Problem 1

(a)
The input signal x is first converted into a NumPy array.
After we make sure x is 1D array and min length of x is 4 elements,
x is truncated to the nearest length that is a power of 2 (2 ** M), where M is the largest integer such that 2 ** M <= n (the length of x).

For each level i from 0 to M - 1 (where M is the number of levels needed to reach the desired length of x), the transformation matrix H is updated using the Kronecker product (np.kron).
Initially (i == 0), H is set as a Kronecker product of the base Hadamard matrix h2 with itself (H = np.kron(h2, h2)).
For subsequent iterations (i > 0), H is updated by taking the Kronecker product of the existing H with h2 (H = np.kron(H, h2)).

The transformed signal y is computed by matrix-multiplying the transformation matrix H with the signal x (y = np.dot(H, x)).
The resulting transformed signal y is normalized by dividing it by 2 ** M to scale it appropriately.

The function returns the transformed signal y, the original signal x, and the number of levels M used in the transformation.

(b)
Image Compression:
The WHT is used in image compression algorithms to efficiently represent image data and reduce storage space.

Digital Communication:
In communication systems, the WHT is used for spreading signals (e.g., in CDMA) and as part of modulation and demodulation techniques.

Statistical Analysis:
In statistics, the WHT can be applied for feature extraction and data compression in multivariate analysis.

Feature Extraction:
WHT is utilized for feature extraction from images or patterns to represent them in a more compact and efficient manner.

Problem 2

(a)
When we apply the Miller-Rabin test to numbers in the form **pq**, where **p** and **q** are large prime numbers, the test typically produce a "composite" result. This occurs because of the properties of **n = pq** and the nature of the test itself.
This is because if **n = pq**, then **n - 1 = pq -1** is divisible by both p and q, as it is **(p-1)(q-1)**. When we compute **a^q mod n** for any base a, due to Fermet's little theorem, **a^q ≡ a mod q**. Since **q divides n - 1**, it follows that **a^q ≡ a mod n**. Therefore, **a^q mod n** will always be congruent to **a mod n**, which means it is likely to yield **a** or **1**.

(b)
No, RSA relies on the difficulty of factoring large composite numbers that are products of two large prime numbers. While the Miller-Rabin test can occasionally give false positive results for such composite numbers, it does not provide a systematic method for efficiently factoring them.