

readme

倪浚桐

202022161224

Lab3-program1

macOS Big Sur 11.5.2(20G95)

Pycharm 11.0.11 x86-64

Python 3.9.5

```
终端: main.py × main.py × main.py × +
/Users/lingfeng/Desktop/python/202022161224-倪浚桐-Lab3/Program1/main.py
(venv) lingfeng@lingfengdeMacBook-Pro Program1 % /Users/lingfeng/Desktop/python/202022161224-倪浚桐-Lab3/Program1/main.py
plaintext:8787878787878787
key:133457799bbcdff1
key:0e329232ea6d0d73
key:133457799bbcdff1
ciphertext: e98a0b8e59b3eeb7
plaintext: 8787878787878787
```

```
1  #!/usr/bin/env python3
2  # -*- coding: utf-8 -*-
3
4  from libdes import DES_Encrypt, DES_Decrypt
5
6
7  def validate_des_key(key: bytes) -> bool:
8      for keyByte in key:
9          binStr: str = "{0:0>8b}".format(keyByte)
10         if sum([1 if b == '1' else 0 for b in binStr]) % 2 == 0:
11             return False
12     return True
13
14
15 def tri_DES_encrypt(plaintext_Hex: str, key1_Hex: str, key2_Hex: str, key3_Hex:
str) -> bytes:
16     ciphertext_ans: bytes = DES_Encrypt(
17         bytes.fromhex(plaintext_Hex),
18         bytes.fromhex(key1_Hex),
19     )
20     ciphertext_ans: bytes = DES_Decrypt(
21         ciphertext_ans,
22         bytes.fromhex(key2_Hex),
23     )
```

```

24     ciphertext_ans: bytes = DES_Encrypt(
25         ciphertext_ans,
26         bytes.fromhex(key3_Hex),
27     )
28     return ciphertext_ans
29
30
31 def tri_DES_decrypt(ciphertext_Hex: str, key1_Hex: str, key2_Hex: str, key3_Hex:
32 str) -> bytes:
33     plaintext_ans: bytes = DES_Decrypt(
34         bytes.fromhex(ciphertext_Hex),
35         bytes.fromhex(key3_Hex),
36     )
37     plaintext_ans: bytes = DES_Encrypt(
38         plaintext_ans,
39         bytes.fromhex(key2_Hex),
40     )
41     plaintext_ans: bytes = DES_Decrypt(
42         plaintext_ans,
43         bytes.fromhex(key1_Hex),
44     )
45     return plaintext_ans
46
47 if __name__ == '__main__':
48     plaintextHex: str = input('plaintext:')
49     key1Hex: str = input('key:')
50     key2Hex: str = input('key:')
51     key3Hex: str = input('key:')
52
53     if not validate_des_key(bytes.fromhex(key1Hex)):
54         raise Exception('Parity check failed on the key.')
55     if not validate_des_key(bytes.fromhex(key2Hex)):
56         raise Exception('Parity check failed on the key.')
57     if not validate_des_key(bytes.fromhex(key3Hex)):
58         raise Exception('Parity check failed on the key.')
59
60     ciphertext: bytes = tri_DES_encrypt(
61         plaintextHex,
62         key1Hex,
63         key2Hex,
64         key3Hex,
65     )
66
67     print('ciphertext:', ciphertext.hex())
68
69     plaintext: bytes = tri_DES_decrypt(
70         ciphertext.hex(),
71         key1Hex,

```

```
72         key2Hex,  
73         key3Hex,  
74     )  
75  
76     print('plaintext:', plaintext.hex())  
77
```