密碼工程 Quiz6

學號:112550090 姓名:曾士珍

Problem1

a) Please showcase the **recursive process** of the Walsh-Hadamard Transform using the pseudocode provided above.

以下是使用上面提供的代碼進行 Walsh-Hadamard Transform 的過程：

假設有長度為 n 的輸入信號 x = $[x_1, x_2, \ldots x_n]$

1. 檢查輸入的信號 x 是否為一維數組，是在繼續執行
2. 檢查信號的長度是否為 2 的次方，如果信號的長度不是 2 的次方，將其調整為最接近的 2 的次方。假設調整後的長度為2^M。
3. 定義 Hadamard fundamental matrix h2= $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
4. 對於每一個 M，將 h2 矩陣進行 Kronecker products，得到更大的 Hadamard matrix H：

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad H_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

直到H_M為止，其中 M 是調整後信號的長度的對數。

5. 將輸入信號 x 乘以最終得到的 Hadamard matrix H，

$$y = H_M x$$

6. 返回轉換後的信號 y、原始信號 x 和 M 的值，這樣就完成了 Walsh-Hadamard Transform。

b) Examine different **applications** of the Walsh-Hadamard Transform, highlighting how its properties offer advantages in each specific application.

1. 信號處理

(1) 影像壓縮：WHT 在 JPEG XR 等影像壓縮技術中應用廣泛，能夠高效表

示頻域內的影像，實現高壓縮比並保持影像品質。

(2) 音頻壓縮：WHT 可用於音頻信號壓縮，減少文件大小而不會顯著降低音頻質量。

(3) 降噪處理：WHT 能夠幫助在嘈雜環境下分離信號和噪聲，廣泛用於降噪應用中。

2. 通信

(1) OFDM：WHT 在 OFDM 系統中用於多載波調製，其正交性有助於避免不同子載波之間的干擾，提高頻譜效率並減少符號間干擾。

(2) 展頻通信：WHT 應用於展頻技術中，用於實現安全可靠的通信，其特性使信號能夠在寬頻段內傳輸，提高抗干擾性。

3. 密碼學

(1) 流式加密：基於 WHT 的流式加密利用其正交性和隨機性進行數據流的加密和解密，提高了密碼的安全性。

(2) 隱寫術：WHT 可用於隱寫術技術中，將秘密信息嵌入到載體媒體中，其特性有助於隱藏嵌入數據的存在。

4. 數據分析

(1) 模式識別：WHT 用於模式識別任務，能夠從信號中提取相關特徵，幫助識別數據中的模式。

(2) 數據挖掘：WHT 可用於數據挖掘中的特徵提取和降維，幫助分析大數據集。

5. 控制系統

(1) 系統識別：WHT 可以幫助分析動態系統的行為，並建模其響應。

(2) 反饋控制：WHT 可用於反饋控制系統中的信號處理和分析，幫助有效控制動態系統。

Problem2

a) What **happens** when we apply the Miller-Rabin test to numbers in the format pq, where p and q are large prime numbers?

將 Miller-Rabin test 應用於 n = pq (其中 p 和 q 是值很大的質數)，通常可以識別出 n 是合數。因為這種數字是數學上的典型結構(由兩個大質數相乘而成)，很難通過 Miller-Rabin test。雖然還是有極小的機率被誤認為是質數，但可以透過選擇其他底數 a，再進行更多次測試來降低該機率。

b) Can we **break** RSA with it?

使用 Miller-Rabin test 無法破解 RSA 加密。RSA 加密依賴於將大數質因數分解的困難性，而 Miller-Rabin test 主要用於概率性質數測試。但如果 Miller-Rabin test 將一個合數誤認為質數，並且該數被用於 RSA 中的一個質因數，那就會削弱 RSA 加密的安全性。