Quiz. 6

Problem 1

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

The provided pseudocode illustrates how to apply the Discrete Walsh-Hadamard Transform to a 1D real-valued signal. The recursive aspect is shown in the repeated use of the Kronecker product to create the transform matrix H.

- Initialization: To ensure WHT compatibility, the input vector x is truncated to the largest power of two in length.
- Hadamard Matrix Generation: Starting with a base 2x2 Hadamard matrix (h2), the transform matrix H is built recursively by performing the Kronecker product of H and h2. This technique causes H to grow exponentially to match the dimension of the input signal.
- Transformation: Finally, the Hadamard transform of the input vector x is computed using the dot product of H and x, scaled by 2^M where M is the power of two that corresponds to the length of x.

While the WHT pseudocode uses an iterative way to build the Hadamard matrix, the underlying concept can be interpreted recursively. In a recursive approach, a Hadamard matrix of a specific size is created by mixing smaller Hadamard matrices generated by recursive calls to the same procedure. This cyclical process repeats until the basic case (the smallest Hadamard matrix) is reached. Each level of recursion effectively doubles the size of the matrix, which corresponds to the requirement that the length of the signal in WHT must be a power of 2.

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

The Walsh-Hadamard Transform is used in a variety of domains. Here are some of its applications and the benefits it provides:

Signal Processing: WHT is used to examine the frequency components of signals. Its recursive nature allows for efficient computation, akin to the Fast Fourier Transform (FFT), but with a focus on binary signals.

Image Compression: WHT aids in image compression by converting pixel values into a format that is more suited to compression techniques.
Telecommunications: The transform is used to encode and decode signals, especially in spread spectrum communications, when signals are dispersed across a large bandwidth.

Data Encryption and Error Correction: WHT is used to generate orthogonal codes, which are essential in secure communications and error detection and correction systems.
Each application benefits from the WHT's capacity to rapidly transform data into a format that can be easily manipulated, analyzed, or compressed. The transform's structure enables computationally efficient implementations, which is critical in real-time processing situations.

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?

When applied to a number of the format pq, where both p and q are large prime numbers, the test will determine that pq is composite. This is because any number that is a product of two or more primes (other than the primes themselves) is, by definition, 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.

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

The Miller-Rabin test cannot be used directly to break RSA encryption. RSA security is based on the difficulty of factoring large composite numbers (specifically, the product of two large primes) into their prime factors i -e 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