_pass'), HEX(AES\_ENCRYPT('user03@example.com', 'my\_secret\_key')), HEX(AES\_ENCRYPT('010-9999-0000', 'my\_secret\_key')));



-- 암호화된 데이터 확인

SELECT id, username, email\_encrypted, phone\_encrypted FROM Users\_Encrypted;



-- 암호화된 데이터 복호화하여 조회

-- 복호화 시에도 암호화할 때 사용했던 '정확히 동일한 키'를 사용

SELECT

id,

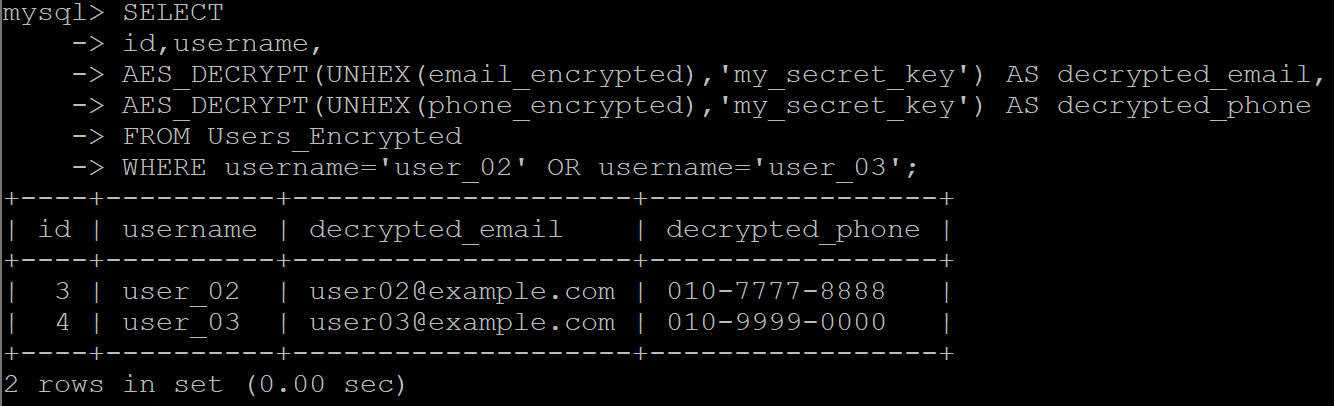
username,

AES\_DECRYPT(UNHEX(email\_encrypted), 'my\_secret\_key') AS decrypted\_email,

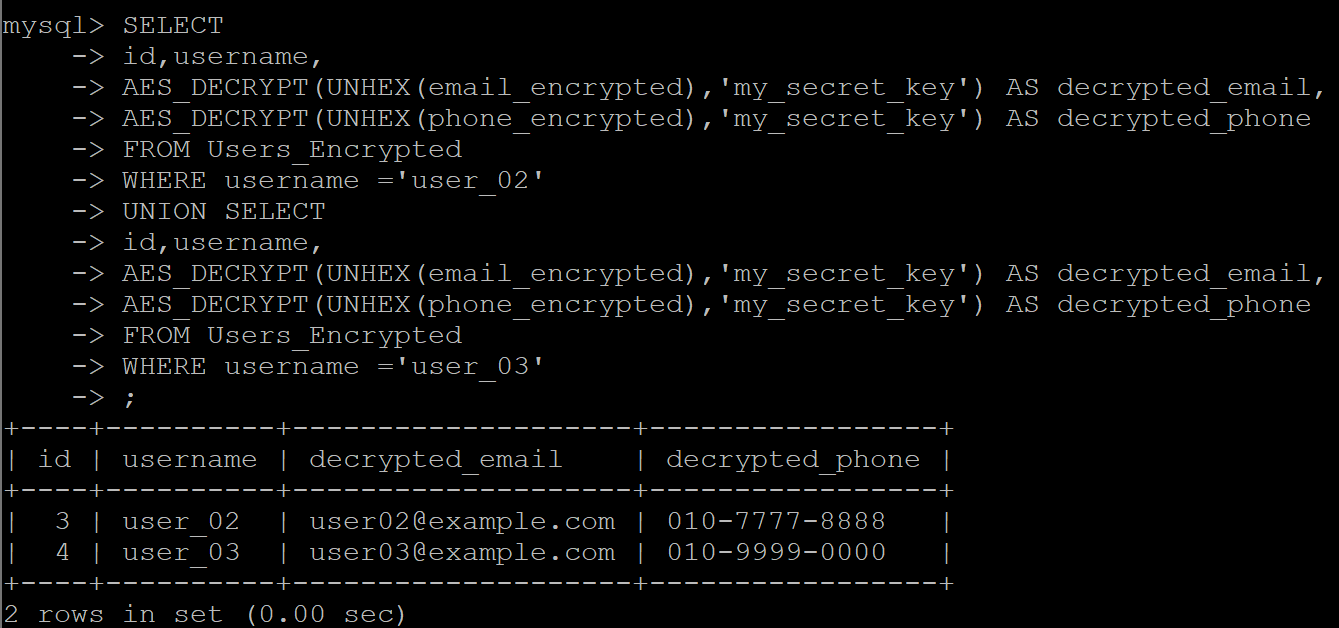
AES\_DECRYPT(UNHEX(phone\_encrypted), 'my\_secret\_key') AS decrypted\_phone

FROM Users\_Encrypted

WHERE username = 'user\_02';



또는(UNION SELECT 사용)



-- 모든 사용자 데이터 복호화하여 조회

SELECT

id,

username,

AES\_DECRYPT(UNHEX(email\_encrypted), 'my\_secret\_key') AS decrypted\_email,

AES\_DECRYPT(UNHEX(phone\_encrypted), 'my\_secret\_key') AS decrypted\_phone

FROM Users\_Encrypted;

