

資訊安全 對稱式密碼作業 2

資訊 115 陳俊安 F74114744

密文 (先以 base64 做 decode)

- FZp57a6p84EUNC7I/ENj4RhPZtryOJr4che9JbA8ng1el8ZMTlsl8kzi
cBDqkOqkFj3lwC69KR2MeA8lscVlig==

```
cipher_text = base64.b64decode("FZp57a6p84EUNC7I/ENj4RhPZtryOJr4che9JbA8ng1el8ZMTlsl8kzicBDqkOqkFj3lwC69KR2MeA8lscVlig==")
```

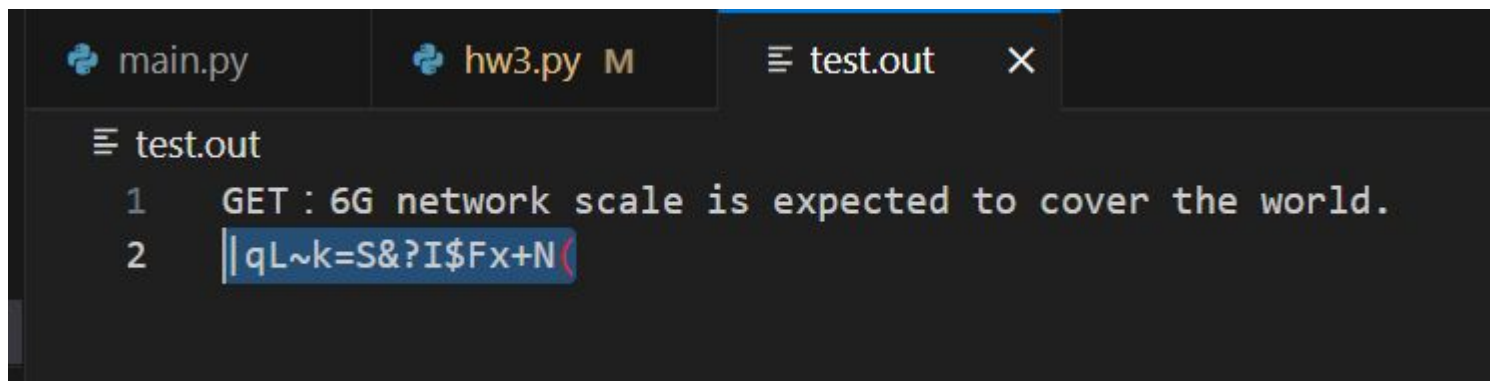
key = lq~k=&?l\$FxN

- 枚舉所有組合並套用 pycrypto 模組
- 當失敗時就換下一個組合，成功則輸出進檔案裡面

```
15 with open("test.out", "a") as o:
16
17     for replacement_chars in combinations:
18         modified_key = key
19         for char in replacement_chars:
20             modified_key = modified_key.replace('█', char, 1)
21         # print(modified_key)
22         try:
23             decryptor = AES.new(modified_key.encode('utf-8'), mode)
24             plaintext = decryptor.decrypt(cipher_text).rstrip(padding.encode('utf-8'))
25             o.write(f"GET: {plaintext.decode('utf-8')}")
26             o.write(modified_key)
27         except:
28             continue
```

結果：

- 明文：6G network scale is expected to cover the world.
- 金鑰：lqL~k=S&?I\$Fx+N(
- 大約跑了 15 分鐘左右



The screenshot shows a code editor with three tabs: 'main.py', 'hw3.py M', and 'test.out'. The 'test.out' tab is active and displays the following content:

```
test.out
1 GET : 6G network scale is expected to cover the world.
2 ||qL~k=S&?I$Fx+N(
```

附件：

- code: https://github.com/ColtenOuO/NCKU_Crypto