Problem 1

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

(a) **Input Check**: Initially, the function verifies that the input 'x' is a one-dimensional array and that it has at least 4 elements.

(b) **Adjusting Signal Length**: Next, the function adjusts the signal's length to the nearest power of 2. where 'n' is the initial length of 'x', and then slicing 'x' to a length of 2^{M}.

(c) **Matrix Creation**: At the heart of the transform is the construction of the Hadamard matrix, 'H'. Starting with a basic matrix $h2,$ the Hadamard matrix is expanded iteratively using Kronecker products.

(d) **Applying the Transformation**: The transformation is then carried out, which applies the Hadamard matrix to the signal 'x'.

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

the function takes a one-dimensional signal and computes its WHT, which is a representation that is useful for various signal processing tasks.

(a)Error Correction: The transform is also used in error correction codes, such as Hadamard codes. These codes take advantage of the orthogonal properties of the WHT, allowing for the detection and correction of errors that may occur during the transmission of data. The WHT's ability to spread error over multiple coefficients makes it easier to detect and correct.

(b)Pattern Recognition: In pattern recognition and image analysis, the WHT can be used to extract features from images for object recognition, texture analysis, and other computer vision tasks. The transform can emphasize certain image characteristics, making it easier for algorithms to classify objects or patterns.

(c)Cryptography: In cryptography, the WHT can be employed in the design of cryptographic schemes that rely on the difficulty of certain mathematical problems related to the Hadamard matrix. It can also be used to generate sequences with good correlation properties, which are valuable in stream ciphers and for generating cryptographic keys.

(d)Quantum Computing: The Hadamard transform, which is closely related to the WHT, is used in quantum computing algorithms to create superposition states. It allows quantum bits to be in a combination of all possible states, thereby enabling parallel computation and the solving of certain problems more efficiently than classical computers.

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 number that is the product of two large prime numbers, such as pq the test will almost always identify the number as composite because it will not satisfy the conditions that would hold if it were prime. The test is designed to recognize prime numbers, and since a product of two primes is not prime, the Miller-Rabin test will correctly determine this, provided enough rounds of testing are performed.

2. Can we break RSA with it?

No, the Miller-Rabin test cannot be used to break RSA encryption. It can tell you if a number is composite, but it does not reveal the prime factors of that number, which are necessary to break RSA.