Problem 1

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

   The WHT, as implemented in the pseudocode, uses a non-recursive approach. It uses a series of matrix operations to compute the transform for a one-dimensional, real-valued signal.

   (a) Input Verification: The function starts by ensuring the input x is a one-dimensional array with a minimum length of 4.

   (b) Signal Length Adjustment: It then adjusts the length of the signal to the nearest power of 2, if necessary. This is done by calculating M = math.trunc(math.log(n, 2)), where n is the length of x, and then slicing x to length 2**M.

   (c) Matrix Construction: The core of the transformation is creating the Hadamard matrix, H. This is done using Kronecker products (np.kron) in a loop. Initially, a base matrix h2 is defined as [[1, 1], [1, -1]]. For each iteration in the loop, the Hadamard matrix is expanded by computing the Kronecker product of the current H with h2.

   (d) Transformation: Finally, the transform is computed as np.dot(H, x) / 2. ** M. This operation applies the Hadamard matrix to the signal.

   While the provided pseudocode for the WHT utilizes an iterative method for constructing the Hadamard matrix, the underlying principle can be interpreted recursively. In a recursive approach, the Hadamard matrix of a particular size would be constructed by combining smaller Hadamard matrices generated by recursive calls of the same function. This recursive process continues until the base case (the smallest Hadamard matrix) is reached. Each level of recursion effectively doubles the size of the matrix, aligning with the property that the length of the signal in WHT should be a power of 2.

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

   (a) Image and Signal Processing: The WHT is commonly used for analyzing and processing signals and images, particularly for compression and noise reduction, due to its fast computation and ability to handle real values.

   (b) Data Encryption and Cryptography: In cryptography, the WHT is useful for developing secure encryption algorithms. Its orthogonality property, where each row or column is orthogonal to the others, is particularly valuable here.

   (c) Error Correction and Data Compression: In telecommunications, WHT is used in error correction techniques and data compression, benefiting from its efficient computation and the ability to represent data in different frequency components.

   (d) Pattern Recognition and Machine Learning: In pattern recognition and some machine learning algorithms, WHT can be used to transform data into a format where patterns are more easily recognizable or classifiable.

Problem 2

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

   When the Miller-Rabin test is applied to a composite number like pq, it is very likely to identify it as composite. However, being a probabilistic test, there's a small chance it might incorrectly identify it as a prime (false positive). The probability of a false positive decreases with the number of iterations of the test.

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

   The Miller-Rabin test alone cannot break RSA encryption. Breaking RSA typically requires factoring the product pq into its prime factors, a task for which there is no known efficient algorithm. The Miller-Rabin test can only determine if a number is probably prime or composite; it does not provide the factors of a composite number.