

Problem 1

(a)

```
import numpy as np
import math

def WHT_recursive(x):
    x = np.array(x)
    if len(x.shape) < 2:
        if len(x) > 3:
            n = len(x)
            M = math.trunc(math.log(n, 2))
            x = x[0:2 ** M]
            return _WHT_recursive(x, M)
        else:
            return x
    else:
        raise ValueError("Input must be a 1D array")

def _WHT_recursive(x, M):
    if M == 0:
        return x
    else:
        h2 = np.array([[1, 1], [1, -1]])
        H = h2
        for i in range(M - 1):
            H = np.kron(H, h2)

        if len(x) < 2 ** M:
            x = np.concatenate((x, [0] * (2 ** M - len(x))), axis=0)

        return np.dot(H, x) / (2 ** M), M
```

```
cassidy@cassidydeMacBook-Air Quiz06 % python3 p1_a.py
test case: [1, 4, 5, 3]
Walsh-Hadamard Transform: (array([ 3.25, -0.25, -0.75, -1.25]), 2)
test case: [2, 7, 4, 2, 3, 1, 6, 2]
Walsh-Hadamard Transform: (array([ 3.375,  0.375, -0.125, -1.125,  0.375, -1.125,  0.875, -0.625]), 3)
```

(b) ① 圖像壓縮 → 信號被轉換為頻域表示,並利用它的稀疏性進行壓縮

→ 利用WTH的正交性

② 數據壓縮 → 通過轉換數據捨棄較小的頻率,減少傳輸所需的數據量

→ 節省帶寬和能源

③ 模式識別、特徵提取 → 將信號轉為WHT域,在高維數據中以緊湊的方式捕捉其基本特徵

→ 降低數據的維度,提高準確性

④ CDMA → 利用WTH的正交性

→ 使多用戶共享頻段時不會互相影響

Problem 2

(a) Miller-Rabin 的測試效果仍是良好的

∴ a 要選到被當成有效數字使 p_q 的性質(質數)受到影響的機率低

(b) 不能

∴ RSA 加密的安全性是基於大質數分解的困難(無法有效的將其分解為其他質因數)

↳ Miller-Rabin 無法破解