tigerconnect.apk
DB decrypt

정보보안암호수학과 20182209 김수빈

tigerconnect.apk database decrypt key 구하기

```python
from hashlib import pbkdf2_hmac
from Crypto.Cipher import AES
import base64


def decrypt(key, enc):
    cipher = AES.new(key, AES.MODE_ECB)
    dec = (cipher.decrypt(enc))
    result = dec[:-1*dec[-1]]
    return result


salt = 'jQx+pvuo3TJ7aN9zPJnGPVTfIfrDG9uEkIHEVOZ6ez8='
ttkey01 = 'oum53H3VwmQoECodZfek7ckgo2qRrtta'
ttkey02 = 'USDNyIf90wXg4ifLTVFb//qRobxlJjqOaAPAn/HHxBV2AmCeLiBi2R4+RZvZjhzaHhFa+HQDdVnw z+/gzSU9Ug=='

salt_decode = base64.b64decode(salt)
ttkey01_byte = ttkey01.encode()
ttkey02_decode = base64.b64decode(ttkey02)

secretkey = pbkdf2_hmac('sha1', password=ttkey01_byte, salt=salt_decode, iterations=1000, dklen=32)
print('secretkey :', base64.b64encode(secretkey).decode('utf-8'))

restsecret = decrypt(secretkey, ttkey02_decode)
print('restsecret :', restsecret)

authtoken = ttkey01_byte + bytes(b':') + restsecret
print('authtoken :', authtoken)
```
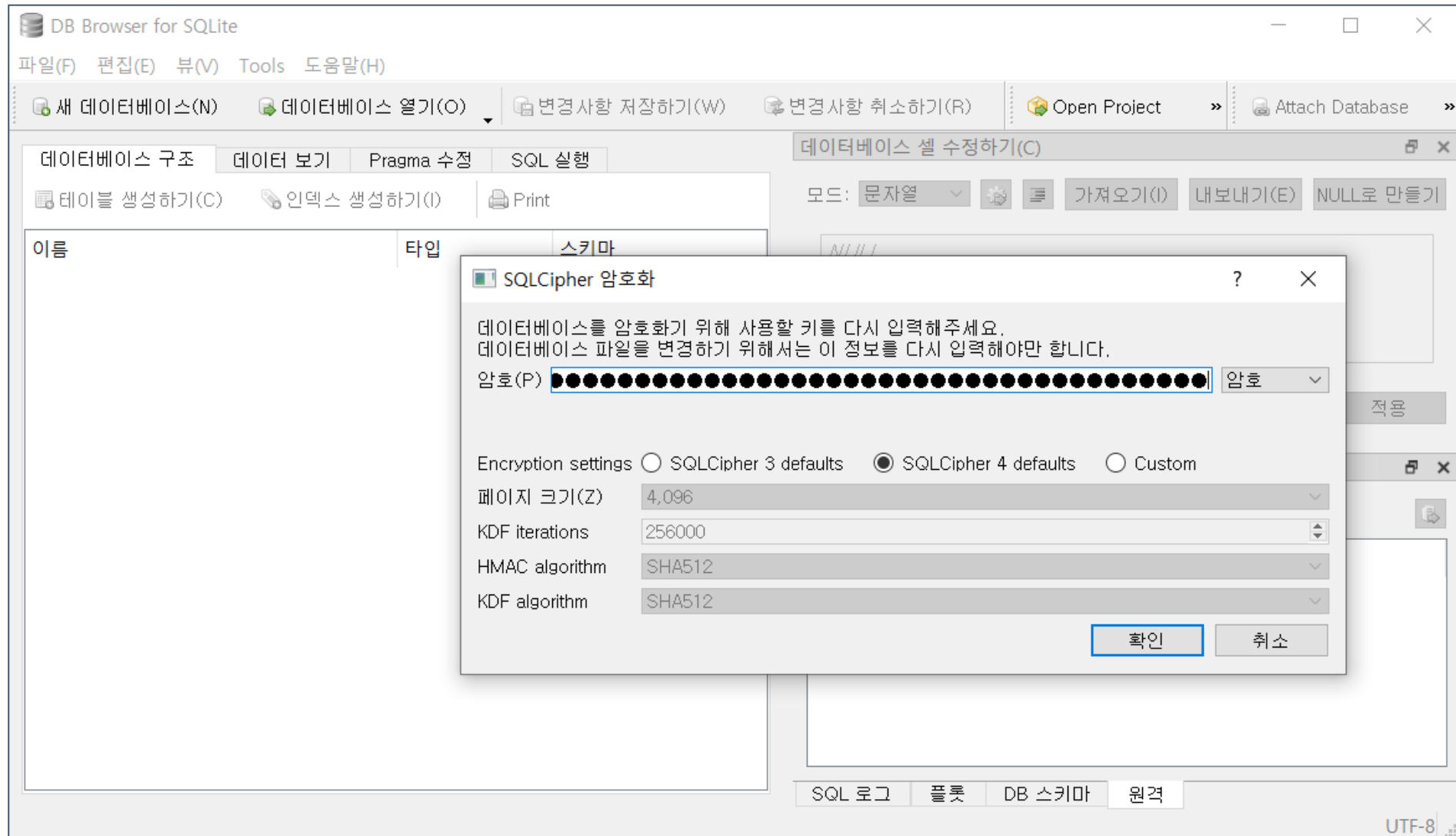
```
secretkey : iYRTSTkR3unnjkNNHvPVllWHtn+jdBElC/o8JWO/Mf4=
restsecret : b'UNql9sXWri3hSSt95vfhXbgoQNFaKLiMMGfcBx1p4YszBhCj'
authtoken : b'oum53H3VwmQoECodZfek7ckgo2qRrtta:UNql9sXWri3hSSt95vfhXbgoQNFaKLiMMGfcBx1p4YszBhCj'
```

tigerconnect.apk database decrypt

tigerconnect.apk database decrypt