

# readme

倪浚桐

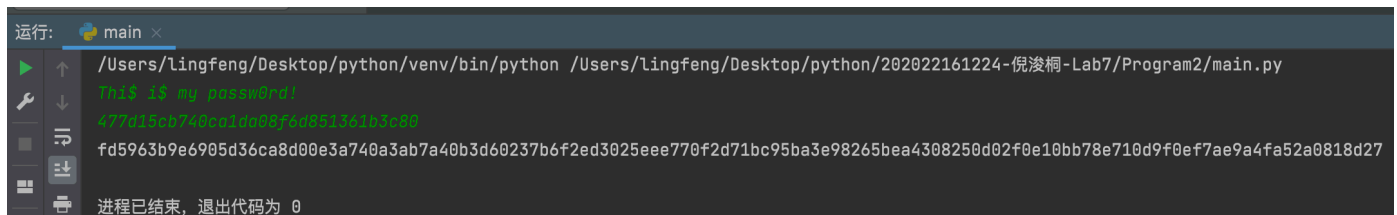
202022161224

Lab7-progarm2

macOS Monterey 12.0.1

Pycharm 11.0.12 x86-64

Python 3.9.5



```
运行: main x
/Users/Lingfeng/Desktop/python/venv/bin/python /Users/lingfeng/Desktop/python/202022161224-倪浚桐-Lab7/Program2/main.py
This is my password!
477d15c0740c01000f0d0513a1b3c00
fd5963b9e6905d36ca8d00e3a740a3ab7a40b3d60237b6f2ed3025eee770f2d71bc95ba3e98265bea4308250d02f0e10bb78e710d9f0ef7ae9a4fa52a0818d27
进程已结束，退出代码为 0
```

```
1  import hashlib
2
3  password_str: str = input()
4  password_bytes: bytes = bytes(password_str, encoding="utf8")
5  salt_hex: str = input()
6  salt_bytes: bytes = bytes.fromhex(salt_hex)
7
8  n = 4
9  r = 8
10 p = 16
11 print(hashlib.scrypt(password_bytes, salt=salt_bytes, n=4, r=8, p=16).hex())
12
13 # hashlib.scrypt(password, *, salt, n, r, p, maxmem=0, dklen=64)
14 # 此函数提供基于密码加密的密钥派生函数，其定义参见 RFC 7914。
15 # password 和 salt 必须为 字节类对象。 应用和库应当将 password 限制在合理长度（例如 1024）。
16 # salt 应当为适当来源例如 os.urandom() 的大约 16 个或更多的字节串数据。
17 # n 为 CPU/内存开销因子，r 为块大小，p 为并行化因子，maxmem 为内存限制（OpenSSL 1.1.0 默认为 32 MiB）。 dklen 为派生密钥的长度。
18 # !!! 注意python中*的含义!!!
```