rox

파일을 다운받고 압축을 풀어보면 enc라는 파일에는 base64 로 인코딩 된 듯한 문자열이 있고,
prob.py에는 다음과 같은 코드가 들어 있었다.

```
key="???????"
flag="cce2021{??????????????????????????????????}"

def encrypt(plain):
  res=""
  for _ in range(len(plain)):
    res+=chr(ord(key[_%7])^ord(plain[_]))
  return res

open("enc","wb").write(encrypt(flag).encode("base64"))
```

이해를 해보면 key랑 flag를 XOR연산 한뒤 base64로 인코딩한 문자열이 enc파일에 들어가는 것 같다.

> b64encode(key^flag) == enc

우리는 key값은 모르지만 flag의 앞에서 7글자와 enc 문자열을 알고 있으므로
key = flag^b64decode(enc)로 구할 수 있다

```
import base64

flag = "cce2021"
enc = "Bg0PXUlMTx46AgYKIRcWMR4HHCENDAMaAxwNCjoBBAomPRELCRgODQ1fGA=="
def find_key(plain, flag):
  plain = base64.b64decode(bytes(plain, 'utf-8'))
  plain = plain.decode('utf-8')
  for i in range (7):
    key = chr(ord(plain[i])^ord(flag[i]))
    print(key, end="")

find_key(enc, flag)
```

실행시키면 `key="enjoy~~"` 라는 걸 알 수 있다.

그럼 이제 flag를 구하기 위해서 key^b64decode(enc)을 해주자

```
import base64
```

```
key = "enjoy~~"
enc = "Bg0PXUlMTx46AgYKIRcWMR4HHCENDAMaAxwNCjoBBAomPRELCRgODQ1fGA=="

def decrypt(plain, key):
  res=""
  plain = base64.b64decode(bytes(plain, 'utf-8'))
  plain = plain.decode('utf-8')
  for _ in range(len(plain)):
    res+=chr(ord(key[_%7])^ord(plain[_]))
  return res

print(decrypt(enc, key))
```

그러면 이제 flag를 알 수 있다! "cce2021{This_is_the_simplest_one_Congrats!}"