Quiz 6

Problem 1

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

Let's consider a 1D signal of length 8, where the length is already a power of 2.

```
x = [1, 2, 3, 4, 5, 6, 7, 8]
```

According to the pseudocode, the first step is to ensure that `x` is a one-dimensional array of a length that is a power of 2. Our example signal already meets this requirement.

Now, let's manually iterate through the recursive steps:

1. When `i = 0`, we perform the first Kronecker product, which will be `h2` with itself:

   ```
   H = np.kron(h2, h2)
   ```

2. For `i = 1` , we again take the Kronecker product of the resulting `H` with `h2`:

   ```
   H = np.kron(H, h2)
   ```

   We would repeat this process `M-1` times, where `M` is `log2(n)` (in our case, `M = 3` since `n = 8`).

Finally, the WHT is computed by multiplying the Hadamard matrix `H` with the signal `x` and then scaling by a factor of `1 / 2.**M`:

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

The Hadamard matrix `H` obtained after the recursive Kronecker product operations is:

```
[[ 1,  1,  1,  1,  1,  1,  1,  1],
 [ 1, -1,  1, -1,  1, -1,  1, -1],
 [ 1,  1, -1, -1,  1,  1, -1, -1],
 [ 1, -1, -1,  1,  1, -1, -1,  1],
 [ 1,  1,  1,  1, -1, -1, -1, -1],
 [ 1, -1,  1, -1, -1,  1, -1,  1],
 [ 1,  1, -1, -1, -1, -1,  1,  1],
 [ 1, -1, -1,  1, -1,  1,  1, -1]]
```

And the result of the Walsh-Hadamard Transform for the example signal `[1, 2, 3, 4, 5, 6, 7, 8]` is:

```
[ 4.5, -0.5, -1.0,  0.0, -2.0,  0.0,  0.0,  0.0]
```

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

1. **Image Processing and Compression**:

   The WHT can be used for image compression because it tends to concentrate signal energy into a few coefficients. This makes it easier to achieve compression by quantizing and encoding these coefficients more efficiently than the rest.

   For image processing, the WHT can facilitate operations like edge detection and texture analysis because the transform captures the spatial domain features in its coefficients.

2. **Signal Processing**:

   In the field of digital signal processing, the WHT is utilized for noise reduction and signal extraction because its coefficients can represent the signal sparsely, isolating important components from noise.

It is also used in multiplexing and de-multiplexing signals because of its orthogonality property, which allows the separation of multiplexed signals without interference.

3. **Data Encryption and Cryptography**:

   The WHT is sometimes employed in the creation of orthogonal codes for data encryption. Its properties ensure that the codes are mutually orthogonal, providing security in data transmission.

4. **Quantum Computing**:

   The Hadamard gate in quantum computing, which is used to create superpositions of qubit states, is a one-qubit version of the WHT. This gate is fundamental in many quantum algorithms, such as the Quantum Fourier Transform and Grover's search algorithm.

Problem 2

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

   The Miller-Rabin primality test is designed to determine whether a single number is prime. When the test is applied to a number of the form pq (where p and q are distinct large primes), the outcome will indicate that the number is composite, which is the correct conclusion.

   Since the test is probabilistic, it doesn't directly provide the factors of the number; it only states whether the number is likely prime or composite. For a composite number like pq, the test will show that the number is composite. Because during the test, it's highly likely that at least one randomly chosen base `a` will not satisfy the conditions for n being prime.

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

   No, the Miller-Rabin test alone cannot be used to break RSA encryption. RSA's security is based on the difficulty of factoring large numbers that are the product of two large primes (commonly denoted as n = pq). The Miller-Rabin test can be used to identify that n is composite, which we already know in the context of RSA. However, it does not provide any information on the prime factors p and q themselves.