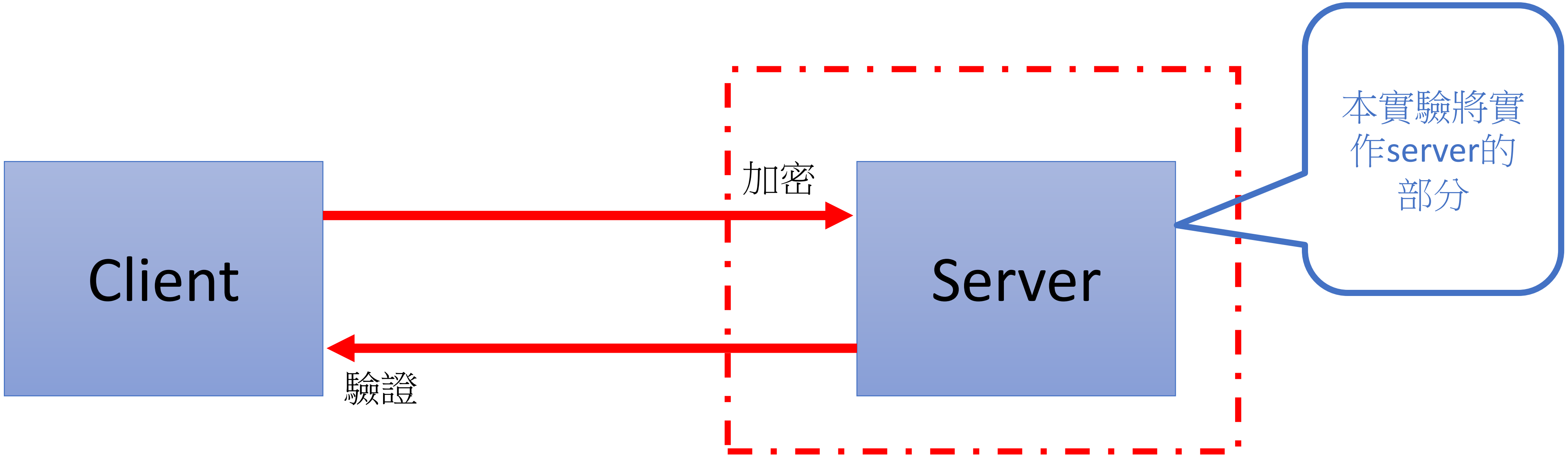
Lab 1: Encryption Server

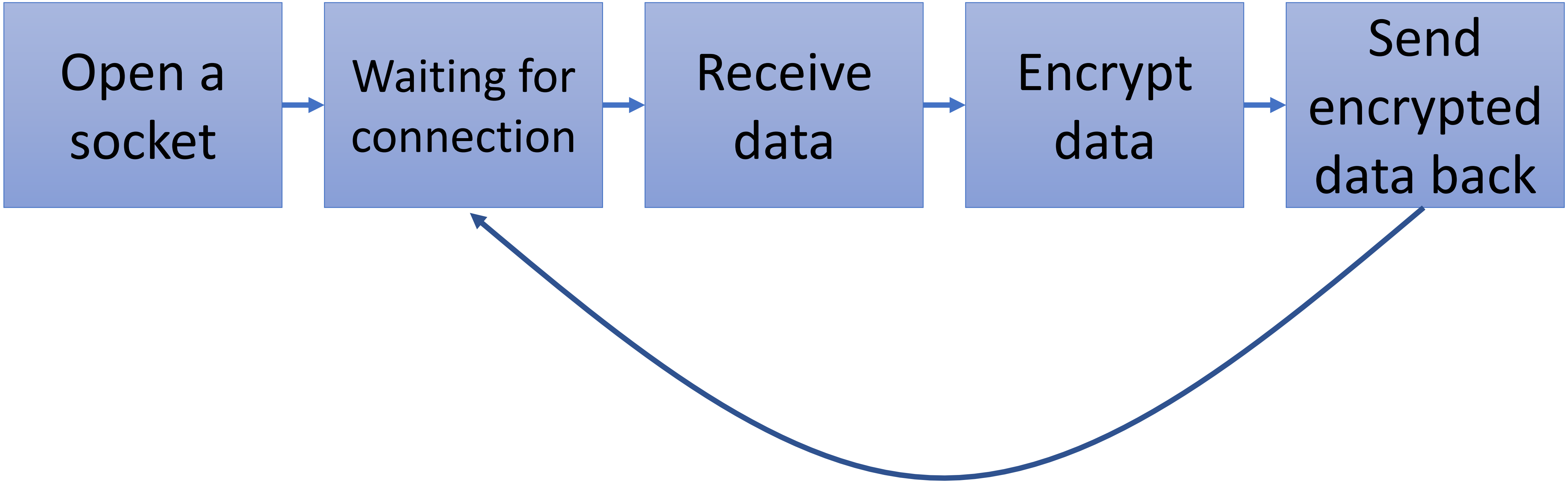
HackMD: https://hackmd.io/@KentShen/Hk_ITCfW5

實驗場景

- 由client端傳送一段資料到server，接著server以AES256加密後回傳
- Client端會檢查是否正確加密



Server端流程



Open a socket

Waiting for connection

Receive data

Encrypt data

Send encrypted data back

Server端 (1/2)

```
import socket
HOST = '127.0.0.1'
PORT = 8000

server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server.bind((HOST, PORT))
server.listen(10)
```

Server端 (2/2)

```
while True:
    conn, addr = server.accept()
    clientMessage = conn.recv(1024)

    print('Client message is:', clientMessage.decode("utf-8"))

    serverMessage = 'I\'m here!'
    conn.sendall(serverMessage.encode())
    conn.close()
```

Client 端

```
import socket

HOST = '127.0.0.1'
PORT = 8000
clientMessage = 'Hello!'

client = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
client.connect((HOST, PORT))
client.sendall(clientMessage.encode())

serverMessage = client.recv(1024)
print('Server:', serverMessage.decode("utf-8"))

client.close()
```

AES 256 Encryption

```
from simplecrypt import encrypt, decrypt
passkey = 'wow’
str1 = 'I am okay’
cipher = encrypt(passkey, str1)
print(cipher)
```

https://www.delftstack.com/zh-tw/howto/python/python-encrypt-string/